Firewall and VPN Investigation on Cloud Computing Performance

Siddeeq Y. Ameen[1], Shayma Wail Nourildean[2]

[1]Department of Computer and Information Engineering, University of Mosul , Mosul, Iraq
[2]Foundation of Technical Institute, Technical Institute – Al-Dour, Tikrit, Iraq

ABSTRACT

The paper presents the way to provide the security to one of the recent development in computing, cloud computing. The main interest is to investigate the impact of using Virtual Private Network VPN together with firewall on cloud computing performance. Therefore, computer modeling and simulation of cloud computing with OPNET modular simulator has been conducted for the cases of cloud computing with and without VPN and firewall. To achieve clear idea on these impacts, the simulation considers different scenarios and different form application traffic applied. Simulation results showing throughput, delay, servers traffic sent and received have been collected and presented. The results clearly show that there is impact in throughput and delay through the use of VPN and firewall. The impact on throughput is higher than that on the delay. Furthermore, the impact show that the email traffic is more affected than web traffic.

KEYWORDS

VPN, firewall, cloud, computing, OPNET

1. INTRODUCTION

Cloud computing has generated a lot of interest and competition. This is due to service delivery model which provides that involves computing and storage for users in all market including financial, health care and government [1]. This advances in computing put cloud computing as one of the latest developments of computing models. Its development can be considered much advanced than that of distributed computing, parallel processing, grid computing and so on. With cloud computing, multi-level virtualization and abstraction can be achieved [2]. This can validated using an effective integration of variety of computing, storage, data, applications and other resources. This integration will allow users to easy use powerful computing and storage capacity of cloud computing with the use of networking as that achieved in distributed processing or grid computing.

Recent literature have mentioned that Google is the biggest users of cloud computing, have its own cloud computing platform [3]. This can be achieved via the use of wireless networks. However, wireless networks have the same risks and vulnerabilities that exist in a conventional wired network and there are also numerous other types of threats specific to them [2]. Therefore, cloud security that use wireless network is becoming a key differentiator and competitive edge between cloud providers [1]. This paper introduced security issues for the cloud and presented firewall implementation with VPN (Virtual Private Network) technology to provide the security to the network. This study was done using OPNET Modeler (v14.5) in number of different scenarios to study the performance of system in terms of delay, throughput and other parameters.

2. SECURITY ISSUES FOR CLOUD COMPUTING

In spite of adoption of cloud computing by Google and other well known powerful computing resources users. This adoption will increase heavily because of the high demand on computing resources in search engine or data warehouses and data mining. This demands comes from the large increase in computing and multimedia in every day duties. However, cloud computing users should aware of security threats that can occur because cloud computing uses networks to grant access to the resources required. Thus any security threats that might occur with network might be occurred with cloud computing. In this aspects researches have been conducted and developed to provide security for cloud computing. Furthermore, the security of cloud computing should consider security issues and technologies related all the field encompasses the cloud computing infrastructure. These include but not limited to networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.

One of the major problems facing cloud computing security is the control by the data owner and the resource allocation and scheduling control. Thus a form of security authority need to be deployed by cloud computing security to provide the owner the control required and the seeker the allocation and scheduling required. This is called an authority coordinator and its presence is essential to secure the data in the untrusted environment such as cloud computing [4]. Within these security aspects, the security concerns can be categorized as [5, 6]:

- *Traditional security:* These concerns involve computer and network intrusions or attacks on clouds [5].
- *Availability:* These forms of security concerns will involve centre on critical applications and data being available [5]. Availability concerns can be extend to migrate to another provider, uptime periods of current provider or long-term viability of the cloud provider [6].
- *Third-party data control:* Within cloud computing, there is a third party that held data and applications. This part is very complex, transparent and need to be understood very well by cloud computing users [5].
- *Data Security:* This security concern will provide the physical and logical control of data. It is concerned with virtualization, vulnerabilities attack, phishing scams and other potential data breaches such as data leakage and interception, economic and distributed denial of service and loss of encryption keys [6].
- *Privacy and Legal Issues:* This issue is essential especially when dealing with globally distributed network [6].

3. PROPOSED CLOUD COMPUTING SECURITY USING VPN AND FIREWALL

The proposed system will attempt to provide secure delivery of data to and from the cloud. One of the adopted technology is the Virtual Private Network (VPN). With VPN private and secured sub networks can be constructed. This principle have been widely applied in wired local-area network (LAN), remote access networks and can be also applied to wireless local-area network (WLAN). This will replaces Wired Equivalent Privacy (WEP) solutions. It adopts standard encryption algorithms to ensure the security of data transmission [7]. Furthermore, VPN usually implemented with the aid of IP security (IPSec). This can be considered as the standard way for VPN implementation. The IPSec and VPN have revised and well established in this way to provide the robust security standard with acceptable data confidentiality, authentication, and access control regardless of the transmission medium. “By integrating wireless LANs into an IPSec infrastructure, allows WLAN infrastructure to focus on simply transmitting wireless traffic, while the VPN would secure it,” as shown in Figure 1 [8].

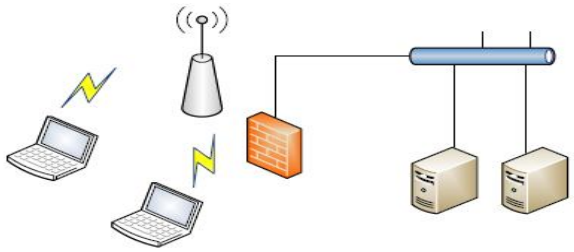

Figure 1. VPN usage within IPSec.

As shown in Fig. 1, firewall is used in conjunction with VPN. The firewall is a packet filtering that stands between the internal network and the world outside. The reason for the usage of firewalls with the VPN is because firewall have been employed on large public networks for many years and are a great starting place in the development of a security strategy and cloud computing can be regarded as a public network [9].

4. NETWORK SIMULATION SCENARIOS

The simulation procedure using of OPNET simulator adopted in this research consists of number scenarios which study the performance of the system in different cases. The cloud computing has been modeled with and without VPN to study the performance of VPN and to study the effect of firewall with VPN in the system to secure cloud in different scenarios. Each scenario have been subjected to three applications types (File Transfer (FTP), web browsing (HTTP) and Email applications). In the simulation, two servers represented two departments have been assumed. The impact of firewall and VPN on cloud computing has been investigated in terms of throughput, load , delay , and traffic received. Further parameters used in these scenarios are:

i- *Two access points:* named (wireless_ethernet_slip4_router), which had two Ethernet interface and 4 serial line.
ii- *No. of workstations:* named (wlan_wkstn) which represent clients that communicate with internet.
iii- *Two IP router: named (ethernet4_slip8_gtwy)*, which represent router with 4 Ethernet interface and 8 serial line interface.ip cloud: named (ip 32 clouds) which represents the Internet
iv- *Two servers:* named (PPP Server) which represents point to point server to represent two departments.
v- *Firewall:* ethernet2_slip8_firewall, which prevent any access for the required application to the server.
vi- *VPN configuration:* VPN tunnel would be used to allow specific clients from the source to access specified application from the server.

Links: named (PPP-DS1) to connect the parameters used for the modeled system.profile and application configuration to define the application of the system.

4.1. Scenario 1: Cloud computing without firewall and VPN

In this scenario, number of workstations connected to two access points (Access Point 1, Access Point 2) which configured two BSS. These access points connected by PPP-DS1 to Router S connected by PPP-DS1 to ip cloud (Internet) connected by PPP-DS1 to Router D connected by PPP-DS1 to two Servers (Server AA, Server BB) which represents two departments. The scenario architecture and layout is as shown in Figure 2.

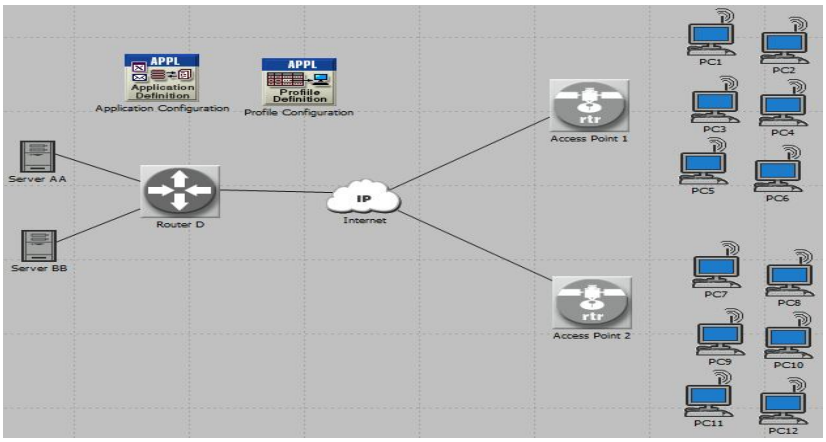

Figure 2.The architecture and layout of scenario 1

4.2. Scenario 2: Cloud computing with firewall only

In this scenario, number of workstations connected to two access points (Access Point 1, Access Point 2) which configured two BSS. These access points connected by PPP-DS1 to Router S connected by PPP-DS1 to ip cloud (Internet) connected by PPP-DS1 to Firewall named (ethernet2_slip8_firewall) which protect servers from any external access to the Email from the servers. This firewall connected by PPP-DS1 to the Server AA and Server BB. The architecture and layout of scenario 2 is as shown in Figure 3.

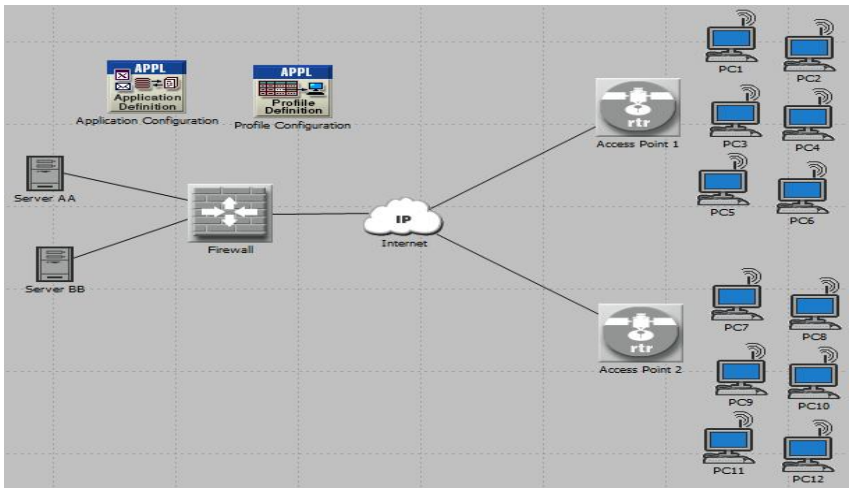

Figure 3. The architecture and layout of scenario 2

4.3. Scenario 3: Cloud computing with firewall and VPN

In this scenario, number of workstations connected to two access points (Access Point 1, Access Point 2) which configured two BSS. These access points connected by PPP-DS1 to Router S connected by PPP-DS1 to ip cloud (Internet) connected by PPP-DS1 to Firewall to Router D connected by PPP-DS1 to the Server. The architecture and layout scenario 3 is shown in Figure4.
In the previous scenario, firewall was used to prevent any external access to email of server regardless the source of the traffic. In this scenario, the VPN tunnel would be used to allow one of the clients (PCs) from Access Point1 to access Email from the server AA. The firewall will not

filter the traffic created by Access Point1 because the IP packets in the tunnel will be encapsulated inside an IP datagram.

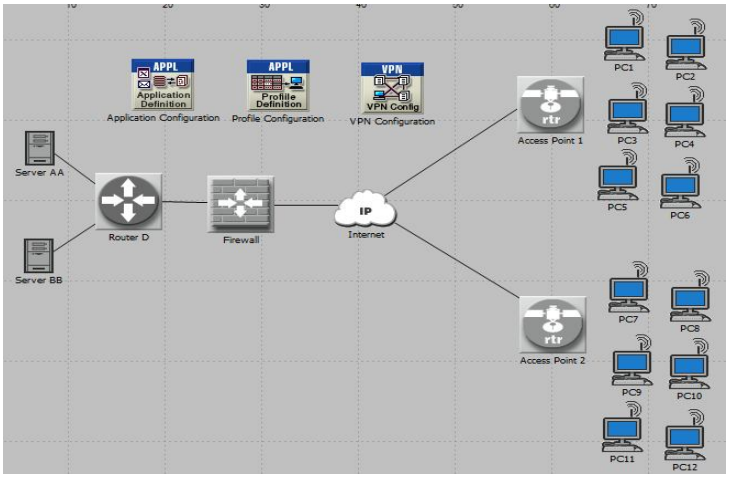

Figure 4. The architecture and layout scenario 3

5. SIMULATION RESULTS AND SYSTEMS EVALUATION

The results of system evaluation show the throughput and delay for the three scenarios. Figs. 5 and 6 show the throughput and delay for scenarios 1-3. It is clear from Fig. 10, that throughput with VPN reach 107,819 at time = 1,782 seconds, but throughput for system with no VPN was large and reach 299,131 bits/sec at time = 1,782 seconds in (no firewall no VPN) system and reach 288,510 bits/sec at time = 1,782 seconds. Delay (Represents the end to end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer.) in all VPN scenarios (No firewall No VPN, firewall No VPN and firewall VPN) reaches 0.001727, 0.00169, 0.001672 at time = 1,782 seconds.

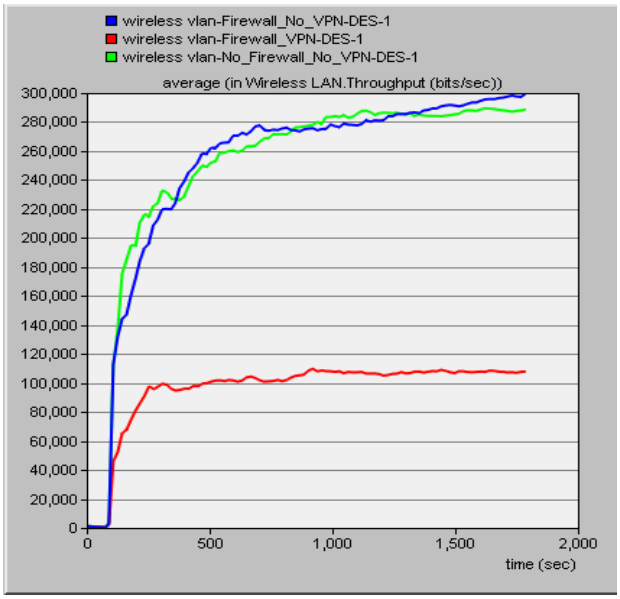

Figure 5. Throughput over scenarios 1-3

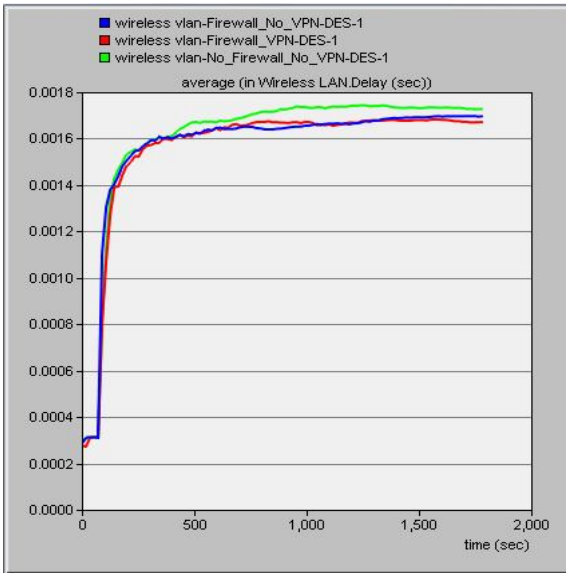

Figure 6. Delay over scenarios 1-3

The Discrete Event Statistics DES was chosen for individual nodes to show the effect of VPN in the WLAN system. In this test and for all scenarios, the traffic received and sent on Server AA for Email application has been investigated as shown in Figures 7 and 8. It is clear that the traffic received and sent was high in system with no firewall no VPN and decreases to reach 163.74 bytes/sec and 153.76 bytes/sec, respectively. There was no traffic in Server AA in the (firewall no VPN system) because the existence of firewall in the system which protect the data in server AA from any Email access from external user. There was small traffic received and sent in Server AA in (firewall VPN system) because VPN tunnel would be used to allow one of the clients (PCs) from Access Point1 to access Email from the server AA. The traffic received and sent will reach 20.337 bytes/sec and 126.72 bytes/sec.

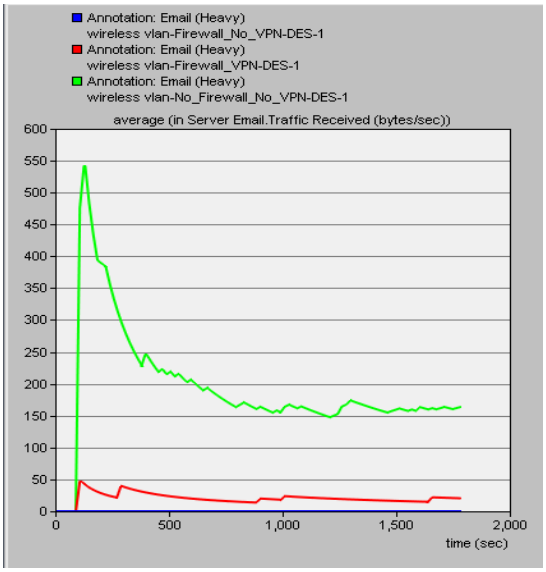

Figure 7. Server AA traffic received over scenarios 1-3

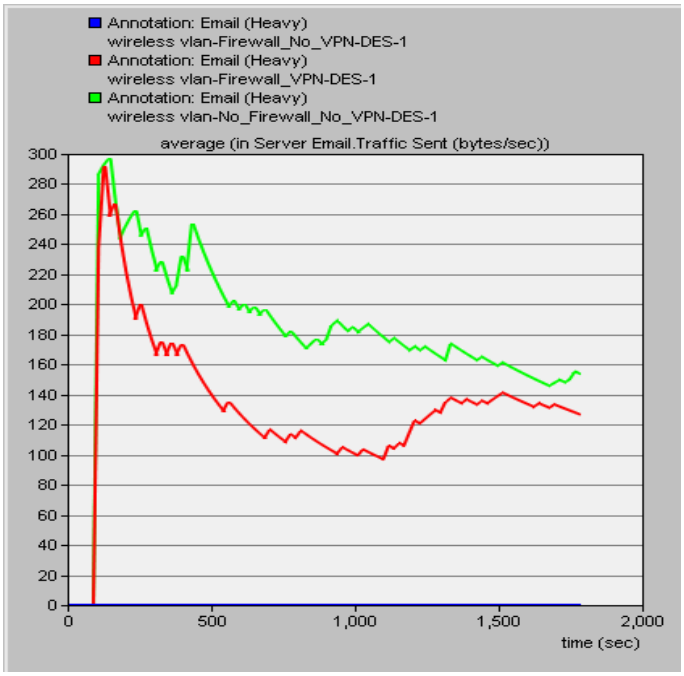

Figure 8. Server AA traffic sent over scenarios 1-3

The three scenarios have been investigated with web browsing application. In this investigation, there would be traffic received and sent on server AA in the three simulated scenarios (No firewall no VPN, firewall No VPN and firewall VPN) because firewall protect the server AA from email access only as shown in Figure 9 and Figure 10.

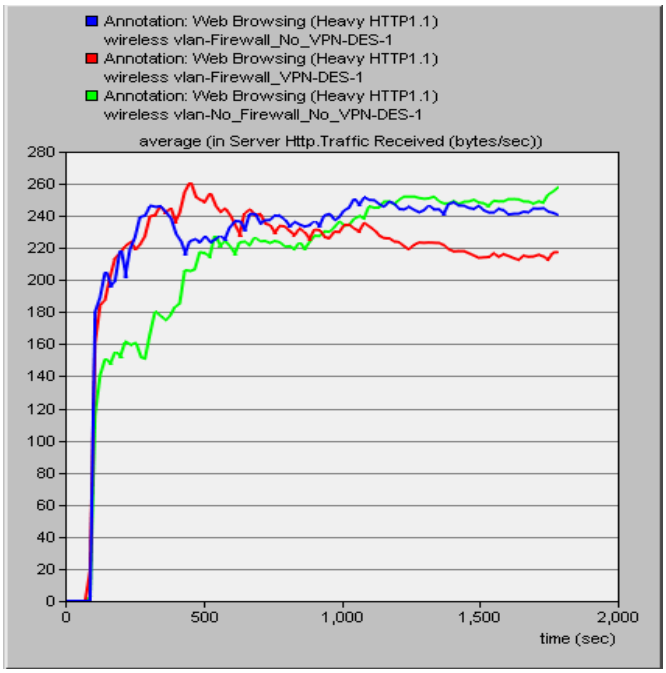

Figure 9. Server AA traffic received over scenarios 1-3

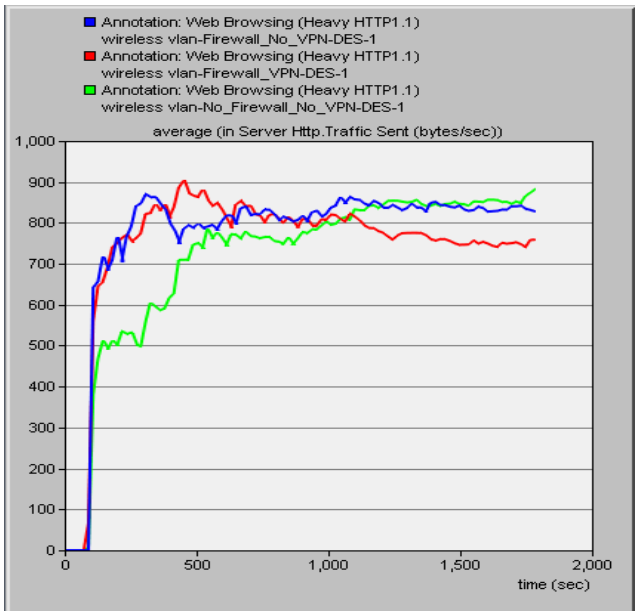

Figure 10. Server AA traffic sent over scenarios 1-3.

Extra investigation have being subjected to the three scenarios but now with traffic received and sent for Email application as shown in Figures 11 and 12, respectively. It is clear from the results that there was traffic received and traffic sent on Server BB in (No firewall No VPN system) only and reach 143.7 bytes/sec and 140.38 bytes/sec respectively. There was no traffic received or sent in the existence of firewall in two systems (firewall No VPN and firewall VPN) because the firewall protect server BB from any email access and the VPN was taken in this case to allow access from PCs of Access Point 1 to access the Email of Server AA but not server BB.

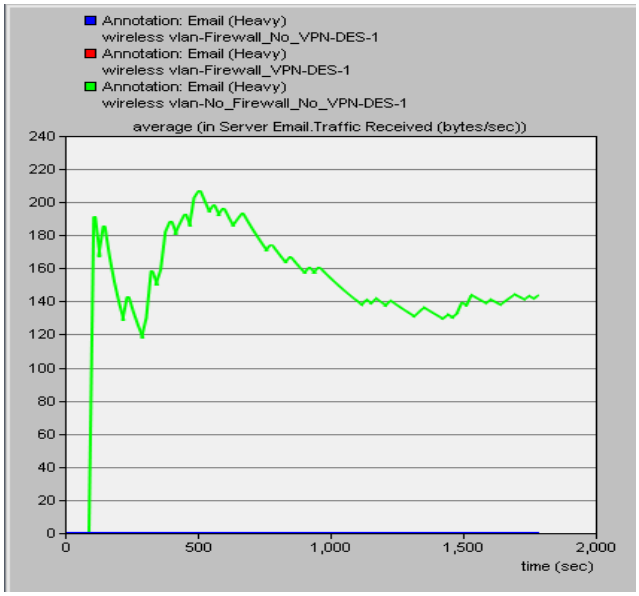

Figure 11. Server BB Traffic Received

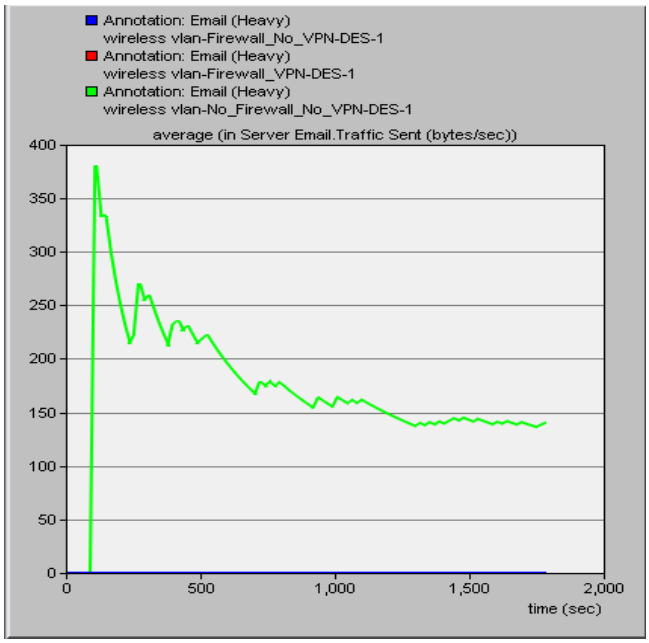

Figure 12. Server BB Traffic Sent

Finally, with web browsing application, the results shows that there would be traffic received and sent on Server BB in three systems (No firewall no VPN, firewall No VPN and firewall VPN) because firewall protect the server BB from email access only as shown in Figure 13 and Figure 14.

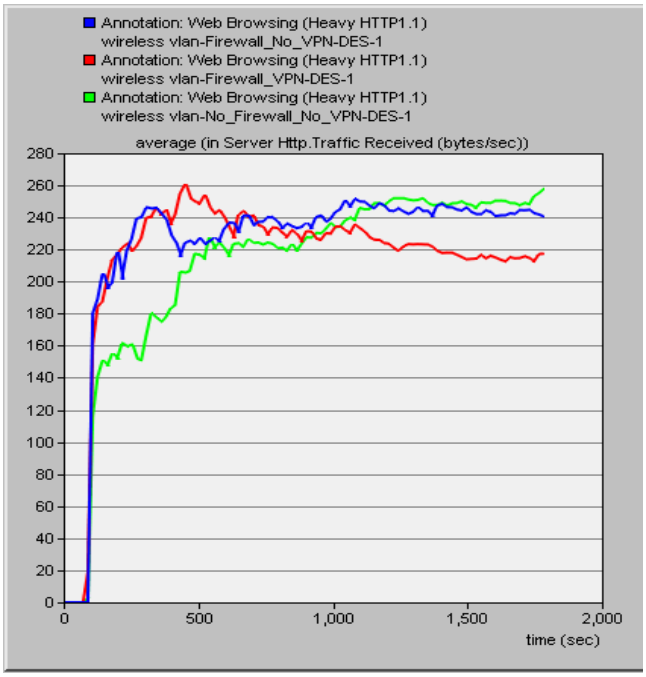

Figure 13. Server BB Traffic Received

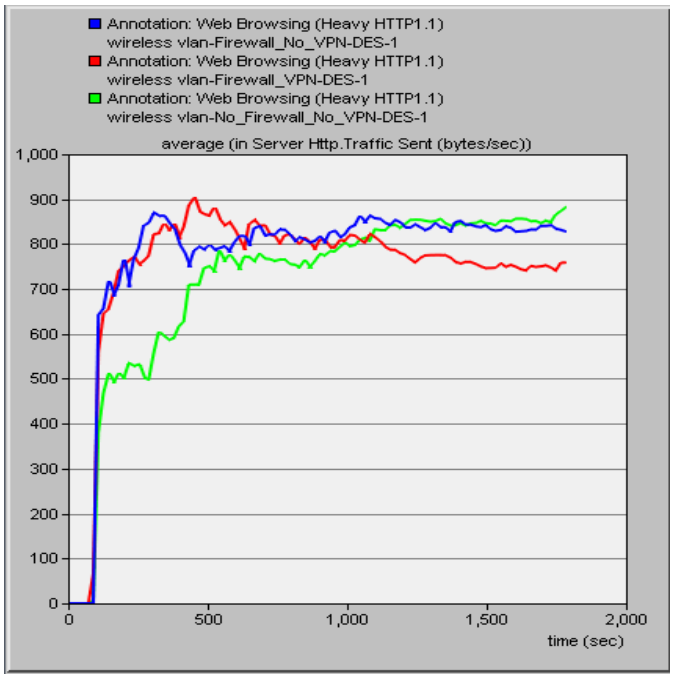

Figure 14. Server BB Traffic Sent

6. CONCLUSIONS

This study introduced VPN technology for securing cloud in wireless network. OPNET Modeler simulator was used as a simulation tools to investigate the impact of VPN and firewall security systems on throughput, delay and traffic received on the system and individual nodes of the network. The applications considered for the mentioned investigation are e-mail application and web browsing application. The presented clearly conclude the followings;

i- The integration of VPN with Firewall in cloud computing will reduce the throughput. This is because the number of bit transmitted per second is less than the cloud computing without VPN. because the VPN with firewall would not allow every access to the server. Furthermore, the delay in system without VPN is slightly larger than the cloud computing with VPN.

ii- No traffic received and sent from server AA for e-mail application in cloud computing with firewall and no VPN. This is because firewall would prevent any email access to the server AA and the existence of VPN in the system would allow specified stations (PC's) to access server AA. However, there would be no traffic received and sent for server BB in (VPN firewall) and (firewall no VPN) systems. This is now because VPN acts as a tunnel to allow email access to server AA only.

iii- In web browsing applications, there would be traffic sent and received in the caese of cloud computing with VPN and without VPN. This is because the VPN firewall would prevent only access to the server for email application but not web applications.

VPN technology is a suitable way to secure cloud computing and decreasing the traffic in the system to achieve the security required. The security was provided in VPN technology should be provided with firewall that allows only specific access to the server.

REFERENCES

[1] Maneesha Sharma, Himani Bansal, Amit Kumar Sharma, "Cloud Computing: Different Approach & Security Challenge", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, pp. 421-424, March 2012.

[2] Young B. Choi, Jeffrey Muller, Christopher V. Kopek and Jennifer M. Makarsky "Corporate wireless LAN security: threats and an effective security assessment framework for wireless information assurance", *Int. J. Mobile Communications, Vol. 4, No. 3, pp 266 – 290, 2006.*

[3] Songjie, Junfeng Yao, Chengpeng Wu, "Cloud computing and its key techniques", International Conference on Electronic & Mechanical Engineering and Information Technology, pp. 320-324, 12-14 August, 2011.

[4] *Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisingham,* "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010.

[5] Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", *CCSW'09*, November 13, 2009, Chicago, Illinois, USA. , ACM 978-1-60558-784-4/09/11, pp. 85-90, 2009.

[6] Aderemi A. Atayero, Oluwaseyi Feyisetan, "Security Issues in Cloud Computing: *The Potentials of Homomorphic Encryption*", Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 10, pp. 546-552, October 2011.

[7] Weili Huang, Fanzheng Kong , "The research of VPN on WLAN" , International Conference on Computational and Information Sciences, 2010 IEEE, PP 250 – 253.

[8] H. Bourdoucen, A. Al Naamany and A. Al Kalbani, "Impact of Implementing VPN to Secure Wireless LAN", World Academy of Science, Engineering and Technology 51, pp 625 – 630, 2009.

[9] Charlie Scott, Paul Wolfe, Mike Erwin, "Virtual Private Networks, Second Edition", O'Reilly, Second Edition January pp 12, 1999.

Authors

Prof. Dr. Siddeeq Y. Ammen., Prof. in Communication Engineering, he worked in Department of Computer and Information Engineering, Mosul University/ Engineering College/ Ministry of Higher Education and Scientific Research, Mosul, Iraq, he presented many papers and participate in many national and international conferences . he is expert in communication Engineering. His current research interests include engineering communication and network.

Shayma W. Nourildean, she received B.Sc. degree from university of Baghdad, collage of engineering in Computer Engineering and received M.Sc. degree in Computer Engineering from university of technology- Baghdad. She is an Assistant lecturer in Department of Electronics, Al-Dour Technical Institute, she presents many papers and participate in number of conferences. Her current research interests include computer communication.