Academic Journal of Nawroz University (AJNU), Vol.12, No.2, 2023

https://doi.org/10.25007/ajnu.v12n2a1155

Performance Investigation of IP Security Virtual Private Network in Ipv6 Environment using Quality of Service

Emad Adil Dawood[1], Rafid Salih Sarhan[2]
[1]Information Technology Center, University of Duhok, Iraq
[2]Department of Electrical and Computer Engineering, University of Duhok, Iraq

Abstract

Different types of data are transmitted through the internet, these data such as Email, HTTP, FTP and VoIP conversation might contain important and sensitive information which can be read or seen by other users. Many attacks such as man in the middle, packet sniffing and phishing are available and used by many attackers, as a way to access the protected information. Based on this fact, security and privacy become a necessity in the field of private network (intranet) and public network (extranet). IP sec VPN is considered to be the strongest technique for protecting packets from any kind of attack. In this paper, an analytical study is accomplished using opnet simulation software to design and analyze the proposed network. The proposed network represents four sites in different cities are communicating using the technique of IPsec VPN, different scenarios are created and studied to investigate the performance of network using IPsec VPN in IPV6 environment with QoS. The investigated metrics were packet delay variation, jitter, packet end to end delay, download and upload response time.

Keywords: IPsec VPN, QoS, Security Protocols, AH, ESP, IPv6 environment, Performance of the network.

1 Introduction

The aim of inventing internet protocol (IP) with TCP, UDP and other protocols was to make the communication over the internet network possible and available, without taking into consideration the target of securing the communication. Because of that, different security threats and attacks have been raised due to the deficiency of security characteristics for internet protocol (IP). (Prabhu and K, 2019). Additionally, the process of detecting an attack is very difficult and complicated, because it does not contain or show any kind of data alteration. In this state, the possibility to prevent the success and progress of these attacks can be made using the process of encryption. In other words, passive attack can be prevented and stopped using the concept of prevention rather than alteration. Based on this fact, protecting data is very necessary and can be accomplished using the technique of Virtual private network (VPN), Vpn is the process of providing security traffic and reduces the latency.

The sections for this research are organized as the following: section 2 presents the technology of IPsec VPN and QoS, section 3 describes the topology of the network. Section 4 investigates and discusses the outcomes. Section 5 compares and evaluates the obtained results. Lastly, section 6 includes the conclusion for this research.

and privacy to LAN and WAN networks, packet in vpn is encapsulated and sent across the network by a tunnel, VPN utilized different protocols to create a secure environment for data, one of these protocols is IPSec VPN (Sabah & Abdul Hadi , 2013), IPsec VPN represents a powerful security means for protecting information over IP networks. Additionally, the requirements of security for example Authentication, privacy, confidentiality, integrity and non-repudiation, no response are needed to supply a secure environment for data. Offering security will improve the level of protection in the network, but at the same time will affect on the performance of network in term of QoS Voice metrics (Masqueen & B.R, 2012). In this case, to improve the performance and efficiency of network while implementing security, IPv6 is utilized because it has a simpler header than IPv4, additionally, IPsec VPN is designed to work with IPv6 which will add a better performance in term of latency and loss of data. Furthermore, QoS is enabled in network to priorities most important

2. IPsec VPN

The IPsec VPN is a technique used to create a secure environment for different types of traffic. It can be utilized between two routers, gateways and firewalls, as well as between a customer and a gateway. There are two various modes for IPsec: Transport mode, used for security between host to host, it protects the payload of IP packet, the second one is tunnel mode which provides

security between two networks, the whole IP packet is protected in this mode. (Masqueen & B.R , 2012).

In other words, to secure and protect virtual networks, VPN uses different protocols to accomplish that, and one of these protocols is known as IPSEC which represents the most robust security protocol in term of protection and privacy, as well as, it is considered a very suitable protocol to connect remote sites with main office as it utilizes a tunnel to link point to point locations. (Sadia & Ibtehaj, 2019)

IPsec uses the Diffie Hellman key in two nodes to create a secure communication and utilizes a shared secret key which is recognized by them only. This shared secret key is produced from the public and private keys for both nodes. (Sharma & Shiwani, 2013).

The implementation of IPsec is very essential and necessary in IPv6 environment and this task can be accomplished by using two protocols which are AH and ESP. Both of them represent the main part of IPSec and provide it with the ability to offer different services, while the absence of them, will not help IPSec to offer the fundamental service it was developed for. (Muhammed & Ali, 2015)

IPsec uses two protocols to add security; those protocols are AH and ESP. The first one offers integrity and authentication for data, in addition to anti packet repetition. Confidentiality is not provided in AH and because of that, it has a simpler header in comparison with ESP. (Ankush, 2012)

ESP offers all the security features provided by AH but it also provides confidentiality during the encryption of traffic. ESP makes some modification in the original packet by inserting additional ESP header with packet trailer. The IP header is located before the ESP header which is situated before the protected data. The entire data payload and a part of trailer are encrypted while the ESP header is not encrypted. Finally, the authentication fields of the packet will include ESP header, data payload and a trailer section as shown in Fig (1). (Masqueen & B.R , 2012).

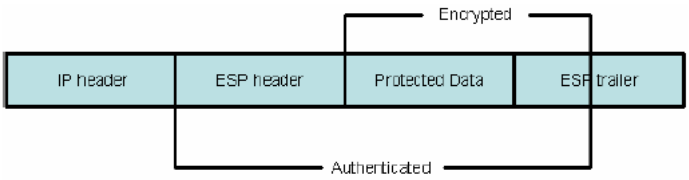


Figure (1) Encapsulated IP packet with ESP

2.1 Quality of Service (QoS)

Is a collection of mechanisms which are used to manage the bandwidth, jitter, latency and packet loss. It is necessary to guarantee that critical traffic is having many resources they need in order to avoid any problems in a converged network. (Paresh et al, 2016). The main objective of quality of service (QoS) is to provide good and planned services for different types of traffic with dedicated bandwidth and controlled delay. By this mechanism, QoS will ensure and guarantee the delivery of significant data. (Aliy & D, 2019). Moreover, the technique of QoS can be enabled in routers by:

- Providing dedicated bandwidth
- Enhancing the characteristic of loss
- Avoiding and managing network congestion
- Shaping traffic and configuring priority of traffic through the network (Muhammed et al, 2014).

Four elements (jitter, end to end delay, bandwidth and packet loss) represent the parameters of quality of service as shown below

- Bandwidth represents different range of frequencies that are utilized by signals in transmission medium. The frequency of signal is calculated by Hertz (Hz), while throughput represents the real bandwidth and is calculated using a particular time unit which is utilized to deliver data of a specific size. (hafiz & susianto,2019). The standard throughput values are shown in table 1 (Winarno et al, 2015).

Table (1) Throughput standards

- End to end delay is the sum of delay from the source node (sender) to the destination node (receiver) including the latency of compression and decompression. (Mahdi et al, 2017). In TCP/IP network, the delay is divided into packetization, queuing, propagation, transmission and processing delay. The standard values of delay are shown in table 2 (Winarno et al, 2015).

	Category	Throughput/Bandwidth Percentage
Through put standard	Excellent	100 %
	Good	75 %
	Medium	50 %
	Poor	<25 %

Table (2) The Quality standards ITU-T G.114 of latency

	Category	Delay
Delay (Latency) Standard	Good	0 - 150 ms
	Medium	150 - 400 ms
	Poor	> 400 ms

- Jitter is the difference in arrival time for sequential packets. (Mahdi et al, 2017). Jitter is produced because of the congestion at IP network and congestion is occurred when the bandwidth is inadequate and the capacity is exceeded by network data traffic. The standard values of jitter are shown in table (3). (Winarno et al, 2015).

Table (3) The Quality standard ITU-T G.114 of jitter

	Category	Jitter
Jitter Standard	Good	0 s/d 20 ms
	Medium	20 /d 50 ms
	Poor	> 50 ms

Packet loss represents a status which indicates the total number of lost packets (Hafiz & Susianto, 2019). There are many factors to packet loss such as congestion, limitation of network devices, excession of nodes buffer and network policing or control. The standard values of packet loss are shown in table (4). (Winarno et al, 2015)

Table (4) The Quality standards ITU-T G.114 of packet loss

	Category	Jitter
Packet Loss Standard	Excellent	0 %
	Good	3 %
	Medium	15 %
	Poor	25 %

2.2 Literature review

In 2017, a comparative study is observed by a group of authors to investigate the scalability of architecture of different technologies: IP, MPLS, MPLS VPN and MPLS VPN with IPsec. The studied network is designed and configured using open source software known as GNS3. The load is increased with changing the type of technology in each scenario to evaluate the effects of tunnel layer on real time applications. Accordingly, they concentrated on VOIP application and generated VOIP traffic using IP SLA probes. Finally, the outcomes obtained from analyzing jitter, delay, MoS score and loss rate. (Faycal et al, 2017)

In 2018, a scientific study is completed by a group of researchers to analyze the effects of encryptions algorithm on quality of service (QoS) network. The measurements of networks were achieved using two methodologies ITU-T Y.1564 and RFC 2544. Many metrics are examined such as bandwidth, latency and data loss. Moreover, two networks were designed to perform the study, one is unsecured and the second one is secured. The studied networks were implemented using real equipments (Cisco devices and ASA firewalls) and the tests were accomplished utilizing EXFO FTB-860 NetBlazer testers. Furthermore, a site to site IPSec VPN was enabled between LAN to LAN 2 with (various mixtures of encryption algorithm and hash functions), and traffic was provided by the testers which also have been used to collect the results. It was found that the utilization of security techniques including IPSec, VPN and IPS which were configured on cisco devices generated a small deterioration on QoS metrics. This deterioration is occurred from IPSec VPN because of the extra data overhead encapsulation, and the required time for processing the encryption and decryption and hash function calculation. (Darius et al, 2018)

In 2019, a scientific research is accomplished by Subhi who studied the effects of implementing the technique of virtual private network (VPN) on the performance of network; the proposed network includes five locations: one location for center server and the other four locations for service sites. He created four scenarios to simulate the network: the first scenario was a network without VPN , the second scenario was a network with VPN with centralized servers , the third one was a network with VPN distributed servers and the last one was a network using server load balance. Furthermore, Opnet and boson simulation software's were used to simulate the networks and the selected time of simulation was 5 minutes to obtain the results. Moreover, two security

protocols have been activated in the network including L2TP and IPSec. Based on their work, it was found that the response time for packet transmission is higher for all different applications in the state of of using VPN in comparison with the same network without VPN. (Subhi, 2019) .

In 2019, a scientific research is achieved by Prabhu and K. to analyze the performance of throughput for IPsec protocol for both Ipv4 and IPV6 networks, three cases have been created, studied and compared and in each case a specific cryptographic algorithm is applied. Furthermore, the researchers have used TCP and UDP to analyze the performance of IPSec in IPV4 and 6. The designed network consisted of two physical devices connected to each other directly and each device has an open source operating system known as Ubuntu 14.04 LTS. Moreover, strongswan software version (5.3.5) is installed on both operating systems to create IPsec tunnel between them and an open source tool known as IPer3 is used to investigate the efficiency of IPSec, as this tool generate traffic for testing the performance of IPsec tunnel under different encryption and authentication algorithm. It was found that the outcomes showed that in AEAD algorithms AES128GCM16 reflected better performance than AES128CCM16 and AES-CTR showed better performance than AES-CBC and 3DES; and SHA1 performed better than SHA256. Finally , the results showed that UDP recorded better performance in comparison with TCP as the size of header in UDP is 8 byte which is smaller than TCP (20 byte). In addition, the overhead on CPU is lesser in UDP because it is a connectionless protocol that does not need acknowledgment messages. (Prabhu & K, 2019)

In 2020, Conrad and Smart evaluated the performance of internet protocol security (IPsec) based MPLS virtual private network, they made a comparative study between two scenarios , the first one was MPLS VPN network without IPsec and the second one was MPLS VPN network with IPsec. Opnet modeller 14.5 was used to simulate the scenarios. As well as. QoS metrics for VOIP and Video conferencing were collected to analyses the outcomes. They concluded that using IPsec increased the size of packets by about 9.98% and that increased jitter and latency in MPLS network. In spite of this increment, jitter, delay and mean opinion score (MOS) for voice over internet protocol (VOIP), and jitter for video conferencing remained acceptable and within the margins of ITU-T. Moreover, it was noticed that the scenario of IPsec based MPLS virtual private network was more secure and stable with higher consumption of bandwidth in comparison with the scenario without IPsec. (Conrad & Smart, 2020)

In 2020, Zaman and Mousa examined the effects of virtual private network (VPN) on network efficiency when using various types of traffic generators such as HTTP , FTP and CBR. They made and simulated two networks using network simulator 2 (NS2); the first scenario was without VPN and the second scenario was with VPN. As well as, each scenario (with VPN vs without VPN) was studied and investigated while generation one type of traffic. Based on that, the time delay and throughput performance for each type of traffic (FTP, HTTP and CBR) were analyzed in the case of using VPN and not. It was noticed that the use of VPN has an apparent impacts on network performance because it increased the time delay for HTTP-UDP and HTTP-TCP comparison with other sorts of packets. On other hand, the throughput found unchangeable for CBR traffic with and without VPN, while it recorded a decrement in the case of FTP and HTTP. (Zaman & Mousa, 2020)

In 2020, a research paper has been published by a group of researchers who did a review and assessment for virtual private network tunnel to compare the features of three types of protocols (IPSec , GRE , Wire guard) to diagnose the strength and weak points of each one of them. The main objective for their study was to show which protocol is the best one based on some criteria and also other reviews of researchers. They studied the advantages and disadvantages for the three VPN protocols at the network layer. They mentioned that the use of IPSec has a stronger authentication in comparison with GRE and wire guard as IPsec uses AH and ESP. In the other hand, they stated that IPsec and wire guard are competitive in many characteristics but at the same time wire guard is better than other protocols, and the weak point of it that it is new and remain untested completely. (Adnan et al, 2020)

3. IPsec VPN Network

Opnet simulator 14.5 has been used in this scientific research which is considered a powerful tool that is utilized to create, simulate and analyze the performance of any network designed topology (Opnet, 2019). It is assumed that there is one productive network connecting 4 sites through Kurdistan region in Iraq, these locations are communicating with each other using IPsec VPN, each site is located in a city, the main site is located in Erbil city which contains the productive servers while the branch sites are located in sulaymania , Duhok and Zakho cities. The clients in Sulaymania, Duhok and

Zakho are requesting the information from the servers in Erbil city. It is also required that the designated network provides privacy, confidentiality and protection from any kind of attack. Based on that, Four servers namely voice, video, http and email are connected to switch (ethernet16_switch_adv) which in turn is connected to cisco router (CS_3620_2s) (R2) ,the branch sites include private networks which are connected to 3 cisco routers from the type (CS_3620_2s), named as (R1,R3,R4) via Ethernet switch (ethernet16_switch_adv) . All the routers are connected together via IP cloud using PPP_DSI at data rate 1.544 Mbps, on the other hand, the clients and the servers are connected with the switches using 100BaseT duplex link at data rate of 100Mbps. Fig (2) shows the simulated network model.

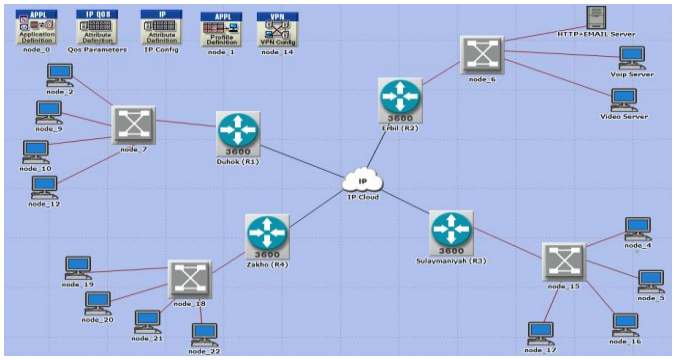


Figure (2) IPsec VPN Network

3.1 IPsec VPN Network Configuration

Various types of applications including normal and real time traffic have been created to simulate the network and to make it close to reality as much as possible, these applications are HTTP, Email, Voice and Video. This process is configured in application definition.

The mechanism of traffic has been determined on the profile definition, the start time has set to 5 sec while the inter-repetition time is set to 5 also, that means each request will be sent every 5 sec. Finally, the duration time is adjusted until the end of simulation as show in in Fig (3).

The tunnel has created between Duhok to Erbil, Sulaymania to Erbil, and Zakho to Erbil, the operation mode for VPN is selected to be compulsory, remote clients list is set to 4 which represents the clients who are requesting the information , This process is configured in IP VPN Config as shown in Fig (4)

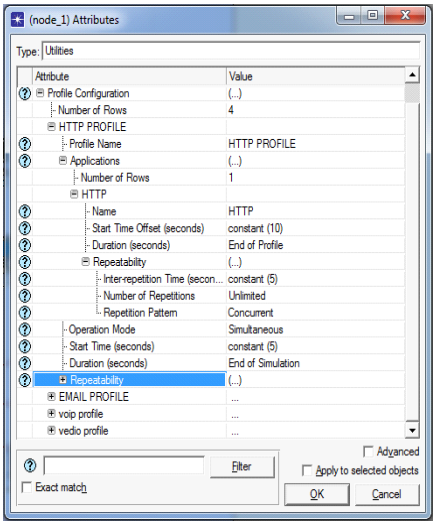


Figure (3) Mechanism of Traffic Generation

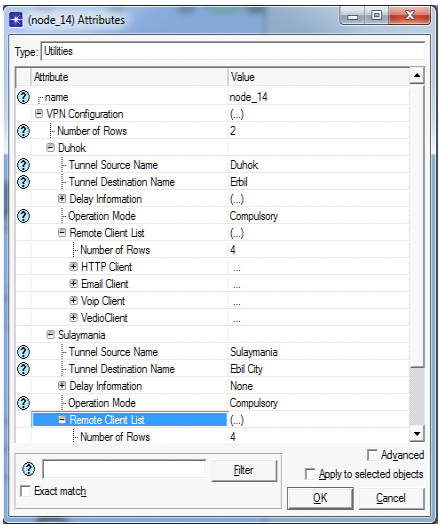


Fig (4) Configuration of VPN

3.2 IPsec VPN Network Scenarios

In this paper, 2 scenarios have been made in order to simulate the network; the network represents four cities in Iraq-Kurdistan region which are connected together in one secured network in order to protect the information from any kind of attack. The main site is located in Erbil city which contains the necessary servers to serve and process all the requests from other cities.

Internet protocol version 6 (IPv6) has been enabled on both scenarios whilst IPsec VPN is configured on all routers in order to create a secure negotiation between the sessions of the routers. The first scenario does not include the utilization of (QoS) while the second scenario involves the activation of QoS, the latter includes enabling a special priority queuing on four routers

interfaces. Both scenarios have simulated for 5 minutes and the network was overloaded to study its performance when it is congested.

The nodes and routers in all scenarios are set to receive IPv6 dynamically. In IPv6 environment, the link local address is set to DEFAULT EUI-64 and the routing protocol is enabled to be RIPng as shown in Fig (5).

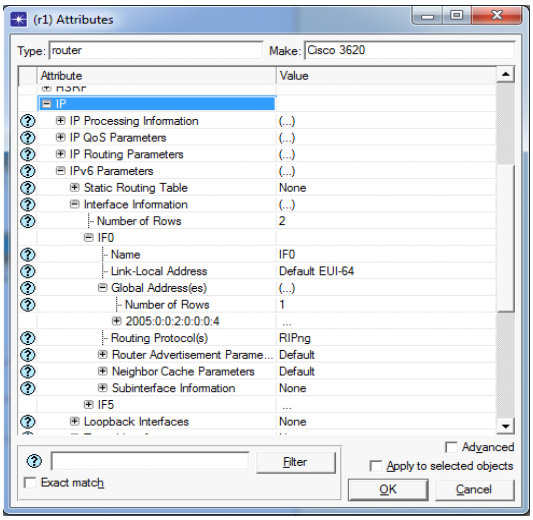


Figure (5) Configuration of IPv6 and routing protocol

Finally, The IPsec VPN has been configured on four router named as r1, r2, r3 and r4. The parameters for an IKE policy are set to: auto negotiate for mode and RSA Signature for authentication method; as well as the setting for IPsec Proposals are set to be as the following: the protocol used for IPsec session is Bundle (AH+ESP); algorithm of authentication is adjusted as HMAC-MD5; encryption algorithm is configured as 3DES and lifetime is set to 28800 as shown in Fig (6).

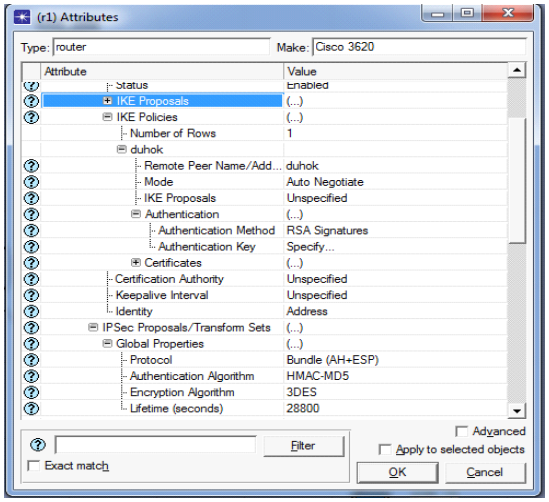


Fig (6) Configuration of IP security

4. Results and Analysis

Email Traffic

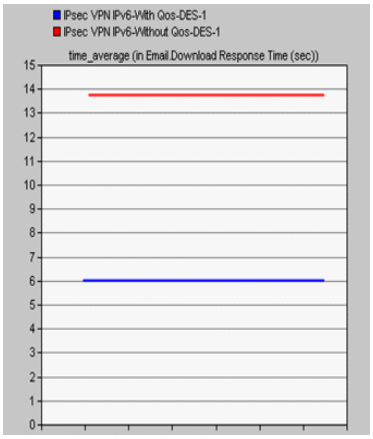


Fig (7) Download response time for Email packets

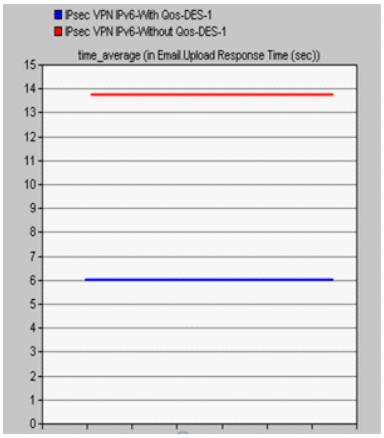


Figure (8) Upload response time for Email packets

Download response time represents the time that is consumed by a server to accept a request. It is noticed form Fig (7) that the time for IPsec VPN was higher in comparison with IPsec QoS. This is because the DR time reached 13.7 sec in the first scenario while it recorded 6 sec in the second one. Finally, the time in both scenarios continued stably.

Fig (8) illustrates upload response time for Email packets in IPsec VPN. It is observed that the response time in the scenario of without QoS has showed a high amount of delay which reaches to a value close to 14 sec whilst the delay in the second scenario with QoS was approximately 6 sec.

HTTP Traffic

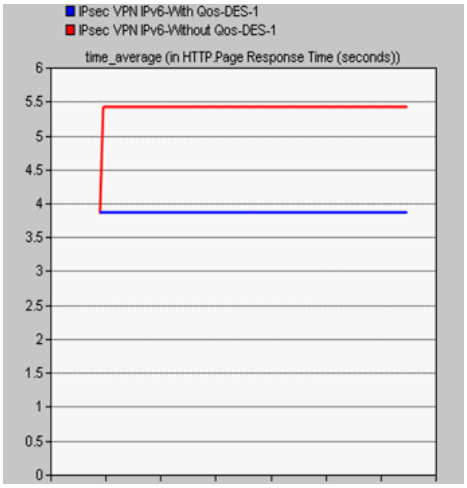
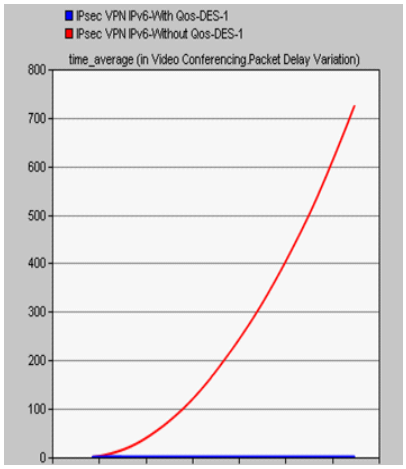


Figure (9) page response time for HTTP packets

Fig (9) shows the page response time in seconds for HTTP data, the first scenario (IPSEC VPN) reflected a high amount of delay in processing the http request as the time started to produce from 3.8652 and increased sharply until it reached to 5.420, after that it continued stably in generation. The second scenario showed another behavior which generated delay at 3.8652 and continued stably for 5 minutes. It is seemed that the response time is lower in the second scenario in comparison with first scenario (IPsec VPN).

Video Conference-Packet Delay Variation



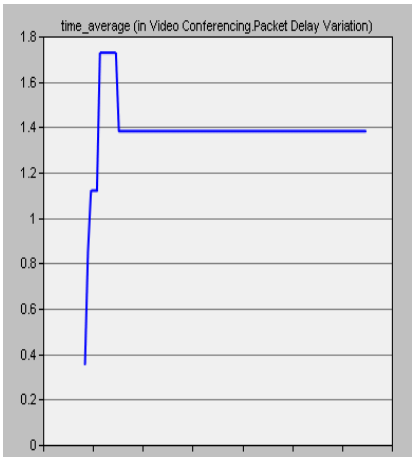


Figure (10) Packet delay variation for video conferencing

Fig (10) shows that the variation in delay for the first scenario (without QoS) recorded more than 700 second while the second scenario (with QoS) reflected a value of 1.7 second.

Packet End to End Delay

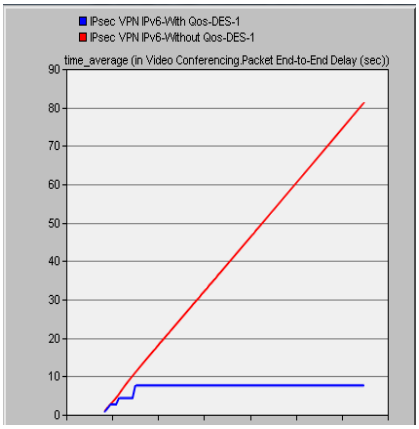


Figure (11) End to end delay for video conferencing packets

Fig (11) illustrates packet end to end delay for video conferencing packets in IPsec VPN. The x-axis shows the time of simulation in minutes while the Y-axis shows the end to end delay in second's units. It is observed that IPsec VPN without QoS has produced a higher latency, as the latter started to increase gradually from the mid of the first minute until it recorded approximately 81.354159 sec. The delay in second scenario (represented by the blue signal) started at the mid of first minute which increased sharply for a while until it recorded more than 4.322471 sec. After that, it increased sharply until it reached 7.621396 sec. Finally, the delay continued to be produced stably. Based on this behavior, the second scenario has shown a better and lower delay which did not exceed 7.621396 sec in its maximum production while the first scenario showed a higher delay which reached to more than 81.354159 sec during the simulation time. Moreover, it is realized that the mechanism of QoS has prioritized the packets, minimizing the delay by queuing the packets in the buffer and serving the most important packets using a specific priority queue.

Voice Jitter

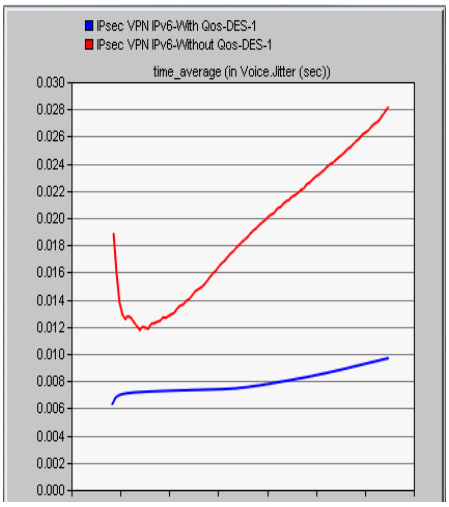


Figure (12) Jitter for voice packets

It is noticed that the voice jitter for IPsec VPN without QoS generated at the beginning of simulation time which was 0.01893, then decreased sharply to 0.01177, after that, the delay started to increase gradually until it reached 0.02825. Furthermore, IPsec VPN with QoS created a delay of 0.00639 and rose smoothly until it reached less than 0.00970. The scenario of QoS produced a lower jitter because of the technique of QoS that enhances network performance through reducing jitter for voice packets.

Voice MOS

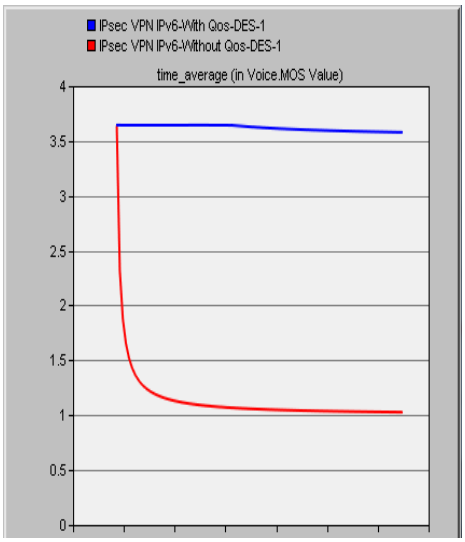


Figure (13) MOS for voice packets

Fig (13) shows that the MOS in IPsec VPN was between 3.644524 to 3.578537 while the MOS value in the scenario without QoS decreased sharply to record a value between 3.646188 to 1.027855. It is clear that the MOS in IPsec VPN with QoS gave a good result.

Packet delay variation

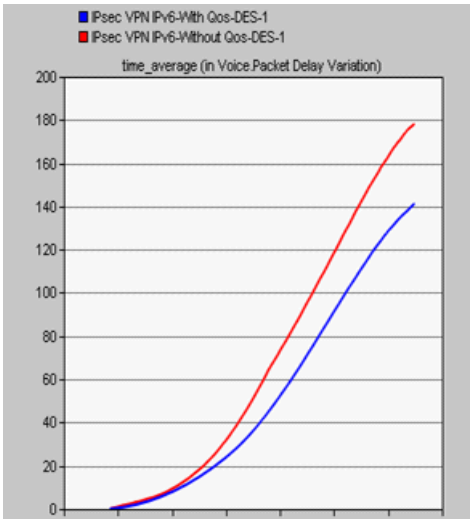


Figure (14) packet delay variation for voice packets

Fig (14) shows that packet delay variation in the scenario without QoS had a variation in delay reached to maximum of 178.138231 sec but the delay variation after using the mechanism of QoS reached a maximum value of 141.284183 sec.

End to end delay

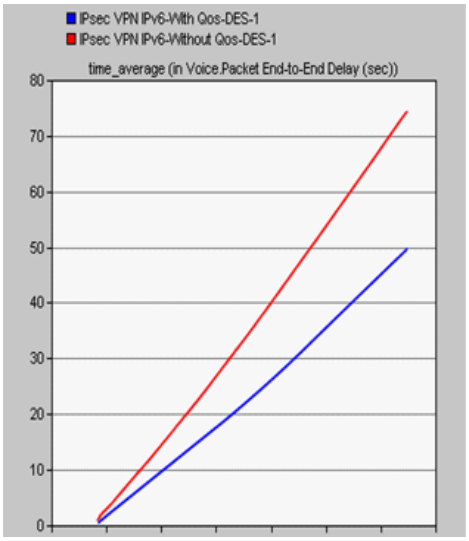


Figure (15) End to end delay for voice packets

It is clearly observed in Fig (15) that the end to end delay for voip packets recorded a value of 49.684454 sec which equals to 49684.454 ms in the scenario of QoS and approximately 74.515766 sec which equals to 74515.766 ms in the scenario of without QoS.

5. Evaluation and Comparison

The results obtained from the paper published in 2017 in the state of IPsec VPN with MPLS showed a close output to our investigated result. In spite of the fact that they used MPLS technique in the network but that did not prevent the increment in delay in the case of high load of traffic. Additionally, our research investigated different types of applications such as real time and normal traffic, and latency was increased after enabling IPsec and affected all the QoS criteria. Also the authors discovered that the MOS for the scenario of IP and MPLS with IPsec recorded a worst result while it was noticed by our research that the MoS in our first scenario (IPsev VPN without QoS) was not good and decreased sharply from 3.6 to 1, but after activating the mechanism of QoS in the second scenario (IPsec VPN with QoS) we discovered that the MoS improved and provided a better result ranging between 3.6 to 3.5. Finally, it is concluded that the proposed network in the research of 2017 (IPsec VPN MPLS) and our research IPsec VPN indicated that both environments were not adequate for VOIP applications, even though they used a faster technology which is MPLS and we used IPv6 with QoS technique for improvements purposes but that was not enough to create a suitable environment for VOIP traffic.

The research paper published in 2018, showed the impacts of using IPsec VPN on network performance and it was noticed that IPsec VPN generated deterioration on QoS metrics because of security protocols and encryption algorithm. Our results from simulating different scenarios showed also an increment in QoS parameters because we used IP security protocol (AH+ESP) which increased the length of packets by adding an AH header and ESP header to the original packets. Moreover, using security protocols impacted on the performance of routers because they need to encapsulate the packets and remove the headers in addition to the process of packet body decryption.

The results from the research accomplished in 2018 showed a negative effect of IPSec VPN with using different encryption algorithms on network performance, and that led us to notice that we experienced the same negative effect of IPsec VPN on QoS metrics, as we utilized and enabled two protocols of IPsec (AH + ESP) with the use of 3DES encryption algorithm and authentication algorithm (HMMAC-MD5), all these techniques degraded the performance of network, as the increase of values for delay and jitter in the mentioned paper with our paper was produced from the methods of authentication, integrity, non-repudiation, confidentiality and privacy. Additionally, the length of original packets increased because of the addition of AH and ESP headers. Furthermore, the performance of routers was affected and consumed by the process of encapsulating the packet and removing the header, as well as the process of decrypting the body of the packet.

The delay in the studied VPN network with IPsec from the research under the title "Performance Analysis of Volume Loads of (Services and Transmission) Traffic in VPN Networks" by Subhi (2019) increased for all applications including Email ,FTP and database, due to the process of encryption and decryption. In our research, we achieved the same type of increment in delay response time. For example the delay for HTTP page response and email download response time reached 5.420 sec and 13.7 sec respectively, while the delay for video traffic recorded 81.354159 sec and for VOIP traffic reached the value of 49.684454 sec. Moreover, as the previous mentioned research; the author did not use the mechanism of QoS and the new

generation of IP version 6 to enhance the performance of network in term of delay and other metrics. As well as, He did not study the impacts of IPsec VPN for real time traffic (voice and video traffic) which were investigated in our studied network and found that, in spite of the fact that the time for VOIP traffic is reduced from 74515.766 ms to 49684.454 ms, but it remained not suitable and acceptable in the simulated network because it is not in the normal range as the accepted range for end to end delay for voice packets is 150-200 (Reyad & Mohanad, 2012). On the other hand, the jitter for voice packets recorded a good value in the state of with and without QoS which was 6.9 ms and 28.25 ms respectively. As a result, the jitter in the network of IPsec VPN was suitable because it did not exceed the accepted range which is 20-50 ms.

The scientific paper published by Zaman and Mousa (2020) showed an increment in delay time for packets traversing between two pairs of networks using virtual private network (VPN) mechanism and this increment generated because of VPN technique which affected on the performance of network. In our research, the delay also increased in the case of VPN for all the types of traffic but we enabled QoS mechanism to prioritize the most important traffic such as video and voice to decrease the delay and jitter. Based on that, we noticed that the end to end delay was reduced in all simulated scenarios in the case of QoS implementation as mentioned in the section of results and analysis. Also the authors did not use high standards of protection and privacy as they enabled the technique of virtual private network (VPN) without using IPsec protocol which considers the strongest method to secure the network, while that protocol was used in the form of AH + ESP to provide the highest standards of security for our proposed network.

In 2020, The results collected by Conrad and Smart from studying the performance of IPsec in MPLS VPN network showed that the network IPsec VPN MPLS represents a suitable environment for VoIP and video conferencing traffic, in spite of the increment in jitter and delay for both (voice and video applications), and also MOS for VOIP. On the contrary, our studied simulated network showed that IPsec VPN using IPv6 environment is not adequate and sufficient environment for real time traffic such as voice and video because the end to end delay was very high with acceptable value of jitter, Furthermore, the technique of QoS improved the performance of network by reducing the end to end delay and jitter, but that was not enough to make the network with IPsec VPN to be the appropriate place for real time traffic. Finally, the MOS of voice for IPsec VPN MPLS was less than 3.5 while it was between 3.646188 to 1.027855 in our studied network (IPsec VPN without QoS), but when QoS was activated, the MOS value increased to record a number between 3.5 to 3.6 which reflected a better value than the one with MPLS network. The results of the scientific research under the title "Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol" in 2020 showed that IPsec is the best protocol in term of authentication and encryption while there are some studies not made yet on a new protocol known as wire guard. Our research used a practical method in term of the use of Opnet modeler to simulate the network and examine the advantages and disadvantages of IPsec VPN. The result was a high standard of privacy and protection was achieved when using IPsec (AH + ESP), but at the same time it impacted the performance of network in term of delay , jitter ,download and upload response time and other metrics for both real time and normal applications.

6. Conclusion

It is noticed that the protocols (AH & ESP) have increased the privacy and security of the network but at the same time added more delay due to the processes of authentication, integrity, non-repudiation, confidentiality and privacy that have been made by these protocols. Also, the security protocols increased the length of packets by adding an AH header and ESP header to the original packets, and impacted the performance and functionality of routers as the latters need to encapsulate the packets and remove the headers in addition to the process of packet body decryption. On the other hand, the technique of QoS has reduced the generated delay and jitter for real time traffic but delay remained not suitable and acceptable in the simulated network. Moreover, it is noticed that there is a clear decrement in download response time and page response time for email and http traffic due to QoS operation. Based on that, it is found that the studied network (IPsec VPN with and without QoS) is not adequate and sufficient environment for voice and video traffic because the end to end delay was very high with acceptable value of jitter, On the other hand, IPsec VPN represented a suitable environment for normal traffic that does not affect by any type of latency or packet loss. In other words, online shopping; online banking and traversing transactions can be implemented in IPsec VPN and will be highly protected and secured. On the contrary, real time traffic cannot sustain packet loss or delay which considered not suitable in this protected environment and problems such as unnatural

conversations with long pauses between phrases might be caused as a result of that.

6. Future Work

Future work can be concentrated on investigating the real time traffic in IPsec VPN with the use of cRTP technique to compress the packets in order to avoid consuming bandwidth. Moreover, it is preferable to utilize the security protocols such as AH and ESP individually to avoid the high latency caused from using both of them together. In this case, it is expected that high bandwidth and low delay can be offered for voice and video traffic.

References

Abdulazeez, A. Salim, B. Zeebaree, D. and Doghramachi, D. 2020 "Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol". International journal of Interactive Mobile Technologies (iJIM) 14(18), November 2020.

Babu, M. & Ambedkar, B. 2012, " Performance Analysis of IPSec VPN over VoIP Networks Using OPNET" International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 9, September 2012.

Bensalah, F. El Kamoun, N. and BAHNASSE, A. 2017. "Evaluation of tunnel layer impact on VOIP performances (IP – MPLS – MPLS VPN – MPLS VPN IPsec". IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.3, March 2017.

Hafiz, A and Susianto, D. 2019. "Analysis of Internet Service Quality Using Internet Control
Message Protocol". Journal of Physics Conference Series, October 2019.

Jabbar, S. and Ahmad, I. "Design and Deployment of IPSec VPN Using CISCO Network Infrastructure". International Journal of Scientific Research in Computer Science, Engineering and Information Technology Volume 5 Issue 6, November-December 2019.

Nagy, Z. and Wali, M. 2020. "Virtual private network impacts on the computer network performance with different traffic generators" , IOP Conference Series: Materials Science and Engineering Volume 881 , 3rd International Conference on Sustainable Engineering Techniques (ICSET 2020) 15 April 2020.

Nassir, S. & HadiQais, A. 2013, "The Impact Of Using Security Protocols In Dedicated Private Network And Virtual Private Network" ,INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY Research Volume 2, Issue 11, November 2013.

Nura, M. & Mohammed, A. 2015," Investigating Space Overhead by IPSec on IPv4 and IPv6 Communication Protocols "Communications, Vol. 3, No.1, 2015, pp. 11-23.

Miraz, M. Ganie, M. , Molvi, S and Ali, M. 2017 "Simulation and Analysis of Quality of Service (QoS) Parameters of Voice over IP (VoIP) Traffic through Heterogeneous Networks). International Journal of Advanced Computer Science and Applications (IJACSA)), Vol. 8, No. 7, 2017.

OPNET PROJECTS TEAM. CUSTOMIZED OPNET SIMULATOR PROJECTS. "OPNET NETWORK SIMULATOR"2005-2019. {Online}.
Available from: http://opnetprojects.com/opnet-network-simulator/
Accessed on [18th June 2022].

Paresh, S. Mukhopadhyaya, U and Sathiamurthi, A. "Overview of QoS in Packet-based IP and MPLS Networks". [online]
Avaliable From: https://archive.nanog.org/meetings/nanog36/presentations/sathiamurthi.pdf
Accessed on [18th June 2022].

Sharma, T and Shiwani, S. 2013. "Statistical Results of IPSec in IPv6 Networks". International Journal of Computer Applications (0975 – 8887) Volume 79 – No.2, October 2013.

Simatimbe, C. and Lubobya, S. 2010. "Performance Evaluation of an Internet Protocol Security (IPSec) Based Multiprotocol Label Switching (MPLS) Virtual Private Network" . Journal of Computer and Communications . Vol 8, 100 – 108 September 2020.

Strzeciwilk, D. Ptaszek, K, Hoser, P and Antoniku, I . 2018. "A research on the impact of encryption algorithms on the quality of VPN tunnels' transmission" . ITM Web of Conferences 21, 00011 (2018).

Sugeng, W. Eko, J. Mustofa, K and Ashari, A. 2015, "The Impact of QoS Changes towards Network Performance" , International Journal of Computer Networks and Communications Security VOL. 3, NO. 2, FEBRUARY 2015, 48–53

Suliman, E. & Babiker, A. 2015, "The Impact of Security Overhead Traffic on Network's Resources Performance",IOSR Journal of Computer Engineering (IOSR-JCE) Volume 17, Issue 1, Jan-Feb 2015.

Thiruvasagam, P and George, K. 2019 "IPSec: Performance Analysis in IPv4 and IPv6".Journal of ICT Standardization. Issue 1, volume 7, Page: 61-80, January 2019.

Vee, A. 2012, "Usage of OPNET IT tool to Simulate and Test the Security of Cloud under varying Firewall conditions". M.sc dissertation, Texas A&M University-Corpus Christi, spring 2012.