I.J. Wireless and Microwave Technologies, **2018, 1, 1-13**
Published Online January 2018 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2018.01.01

***Available online at** http://www.mecs-press.net/ijwmt*

Evaluation the Performance of DMZ

Baha Rababah[a], Shikun Zhou[b], Mansour Bader[c]

[a] *Islamic University in Madinah, Almadina Almonawara, KSA*
[b] *University of Portsmouth, Portsmouth, UK*
[c] *Al-Balqa Applied University, Salt, Jordan*

Received: 12 May 2017; Accepted: 18 June 2017; Published: 08 January 2018

Abstract

Local area networks are built mainly for two essential goals, the first one is to support the framework's business functionality such as email, file transferring, procurement systems, internet browsing, and so forth. Second, these common networks should be built using secure strategies to protect their components. Recent developments in network communication have heightened the need for both secure and high performance network. However, the performance of network sometime is effected by applying security rules. Actually, network security is an essential priority for protecting applications, data, and network resources. Applying resources isolation rules are very important to prevent any possible attack. This isolation can be achieved by applying DMZ (Demilitarized Zone) design. A DMZ extremely enhance the security of a network. A DMZ is used to add an extra layer of protection to the network. It is also used to protect a private information. A DMZ should be properly configured to increase the network's security. This work reviewed DMZ with regard to its importance, its design, and its effect on the network performance. The main focus of this work was to explore a means of assessing DMZ effectiveness related to network performance with simulation under OpNet simulator.

Index Terms: DMZ (Demilitarised Zone), Firewall, Network Security, Network Performance, OpNet.

1. Introduction

Security is one of the most critical challenges of computer and communication networks. Network design should accomplish three security aims: confidentiality, integrity, and availability. Actually, protecting a network that is connected to internet is a big challenge. The solution for this challenge is to divide the network

* Corresponding author. Tel:
E-mail address:

into two segments. The first segment can contains a public access machines such as HTTP server, DNS server and Mail server, this segment is called Demilitarized zone (DMZ). The second one can contain a private access machines such as application server, database server and workstations. A DMZ is a network added between a protected network and an external network in order to provide an additional layer of security [1].

A DMZ is front line of a network that protect the valuables resources from untrusted environments. A DMZ is an example of the principle of defence in depth. The defence in depth principle points out that no one thing, no two things will always provide complete security. It points out that the only way the system is reasonably protected is to consider every part of the system and to ensure that they are all secure. A DMZ adds additional security layer beyond a single perimeter [2]. It separates the external network from the direct reference to the internal network. It is achieved by isolating machines that are directly accessible by all other machines. Most of the time the external network is the Internet, the web server in a DMZ, but this is not the only potential arrangement. A DMZ can be used to isolate specific machines in the network from other machines. This can be done for a department that requires internet access and corporate network as well. In DMZ nomenclature, internal network should have more secure information than external one [2].

Separation is important. Any system should separate its important applications and information. This is a checks and balances to ensure that any untrusted area cannot corrupt the whole area. The separation principle is renowned by the government. Generally, government has three divisions the executive, the legislative and the judicial. The same design is required on a computer network system. Separation of information is necessary, so the attacker cannot get all the systems. An attacker could access a web server, but it would be worse if the attacker could access the database through a web server. This is the type of problem DMZ is designed to prevent.

This work will discuss a way of evaluating the performance of DMZ with regards to network performance. Different scenarios will be investigated and analysed using OpNet simulator.

2. Related Work

Small number of researches studied the performance of DMZ. Most works concentrated either on the infrastructure of science data DMZ to transfer a huge amount of data or evaluating the performance of firewall types. Large number of researchers studied a DMZ in regard to security only.

In [3] researchers studied the Science DMZ architecture, configuration, cybersecurity and performance. They used supercomputing centres and research laboratories to highlight the effectiveness of the science DMZ model. They concluded that Science DMZ model enhance collaboration, accelerating scientific discovery.

In [4] researchers studied network firewalls with regards to network performance using parallel firewall. The results pointed out that the network delay and average response time were degraded by using parallel firewall. It also showed that firewall deployment has some advantages and disadvantages with regard to network performance. Furthermore, it demonstrated that Firewall improved link utilization and throughput. However, the inspection process caused delay. They concluded that parallel firewalls are cost effective from the network performance point of view.

In [5] researchers evaluated different types of firewall platforms and their effects on network performance. Their analysis depended on delay, throughput, jitter, and packet loss. They also tested the security of firewalls by applying a set of attacks. The results represented that network based firewall Performance is better than personal firewall in all metrics. It also showed that using both type of firewalls provide layered security.

In [6] researchers studied firewall in regards to performance, efficiency, and security. They studied the relation between firewall's security and firewall's performance. The results showed that extra processing increased response time such as degrade system performance. However, filtering unauthorised traffic increased the network performance. They concluded that the deployment of firewalls is not only enhances network security but also they contribute to meet service level agreements and quality of service in terms of availability and performance.

To sum up, none of the previous work go straightforward to evaluate the performance of DMZ. Thus, this work aims to study the effect of a DMZ on network performance.

3. Firewall

Firewall is a hardware, software or combination of both to apply security policies for controlling network access. The main role of firewalls is protecting a network from unauthorised access. In general, firewalls can accomplish three security aims: confidentiality, integrity, and availability [4]. There are three main firewall types.

- **Packet filters:** Also known as static packet filters. It works Based on checking the exchanged packets between computers on a network [7], it works at both network and transport layers of the OSI model [8]. By checking the packets of a network, the packet filter firewall verifies that the packet conforms to one or more rules set by the network administrator. These rules determine whether the packet will be allowed to pass or not based on the information contained in the packet itself. This type of firewalls enables administrators to pass or block data streams by using the following controls: physical network interfaces, destination and source IP addresses, and destination and source ports.
- **Stateful inspection:** Also known as dynamic packet filter. It works at layer 3, layer 4, and layer 5 [8]. **:** it improves the packet firewall filters by tracking the state of connections and blocking packets that deviate from the expected state [4]. In more details, this type of technology is not only processes the packet header, but also checks incoming and outgoing packets for a period of time and maintains the connection state information in the operating system kernel and parses the IP packet [7]. This type after examines TCP/IP header and permits it, all answers are automatically permitted for. As a result, all ports are closed excluding of incoming packets queries a connection to a particular port then only requested port opens and such method avoids port scanning and a common hacking methods.
- **Application-proxy gateway:** The aim of the second generation firewall is to enhance the packet filter firewall exclusion at layer 3 and layer 4 of the OSI model and extending to assess network packets for valid data at layer 7 of the OSI model before allowing to start the connection [9]. Generally this type is a host running proxy server that does a separation (no direct traffic) between networks. The application firewall uses a NAT (network address translator) to cover the traffic that passes from side to the other in different network address. Understanding certain protocols (such as FTP, DNS, HTTP) are very important to the application layer firewall that helps to identify undesirable protocol trying to bypass the firewall through open port [7]. Each successful connection attempt actually results in the creation of two separate connections one between the host and the proxy server, and another one between the proxy server and another host [4].

4. OPNET

Simulation is a common way to evaluate the design and performance of computer network. Building a simulation model is not a fiddling task. It needs deep understanding of simulation, modelling, system properties, and mathematical background [10].

OpNet simulator is a program to simulate the activities and performance of computer and communication networks. The main advantages of OpNet over other simulators are its power and versatility [11]. OpNet offers a complete development environment to design and configure communication networks and distributed systems. The performance of designed system can be analysed using discrete event simulations. This simulator deals with OSI model starting from layer 7 to the adjustment of the most crucial physical parameters [11].

OpNet modeller is the most popular product for network simulation. It is used in educational and industrial sectors. Several universities use OpNet in teaching communication and computer networks, as well as, companies for modelling, study, analysis, and performance predication of several network systems. Nowadays, major companies need computer network professionals who can evaluate the performance of their network in

order to identify and fix the network problems. OpNet can achieve the aims as well as preventing the problems from arising [10].

5. Network Design

As shown in Fig. 1. , DMZ network is neither inside nor outside the firewall. It is accessed from both inside and outside networks. Security rules prevents devices in the outside to connect to inside devices. A DMZ is more secure than the outside network, but less secure than the inside one [12]. The Internet (outside network) is connected to a firewall on the outside interface. Users and servers that do not need to be accessible from the internet are connected to the inside interface. Servers that are accessible from the Internet located in the DMZ. A DMZ mainly has two goals. The first one is to separate the public access resources from the rest of the network. The second is to reduce complexity [3].

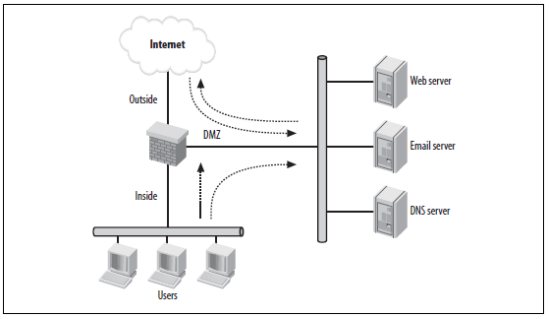

Fig.1. DMZ network

5.1. Firewall

The firewall is configured as the following: the inside network can establish connections to the outside and DMZ networks, but the outside and DMZ networks cannot establish connections to it. Outside network cannot establish connections to the inside network, but it can establish connections to the DMZ. The DMZ cannot establish connections to the inside network, but it can establish connections to the outside network [12].

5.2. DMZ

The DMZ is public access network. It contains servers which can be accessed from the outside and the inside network. It can contains HTTP server, Mail server, DNS, etc. Its location reduces the network complexity and increase the network security [3]. Local users get credible performance because the latency between DMZ and them is low.

5.3. Inside network

The inside or protected network contains the organisation’s devices and private access servers such as database and FTP servers. Isolation of inside network protects the organisation’s data from public access [13]. The users of the protected network can access the outside and the DMZ network [13].

6. Case design and discussions

In this work, the aim is to study the effect of DMZ in network performance. Three topologies are produced according to DMZ network design. The topologies are built with and without firewalls. Those topologies are used to build three scenarios and to compare between them in order to study the effectiveness of DMZ. The three scenarios are proposed as the following:

6.1 No DMZ No Firewall scenario

As shown in Fig. 2. , the network consists of two main segments:

- Outside network: it contains Internet Lan, Internet Switch, Internet Router, and Internet. Internet Lan consists of 500 users trying to access all the servers of the inside network.
- Inside network: it consists of Edge Router, Lan Switch, Employee Lan, FTP server, DB server, Email server, and HTTP server. Employee Lan consists of 50 users.

The IP addresses are assigned for connected routers interfaces and servers. Network address translation is implemented on both routers. This allows inside network to connect with the internet. The edge router is not configured to filter any packet coming in/out the inside network, so it passes all the requests of internet Lan to the all servers.

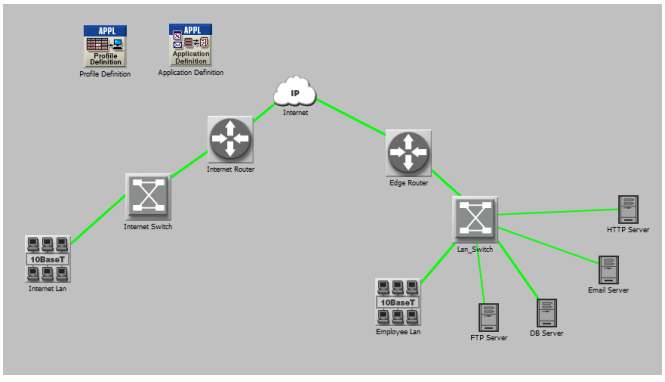

Fig.2. No DMZ No Firewall

6.2 No DMZ with Firewall scenario

As shown in Fig. 3. , internet users are not able to access the ftp and database servers. Access control list is implemented on edge router to allow outside users to access HTTP server and Email server only. It is also configured only to prevent internet users to acess FTP and DB servers. This means that all the database and ftp requests from outside network are blocked by the firewall. All the requests that reach to FTP server and DB Server are from Employee Lan. All in all, the edge router acts as a firewall.

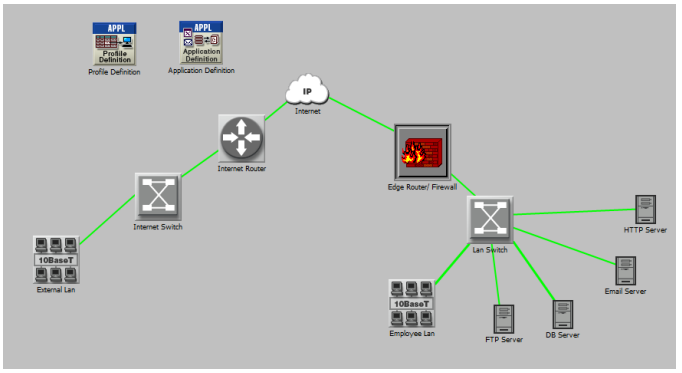

Fig.3. No DMZ with Firewall

6.3 DMZ scenario

As shown in Fig. 4. , public access servers are separated from other devices. The edge router/firewall is configured to block any request to connect to the inside network. It also configured to pass any outside reply to inside network. The firewall is configured to allow any request to access DMZ network. Furthermore, the firewall is configured to allow inside network to access the DMZ. All the configurations are applied using access control list that mainly depends on ip addresses and port numbers of the machines.

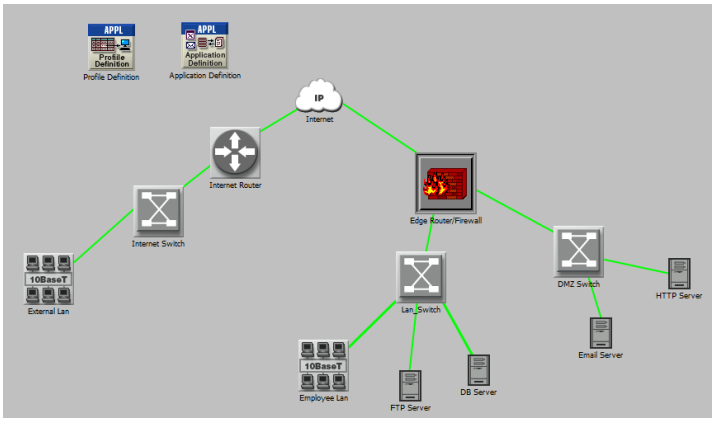

Fig.4. DMZ

Tables 1 and 2 show a summary of the network topologies and application configurations using OpNet.

Table 1. Summary of the Network Topologies design using OpNet

Object Name	**Object Model**
DB Server, HTTP Server, FTP Server, and Email Server.	*ethernet_server* node object
External Lan and Employee Lan	*10BaseT_LAN* node object
Internet Switch, Lan Switch, and DMZ Switch.	ethernet16_switch
Internet Router, Edge Router, and Edge Router/Firewall.	ethernet4_slip8_gtwy
Internet	*ip32_cloud* node object
Servers <-> Switches 10BaseT_LAN <-> Switches Switches <-> Routers	10BaseT
Routers <-> Internet	PPP_DS3

Table 2. Application Configuration Settings

Application name	Application model attribute	Application model attribute values
Web browsing	HTTP	Heavy browsing
File transfer	FTP	Medium load
Database	Database	High load
E-mail	SMTP	High load

7. Simulation results and analysis

Related Simulation statistics are chosen to assess the performance of DMZ. The results are compared and presented as the following Figures.

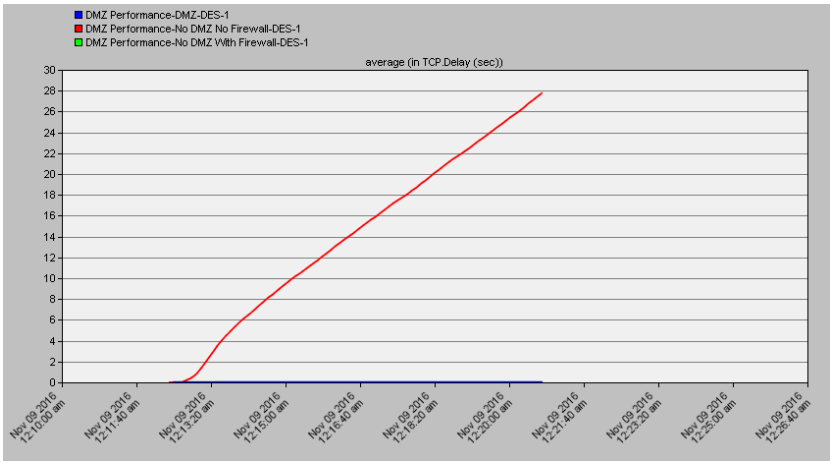

Fig.5. TCP delay

Fig. 5. represents the average TCP delay. The TCP delay of the “No DMZ No Filter” is the largest because the network traffic is not filtered, this make high traffic inside the network. The high traffic increases the probability of congestion and packet loss that are the main reasons of retransmissions and TCP delay.

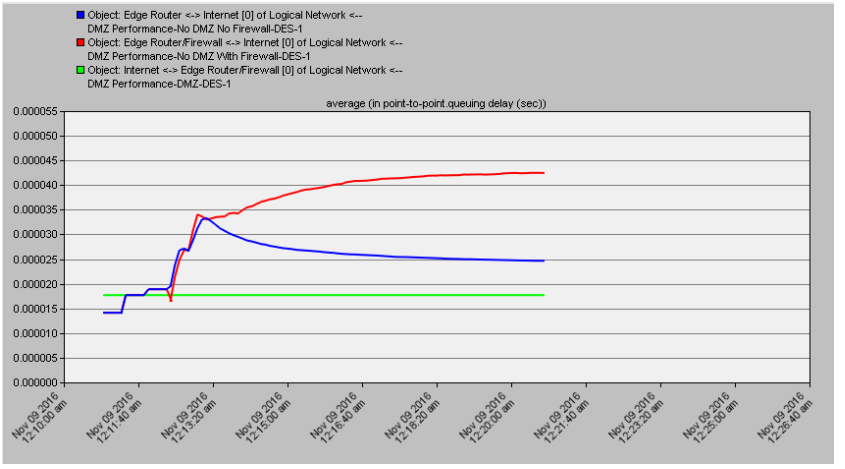

Fig.6. Queuing delay.

Fig. 6. represents queuing delay from internet to edge router. It is clear that the queuing delay of the DMZ scenario is the lowest queuing delay. The queuing delay of the “No DMZ with Filter” is the largest because the traffic coming to inside network will be filtered by edge router/firewall, then the authorized traffic will be passed to local network. On the other hand, queuing delay of DMZ scenario is the lowest because the authorized traffic will be passed to the inside network and DMZ through two different interfaces. So, it is clear that DMZ reduces the queuing delay because it divides the LAN into two segments which reduces the load on network machines. Furthermore, filtering will prevent unauthorised traffic to reach to Lan switch. This policy degrades the queuing delay.

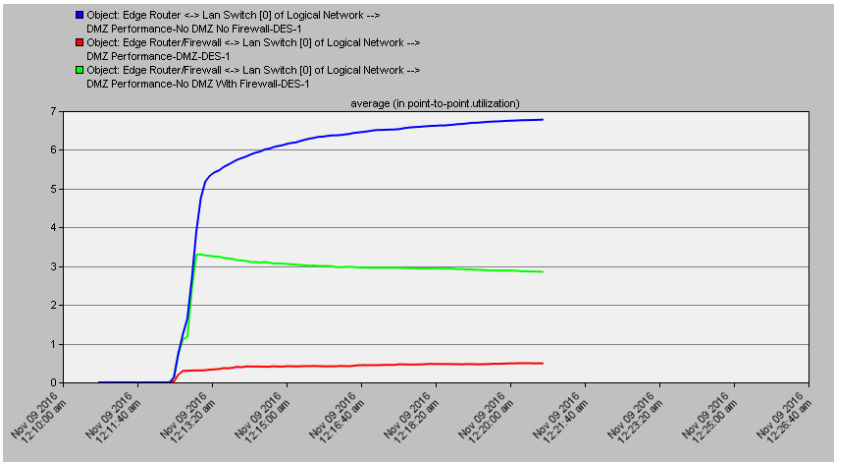

Fig.7. Link utilisation (edge router/firewall to LAN switch).

Fig. 7. shows outgoing link utilisation from edge router to Lan switch. It is clear that DMZ scenario has the lowest link utilization. The utilisation of “No DMZ with Firewall” is greater than “DMZ” because http and email servers are not separated from inside network, so the requested traffic to email and http server pass through edge router to Lan switch. But in “DMZ”, the requested traffic to email and http pass from the edge router to DMZ switch. Thus it can be estimated that DMZ optimised the overall utilisation of the network.

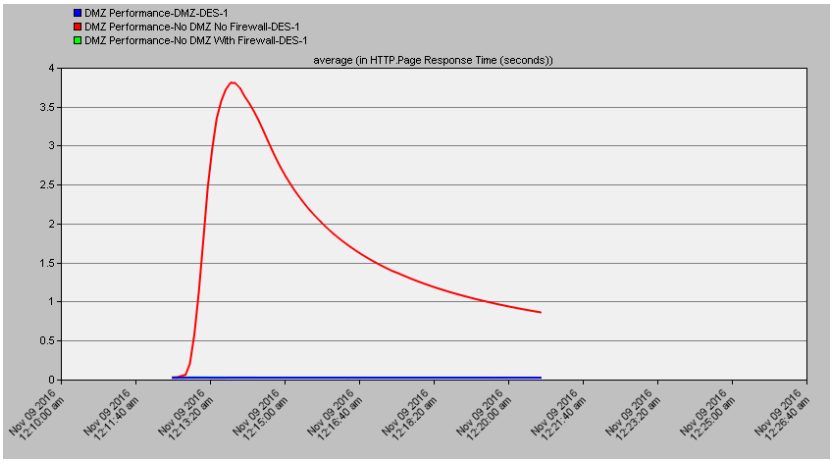

Fig.8. HTTP page response time.

Fig. 8. represents HTTP page response time measuring in seconds. “No DMZ with Firewall” and “DMZ” scenarios are the fastest page response because the filtering allows a smaller amount of traffic to go inside the local network. Http and email traffic only are allowed to go inside the network. Small amount of traffic to process is faster than a large one. So, allowing only the authorised packets to pass decrease page response time.

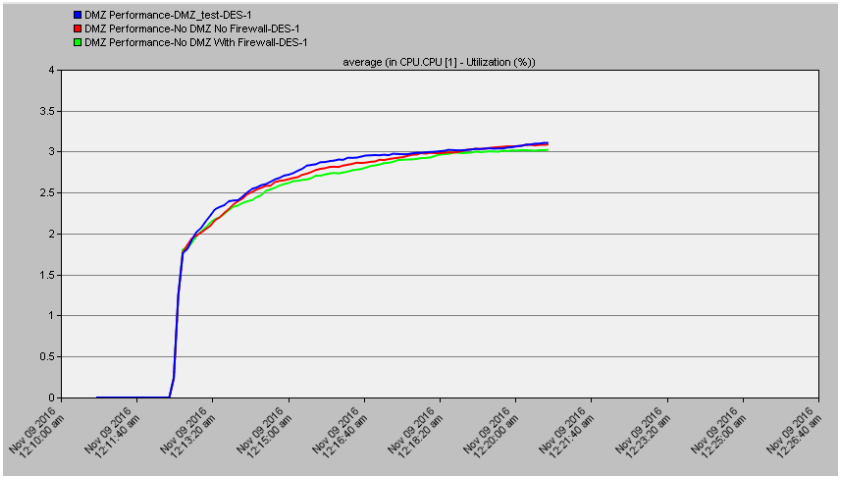

Fig. 9. CPU Utilisation of HTTP Server

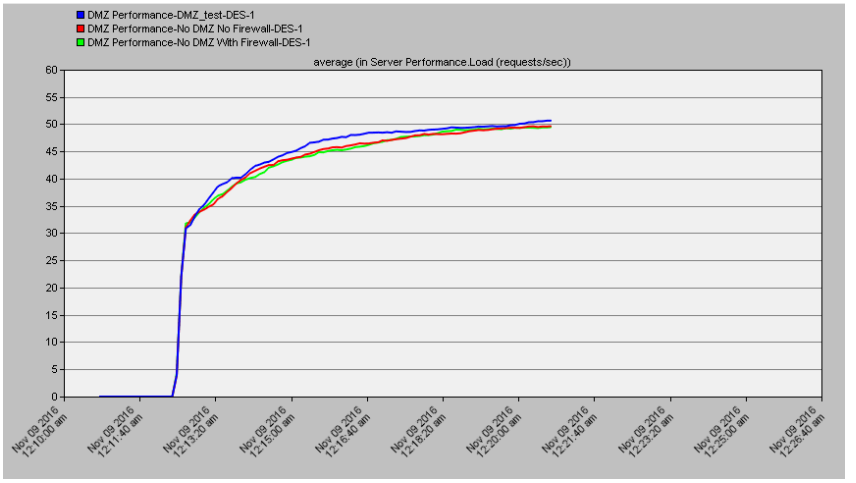

Fig.10. Performance of HTTP Server

Figs. 9 and 10 shows CPU Utilisation of HTTP Server and performance of HTTP Server respectively. It is clear that The CPU utilization and performance of the three scenarios are almost the same because the two Lans are able to access http server in all scenarios. So, switching to DMZ network design does not degrade the http server performance.

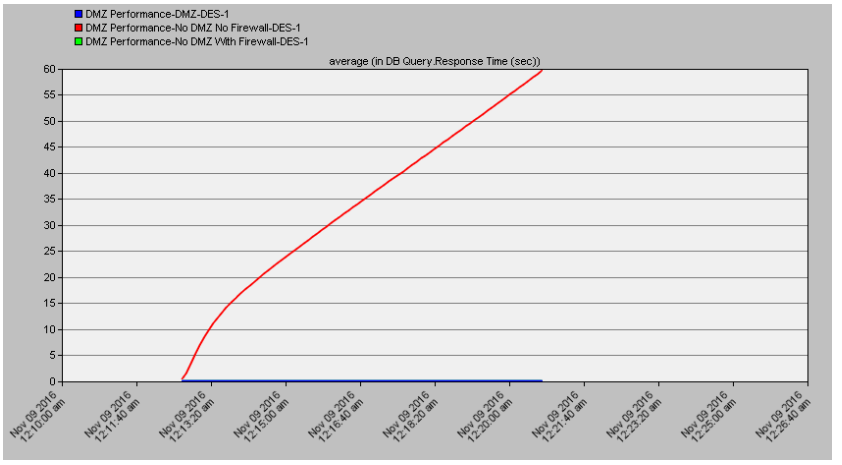

Fig.11. A DB query response time (sec).

Fig. 11. shows the database's query response measured in seconds under three different scenarios. It is clear that "No DMZ with Firewall" and "DMZ" scenarios are the fastest DB query response. The edge router/firewall does not allow internet users to access DB server. The DB server receives requests only from local users, packets pass through Lan switch to the server in both scenarios. Implemented security prevents high load on inside network.

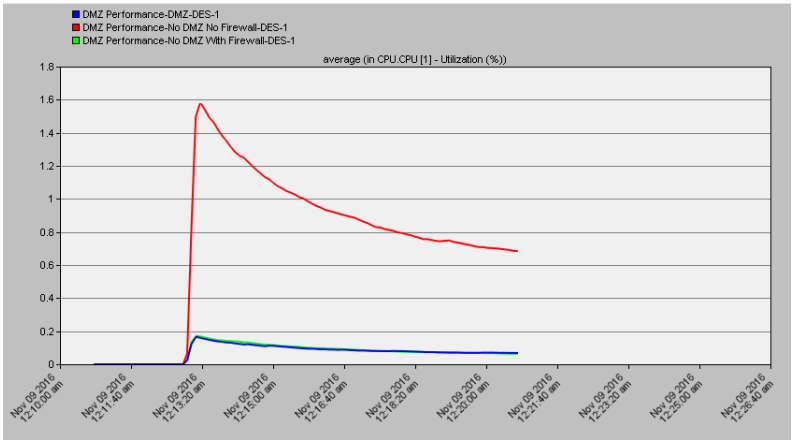

Fig.12. CPU Utilisation of FTP Server

Fig. 12. shows CPU Utilisation of FTP Server. It is clear that DMZ Scenario and No DMZ with Firewall are the lowest CPU utilization. The explanations of this results that the edge router/Firewall blocks each FTP requests from the internet. So, FTP Server receives requests only from local users.

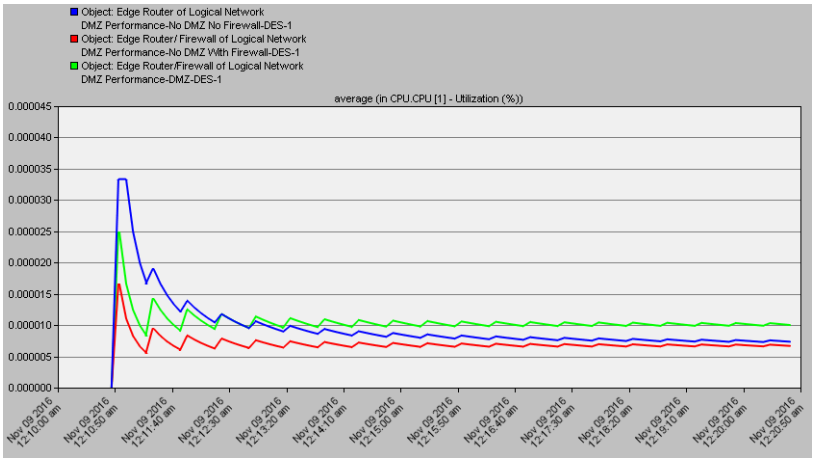

Fig.13. CPU Utilisation of edge router/firewall

Fig. 13. shows CPU Utilisation of edge router/firewall. It is clear that DMZ Scenario is the largest CPU utilization. The explanations of this results that the edge router/Firewall filters all packet coming from internet. It also decide to send the filtered packets either to inside network or DMZ. Those processes make the CPU utilisation the largest.

8. Conclusions

This work has discussed a case study of evaluating the performance of DMZ. OpNet simulation has been used to build three indicative scenarios and results are compared and discussed. The performance evaluation considered TCP delay, queuing delay, link utilisations, http page response time, CPU utilisations, servers' performance, DB query response time. The results have shown that the DMZ and No DMZ with firewall

scenarios have the best TCP delay, DB query response time, HTTP page response time, CPU utilisation of FTP Server. Moreover, DMZ Scenario queuing delay, links utilisation, and servers' performance are much better than No DMZ with firewall. The results have shown that DMZ solves many critical performance problems. To sum up, DMZ is not only to improve the network security, but it is also to improve the network performance.

References

[1] T. B. D. L. E. Q. J. P. D. M. Z. N. O. Christian Barnes, Hackproofing Your Wireless Network, USA: Syngress, 2002.

[2] S. Young, "Designing a DMZ," *SANS Institute InfoSec Reading Room.*

[3] E. Dart, L. Rotman, B. Tierney and J. Z. Mary Hester, "The Science DMZ: A Network Design Pattern for Data-Intensive Science".

[4] E.-S. N. A. Sabry NASSAR, Improve the Network Performance By using Parallel Firewalls.

[5] J. M. ,. A. I. a. A. N. Q. Thaier Hayajneh, "Performance and Information Security Evaluation with Firewalls," *International Journal of Security and Its Applications,* 2013.

[6] O. G. H. Garantla, "Evaluation of Firewall Effects on Network Performance".

[7] S. E. John R. Vacca, Firewalls: Jumpstart for Network and Systems Administrators, MA, USA: Elsevier Digital Press, 2005.

[8] Sequeira, CCNA Security 640-554 Quick Reference, Cisco Press, 2012.

[9] E. Romanofski, "A Comparison of Packet Filtering Vs Application Level Fire wall," *Global Information Assurance Certification Paper*.

[10] &. Y. H. S. S. Sethi, The practical OPNET User Guide for Computer Network Simulation, 2012.

[11] "OPNET Simulator," [Online]. Available: http://users.salleurl.edu/~zaballos/opnet_interna/pdf/OPNET%20Simulator.pdf. [Accessed 24 06 2017].

[12] G. A. Donahue, Network Warrior, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472., 2007.

[13] M. Bishop, Computer Security: Art and Science, Addison Wesley, 2002.

[14] W. Stallings, CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE, 5 ed., Pearson Education, 2011.

[15] J. Webb, Network Demilitarized Zone (DMZ).

[16] S. E. John R.Vacca, Firewalls Jumpstart for Network and Systems Administrators.

[17] M. K. E Aboelela, Network Simulation Experiments Manual.

[18] R. . J. Shimonski, W. Schmied, T. W. Shinder, V. Chang, D. Simonis and D. Imperatore, Building DMZ Enterprise Network, Syngress Publishing, 2003.

[19] F. F. R. A. M. M. S. Marco Antonio Torrez Rojas, "Science DMZ: Support for e-science in Brazil," 2016.

[20] K. E. a. R. B. K. Salah, "Performance modeling and analysis of network," *IEEE*, 2012.

Authors' Profiles

Baha Rababah is a lecturer at faculty of computer and information system, Islamic University, KSA. He obtained BSc Computer Engineering, Al-Balqa Applied University, Jordan in 2010. He also obtained MSc in Computer Network Administration and Management, University of Portsmouth, UK in 2015. His researches of interest are network performance, network security, and cloud computing.

Shikun Zhou, PhD is a senior lecturer in Internet applications and formal computing, university of Portsmouth, UK. He also is the Intranet and Web forum Administrator and also a member of the Communications and Networks Engineering Research Group.

Mansour Bader holds a MSc in computer engineering and networks, University of Jordan, Jordan, 2016. BSc Computer Engineering, Al-Balqa Applied University, Jordan, 2008. He is a technical support engineer of computer networks at computer centre of Al-Balqa Applied University for 8 years. He has 3 papers in the cryptography field and has participated in two conferences, one in Sydney, Australia called SPM2016 the other were held in Geneva, Switzerland titled CRIS 2017.

How to cite this paper: Baha Rababah, Shikun Zhou, Mansour Bader," Evaluation the Performance of DMZ", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.8, No.1, pp. 1-13, 2018.DOI: 10.5815/ijwmt.2018.01.01