THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Study of SSL-VPN Performance with Intrusion Detection Systems (IDS)

Ahmad Ajiya Ahmad
Lecturer, Department of Computer Science, Federal University Gashua, Nigeria
Souley Boukari
Professor, Department of Mathematical Sciences,
Abubakar Tafawa Balewa University (ATBU), Bauchi State, Nigeria
Usman Suleiman Idriss
Lecturer, Department of Computer Science, Federal University Gashua, Nigeria
Abubakar Muhammad Bichi
Lecturer, Department of Computer Science, Federal University Gashua, Nigeria
Murtala Muhammad Adamu
Senior System Analyst, Department of ICT, Federal University Gashua, Nigeria

Abstract:
The largely used of cyberspace has brought the attention of business interposes across the globe in modern era which resulted in numerous security issues. Business enterprises find it difficult to protect and manage resource sharing and data infrastructure effectively. The business enterprises consider Virtual private network (VPN) as a novel development to protect data and information, and to create a VPN connection, it is significant to consider the type of security protocols to use to make VPN more efficient and more powerful. The significant issue in this research is to study the performance of Secure Socket Layer (SSL) in VPN with intrusion detection systems (IDS) on Linux operating system in terms of Quality of Service (QoS) parameters (throughput, latency and packet loss). We also used two different encryption algorithms, Triple Data Encryption Standard (TDES/3DES) and Advance Encryption Standard (AES). Encryption algorithms are used to encrypt data, so it cannot be read or modify by a third-party while in transit between two end points of a network. This research found that when considering throughput, packet loss and latency in network infrastructures, SSL/3DES offers fair and reasonable performance than SSL/AES. VPN protocols with higher throughput have the best performance and VPN protocol the low packet loss has the best performance. The research indicated deploying SSL/3DES is more effective in business enterprises also indicated that IDS could be able to function effectively on both protected traffic packets (VPN packets) and server log files.

Keywords: *Virtual Private Network (VPN), Secure Socket Layer/Transport Layer Protocol (SSL), Advance Encryption Standard (AES), Data Encryption Standard (3DES), Intrusion Detection System (IDS), Quality of Service (QoS), Transport Layer Protocol (TLS)*

1. Introduction

The VPN technology has adapted to access the Enterprises Intranet. Now VPN security is a big issue for almost every organization in order to provide protection for system infrastructure. The Truth is that no one assertions full evidence on security scheme since the internet usage is growing exponentially across the globe. Particularly, according toRama and Anup (2020), revealed that in COVID-19 Pandemic, Internet usage has been improved by up to 90% due to the culture Work from-home by nearly every business. VPN technology offers a fashion of protecting data information being carried over the Internet, by granting remote users to set up a secure virtual private 'tunnel' to get into an internal network, gain access to available resources, data information and communications through an unsafe network such as the Internet cyberspace (United States Patent Burns, 2018). The review Giris and Vishal (2021) stated that, many businesses protected themselves from the cyberspace by means of firewalls and VPN encryption techniques. VPN considered to be an effective and efficient mechanism to transport traffic on an unsafe network. It comprises a union of encrypting, authentication and tunnel. VPNs has been established and proved to be that effective to substitute previous system of lease lines to make private network in a business enterprise (Natalia, 2021 and Mazlan et al., 2010). VPNs usually oppressed by business enterprises to link central office/Head-office with subdivision office, main office for distant employees or roaming users, business collaborator sites and remote network users of their join network. There are numerous unlike types of VPNs available. The most commonly types of VPN used in nowadays are as follows: (a) *Point-to-Point Tunnelling Protocol VPN (PPTP VPN,* PPTP VPN) is an easy method for VPN and can also be called as Dial-up VPN. It is software-built VPN that uses an existing internet network to create VPN connection. Using this existing connection, a remote client will be able to link to remote network because of secure VPN tunnel created by the software between these remote endpoints

(Skullbox.Net, 2008). (b) *Site-to-Site VPN,* this type of VPN and point-to-point VPN are almost the same, the primary difference between them is, in site-to-site a devoted or dedicated path is not use. For each one of the sites has its own personal network connection (internet) and the internet could be or not from same Internet service provider (ISP). (c) *Point-to-Point VPN,* Point-to-point VPN is another example of conventional VPN type. These types of VPN are also referred to as Leased-line VPNs. In this type of VPN two or more networks are link with a dedicated single path (circuit or packet switching line) from an internet service provider (ISP). The main significant of using dedicated paths or line in point-to-point VPN is because it behaves not to get out over the public Internet network (Giris and Vishal, 2021). (d) *Multi-Protocol Label Switching (MPLS) VPNs, w*as purposely developed to improve the technique 'store-and- forward' (technique in which data is conveyed to an intermediate node where it is stored and transmitted at a later time to its next intermediate node or to final endpoint) speed of routers (Skullbox.Net, 2008).

VPN allows for access to information, data and files on a particular network location remotely (Rama and Anup, 2020). When organisation or business establishment intended to create a VPN, it is significant to regard these types of technologies (VPN Protocols) and determine which one is better to use and suits its own requirements (United States Patent Burns et al., 2018). These are the type of VPN tunnelling protocol: *Internet Protocol Security (IPSEC),* IPsec protocol deployment is expensive, the installation requires intensive time consuming and these are regarded as it disadvantages (Anon 2010). IPsec protocol correlates with Layer two Tunnelling Protocol (L2TP) protocols to provide encryption. As a result, this Study experimented and analysed the performance of SSL security protocol. The objectives of this research are, to find the performance of secure socket layer (SSL) tunnelling protocol in VPN by using Triple Data Encryption Standard (TDES/3DES) and Advance Encryption Standard (AES) encryption algorithms, to describe and provide evidence on how IDSs works on VPN and to ensured that the performance results was effectively efficient and accurate.

2. Overview of Secure Socket Layer (SSL)

As mentioned above, SSL is a security protocol that offers secure connection between two endpoints over the public network (Rama and Anup, 2020). SSL is a basic cryptographic protocol that used to create a secure VPN connection for authenticated and ciphered communications between VPN clients and VPN servers on the public network (Narayan et al., 2010). SSL is also used on business environments, such as internets leverages/purchases and web browsers-built transactions (Natalia, 2021). All these business activities are secured by SSL. Nevertheless, SSL is not based on ensuring security on e-brassiness deals; SSL can also be used in the following sectors: *Financial Organizations (Private or Public),* Financial organisation like banking companies, use SSL to ensure security on business transmission of Personal Identification Numbers (PIN) numbers and other secrete data or account report/details to or from employees (BCSI, 2008 and Girish and Vishal, 2021). *Insurance institutions/firms,* Insurance firms like non-depository financial institution uses SSL to ensure security on transmission of secrete insurance policies data (Giris and Vishal, 2021). *Web Email,* Web Email suppliers uses SSL to insure web electronic mails for users (Adeyinka and Shoniregun, 2007). According to CISCO (2007) Institutions that based on e-business deals among business, like Business to Business (B2B) organisation, make use of SSL to provide security to their confidential transactions between manufacturers and its customers, retailers etc.

2.1. How SSL Works

According to Wu et al. (2011), SSL is an example of client/server protocol that set up secure a connection between client/server VPN endpoints and SSL starts with SSL handshake process to establish this secure communication. The SSL handshake process involves negotiation between endpoints for security parameter (such as encryption algorithms, authentication keys etc.) to use for possible communication session to be establish (Kotuliak et al., 2011). Firstly, SSL client and SSL server make use of digital certificates to identify themselves (Alshamsi and Saito, 2005). Digital certificate provides full identity details and public keys of these client and server endpoints. The digitals certificate is generally published by certificate authority (CAs). Using digital certificates, a client VPN endpoint authenticate VPN server to find out the authenticity of that server, which is to know if the key is coming from a trusted server (Giris and Vishal, 2021).
Secondly, the SSL client and server make use of digital signature on each packet to assure data integrity (Likhar et al., 2011). Digital signature is a security property (harsh message digest e.g., SHA and MD5) that can be attached to each data stream with a public key detail. Both VPN client and VPN server exchange and compute the security property and check if there is a match (Alshamsi and Saito, 2005). If the both results of the client and server matches that show that the message is unmodified (Likhar et al., 2011). The figure 1 and table 1 explained digital signature process between client and server.

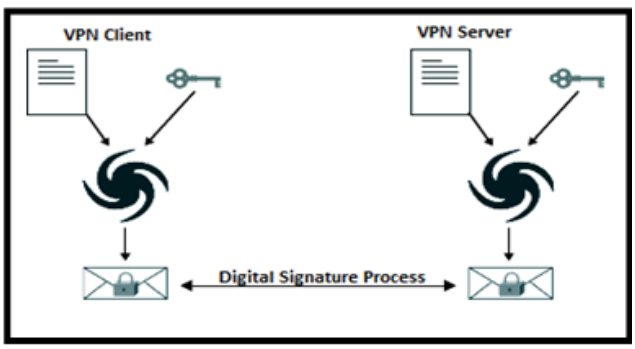

Figure 1: Digital Signature - Message Digests Exchange

Digital Signature Process	
VPN Client	VPN Server
1 - Client message a data 2 - Client has message and public key 3 - Client hashes message with public key 7 – Client compares its own hashed message to server's message 8 – If the two matches, then the message has not been tampered.	4 – Server takes random message with public key 5 – Server hashes message with public key 6 – Server sends hashes message

Table 1: Digital Signature Process in Details (Alshamsi& Saito 2005)

The main Significant of formalising the digital signature on certificates is for the client and server to ensure that a fake user or an intruder has not tempered with the transmission (Cisco 2002). This secure tunnel that SSL establishes between VPN client and server is an encrypted link to ensure all data travelling through the tunnel is private (Alshamsi and Saito, 2005). Also, SSL checks for message integrity by using the message digest to find out if the message is altered or not (message reliability). If SSL detected an attack or insecurity of the connection, it will end the session and client and server has to establish a new connection (BCSI, 2008 and Jaha et al., 2007).

3. Intrusion Detection System (IDS) with Virtual Private Network (VPN)

VPN provides encryption/decryption on low level of the Internet at a time of communication process (Yousaf, 2018). Hence, they permits the application of unsafe services be carried through them with security (Likhar et al., 2011). This can be enforced by employing several open-source and commercial hardware or software solutions. Intrusion Detection Systems (IDS) have conventionally been applied to discover security attacks on either network or at a host level (Policy violations). In this section the study explained how IDS works on VPNs. An intrusion detection system is a device or process that capable of analysing network activities or a computer system for illegitimate malicious entry by intruder(s)(Rama and Anup, 2020). It was stated by Vik et al. (2010) that IDS are used to detect offenders (intruders) in the play or intending to damage network resources. IDS shield a system or network from recourses misuse, compromise or a real attack. It can also be able to examine network behaviours, computer systems for potential system configuration errors, audit network and analyses information integrity (Depren, et al. 2005). This study discussed on how these scenarios will be employed on VPN to protect its network system and traffic from malicious attacks. Vik et al. (2010) found that there are two types of IDS, Host-based IDS and Network-based IDS. *Host-based IDS,* (Natalia, 2021).mentioned that, this type of IDS can examine various areas on a computer system to discover intrusion entries. These areas include types of log files, such as network, kernel, server, firewalls and systems. Moreover, it compares these log files versus an inner database of common signature for recognised attacks (Markku, 2019). The next thing, it will filter and analyses the exploited log files. Then it will retag the abnormal packets with its systematic message informing danger. Finally, the IDS will evaluate, rate and accumulate them in its own specified log for executive or administrative analysis. *Network-based IDS,* Giris and Vishal (2021) and Vik et al. (2010).stated that, this type of IDS is personally responsible to function on network packets and it can scan traffic at the host-level or router and examine packets data. After finding suspicious packets, then it logs them into its own specified database log file for executive or administrative analysis tagged with warning system message (Goh et al., 2009). SNORT – is one of the latest and popular effective network-based IDS software available in market, it altered to suit various UNIX platforms and it has updated database of maliciousattacks that an individual can contribute and update through the internet. Snort was designed to be complete versioned and effectively logging malicious attack and giving notice to administrators when malicious attack occurs or about to occur (Natalia, 2021).

3.1. How IDS Works on VPN

The study started by discussing on how IDS generally works and then it explained on how IDS can be exploited on VPNs. Data mining techniques plays a special role in Intrusion Detection System. Intrusion detection is information analysis process and data mining help by applying a specific algorithm to extract particular patterns of data from database, e.g., suspicious activities. According to Ya-qin et al. (2010) the process of intrusion detection is categorised as follows: (I) Information (data) collection. (ii) Information pre-processing (iii) data mining (IV) intrusion detection (ID). This model or process of Intrusion detection is based on set of rules and algorithms connected to together to carry out the analyses (Rama and Anup, 2020).

The sniffer, on network or host based is accountable for gathering data that is kept on the original database, and then the data will be pre-processed into processed data set (Jabez and Muthukumar, 2015). Additionally, re-use rules and algorithm association will be placed on this processed data set to extract particular patterns (suspicious activities) of data and this information is saved to model the knowledge base and rule base. The next step is to analysis the data to study rules and identify the invasions from the knowledge base, at the same time, from the rule base for modifying the warehouse updates (Adeyinka, 2008 and Jaha et al., 2008). The final step involves sending or reporting the results to the executive or administrator for validations.

Generally, these types of IDS could be summed as (i) analysing the network traffic packets for intrusions and (ii) analysing the log files for questionable activities (intrusions). From the scenario above, in (i), the IDS will not be capable to analyses the traffic packet since VPN requirement is to employ encryption/decryption functionalities between endpoints

(Vik et al., 2010). In some manners IDS will require to decrypt all the traffic packets to be able to see the data content (Natalia, 2021). Precisely, for VPN settings, it is not an ordinary or usual to constitute network IDS (Khalil, 2018). Generally, considered to this scenario an intruder or attacker would require being VPN group member (legitimate or authorised member) before establishing an attack. For an intruder to be a legitimate member, he/she will need to have a legitimate username/password directly without any sophisticated method (brute force). This contextual attempt will come out in log file which result to host base intrusion (ii), where the log files are analyse for potential intrusion. That showed that Intrusion detection systems can easily works on VPN with host base intrusion rather than network base intrusion.

According to Giris and Vishal (2021) and Goh et al. (2009) IDS could only analyse network traffics to discover malicious actions when the network traffic is approachable or visible for analysis. Still, this explained the fact that, IDS have no access to VPN packets, since the VPN is responsible to protect all traffic packets. Because of the problem in the IDS scenario mentioned above, Goh et al. (2009) proposed a solution that could allow IDS to proceeds and function on VPN traffics without tempering with the data confidentiality. Vik et al. (2010) conducted a study into the proposed solution and evaluated it. The research conclusively proved that based on using Shamir's secret-sharing scheme and randomised network proxies, IDS could be able to detect all malicious activities in encryption tunnel like VPN (Rama and Anup, 2020 and Narayan et al., 2008).

4. Methodology

This section described the methodological analysis used to explain and evaluate the performance of SSL in VPN with intrusion detection system. This research used an experimental test bed analyses the performance of SSL. It also used observational studies as types of empirical study to describe and provide evidence on how IDSs works on VPN as described in section 3. It discussed about SSL protocol benefits and how it used to authenticate VPN endpoints and provide secure communication with IDS. The major goal of this research is to evaluate the performance of SSL VPN protocols on Debian Linux environment. To measure and analyses the performance of VPN protocols, this study used OpenVPN Dd-wrt.com (2011) is a free open sources software application for SSL VPN implementation. It is installed to evaluate different aspects of the SSL protocol.

The experimental tested of this consists of a HUB and four Nodes included with their IP addresses and 100Mbps Ethernet interface cards (eth0 and eth2) used. These nodes are Node A, Node B, Node C, Node D and they run Debian Linux operating system. The experimental testbed is a network of two private networks (192.168.1.x and 192.168.2.x), Node A (192.168.2.2) and Node C (192.168.2.1) formed one private network including the hub between them. Similarly, Node B (192.168.1.2) and Node D (192.168.1.1) formed another private network including the hub between them. The important matter in this study is to create a secure VPN tunnel between these two private networks through unsafe public network (Internet).

Node A and node B, each is connected to a hub through its private's network to a VPN endpoint. Node A and Node B, runs Iperf 2.0.0 tool, Iperf 2.0.0 Openmaniak.com (2010) is network traffic generator, monitoring and designed tool that used in this research to generate UDP traffic and measure the packets bandwidth/throughput (Wu et al., 2011). Node B runs Iperf client software to generate traffic and measure the performance. Node A runs Iperf server to listen to traffic generated from Node B and measure the performance.

Node C and Node D are software gateways machines that acted as a point where SSL VPN installed for both client and server VPNs. Node C runs VPN server while Node D runs VPN client and all are connected to the public network (internet) as well connected to a hub through private network to client machines (Node A and Node B).These VPN client and VPN server gateways acted as a VPN tunnelling end-point and software router for forwarding UDP traffic generated from Node B through the VPN tunnel to Node A. Each one of these VPN endpoints contains an IP forwarding details that enables the forwarding capabilities.

Generally, in this study we ran Open VPN (SSL VPN software) on Node C and Node D to create a secure VPN connection. Kotuliak et al. (2011) and Likhar et al. (2011) described that, Security in Open VPN is addressed by the cryptographic program library which supplies solid protection above SSL using standard encryption algorithms such as AES and 3DES. This study exploited these open-source applications cited above for implementing the SSL VPN. To ensure effective performance analysis and integrity, the research ran multiple executions for sufficient durations to produced results. The experimental tests are taken between Node A and Node B through Node C and Node D and the specification for these four nodes used in this research are shown in table 2 below.

Node	Description
Node A: Iperf Server endpoint (Traffic listener)	• Operating System - Debian 6.0.5(squeeze), kernel Linux 2.6.32-5-688, Hardware memory (RAM): 946.7MiB, Processor: AMD Athlon(tm) XP 3000+, Channel Capacity: 100Mbps, Fast ethanet adapter with interface cards • Mesurement tools installed – Iperf 2.0.0 network traffic genarator and monitoring tool, tcpdump tool (Thegeekstuff.com, 2010) and ping tool.
Node B: Iperf Client endpoint (Traffic Generator)	• Debian 6.0.5(squeeze), kernel Linux 2.6.32-5-688, Hardware memory (RAM) : 1.9GiB, Processor: AMD Athlon(tm) 64 X2 Dual core processor 5000+, Channel Capacity: 100Mbps, Fast ethanet adapter with interface cards • Mesurement tools installed – Iperf 2.0.0 network traffic genarator and monitoring tool , tcpdump tool and ping tool.
Node C: VPN Server	• Debian 6.0.5(squeeze), kernel Linux 2.6.32-5-688, Hardware memory (RAM) 946.7MiB, Processor AMD Athlon(tm) XP 3000+, Channel Capacity: 100Mbps, Fast ethanet adapter with interface cards • VPN tools installed – OpenVPN 2.0 used to create SSL VPN connection. This node acted as an SSL VPN server.
Node D: VPN Client	• Debian 6.0.5(squeeze), kernel Linux 2.6.32-5-688, Hardware memory (RAM): 946.7MiB, Processor: AMD Athlon(tm) XP 3000+, Channel Capacity: 100Mbps, Fast ethanet adapter with interface cards • VPN tools installed – OpenVPN 2.0used to esterblish SSL VPN connection. This node acted as an SSL VPN client.
HUB	10 ase Hub-24, Hewlett packard Advance HP J2601A

Table 2: Test-Bed Hardware and Software Components Specifications

5. Experimental Results Discussion and Evaluations

This section explains the test result obtained from the experiment conducted in this research. This experiment repeated several times in other to obtained fair and effective result. The description of these results is as follows:

5.1. Throughput

To measure the throughput, this research used Iperf measuring tool to analysed and generate packet with different frame size. The experiment repeated so many times to obtain accurate result. It showed that without VPN connection it has the lowest throughput and less secure. With VPN connection, as you sent traffic with bigger frame size, the throughput gets increased 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 (Ajiya et al., 2019). The result indicated that SSL/3DES has the highest throughput followed by SSL/AES as showered in figure 2 below.

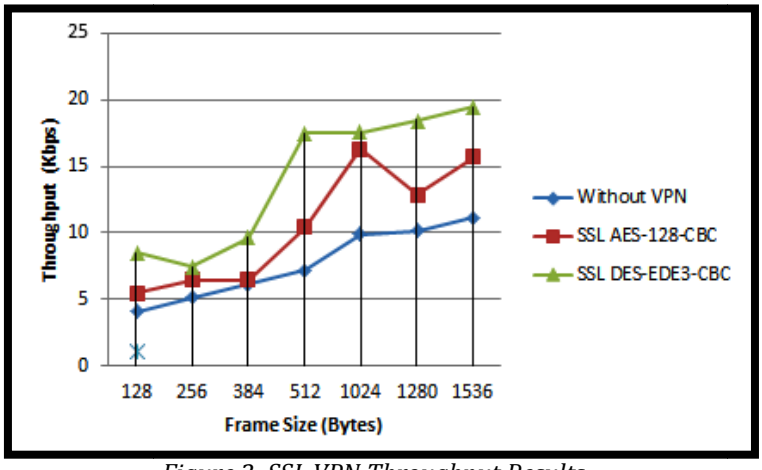

Figure 2: SSL VPN Throughput Results

5.2. Packet Latency

The packet latency is measured using ping tool and analysed for generated traffic for differed frame size. This experiment is replicated many numbers of time to find the average latency samples for different frame sizes. The overall latency results of this experiment are shown in figure 3. It indicated that latency values get increases when the frame size increases. Also, it showed that the latency without VPN is less than all the latency values for SSL/AES and SSL/3DES. Ajiya et al. (2019) explained that, it happens because of the traffic load with encrypted packets over packets without encryption. The result also indicated that, SSL/3DES win, because it has the highest maximum latency then followed by SSL/AES.

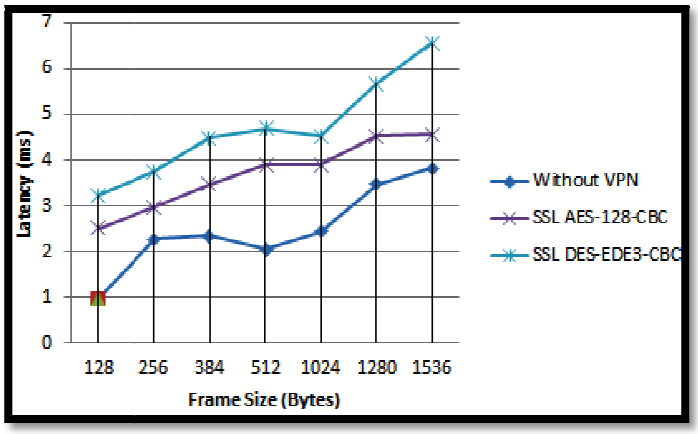

Figure 3: SSL VPN packet latency results

5.3. Packet Loss

The packet loss is measured using tcpdump. This experiment is repeated many numbers of time to find the average packet loss for different frame sizes. The overall percentage packet loss results of this experiment are shown in figure 4. It indicated that SSL/AES has the highest packet loss. Evidently, because of the packet loss prominence for SSL\AES, SSL/3DES win over SSL/AES.

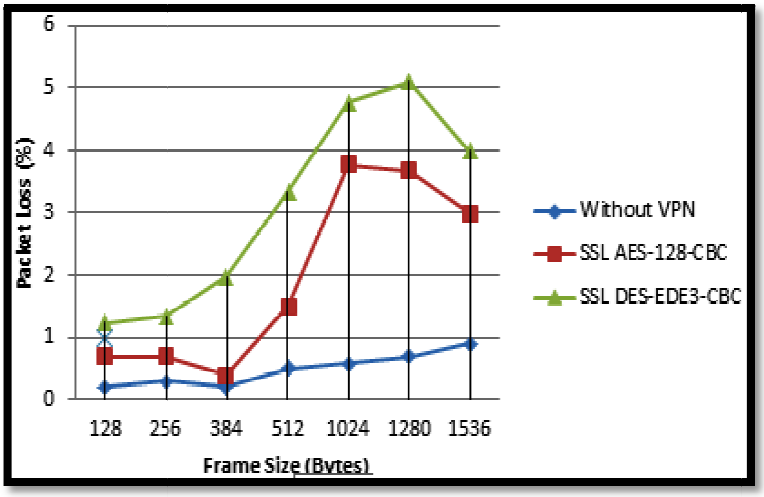

Figure 4: SSL VPN Packet Loss Results

6. Summary and Conclusion

In this study, through empirical observation we examined the performance of two VPN tunnelling protocols SSL and IPsec configured with AES and 3DES cryptographic algorithms. These protocols were 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.

7. References

i. Adeyinka, O. and Shoniregun, C. (2007) Secure Communication with SSL Remote Access VPN. *School of Computing and Technology: University of East London,* p.1 - 10.

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

iii. Ajiya A.A. et al. (2019). Performance Evaluation of IPSEC-VPN on Debian Linux environment. *International Journal of Computer Applications.* Volume 181, issue 45, p.0975 – 8887.

iv. 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.

v. BCSI. (2008). Blue Coat Systems: *Technology Primer: Secure Socket Layer (SSL).*

vi. CISCO. (2002). Cisco Systems: Introduction to Secure Sockets Layer.

vii. Dd-wrt.com (2011). *Open VPN-DD-WRT Wiki*. [Online] Available at: http://www.dd-wrt.com/wiki/index.php/OpenVPN#Server_Configuration [Accessed: 31 Jul 2019].

viii. Depren, O. et al. (2005). An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. *Expert Systems with Applications. p.* 713–722. Issue 26.

ix. Girish B. and Vishal K. (2021). Technical Review on Network Security. P.E.S College of Engineering Aurangabad: Case Studies for Research in Computer Science and Engineering. 978-81-951800-4-2.

x. Goh, V.T. et al. (2009). 'Towards intrusion detection for encrypted networks', *IEEE 4th International Conference on Availability, Reliability and Security*.pp.540–545.

xi. Jaha, A. et al. (2007). Performance Evaluation for Remote Access VPN on Windows Server 2003 and Fedora Core 6. *IEEE: TELSIKS,* p.587 - 592.

xii. Jaha, A. et al. (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.

xiii. Jabez, j. and Muthukumar B. (2015). Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach. *International Conference on Intelligent Computing, Communication & Convergence*. Issue 48, p. 338 – 346.

xiv. Kotuliak, I. et al. (2011). Performance Comparison of IPSec and TLS Based VPN Technologies. *9th IEEE International Conference on Emerging eLearning Technologies and Applications*, p.217 - 221.

xv. Khalil. M. M. A. (2018). Hybrid Based Network Intrusions Detection Systems. *Sudan University for Science and Technology. P. 1-79*

xvi. Likhar, P. et al. (2011). Performance Evaluation of Transport Layer VPN on IEEE 802.11g WLAN.*Journal of Institute of Electrical and Electronics Engineers*, (197) p.407 - 415.

xvii. Mazlan, Z. M. et al. (2010). Technical Comparison Analysis of Encryption Algorithm on Site-to-Site IPSecVPN.*International Conference on Computer Applications and Industrial Electronics*, p.641 - 645.

xviii. Markku, H. M. (2019). Open source IDS evaluation for small and medium-sized enterprise environments. *Jamk.fi. p. 1-41.*

xix. Narayan, S. et al. (2008). Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Environment.*IEEE International Conference on Advanced Computer Theory and Engineering*, p.69 - 73.

xx. Narayan, S. et al. (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*.

xxi. Natalia M. (2021). Network Protection Tools for Network Security Intelligence Centers. 2020 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: Eleventh Annual Meeting of the BICA Society. 190 (2021) 597–603.

xxii. Openmaniak.com (2010). *OPENVPN - The Easy Tutorial - Tutorial*. [Online] Available at: http://openmaniak.com/openvpn_tutorial.php [Accessed: 31 Jul 2019].

xxiii. Rama B. and Anup G. (2020). Common Vulnerabilities Exposed in VPN – A Survey. Journal of Physics: Conference Series: 1714 (2021) 012045. doi:10.1088/1742-6596/1714/1/012045.

xxiv. Skullbox.Net (2008). *Types of VPNs*. [online] Available at: http://www.skullbox.net/vpn.php [Accessed: 22/07/2018].

xxv. Vik, G. et al. (2010). Experimenting with an intrusion detection system for encrypted networks. *International Journal of Business Intelligence and Data Mining*, 5 (2), p.172 - 191.

xxvi. United States Patent Burns (2018). Identifying applications for intrusion detection systems. Pat .No .8 , 291, 495.

xxvii. Wu, K. et al. (2011). Test and Analysis of Sensitive Factors of SSL VPN on Kylin.*Journal of Institute of Electrical and Electronics Engineers*, p.3207 - 3211.

xxviii. Ya-qin, F. et al. (2010). Data Mining Based Intrusion Detection System in VPN Application.*IEEE: WASE International Conference on Information Engineering*, p.50 - 52.

xxix. Yousaf, A. (2018). Asymptotic Intrusion Detection System for Stealthy Intruders.*Faculty of the Electrical Engineering Department University of Engineering and Technology. p. 1 – 126.*