Al-Nahrain Journal for Engineering Sciences **NJES** 22(4)283-293, 2019
http://doi.org/10.29194/NJES.22040283

Performance Analysis of Volume Loads of (Services and Transmission) Traffic in VPN Networks: A Comparative Study

Subhi Aswad Mohammed

Authors affiliations:
1) Dep. of System Engineering, College of Information Eng., Al-Nahrain University,
Baghdad- Iraq
subhiaswad@coie-nahrain.edu.iq
subhiaswad1958@gmail.com

Paper History:

Received: 3rd July 2019

Revised: 8th Aug. 2019

Accepted: 17th Nov. 2019

Abstract

This paper proposes a design for a network connected over public networks using Virtual Private Network (VPN) technique. The network consists of five sites; center server and four customer service sites, each site consists of a number of LANs depending on the user services requirements. This work aims to measure the effect of VPN on the performance of a network. Four approaches are implements: Network design without using VPN, network design using VPN with centralized servers, network design using VPN with distributed servers, and network design using server load balance .

The OPNET and BOSON simulation results show higher response time for packet transmission due to effect of VPN tunneling. The concurrent activation of application execution is used as a solution to the delay problem of the initial timing period while the application proceeds. The results dealing with QoS are E-mail, FTP, voice services traffic and IP traffic dropped. The VPN Tunnels is in the range of (0.01 to 0.02) sec.; along with this simulator there are four VPN tunnels in the network. Also, a special server's load balance is used to manage distribution of the server processing load across all other network servers to achieve the best response

Keywords: VPN, Virtual Private Network, VPN Tunneling, QoS, Load Balancer, Network Performance, IPsec, L2TP

دراسة مقارنة: تحليل كفاءة الأداء وحجم الأحمال لحركة المرور (الخدمات وتناقل البيانات) في الشبكات الخاصة الافتراضية

صبحي أسود محمد

الخلاصة:

هذا العملِ يُقدّم تصميم لشبكة خاصة إنترانت مدمجة بتقنية الشبكة الخاصة الافتراضية (VPN). الإنترانتَ طُبّقتْ لمشروع يَشْملُ مركزِ خدمة رئيسي وأربعة مواقع مُوَزَّعة على منطقة جغرافية واسعة ربطت بإستخدام الشبكة العامة الأنترنت. يَتضمّنُ كُلّ موقع عدد من الشبكات المحليةِ والذي يَعتمدُ على متطلبات خدمات المستخدمين. توفر الشبكة خدمات المعلومات والتطبيقات الضرورية مثل التصفّحُ، قاعدة البيانات، بريد إلكتروني، ارسال الملفات وخدمات الصوت (IP Telephony).

يهدف العمل تقييم ودراسة تأثيرَ أستخدام الشبكة الافتراضية الخاصة على خصائص الشبكةِ المُصَمَّمةِ ومُقَارَنَة النَتائِجِ في حالة عدم أستخدامها. كما تم استخدام تقنيةً موازنة الحمل باستخدام خوادم خاصة لإدارة عملية توزيع حمل الخادم عبر كل خوادم الشبكة للحصول على أفضل إستجابة للمنظومة.

تم تطبق الاختبارات على أربع تصاميم مختلفة للشبكات؛ تصميم الشبكة بدون إستخدام تقنية الشبكة الخاصة الافتراضية، تصميم الشبكة بإستخدام تقنية الشبكة الخاصة الافتراضية، تصميم الشبكة بإستخدام خوادم مركزية وأخرى موزعة وتصميم الشبكة تحت تأثير إستخدام خوادم لموازنة الحمل. تم تنفيذ الاختبارات على الشبكات المقترحة باستخدام نوعان من البروتوكولات (L2TP) و (IPSec). ان تحليل النتائج بين بأن زمن استجابة التطبيقات هي أعلى عند أستخدام الشبكات الخاصة الافتراضية ولمختلف انواع البيانات بالمقارنة مع نفس الشبكة التي لاتستخدم القنوات الافتراضية. أفضلية استخدام التنشيط المتزامن لتفعيل التطبيقات كحل لمشكلة التأخير في أنطلاق التطبيق للفترة الزمنية الأولية أثناء تشغيل التطبيق. تناول البحث تحليل كفاءة ألاداء وفحص درجة رضاء المستخدم وتقنيات فحص نوعية الخدمة (QoS). كذلك فحص مقدار تأخير هذه القنوات هو بسبب عمليات التشفير وفك التشفير لقنوات الـ (VPN).

NJES is an **open access Journal** with **ISSN 2521-9154** and **eISSN 2521-9162**

1. Introduction

Virtual private network service is scalable and cheap solution to provide secure networks and capability of VPNs remote access telecommunications [1]. A VPN is a network that deploys customer connectivity in multiple sites on a shared infrastructure, with the same access or security policies as a private network.

VPN allows safe connections over non-secure networks using protocol suite called IP Security (IPsec). Fig. 1 show the typical VPN organization [2].

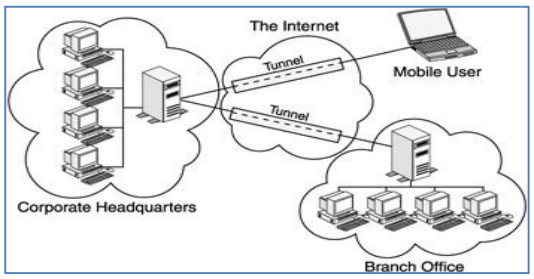

Figure (1): Typical VPN organization

VPN offered protection is encryption through tunnels and provides logical, point-to-point connections across a connectionless IP network.

Several researches concerned with the different VPN types and methods were developed.

O. H. Ahmed (2003) [3] Implemented a remote access VPN using IPsec protocol and open VPN as a nonstandard protocol, comparing the resulting performance from each protocol when the transmit packet size grows and deciding the preferable choice of a tunneling protocol.

A. N. AL Shamsi and T. Saito (2004) [4] gave a detailed analysis of security and performance properties for IPsec and Secure Sockets Layer (SSL) providing a technical comparison of both, similarities and differences of the cryptographic properties.

K. S. Munasinghe (2005) [5] Presented a study of the performance and QoS levels of using VPN in an IEEE 802.11b wireless infrastructure Security IPsec. The study covers multiple platforms to include a range of practical VPN implementations.

S. M. Rosu, et al. (2012) [6] the study presents a solution for network management in large enterprises that are separated geographically using open source software. They implemented product development in the PREMINV e-platform which is a solution based on a VPN IPsec solution concept using integrated data sets and tools.

Shi-Hai Zhu (2013) [7] this report suggested an algorithm for safe data transfer based on OpenSSL and VPN. It combined the characteristics of both symmetric crypto-system and asymmetric password system, and provided a fast and reliable method for secure data transmission.

D. Parmar and T. P. Patalia, (2013) [8] this report, analyzed the behavior of RIPv2 (Routing information protocol version 2) based MPLS VPN architecture using heavy VoIP traffic and Analysis of QoS as well as special network architecture. The statistical data is derived from different VPN statistics like delay, load, throughput and flow delay. The paper proved that RIPv2 routing protocol can be deployed inside a medium range network infrastructure.

2. Virtual Private Network Infrastructure and Technology

VPN is defined as emulating a private Wide Area Network (WAN) by using shared or public IP facilities, i.e. the internet [9]. A VPN is a private network that uses public telecommunications infrastructures, maintaining privacy by using of a tunneling protocol and data encryption. VPNs were developed into three categories; (Remote Access VPNs, Intranet VPNs and Extranet VPNs).

2.1 VPN Mechanism

Tunneling is the most important part of VPN technology. It enables the creation of virtual networks over the public networks. Tunneling is the procedure that put in a nutshell a data packet in the packet of a different protocol presentation. Which means that the header of the tunneling protocol is appended to the first packet. The resulting packet is then sent to the destination node or network through the intermediate infrastructure. When a tunneled packet is transferred to the destination node, it travels across the internetwork through a logical pathway. This pathway is called a *tunnel*. Upon receiving a tunneled packet, the recipient changes the packet back to its previous format. Fig. 2 represents the tunneling process.

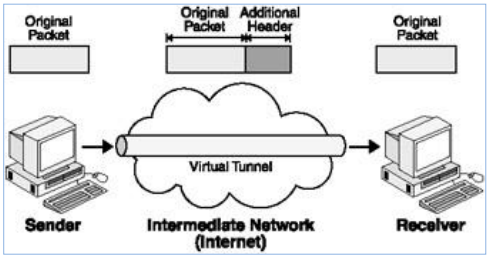

Figure (2): The Tunneling Process [9]

2.2 Parts of VPN System

To successfully create a pathway between two interactive ends, four modules are required:

1) **Target (Home Network):** The network that stores the data to be used by the remote client.
2) **Initiator Node:** The client or server that starts the VPN session.
3) **HA (Home Agent):** The interface at the target network. The HA receives and authenticates the incoming requests and allows the formation of a tunnel.
4) **FA (Foreign Agent):** The interface at the initiator node. The initiator node uses the FA to request a VPN session from the HA at the target network.

2.3 VPN Tunnel Technology Operations

Tunneling technology operations can be divided into two phases [9].

1) Phase I: Tunnel Establishment Phase

The initiator node (or remote client) asks for a VPN session and is then authenticated by the corresponding HA. A request for connection is then initiated and

session parameters are negotiated. This occurs in the following manner:

a. The initiator sends the request for a connection to the FA that is located in the network.
b. The FA accepts the request by validating the login name and the password supplied by the user.
c. If the supplied username and password by the user are not valid, the request for the VPN session is rejected. However, if the FA authenticates the identity of the initiator successfully, the request is forwarded to the target network HA.
d. If the HA accepts the, the FA sends the encrypted login ID and the corresponding password to it.
e. The HA verifies the supplied information. If verification is succeeding, the HA sends Register Reply and a tunnel number, to the FA.
f. When the Register Reply and the tunnel number reaches the FA, the tunnel is created.

2) Phase II: Data Transfer Phase

The transactions in data transfer phase occur as follows:

a. The initiator begins forwarding data packets to the FA.
b. The FA creates the tunnel header and appends it to each data packet. The header information of a routable protocol is then appended to the packet.
c. The FA forwards the resulting encrypted data packet to the HA using the supplied tunnel number.
d. On receiving the encrypted information, the HA strips off the tunnel header and the header of the routable protocol, thus bringing the packet back to its original format.
e. The original data is then sent to the intended destination node in the network. Fig. (3 and 4) depict the two phases of tunneling.

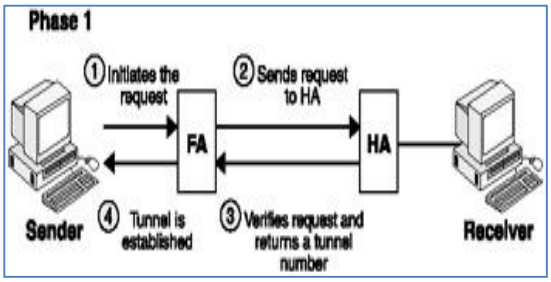

Figure (3): **The** Process of Establishing a Tunnel

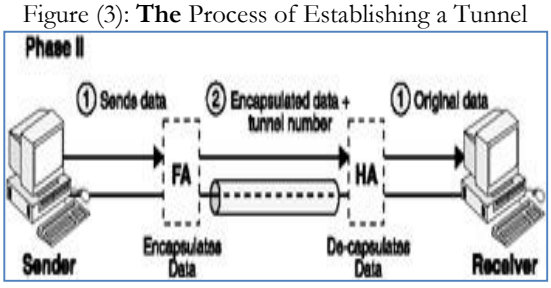

Figure (4): The Process of Transferring Data across a Tunnel

2.4 VPN Tunneled Packet Format

The FA encrypts the original data packet before it is sent to the target network via the tunnel. This encrypted packet is referred to as the tunneled packet. The format of a tunneled packet is shown in Fig. 5 [10].

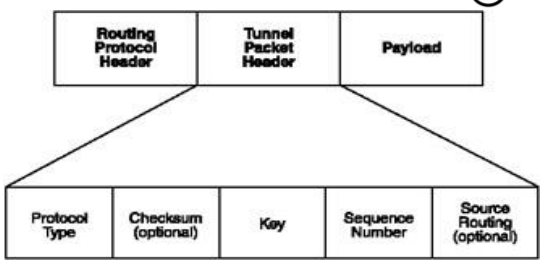

Figure (5): The Format of a Tunneled Packet

A tunneled packet is made up of three components:

1) Header of the routable protocol: contains the IP addresses of the FA and HA of the transaction.
2) Tunnel packet header: This header covers the following five fields:
a. Protocol type: means the type of the original data packet (or pay-load) protocol.
b. Checksum: used to verify if the packet is corrupted during transmission or not.
c. Key: used to identify or authenticate the actual source of data (initiator).
d. Sequence number: the sequence number of the packet in the series of transmitted packets.
e. Source routing: contains additional routing data.
3) Payload: The original packet transmitted by the initiator to the FA.

2.5 Tunneling Protocols at Layer 2

Tunneling protocols are essential for creating VPNs and securing their data transfer. Some of the widely used VPN tunneling protocols work at the second layer (Data Link layer) of the (OSI) model. These include the (PPTP), (L2F), and (L2TP) protocols.

3. VPN Design and Simulation

This section suggests different approaches of network topologic designs, specifically using farm servers, distributed servers and server load balancing. OPNET simulator is used in network performance analysis. The network simulation is performed through four proposed design approaches. The proposed network designs are implemented using BOSON simulator and cisco routers.

3.1 Proposed Network Design and Modeling

The proposed network design contains five sites, one of these sites is the center site of the network, the others sites are (site1, site2, sit3, and sit4). Each site contains a subnet which contains many LANs. Table (1) describes the network topology, services and applications, the distance between the network nodes, number of users, and the type of transmission media between network nodes and internet.

The network simulator specifies; services, topology, traffic, configuration of a subnet, modeling and the application run time pattern. The behavior of an individual user or group of users is called a "profile". The proposed system suggests four user group profiles. The timing sequence of the applications running within a profile can be configured to be executed in the following manner:

- **Parallel Mode**: In this manner, the timing sequence of applications activation are at the same time (concurrently)
- **Serial Mode:** In this manner, the timing sequence of applications activation are one after the another in a specific predetermined order. There is special case for this manner when the applications running are in a random order.

The modes of timing sequence and the applications profiles defines the application execution specifications including; starting time, duration time, minimum and maximum time, and duration fields which appear as a pull-down list.

The design of the experimental VPN system requires the specification of application running profiles. Also, a view to measure network performance, the characteristics under different operating conditions, traffic and network loads. A user profile is made up of various application definitions. The application's tasks/transactions execution may have multiple phases, and each phase can have many request and response commands [10]. The profile of applications configuration permits defines of the amount of transmission traffic that the applications makes such as "Low, Medium, or High" Load.

3.2 VPN Design Methodology

This section presents the suggestions for different networks topologic designs and their configuration. The following are four network design approaches:

1) **First approach:** In this approach, the network is designed without using VPN technology
2) **Second approach:** In this approach, the network is designed without using VPN tunnels with centralized servers.
3) **Third approach:** In this approach, the network is designed without using VPN tunnels with distributed servers.
4) **Fourth approach:** In this approach, the network is designed without using VPN tunnels with server load balancing.

Table (2) describes the characteristics of each network design approach with respect to VPN and application activation.

3.2.1 Design Without Using VPN Network Technology

This is the first approach of the suggested network design, as shown in Fig. 13. The network sites are configured with no VPN tunnel facilities. The internet represents the main transmission media to connect the network components.

3.2.2 Network Design using VPN and Centralized Servers

This represents a second approach of a proposed network design. The VPN tunnel facilities was added to the network between each site in the network. The network topology is shown in Fig. 7. The subnetworks in this approach are: center site, site1, site2, site3 and site4. The network servers are represented as a centralized subnet. The VPN tunnels configuration is shown in Fig .8. There are four VPN tunnels, their operation mode is defined as compulsory mode, and there is a VPN tunnel between the center site and each other site in the network. The VPN configuration table is shown in Fig .9, which explains the tunnel source and tunnel destination name, delay information, and remote client list.

3.2.3 Network Design using VPN And Distributed Servers

This represent a third approach of the proposed network design. The VPN tunnel facilities was added to the network between each site in the network. The network design topology is shown in Fig .10. This approach includes specific arrangement with respect to network servers, where a distributed server is used instead of using centralized servers as the central site for application services in the network. This means that each site contains its special servers to perform dedicated and local applications to the behalf of the local users of each site, which represent as the major activity of the user's site. In addition to providing service to the remote users from other sites. A study must be applied to see the effect of this distribution on the network performance especially the delay and the traffic load.

3.2.4 Network design using VPN and Load Balancing

This represent a fourth approach of the proposed network design. The load balancing facilities is added to the center site of the network organization with proxy server as shown in Fig. 9. In this approach the load balancer follows the number of open connections with each server, when it receives a new request, it chooses the server with the least number of connections.

Table (1): The Network Topology Description

Network site	Distance (km)	No. of users	Application and services for each site						Transmissions media
			Database access (Heavy, Light)	Web browsing (Heavy, Light)	File Transfer (Heavy, Light)	E-mail (Heavy, Light)	File Print (Light)	IP Telephony	
Center	**0**	**60**	**X**	**X**	**X**	**X**	**X**		**Microwave**
Site1	**18**	**50**	**X**	**X**	**X**	**X**	**X**	**X**	**Microwave**
Site2	**40**	**90**	**X**	**X**	**X**	**X**	**X**	**X**	**Microwave**
Site3	**450**	**70**	**X**	**X**	**X**	**X**	**X**		**Microwave**
Site4	**469**	**60**	**X**	**X**	**X**	**X**	**X**		**Microwave**
Total number of users: 330									
Total number of sites: 5									

Table (2): Characteristics of the four network design approaches

approach		Service type				Application and services for each site					
		VPN	Centralized server	Distributed server	load balance	Database access (Heavy, Light)	Web browsing (Heavy, Light)	File Transfer (Heavy, Light)	E-mail (Heavy, Light)	File Print (Light)	IP Telephony
First approach	Center	-	x			x	x	x	x	x	x
	Site1	-	x			x	x	x	x	x	x
	Site2	-	x			x	x	x	x	x	x
	Site3	-	x			x	x	x	x	x	x
	Site4	-	x			x	x	x	x	x	x
Second approach	Center	x	x			x	x	x	x	x	x
	Site1	x	x			x	x	x	x	x	x
	Site2	x	x			x	x	x	x	x	x
	Site3	x	x			x	x	x	x	x	x
	Site4	x	x			x	x	x	x	x	x
Third approach	Center	x	x	x		x	x	x	x	x	x
	Site1	x	x	x		x	x	x	x	x	x
	Site2	x	x	x		x	x	x	x	x	x
	Site3	x	x	x		x	x	x	x	x	x
	Site4	x	x	x		x	x	x	x	x	x
Fourth approach	Center	x			x	x	x	x	x	x	x
	Site1	x			x	x	x	x	x	x	x
	Site2	x			x	x	x	x	x	x	x
	Site3	x			x	x	x	x	x	x	x
	Site4	x			x	x	x	x	x	x	x

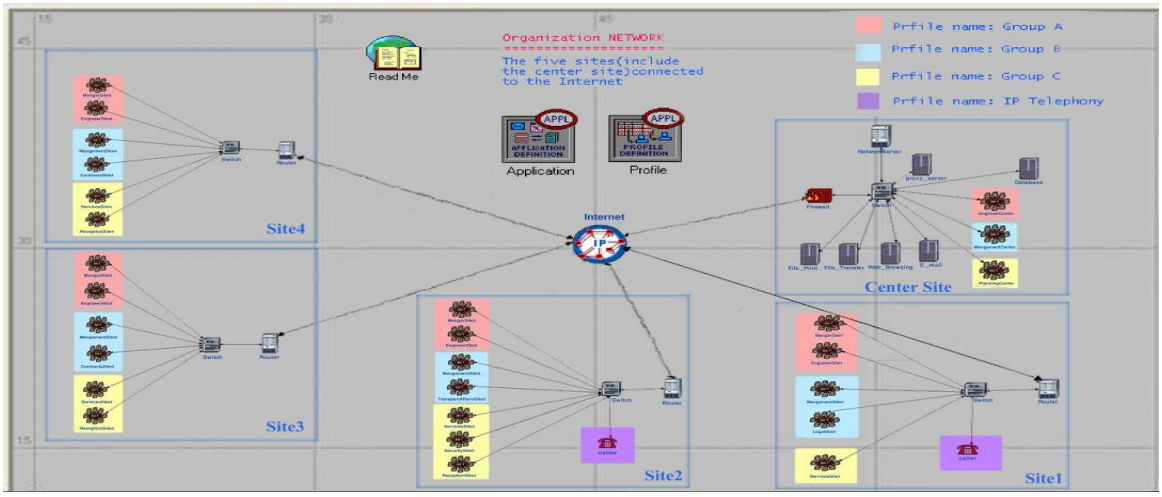

Figure (6): Approach No.1: Network Design Without Using VPN Technology

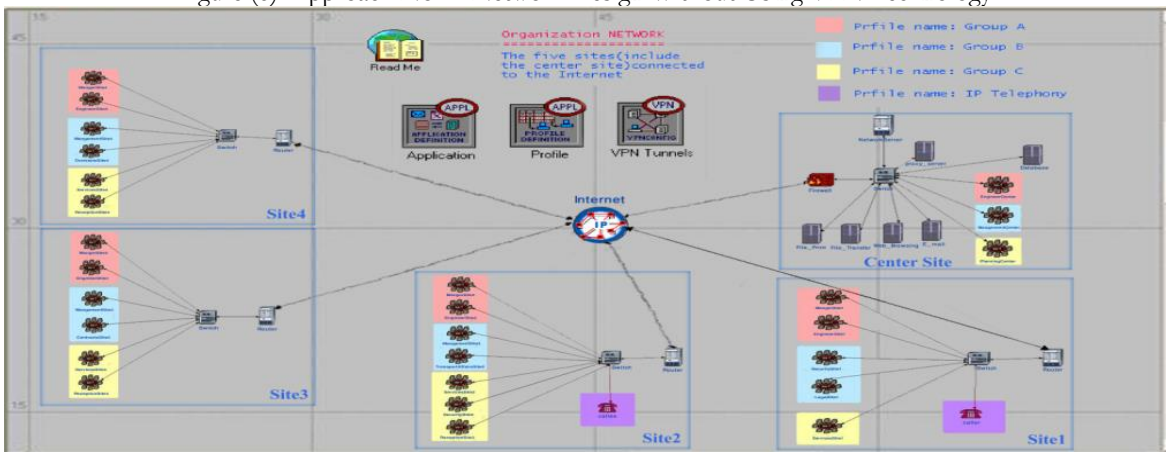

Figure (7): Approach No.2: Network Design Using VPN Tunnels and With Centralized Servers

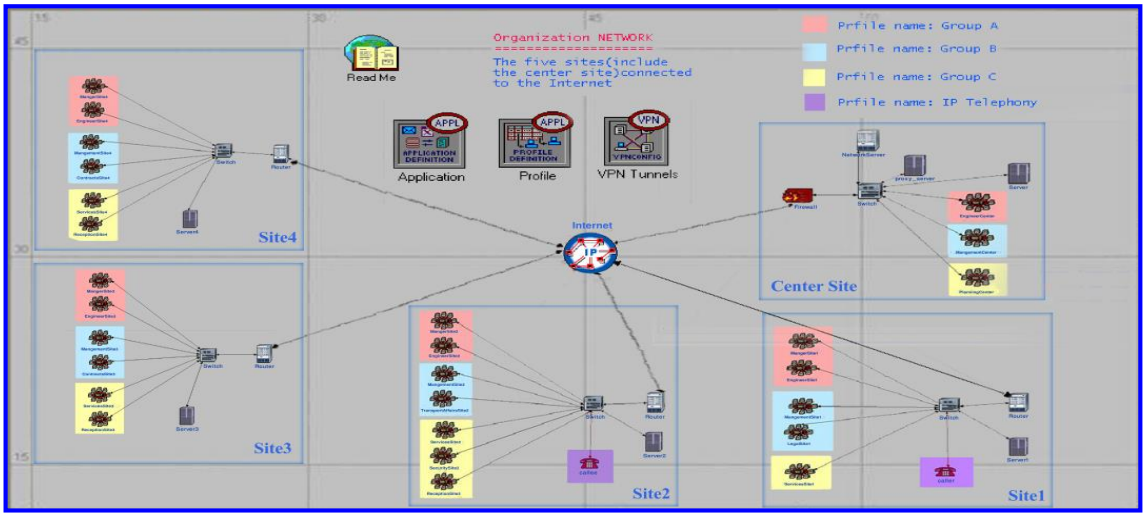

Figure (8): Approach No.3: Network Design Using VPN Tunnels and With Distributed Servers

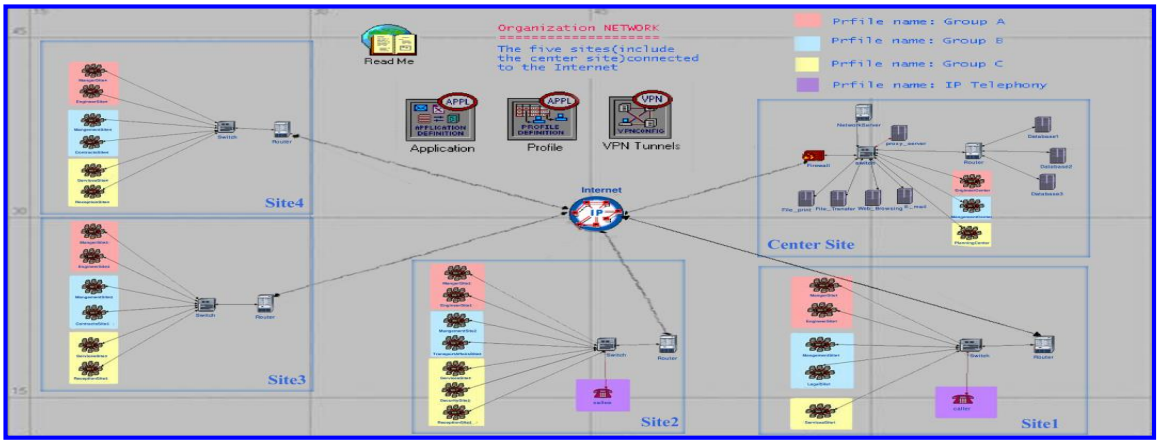

Figure (9): Approach No. 4: Network Design Using VPN Tunnels and With Server Load Balancing

4. VPN Implementation and Performance Evaluation

This section presents the results of the simulation of different network design approaches. The results are shown as a set of graphs and configuration profiles which describe the performance and behavior of the networks. These results are achieved after running the network for a define time (5 minutes) by the OPNET. The results show that the key differences between the four different design approaches.

4.1 Access Response Time for Database Application services

The access response time to perform the (entry and query) transactions for the database application services of the four network design approaches are shown in the Fig. (10.a and 10.b). It is clear that the database access responses are faster for the two approaches (no.2 and no.4). When database access transactions are issued, the server load balancer chooses the server with the least number of connections. There are differences in the access response behavior of the approaches (no.1 and no.2), in the first period of the network runtime (i.e. the initial condition) meanwhile the period between (0.00 to 0.04) second. The differences are due to the effects of the type of activation sequence of the services.

Two simulation scenarios of the network runtime are considered based on different initial condition periods. The first depends on the stochastic approach and repeated running to get the best timing sequence of the services activation. This stimulates an acceptable response and avoids the sharp variation in the response. This simulation is implemented by using parallel timing mode, as shown in Fig. (11.a and 11.b). However, the initial condition during the period (0.00 to 0.04) seconds for DB entry transaction the response time decrease from 10 sec. to 6.5 sec. as shown in Fig. 12.a and for DB Query transaction the response time in the same period decrease from 9 sec. to 6 sec. as shown in Fig. 12.b. The second simulation scenario which was applied depends on using a server load balancer to manage the distribution of the network activities across all other network servers to achieve the best response.

The main disadvantages of the first scenario are that they consume time and they cause a change in the network configuration. While, the main disadvantages of the second scenario are that they are costly because of need to add new hardware servers in addition to the requirements for the network management.

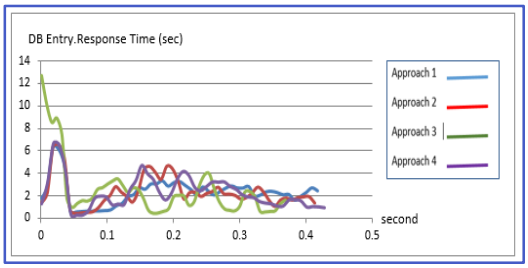

Figure (10.a): Response time of DB for entry transactions when using serial mode activation

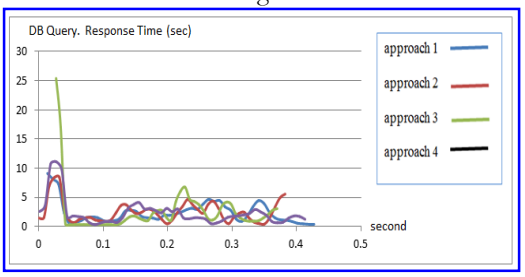

Figure (10.b): Response time of DB for query transactions when using serial mode activation

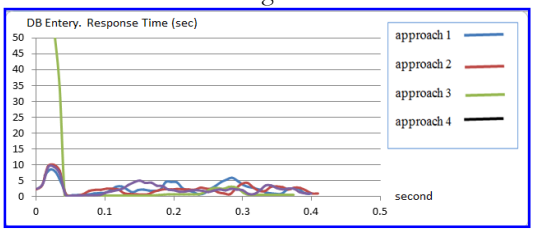

Figure (11.a): Response Time of DB for Entry transaction when using parallel Mode activation

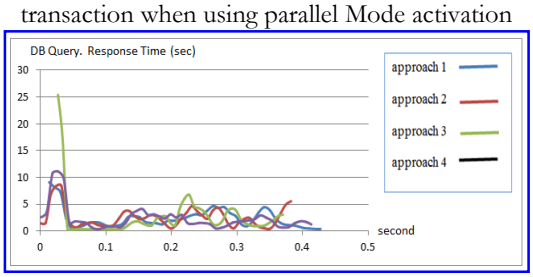

Figure (11.b): Response Time of DB for Query transaction when using parallel Mode activation

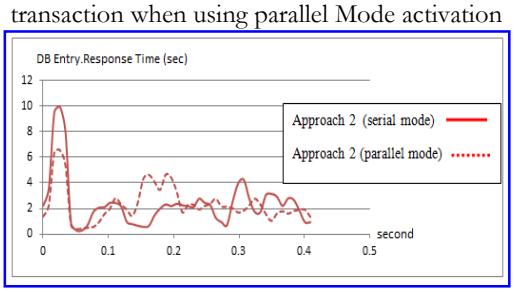

Figure (12.a): Response Time of DB Entry transaction when using design approach no.2

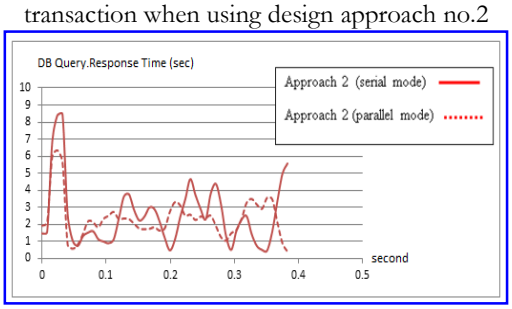

Figure (12.b): Response Time of DB Query transaction when using design approach no.2

4.2 Packet Traffic for E-mail application

This section presents the packet traffic sent during E-mail application as shown in Fig. 13.a, where the traffic sent is the average number of bytes per second sent to the transport layer by E-mail applications in the network. Fig. 13.b shows the E-mail traffic received (bytes/second). The E-mail traffic received is the average number of bytes per second forwarded to E-mail applications by the transport layer in the network. These two figures show that, there are differences between the traffic sent and received due to loss of packets.

4.3 Response Time for E-mail (Download and Upload)

The response time of E-mail services for different network design approaches are shown in Fig. (14.a and 14.b). Fig. 15 shows the response time of E-mail for network design approach no.2, when using serial time mode application activation. The results show that the E-mail response time for network design approach no.2 is greater than the E-mail response Time for network design approach no.1. The response time for the network design approach no.4 is greater than network design approach no.3.

The server loads balancing network design approach achieves a better response time for the network due to the load management facility. The response time difference occurs as the consequence of the VPN security property (encryption and decryption processes). However, the difference is still considered normal for the behavior of the network. As a solution to the initial condition, the parallel timing modes are used for E-mail downloads, this leads to reduction in the response time from 0.3 to 0.12, and for E-mail upload, the response time is decreased from 0.31 to 0.13, as shown in Fig. (16.a and 16.b).

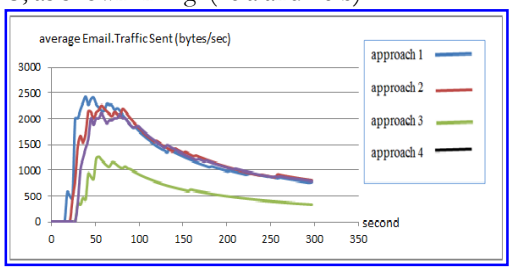

Figure (13.a): E-mail Traffic (Sent) bytes/sec.

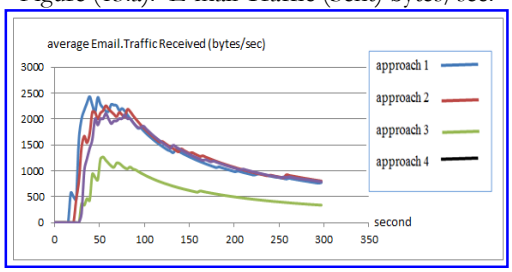

Figure (13.b): E-mail Traffic (Received) bytes/sec.

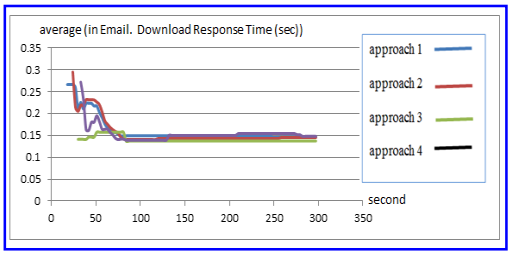

Figure (14.a): E-mail Response time for (Download) by using Serial Time Mode Activation

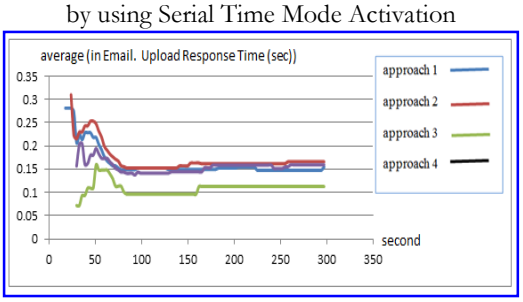

Figure (14.b): E-mail Response time for (Upload) by using Serial Time Mode Activation

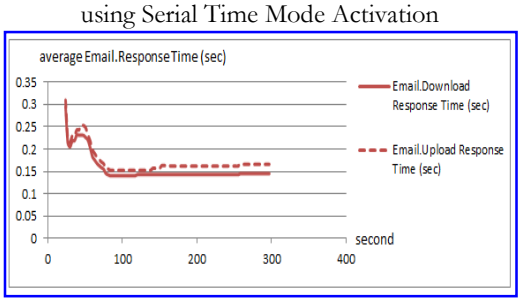

Figure (15): Email Response time for network design approach no.2 by using Serial Time Mode activation

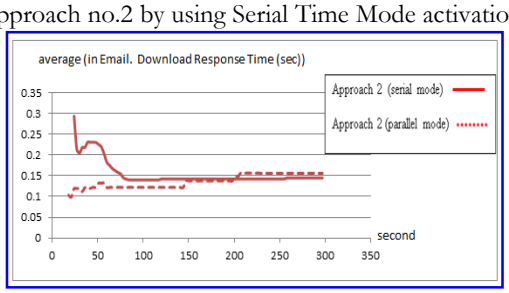

Figure (16.a): Email Response time (download) for network design approach no.2

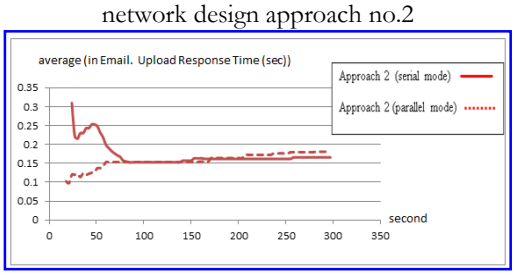

Figure (16.b): Email Response time (upload) for network design approach no.2

4.4 Packet Traffic for File Transfer Applications

The average bytes/second sent to the transport layer by FTP applications in the network (i.e. packets traffic sent) is shown in Fig. 17.a. The average bytes/second are forwarded to FTP applications by the transport layer in the network (i.e. received packets traffic) is shown in Fig. 17.b. The FTP received traffic is different from the sent traffic but with less packets dropped than the E-mail case.

4.5 Response Time for File Transfer (Download and Upload)

The response time of FTP (download and upload) for all network design approaches are shown in Fig. (18.a and 18.b). As shown in these figures, the response time behavior for the non-VPN network (approach no.1) is low compared to the VPN network (approaches no.1, no.2 & no.3). The small difference in response time between the non-VPN approach and others using VPN security property is due to the requirements of the (encryption and decryption) processes.

4.6 IP Traffic Dropped

The simulation results show that using VPN has a lower IP traffic dropping than the non-VPN network design approaches. The network design approach using server load balancing has IP traffic dropped less than the VPN network and non-VPN network approaches. The amount of dropped packets has an effect on the network efficiency. Fig. 19 shows that the values of a packet dropped is considered good with respect to the system throughput.

4.7 IP Processing Delay

The IP processing delay in the center site subnet is shown in Fig. 20. Since this subnet is performing the services by using several servers, therefore the IP processing delay will be obvious for its behavior. From the obtained graph, the delay in the VPN network approaches (no.2, no. 3 & no.4) are equals to (0.004 MS), while for the non-VPN approach (no.1) is equal to (0.02 MS).

4.8 Point-to-Point Link Throughput

The point-to-point link throughput of three network design approaches shown in Fig. (21.a and 21.b). This throughput gives the bit rate per second of the link between the center site subnet of the network and the internet. The center site subnet is considered the main subnet and contains the essential servers in the network. These figures show that the throughput for the non-VPN network approach is near equal to that of the VPN network and VPN load balance approaches. The throughput of the link between the center site and the internet in the two directions is almost equal for both approaches. Fig. 22 show the point-to-point throughput of the link in the two directions for approach no. 2. This Throughput means the good behavior of the network due to minimal packet losses. The throughput in the both graphs have an accepted range value approximately (80.000 bit/sec).

A parallel timing mode is used to increase the throughput of the network point-to-point link. Fig. (23.a and 23.b) show a comparison between a throughput of parallel and serial timing mode and for the two directions of transmission.

4.9 Voice (IP-Telephony) Traffic

The voice traffic analysis comprises two parameters, the traffic and the packet delay. The voice traffic (sent and received) in the network are shown in the Fig. 24. These figures show differences between the voice traffic sent and received. Fig. 24.a shows the different results between all networks approaches which approximate to (1,000) byte/sec. Also Fig. 24.b

shows a difference in results of about (2,000) byte/sec. The other parameters of voice deals with delay concepts.

Fig. (25 and 26) show voice packet end-to-end delay and voice packet delay variation respectively. Fig. 25 shows that the packet delay in the distributed servers (approach no.3) has increased a value of about (8.366) MS, and the packet delay when using VPN and load balancing (i.e. approach no.4) about value (8.36) Ms. Fig. 26 shows the voice packet delay variation. Here, the variation values when using VPN in distributed servers are applied is considered a large value of about (6 E-10); while in load balancing network approach is less than that of the VPN network, and the difference between them is approximately to (1 E-10).

4.10 Load Balancing

The percentage load of the CPU servers is considered in this section. The load balancing is implemented for servers in the center site subnet of the network and when a server deals with the (database services). The average utilization of the CPU servers is illustrated in Fig. 27. The IP Traffic (sent and received) for the load balancer network approach and in the center site subnet of the network is shown in the Fig. (28.a and 28.b). The IP processing delay is in the range of (0.004 to 0.01) MS as shown in Fig. 29.

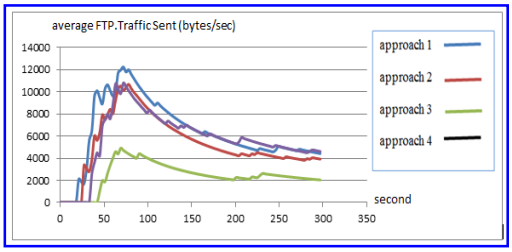

Figure (17.a): FTP Traffic (Sent) during different network design approaches

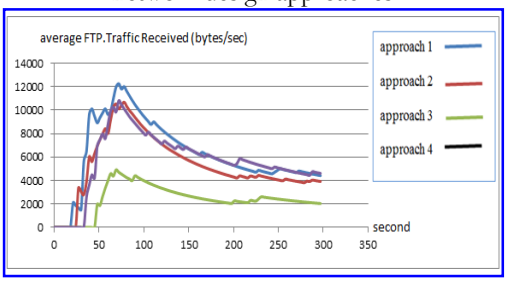

Figure (17.b): FTP Traffic (Received) during different network design approaches

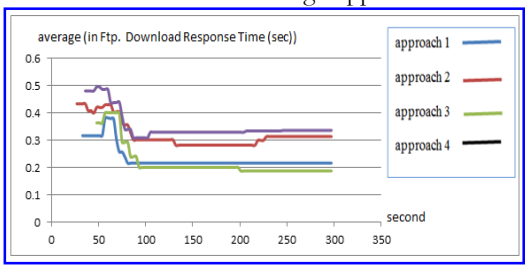

Figure (18.a): FTP Response Time (Download) for all networks design approaches

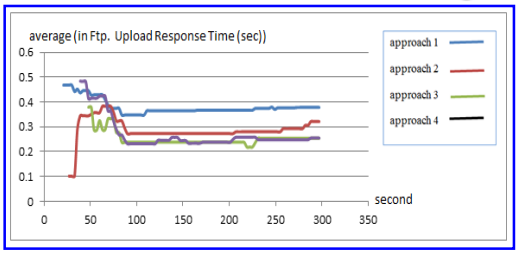

Figure (18.b): FTP Response Time (Upload) for all networks design approaches

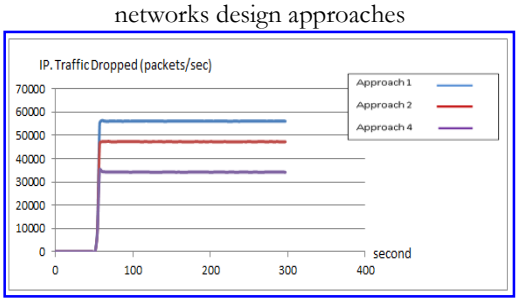

Figure (19): IP Traffic Dropped

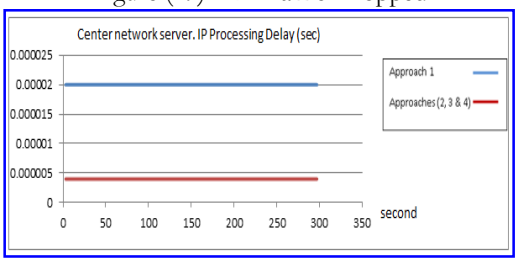

Figure (20): IP Processing Delay

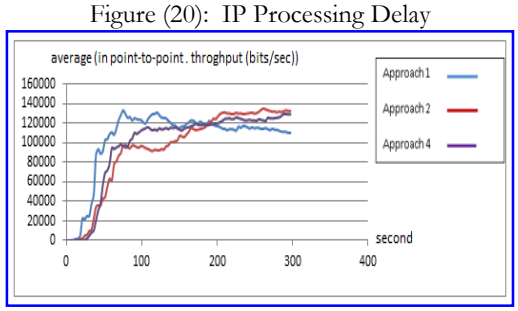

Figure (21.a): Throughput of The Link Directed from the Center site to internet

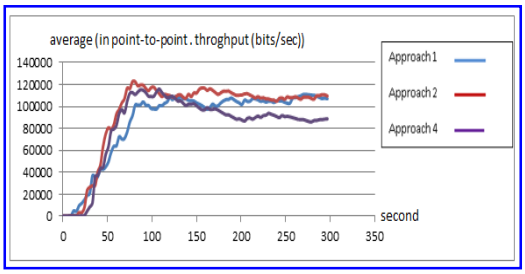

Figure (21.b): Throughput of the link directed from internet to the center site

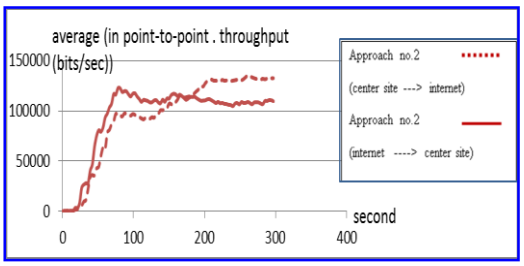

Figure (22): Throughput of the link between the internet and the center site in the two directions for approach no.2

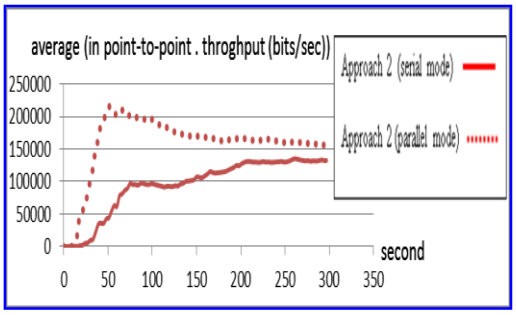

Figure (23.a): Throughput of the point to point link when transmission directed from the (center site to internet),

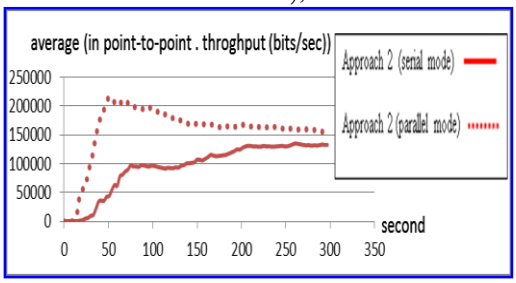

Figure (23.b): Throughput of the point to point link when transmission directed from (internet to the center site)

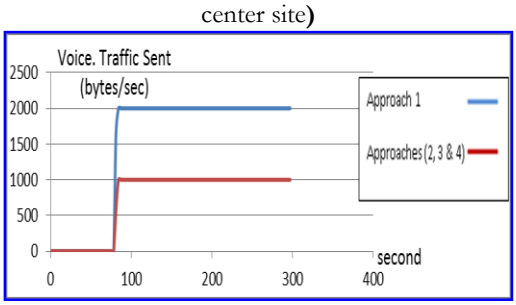

Figure (24.a): Voice sent Traffic

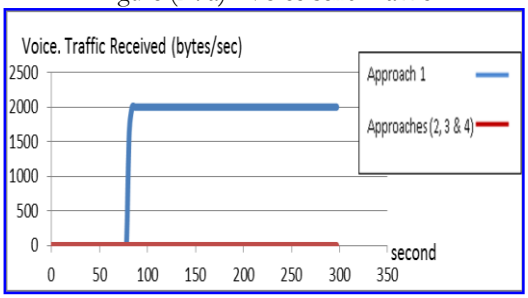

Figure (24.b): Voice Received Traffic

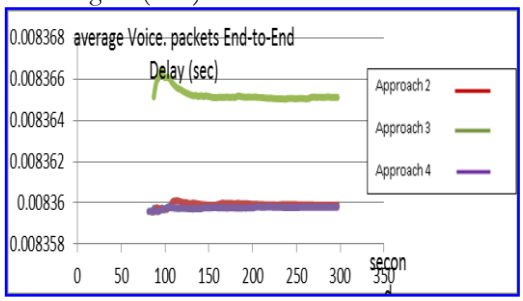

Figure (25): Voice Packet End-to-End Delay

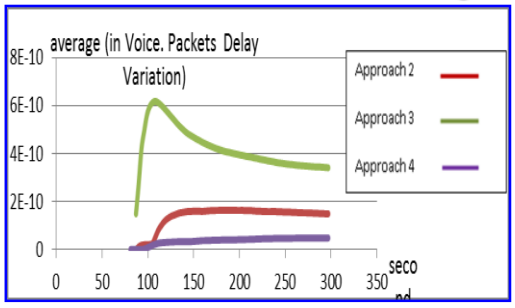

Figure (26): Voice Packet Delay Variation

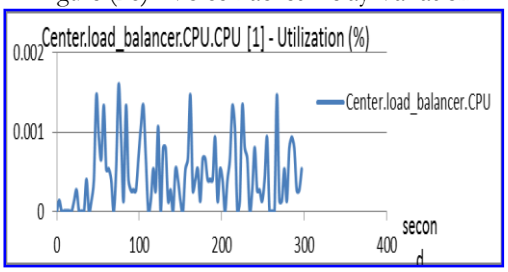

Figure (27): load balancer of the center site CPU server

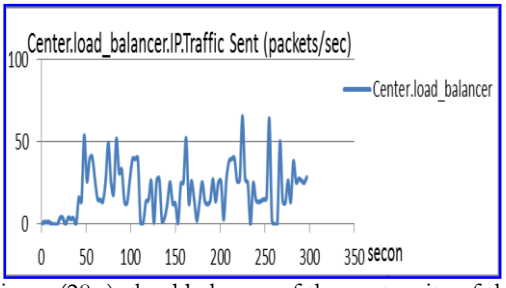

Figure (28.a): load balancer of the center site of the network; (traffic sent)

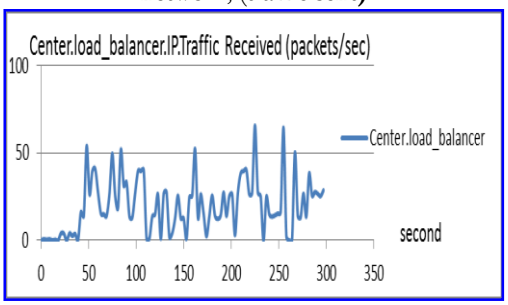

Figure (28.b): load balancer of the center site of the network; (traffic received)

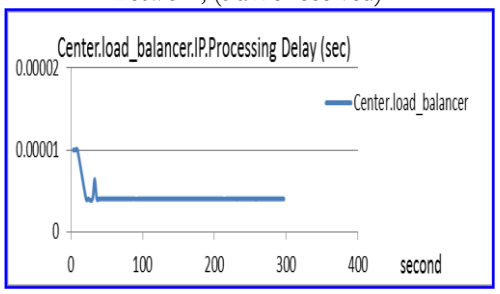

Figure (29): load balancer of center site of the network IP processing delay

5. Conclusion

The network simulations and the implementation tools that have been presented in this work are based on using OPNET software. Several conclusions are considered. In respect to the four network design network approaches, the results show that the application response times are higher due to VPN

tunneling of all packets. The server load balancing (approach no. 4) improves the characteristic of the network, and the IP processing delay reduced to (0.004) Ms. The VPN Tunnel average delay is (0.0125) sec. for the VPN approach, and the delay is (0.12) sec. for the server load balancing approach. The parallel timing mode is a good solution for the initial condition problem. Centralizing the servers in one place will reduces the operational complexity and simplify maintenance. Enhancing flexibility and service performance through dealing more with many technologies to improve the connectivity along the network such as QoS.

Reference

[1] "Virtual Private Network", White paper, Into to Inc., Santa Clara, USA 2002.

[2] "VPN Interoperability Using IPSec", Adtran, Inc., Huntsville, Alabama 2001..

[3] Omar H. Ahmed, "Design and Implement VPN", Master's thesis, the university of Technology, Iraq, 2003

[4] Abdel Naser Alshamsi, Takamichi Saito "A Technical Compression of IPSec and SSL", White paper, Tokyo University of Technology, 2004.,

[5] K. S. Munasinghe, "VPN over a Wireless Infrastructure: Evaluation and Performance Analysis" Master of Science, University of Western Sydney, March 2005.

[6] Sebastian Marius Rosu, Marius Marian Popescum , George Dragoi, Ioana Raluca Guica, "The Virtual Enterprise Network Based On Ipsec Vpn Solutions And Management" , (Ijacsa) International Journal Of Advanced Computer Science And Applications, Vol. 3, No. 11, 2012

[7] Shi-Hai Zhu , " Algorithm Design Of Secure Data Message Transmission Based On Openssl And Vpn ", Journal Of Theoretical And Applied Information Technology, February 2013. Vol. 48 No.1

[8] Dhaval Parmar, T. P. Patalia , "Analysis Of QOS Enabled Mpls Vpn Voip Network With RIPV2 Routing Protocol.", Journal Of Information, Knowledge And Research In Computer Engineering , Oct. ,2013, Vol. 02, No. 02

[9] Meeta Gupta, "Building a Virtual Private Network", Premier Press, USA, 2003

[10] "Configuration Application and profiles", OPNET Technologies Inc.,2003, **Site:** http://www.opnet.com/products/modeler/home.ht