# Building Security Perimeters to Protect Banking Sector in Libyan

Salima Benqdara
University of Benghazi
Benghazi, Libya

Almabruk Sultan
University of Benghazi
Benghazi, Libya

Awad Elfergani
University of Benghazi
Benghazi, Libya

## ABSTRACT
Information security in the banking sector is heavily controlled as banks store and manage their clients' private information. Information security has always been the responsibility of the information technology (IT) department in organizations. Banks have become a component of the internet and daily lives. It is a real task to protect these bank procedures, systems from the attackers and minimize the security threats. With this Cyber-attacks increasing day by day, and this is the challenge facing by countries and organizations like banking where data is critical. These banks should be built networks using secure strategies to protect their components. However, the performance of the network is affected by applying security rules. Network security is an essential priority for protecting applications, data, and network resources. Applying resource isolation rules are very important to prevent any possible attack. This isolation can be achieved by applying the DMZ (Demilitarized Zone) design. A DMZ extremely enhances the security of a network. In this paper perimeter network security framework is proposed to the protection and minimize the cybersecurity issue that exists in Libyan banks effectively.

## General Terms
Information Security, Network Security.

## Keywords
Keywords: Information Security, DMZ, Firewall, Network Security, Network Performance, OpNet, perimeter defense.

## 1. INTRODUCTION
Nowadays technology has become a part of almost every field particularly the business sector and the banking division. The reliance on technology is so much that managing an account segment cannot be thought of without the use of innovation. But innovation has too brought an entire set of challenges to be managed with which incorporate outside dangers driving to cyber fakes, the higher effect due to purposefulness or inadvertent acts of inner representatives, unused social building procedures utilized to pick up secret accreditations [1]. The competitive nature of managing the banking, at the side the critical esteem of the assets they oversee, commerce and innovation organizations must take all steps essential to secure their resources. A compromise of these data resources seems to have a serious effect on the bank, bank clients, shape an infringement of laws and directions and adversely influence the notoriety and money related soundness of the bank [2].

Security is one of the most critical challenges of computer and communication networks. The network design should accomplish three security aims: confidentiality, integrity, and availability. Protecting a network that is connected to the internet is a big challenge. To establish a secure network a defense-in-depth strategy where security measures are placed in many layers that create an entire network, from the end-user to the Internet, will be essential. The network perimeter layer has historically been the focus of protecting a private network and is still essential for keeping intruders at bay and providing detection of possible intrusions [3]. A DMZ is a network added between a protected network and an external network to provide an additional layer of security. A DMZ is the front line of a network that protects the valuables resources from untrusted environments. It is an example of the principle of defense in depth [4].

The banking sector in Libya, like other countries in the region, is the foundation financial services provider for the economy. As Libya is from developing countries face several challenges in the development of technology compared to most developed countries [5]. Libyan banks deployed online electronic banking payments through mobile phones [6]. Due to reports, researches, and results of the interview, e-banking services require information security controls related to internet-based services that are not adopted in public Libyan banking [7]. Besides, a recent report from Microsoft announced that the computer system in Libya has faced the highest infection of malicious and unwanted software compared to worldwide [9]. For the country like Libya, it is important to develop a perimeter network security framework to the protection and minimize the cybersecurity issue that exists in Libyan banks effectively.

The main objective of this paper is to develop perimeter network security framework to provide an additional layer of security in a Libyan bank. The rest of the paper is organized as follows: Section 2 discusses the related works. Section 3and 4 present a brief overview of the perimeter security and DMZ to provide a proper background. Data collection method present in section 5. In section 6 present the proposed approach. Section 7 describes the flow of the experiment. The results and discussion of findings are presented in Section 8. Finally, Section 9 concludes the paper.

## 2. RELATED WORK
In this section discuss the published papers have provided solutions in an organizational or technical approach.

Angelakopoulos and Mihiotis (2011) studied the challenges of e-banking for the banking sector in Greece, during the e-commerce era and the study shown that the low response rate from customers and the implementation of security and data protection mechanisms are the main problems faced by banks.

Shuaieb (2013) suggested an analysis of the factors affecting Internet banking adoption in Libya. The author highlighted the challenges facing the spread of electronic banking in Libya, such as, the weakness of security systems achieved in the field of electronic commerce and the lack of an appropriate environment for electronic commerce.

Folorunso et al. (2016) introduced an online questionnaire to assess the computer and network security strategies for Nigerian Banks as a case study, the samples are limited to computer security experts and information technology department staff in banks. The security strategy that they are asking is regarding passwords, antivirus, firewalls, encryption, IDS, and IPS. Also, the study investigates if the Nigerian banks have experienced any form of attacks on their systems. The security strategy of the Internet-based services, which require more security strategy such as DMZ, is not mentioned in the study. The study findings that Nigerian banks are using effective computer and network strategies after, implementing almost all security strategies and they rarely experience malicious attacks of any form.

Tytarenko (2017) proposed study to design the first line of defense enterprises based on the selection of the best security controls. A NIST SP 800-53, revision 4 uses as a primary reference for selecting the best security controls. The author selected thirteen of controls to build the first line of defense. However, some important controls did not appear in the study result, which they are necessary to build the first line of defense.

Dart et al. (2018) studied the Science DMZ architecture, configuration, cybersecurity and performance. They used supercomputing centers and research laboratories to highlight the effectiveness of the science DMZ model. They concluded that Science DMZ model enhance collaboration, accelerating scientific discovery.

Rababah et al. (2018) used OPNET simulator to assess the effect of DMZ on network performance. The author used three scenarios, first without DMZ and Firewall, second with Firewall and third with DMZ. The results show that DMZ solves many critical performance problems, also they found that DMZ is not only to improve network security, but it is also to improve network performance.

## 3. PERIMETER SECURITY

The perimeter network is an architecture and components that provide security to the perimeter of an internal network from an external network like the Internet. The most components use to protect network boundaries are technical safeguards such as firewalls, IDS, and IPS that monitoring and control of communications at the external boundary of a system to prevent and detect malicious and other unauthorized access [10]. The network perimeter can be comprised of devices that block unwanted traffic, allow remote access, filter for potentially dangerous content, and detect or block probable attacks. Additionally, the perimeter may contain email and web servers that provide services to customers and employees externally via the Internet. A private network will be at risk from many threats because of the need to establish connections to other networks, especially the Internet. By implementing established practices for securing the perimeter of a private network, a community bank can secure itself from the majority of threats without exhausting its' entire IT budget [11]. A DMZ can be considered a type of perimeter network. The primary difference between a DMZ and a perimeter network is the way packets arriving and departing the subnetwork are managed. In a perimeter network, the device that connects the external network to the perimeter network is a router, whereas a DMZ uses a firewall to connect to the Internet. For a DMZ, a firewall policy will be applied to all packets arriving from the external network (Internet) [12], [13].

## 4. DEMILITARIZED ZONE (DMZ)

DMZ is well known as the security layer and also as a perimeter network that is used to protect the internal system where all ports are open so that they are possibly seen by outsiders. In most computer networks, the most vulnerable components are those computer hosts that are responsible for providing end-user services such as web, DNS (Domain Name System), and email servers. Due to the chances of one of these servers becoming compromised through newly found misuses, when utilizing the DMZ concept they are designed to dwell inside their own sub-network. This permits the remainder of the network to be secured if the hacker can succeed in attacking any of the servers. The concept of DMZ begun when companies starts to manage services to public clients by hosting a web server interior the organization for giving internet-based services. Web server zone needs a more complex perimeter design as a secure layer to isolate the web server zone, this isolation is commonly accomplished by employing a physical or logical subnetwork called a DMZ[14]. In this way, when there's an attack or somebody intentioned attacks the server which employments DMZ, the attacker can only access the host in DMZ, not within the inside network [15]. The primary reason of the DMZ is to provide another layer of security for a local area network (LAN). If an attacker can get access to services located within the DMZ, they are not able to gain full access to the main portion of the network.

## 5. DATA COLLECTION METHOD

Collecting the study data was carried out as follows:

- The literature study was conducted to find references and theories related to the focus of the research being done. It aims to have enough knowledge and theoretical basis that support to find the solution to study problems related to network security system using DMZ Firewall or perimeter network.
- Determine the known potential threats related to the perimeter network and their impact on the CIA.
- Collection data from previous researches banks regarding the security of internet electronic services on Libyan banks
- Collection data from previous researches concerning about security of internet electronic services on Libyan banks.
- A Libyan bank conducted by interview information security staff to collect data on the current security devices and appliances that protect the current perimeter network.

## 6. PROPOSED APPROACH

This paper presents a perimeter network security framework for a Libyan bank and proposes an approach to protect networks and system applications. The approach focuses on network security and application security because these two components form the core of cyber banking, as transactions happen through the network and available applications. The proposed framework represents the low level of technical security controls that will enforce high-level security controls mentioned in NIST 800-53-r5 such as Controls that address Defense-in-depth and Attack surface reduction and; Controls that address Layered structures and Boundary protection; Controls that Prevent exfiltration and Denial of service

protection; Controls that Transmission confidentiality and integrity; Controls that address Least functionality and System monitoring; Controls that address Information output filtering and System interconnection. The proposed framework starts with define network segmentation (security zones) as an up-down design approach as shown in figure 1. The following is a brief description of the security zones framework.

- Untrusted segment: this layer face the internet entrance, this zone connects the internet to the internal network of bank, after this zone the internal network starts. The switch separates physically the zones and connects the edge router to internet network at internet edge which are perimeter defense, DMZ and VPN zones. The primary security capability for this segment is DDoS protection, filtering router ACLs and flow analytics,
- Perimeter defense zone: this segment contains next-generation firewall and intrusion prevention system, the next generation of firewalls also including IPS feature, and web and email security appliance. The primary security capability is attacked, data loss via exfiltration and web server weakness.
- DMZ layer: this layer containing web servers for public-facing services, also this zone protected by a next-generation firewall and IPS/IDS and WAF appliances. The primary security capability is Web server vulnerabilities.

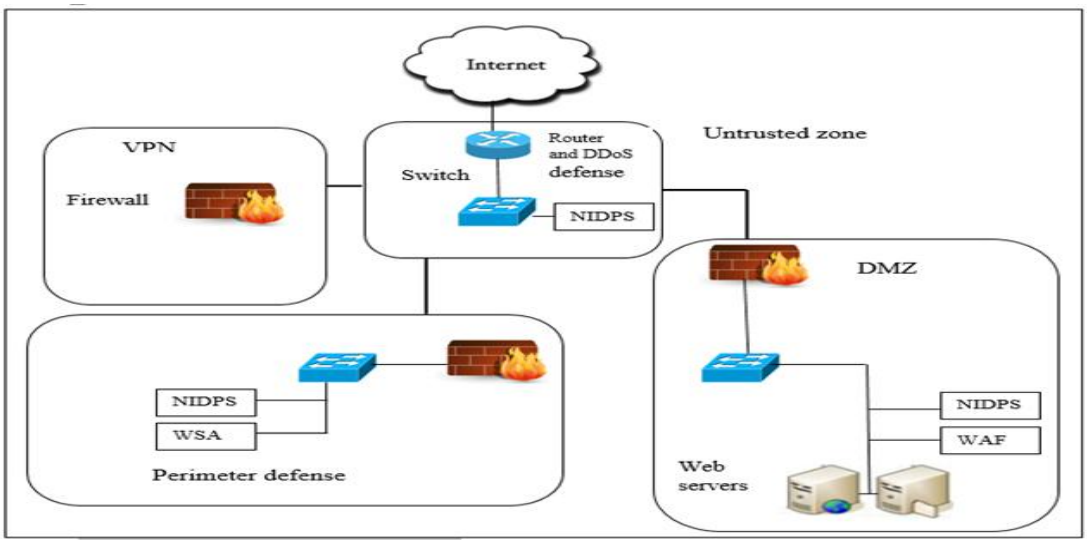


**Fig 1: Proposed perimeter network segmentation**

## 7. EXPERMENTAL SETUP

### 7.1 Framework Implementation:

In this stage, the experiments are performed in three topologies according to DMZ network design. The topologies are built with DMZ and without DMZ. Those topologies are used to build three scenarios and to compare them to the effectiveness of DMZ. The three scenarios are proposed as the following:

- Scenario one: without DMZ segment

The first network scenario as in Figure 3 consists of two segments:

- Internal network: The internal network consists of one segment including a Database (DB) User 4, HTTP User 1 station, DB server, HTTP server. Station and DB User 4 request data from DB server while HTTP User 1 station requests data from the HTTP server.
- External network: The external network is an internet environment including HTTP User2 request for HTTP server and DB User 3 request for DB server. The DB User 3 is considered as an external attacker and DB User 4 is considered as an internal attacker. Whereas The HTTP users 1 and 2 are legitimate users and have the right to access the HTTP server (webserver).

In this Scenario, both attackers tried to access DB server by sending packets, the route of packets from attackers to DB server is assigning statically. The purpose of the router R1 is to send the packets to the Internet and receive them from the internet while the purpose of router R2 is to send the packets to the proxy server and receive them from proxy to internet. Besides this router is working as a packet filtering firewall. The purpose of the proxy is to send packets to the internal network (stations and servers) and receive them to router R2. This proxy work on applications layer so it can deploy or not any application like database and HTTP, deploying meaning make a connection to application in the server.

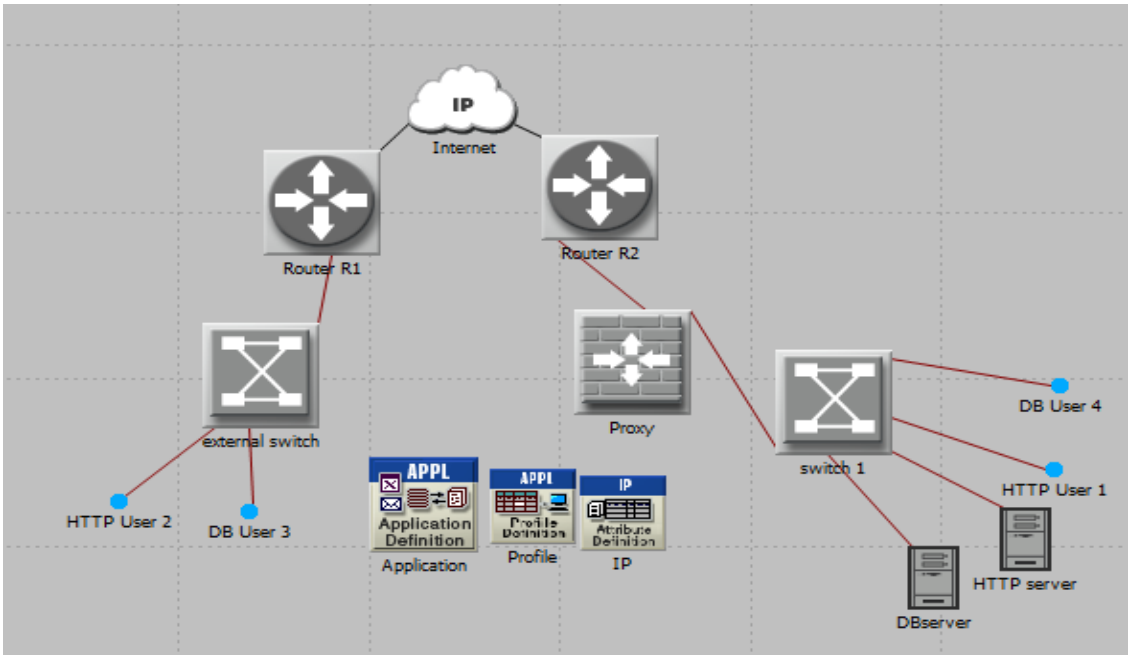


**Fig 2: one segment for internal network**

- Scenario two: DMZ segment: In the second scenario, more security layers and segments are added to scenario one, the security layer router R3 is added to create a new segment called DMZ which is placed between router R2 and router R3 for separating servers HTTP server and DB server as shown in Figure 3. The second segment is an internal network separated by router R3 for stations DB User 4 as an attacker and HTTP User 1, the router R3 separates the internal network away from DMZ.

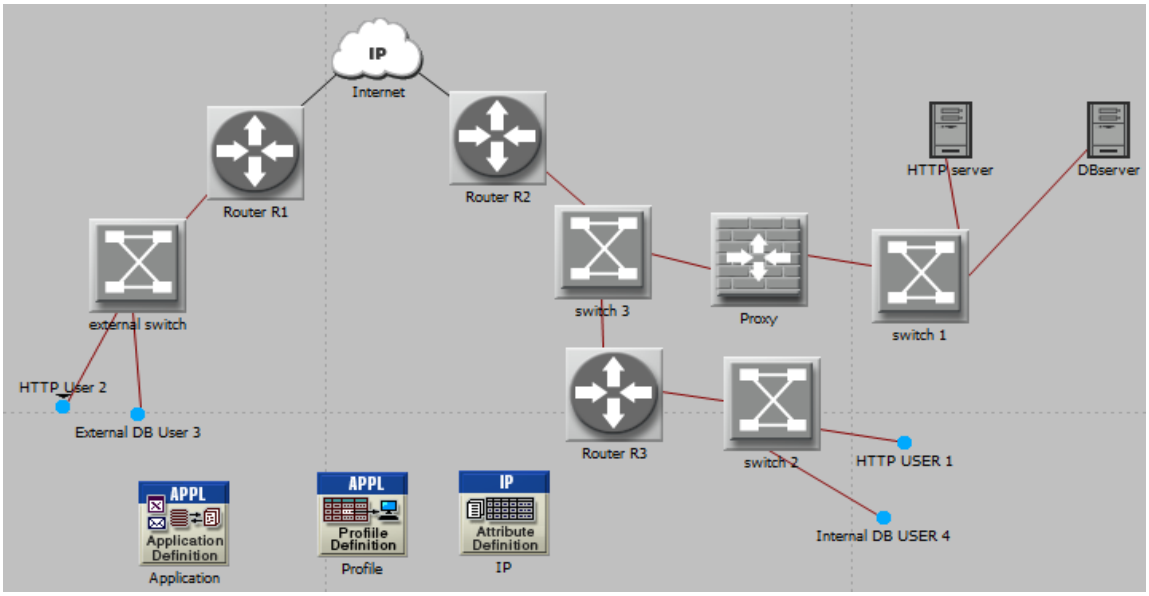


**Fig 3: network with DMZ segment**

- Scenario Three: Duplicate request with DMZ segment: In this scenario two work stations are added to scenario 2 as shown in Figure 4.21, (DB and HTTP User5) and (DB and HTTP User 6). Both work stations request two applications web browsing and Database. Whereas, User 5 has no right to access DB server but has the right to access the HTTP server. User 6 has the right to access DB server and HTTP server. User 6 has right to access DB server and HTTP server

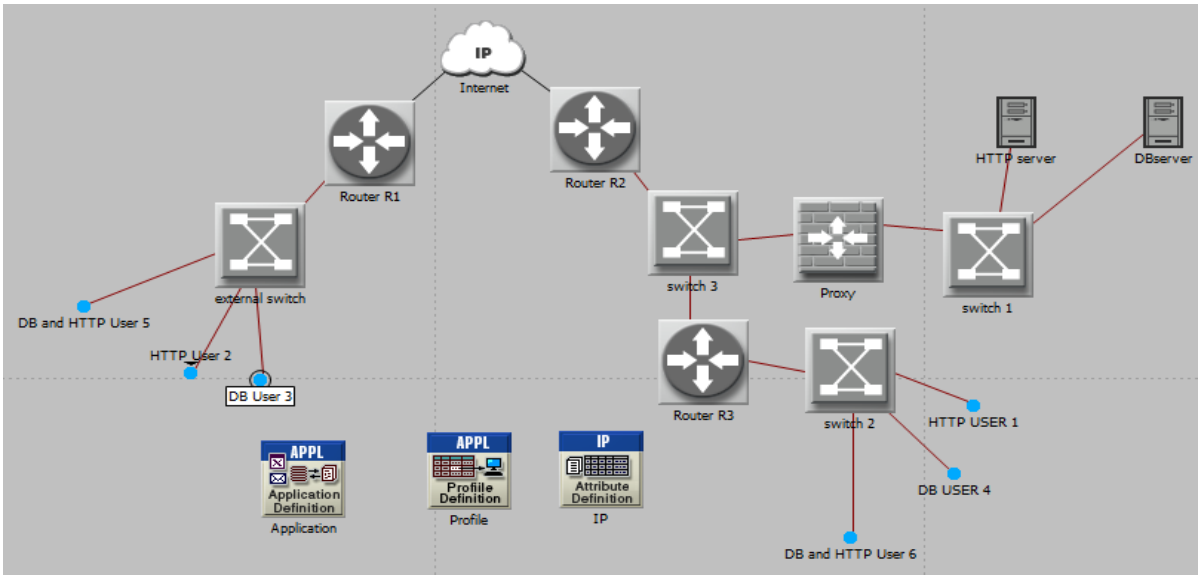


**Fig 4: network with adding two workstations**

## 7.2 Framework Evaluate

The OPNET software is selected to simulate some of the perimeter security controls. The goal of the simulation simulates the impact of applying network security controls to deny an attacker from accessing database server using following perimeter network controls:

- Segmentation: divided the network into security zones.
- Packet filter: filtering the packet based on the Access Control List (ACL) using source IP and destination IP for the packet.
- Security Layering: using security appliances as a layers between segments such as routers and proxy server.

# 8. EXPERMENT SIMULATION RESULTS AND ANALYSIS

To evaluate the Framework, one of the targeted Libyan banks is selected to test the framework. Some controls are simulated using OPNET program.

## 8.1 Scenario One

This Scenario discusses the results of simulation-based on statistics of packets sent and packets received. Also pinging of attackers to and from DB server.

Figures 5 and 6 explain the simulation based on statistics of packets. In these Figures, there are no controls on sending packets that mean router R2 packet filtering is OFF and the Proxy server deployed at DATABASE is YES. Figure 5 illustrates the DB User 3 sent and receive packets as an external attacker without controls. Whereas Figure 6 illustrates the DB USER 4 sent and receive packets as an internal attacker without controls. The results show that there are signals of packets sent and received for attackers. The results concluded that in this scenario (without the DMZ segment) will allow resources even to use by unauthorized users. It is a great weakness in the availability of the resources for the unauthorized user. It makes a vulnerable attack in the form of any Client.

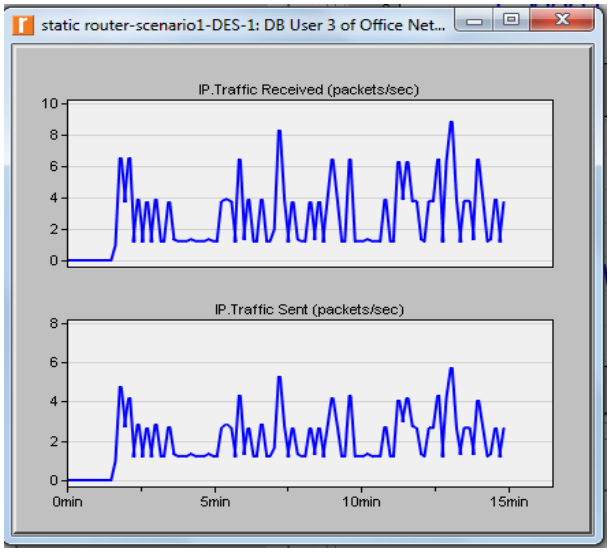


**Fig 5 DB User 3 sent and receive packets as an external attacker without controls**

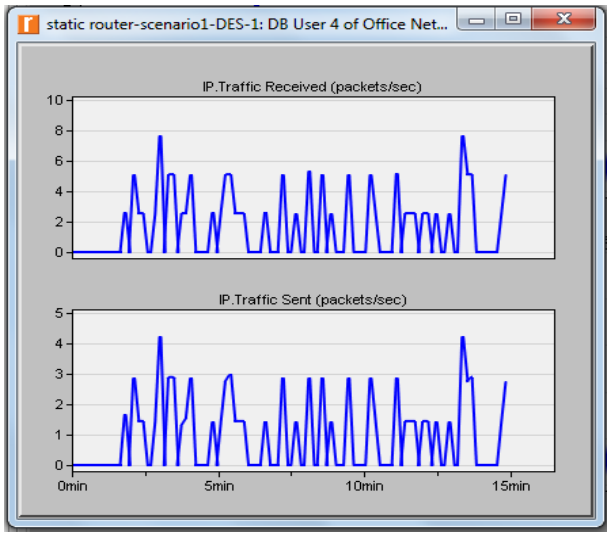


**Fig 6 DB USER 4 sent and receive packets as an internal attacker without controls**

Figures 7 explain the connection to the database server at the application layer. In this Figures, Packet filtering is OFF at router R2 and proxy server deployed is NO at DATABASE. The results in Figure 7 show that there is no packet received from DB server when setting NO for proxy servers deployed at a database. Figure 8 illustrates the log viewer of attacker DB User 3 which displays no connection with the database at the application layer. The results concluded that the Applications layer cannot deploy any application like database and HTTP.it is meaning cannot make a connection to application in the server.

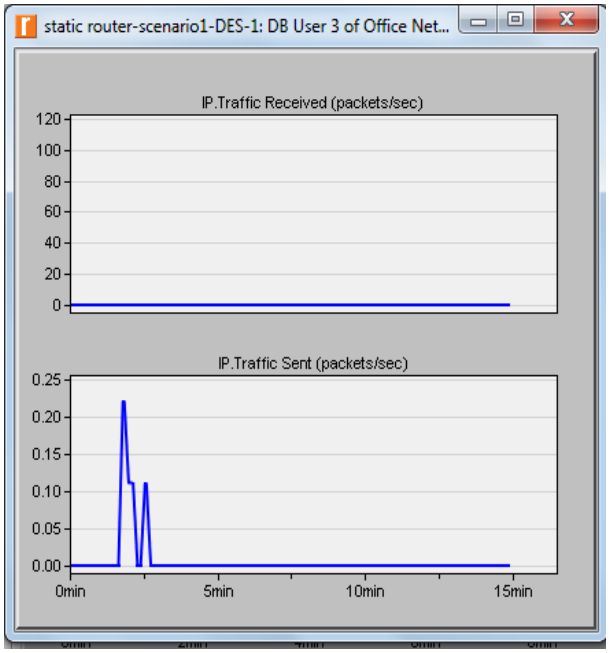


**Fig 7 connection to the database server at the application layer**

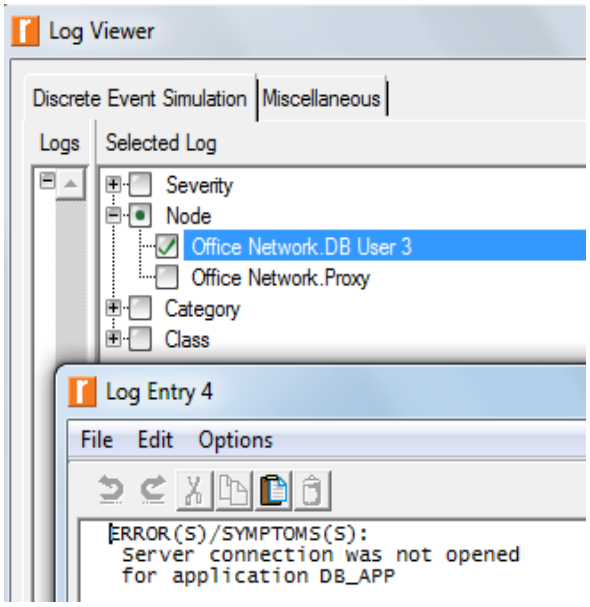


**Fig 8 Log viewer for DB user 3**

Figures 9 explain the case of closing connection to the database. The Figure illustrates the ping received from DB server to DB User3. The results show that there is high ping received from DB server to DB User3. The results concluded that the Proxy server is not enough to deny attackers to access to DB server

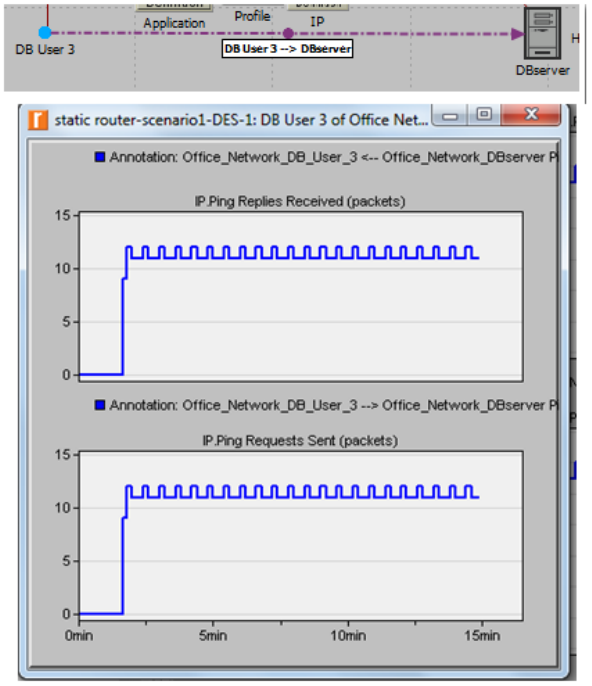


**Fig 9 the request and received of DB User 3**

Figures 10 and 11 explain the simulation based on the ACL controls the setting. Figure 10 illustrates ACL control is activated in router R2 by rejecting any IP that is sent to DB server. Whereas Figure 11 illustrates internal packets sent and received from DB server. The results in fig 10 show that there is no response from DB server. Whereas, the results in figures 11 show that the internal attacker still has packets sent and received from DB server.

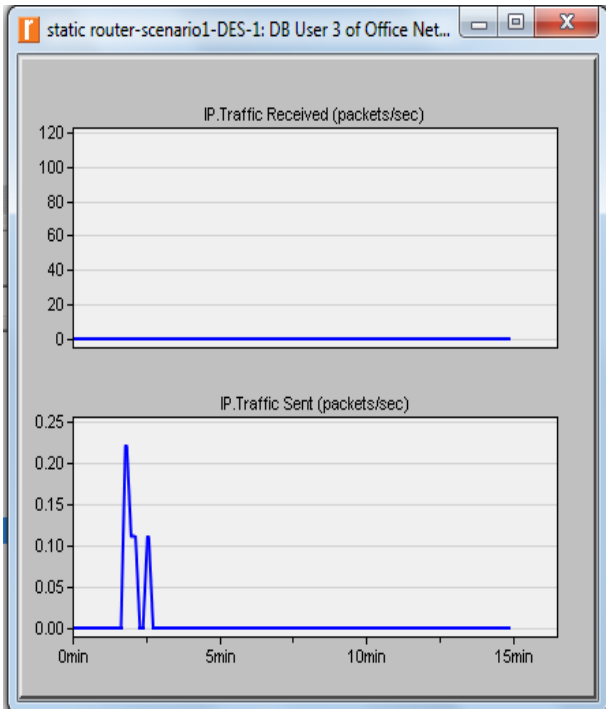


**Fig 10 DB User 3 traffic with no proxy server**

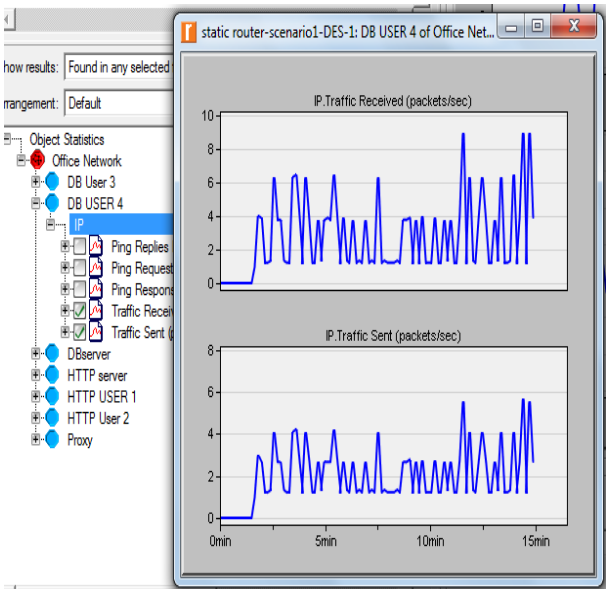


**Fig 11 DB User 4 traffic with no proxy and activation ACL for packet filtering.**

The results from scenario one concluded that stopping the attacker DB User 3 requires more than one control represent in the application layer which is a Proxy server and network layer which is a packet filter firewall (router). On the other hand, the other attacker DB User 4 still has access to the webserver. Solving these problems requires more segments and layers as it clears in scenario two. Although authorized users have access to the Web server in all tests.

## 8.2 Scenario Two: DMZ Segment

This scenario, discusses the results of the simulation after added more security layers (DMZ).

Figure 12 illustrates the internal network separated by router R3 for stations DB User 4 as the attacker and HTTP User 1and 2. In this Figure ACL of a router, R3 is modified to reject any IP sent packets to DB server. The result shows that attacker DB User 4 cannot receive a packet from DB server. The results indicated that the router R3 rejected attacker DB User 4 IP since more security layers and DMZ are added to scenario one. The security layer router R3 is added to create a new segment called DMZ which is placed between router R2 and router R3. Although HTTP users 1 and 2 still have the ability to access to the HTTP server.

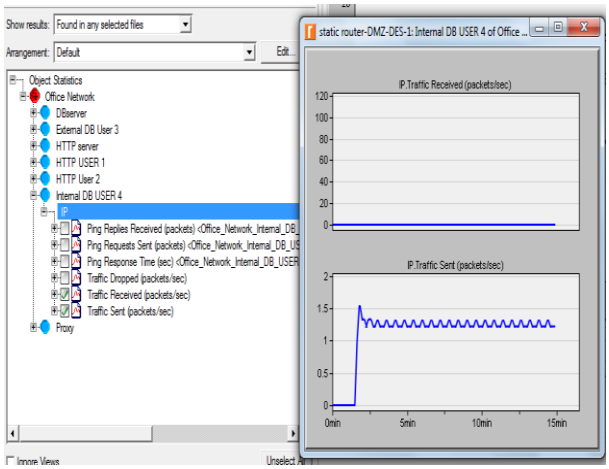


**Fig 12 DB User 4 after separated internal network**

The results from scenario two concluded that the DMZ implementation is a vital component that will help the network to be separated by a zone that would make it harder for the attacker. Moreover, DMZ will be able to restrict access to the database which means the attacker will need to make a deeper scan and find other methods to access the system. Therefore, the security strategies for the DMZ are required to prevent and detect malicious and other unauthorized communications

## 8.3 Scenario Three: Duplicate request with DMZ segment

In this scenario, discusses the results of the simulation after added two work stations to scenario 2.

Figure 13 explains the two work stations which are (DB and HTTP User5) and (DB and HTTP User 6). In this Figure User, 6 has the right to access DB server and HTTP server. The result shows that DB and HTTP User 6 cannot get a response from DB server since the ACL of router R3 rejected any IP tried to access DB server. On the other hand, when setting YES for connection to Database application in proxy, the User 6 can access the database. However, in this case, the risk remains because there is no protection at the application level. The results indicated that the ACL packet filtering guarantees that attackers DB user4 and DB user 3 cannot access DB server at the network layer and User 6 can access DB server. The results decided that solving these problems requires more modern technologies to treat such problems such as IPS, WAF, and DDOS protection.

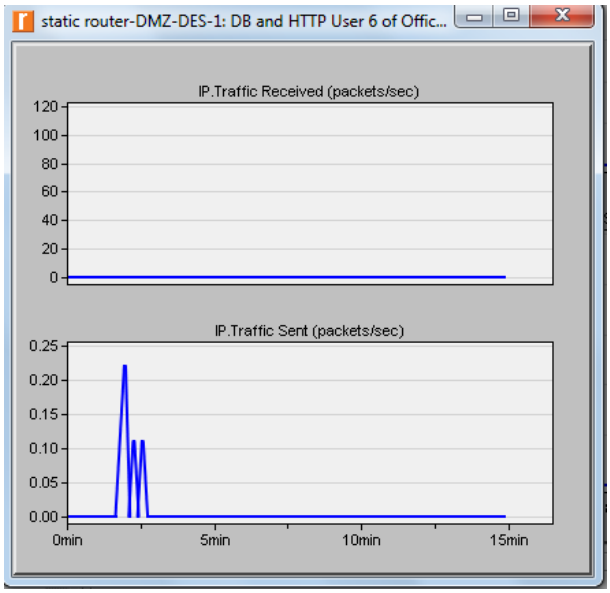


**Fig 13 DB and HTTP User 6 work stations**

The results from scenario three concluded that ACL will help the network to restrict access to the DB , also will create a logical log for the users who have the right to access DB server. In fact, this will make it more difficult for the intruder to penetrate and change the attacker's approach to use social engineering skills to gain the credential of the user who has access to the database.

# 9. CONCLUSIONS

This work has discussed the perimeter network security framework to provide an additional layer of security in a Libyan bank. The approach focuses on network security and application security since these two components form the core

of cyber banking, as transactions happen through the network and available applications. The proposed framework represents the low level of technical security controls that will enforce high-level security controls. 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 DMZ and without DMZ. OpNet simulation has been used to build three indicative scenarios and results are discussed. The results show that in the first scenario of simulation, in which configuring the network parameters without the DMZ segment will allow resources even to use by unauthorized users. Also in the second scenario when configuring the network parameters with a DMZ segment, the router rejected the attacker to access the HTTP server. The results in the third scenario shown that the ACL packet filtering guarantees that unauthorized users cannot access DB server at the network layer and authorized users can access DB server when duplicate requests with DMZ segment. The results have shown that DMZ solves many critical performance problems. To whole up, DMZ is not only to improve network security, but it is also to improve network performance. However, acquiring the necessary systems is not enough; the security personnel equally need to be prepared with the skills that are necessary to carry out their jobs.

## 10. REFERENCES

[1] G.Gopalakrishna. "Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds", RBI, Mumbai, Maharashtra, January 2011 Available: https://rbi.org.in/ scripts/ Notification User.aspx?Mode=0&Id=6366.

[2] Zahoor, Z., Ud-din, M., and Sunami, K, "Challenges in privacy and security in banking sector and related countermeasures", International Journal of Computer Applications, 144(3), 2016, 24-35. .

[3] Maharjan, R., and Chatterjee, J. M," Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal", LBEF Research Journal of Science, Technology and Management, 1(1), 2019.

[4] Boland, H. and Mousavi, H., Security issues of the IEEE 802.11 b wireless LAN. In Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No. 04CH37513) (Vol. 1, pp. 333-336). IEEE.

[5] Elmadani, M. (2015). The Study of Service Quality in Libyan Commercial Banks (Doctoral dissertation, University of Huddersfield).

[6] Ibrahim, A. (2017). Cash crisis pushes Libyans to virtual payments. Accessed Nov, 2018. In Australia Conference, Edith Cowan University, 75-82.

[7] Pack, J. (2017). Libya's Liquidity Crunch and the Dinar's Demise: Psychological and Macroeconomic Dimensions of the Current Crisis." US-LIBYA Business association Washington. Accessed Sep, 2018. http://www.us-lba.org.

[8] Elgahwash, F., Freeman, M. and Freeman, A.E., 2014. Improving online banking quality in developing nations: A Libyan case.

[9] Microsoft, "Security Threats", Microsoft Corporation, 2018. Accessed Feb, 2018 https://msdn.microsoft.com/en-us/library/cc723507.

[10] Angelakopoulos, G. and Mihiotis, A., 2011. E-banking: challenges and opportunities in the Greek banking sector. Electronic Commerce Research, 11(3), pp.297-319.

[11] Alabed, S.H. and Hanandeh, R., 2013. The Impact of Implementing Information Security Management Systems on E-Business Firms: Case Study in Jordanian Banking Sector. Middle East University.

[12] Ogunwobi, Z.O., Folorunso, S.O. and Alebiosu, O., 2016. Evaluation of Computer and Network Security Strategies: A Case Study of Nigerian Banks. In *OcRI* (pp. 85-90).

[13] Tytarenko, O., 2017. *Selection of the best security controls for rapid development of enterprise-level cyber security*. Naval Postgraduate School Monterey United States.

[14] Dart, E., Rotman, L., Tierney, B., Hester, M. and Zurawski, J., 2014. The science dmz: A network design pattern for data-intensive science. Scientific Programming, 22(2), pp.173-185.

[15] Rababah, B., Zhou, S. and Bader, M., 2018. Evaluation the Performance of DMZ. *Assoc. Mod. Educ. Comput. Sci*, pp.0-13.

[16] Madje, Uma. "Design And Analysis Of Network Security Model." In Proceedings of the International Conference 69th IRF International Conference, Pune, India, 19th March, 2017.

[17] Puthal, D., Mohanty, S.P., Nanda, P. and Choppali, U., 2017. Building security perimeters to protect network systems against cyber threats [future directions]. *IEEE Consumer Electronics Magazine*, *6*(4), pp.24-27.

[18] ISO/IEC 27033-4. "Information Technology - Security Techniques - Network Security - Part 4: Securing Communications Between Networks Using Security Gateways" , 2014, Single user license, ISO Store Order: OP-177008.

[19] - Byres, E.J., J. "Automation IT: Defense in Depth - ISA". 2012. Accessed June,2018. https://ww2.isa.org/standards-publications/isa-publications/intech-magazine/2012/december/automation-it-defense-depth/

[20] Launius, S., 2009. Securing the Network Perimeter Of A Community Bank'. *SANS Institute*, pp.1-41.

[21] Shrimali, S., 2017. DeMilitarized Zone: Network Architecture for Information Security. *Int. J. Comput. Appl*, *174*(5), pp.16-19.