Improve the Network Performance By using Parallel Firewalls

Sabry NASSAR
Atomic Energy Authority,
Cairo, Egypt.
sabry_nassar@yahoo.com

Ayman EL-SAYED (IEEE Member)
1. Faculty of Electronic Eng., Menoufyia University, Menouf, Egypt.
2. Community College in Alquwayiyah, Shaqra University, KSA
ayman.elsayed@free.fr

Nabil AIAD
Atomic Energy Authority,
Cairo, Egypt.
n_ayad51@yahoo.com

Abstract- **The network security nowadays has become a major priority for both network design and implementation to protect the valuable applications, sensitive data, and network resources from unauthorized access. The firewall is one of the network security devices which effective in defending known intrusions. This paper provides an overview of network firewalls, its importance, and different types of network firewalls, studying the effect of implementing the firewall on the network performance and how using parallel firewalls. We note that by using parallel firewalls the network performance is improved in order to limit the network delay and average response time.**

I. INTRODUCTION

Network security becomes an ever increasingly critical element of any network designs and implementations. A typical network security involves the planning and design of an organization's networks and information technology (IT) security infrastructures, so as to protect its valuable applications, sensitive data, and network resources from unauthorized access. Unauthorized access causes misuse and damage of the organization valuable resources. Such resources could be information, hardware, and software [6]. The information security management has to insure three requirements of the organization's information resources: (1) availability, (2) integrity, and (3) confidentiality. Availability: is the assurance that a computer system is accessible by authorized users whenever needed. Integrity: is the protection of system information or processes from accidental unauthorized changes. Confidentiality: is the protection of information within systems so that unauthorized people and processes cannot access that information [11].

The authors in [16] proved that when firewall filtering is involved, due to the filtering of unwanted traffic, network performance can increase considerably. So the employment of firewalls is not only essential for improved network security but also they contribute to meeting service level agreements and improving quality of service not only in terms of availability, but also in terms of performance. Finding show that, the intuitive belief about firewalls that security and performance efficiency are inversely proportional does not necessarily hold in every situation.

In our research we give an overview of network firewalls definition, its types and we study the impact of applying firewall of application proxy type on different network performance parameters in simulated environment. In our network model we try to involve the most available applications that used in the most of recent networks, such as File Transfer Protocol (FTP), Hyper Text Transport Protocol (HTTP), mail, Multimedia, and Data Base (DB) servers. The experimental results of different network performance parameters are measured and reported using OPNET IT GURUE Academic Edition simulator.

The remainder of the paper is organized as follows: the firewall is described in section 2. In the section 3, the network models with/without firewall are presented. Our parallel firewall is explained in the section 4 and the results and discussion of our suggested firewall are shown in the section 5. Finally, the paper is concluded in section 6.

II. FIREWALL

Firewall is a hardware or software solution implemented within the network to enforce security policies by controlling network access. The traditional function of firewalls has evolved from the original function of protecting a network from unauthorized external access [6]. Today's firewalls inspect and filter traffic arriving or departing a network by comparing packets to a set of rules and performing the matching rule action, which is accept or deny [5]. In general, firewalls can offer data privacy (confidentiality), integrity, and availability. A firewall is often seen as the first step toward a network security solution.

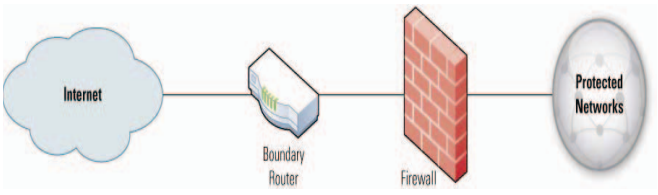


Fig. 1. Packet Filter Used as Boundary Router

Types of Network Firewalls***: Packet filters*** examine incoming and outgoing packets and apply a fixed set of rules to the packets to determine whether they will be allowed to pass. The packet filter firewall is typically very fast because it does not examine the data in the packet. It simply examines the type of the Packet along with the source and destination addresses, including URLs, domain names, etc., as well as the port combinations, and then it applies the filtering rules [6]. Figure1 shows the packet filter firewall used as boundary router [13].

Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer. As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule, but unlike packet filtering, stateful inspection keeps track of each connection in a state table. While the details of state table entries vary by firewall product, they typically include source IP address, destination IP address, port numbers, and connection state information. Three major states exist for TCP traffic connection establishment, usage, and termination [13].

Application-proxy gateway is a feature of advanced firewalls that combines lower layer access control with upper layer functionality. These firewalls contain a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between the two hosts. 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 as shown in Figure 2.

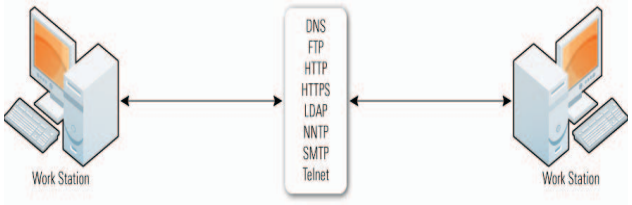


Figure 2: Typical Proxy Agents

The proxy gateway operates at the application layer and can inspect the actual content of the traffic which means that it breaks down the data and examine packet content distinguishing between normal traffic for a specific protocol and traffic that could contain exploits for known flaws. The advantages of Application-Proxy gateway compared to packet filtering and stateful inspection are:

1. An application-proxy gateway offers a higher level of security because it prevents direct connections between two hosts and it inspects traffic content to identify policy violations.
2. They have more extensive logging capabilities because they can examine an entire packet rather than just network addresses and ports.

The disadvantages of Application-Proxy gateway compared to packet filtering and stateful inspection are:

1. Because of the "full packet inspection" of application-proxy gateways, the firewall spends much more time reading and interpreting each packet compared to packet filtering firewall.
2. The limited in supporting a newer network application and protocols so an individual, application-specific proxy agent is required for each type of network traffic that needs to transit a firewall [13].

III. NETWORK MODELS

Our network model consists of different scenarios. First scenario as shown in Figure 3 that represents a computer network that consists of four LANs connected by a backbone switch. Each LAN consists of 100 workstations (users). The router used to connect the internal network to external world (Internet), and a four application servers represents the most applications user can use. These application servers are FTP, HTTP, mail, multimedia, and DB server. In this scenario no firewall applied which means that any user can access any applications without any access control. So this scenario named "without firewall".

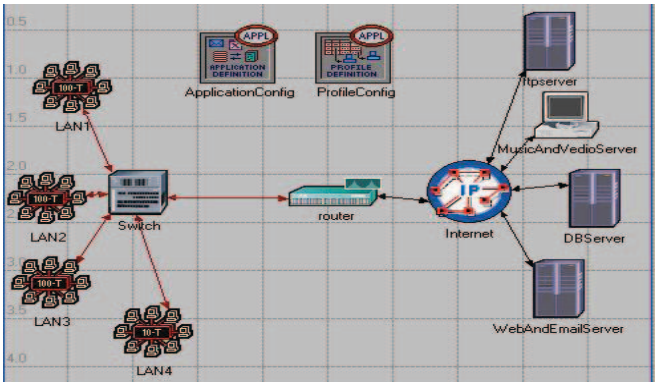


Fig. 3. Network model without Firewall.

The second scenario as shown in Figure 4 model the same network with firewall added so this scenario named "Proxy firewall". The firewall type implemented in this paper is application proxy firewall which working on the upmost OSI layers and the firewall policy applied will depend on the application type.

Firewall configuration: As mentioned above the firewall in this network model with type of application proxy firewall so the security policy (permit/deny) applied depends on the application type [13]. And the firewall configured to block or permit a specific application by configuring the proxy server

information in a firewall attributes. Here we will prevent the users from accessing multimedia and FTP applications and permit other applications to be accessed.

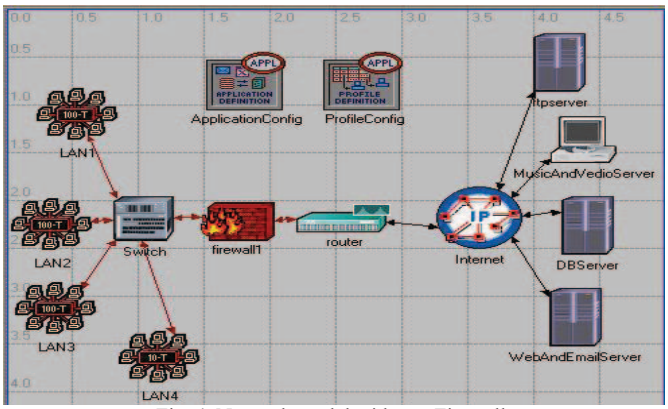


Fig. 4. Network model with one Firewall.

IV. NEW SUGGESTED FIREWALL

We will implement a two identical firewall in a parallel fashion and the complete security policy applied on every firewall and we divide or distribute the network traffic to two firewalls by specifying every firewall to serve or monitor only a part of network user's traffic not all network users' traffic as in traditional firewall in the second scenario" Proxy firewall". .The network design after applying two parallel firewalls shown in figure 5 which is the third scenario of simulation called "2proxyfirewalls".

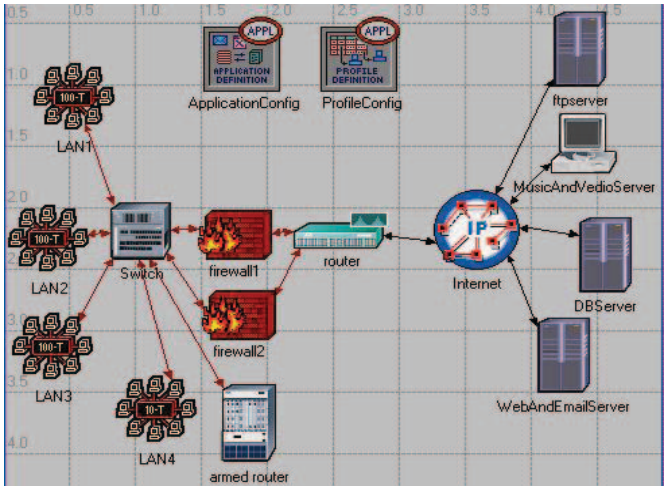


Fig. 5. Network model with two parallel Firewalls

The new approach, as shown in Figure 5, consists of two identical parallel firewalls connected to the backbone switch which the inbound and outbound traffic from and to external world (internet) is filtered and security policy (permit/deny) which applied to the firewall in the second scenario is completely applied to every firewall in our approach of parallel firewalls.

The virtual local area network (VLAN) [6] technology is used to segment the network logically into two VLANs every VLAN traffic monitored or filtered by one of the two firewalls. Because of the VLANS is completely isolated from each other so the armed router used to enable the inter VLAN communications. We suggest this solution of two parallel firewalls architecture to improve the performance parameters which affected by applying single firewall in a traditional fashion. Some of these parameters are the average Ethernet delay which increased and the average page response time of http server which also increased due to the usage of traditional firewall. Creating VLANs improves network performance and security by controlling broadcast propagation and requiring that communications between these broadcast be carried out by a Layer 3 device that is capable of implementing security features [9].

V. SIMULATION AND RESULTS ANALYSIS

Most researchers perform testing and studies in experimental or simulated environments, due to the high risk of performing tests in a real environment. In this paper we present a study based on OPNET IT Academic Edition 9.1A [14].

We are using OPNET for our research because of the several benefits it offers. OPNET provides a GUI for the topology design, which allows for realistic simulation of networks, and has a performance data collection and display module. Another advantage of using OPNET is that it has been used extensively and there is wide confidence in the validity of the results it produces. OPNET enables realistic analysis of performance measures [15].

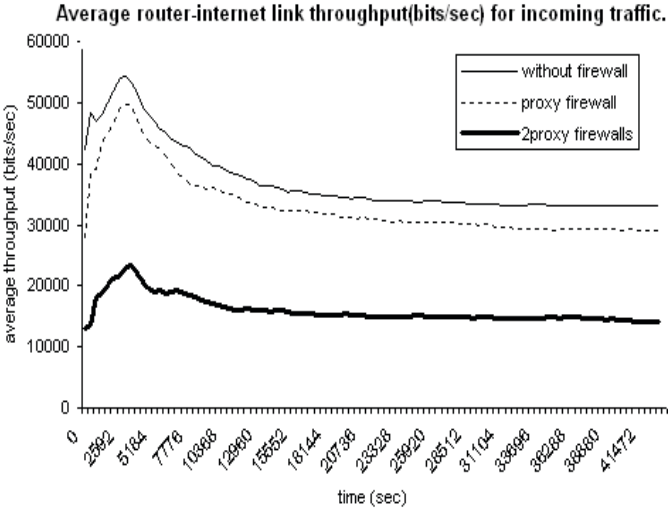
A. Simulation Environment

The Simulator is running on a Notebook PC Compaq Hp Presario CQ61-105EE (Intel Pentium Dual-Core Mobile Processor T3400, 2.16 GHz and 2048MB DDR2 SDRAM (2 Dim)) with operating system Windows Vista Home Premium (32-bit) with Service Pack 1. VMware tool is used to create another machine with windows XP that OPNET IT Guru simulator is installed on.

B. Simulation Results

We configure simulation statistics that help in studying the different network performance parameters and the effect of applying firewall as a security device on these parameters. After running the simulation the results of every scenario are collected and compared in the same figure for three scenarios "without firewall", "Proxy firewall", and "2proxyfirewalls. Figure 6 shows the average database query response time measured in seconds. From the figure we can see that there is no significant change in the average database query response time due to applying single firewall but after implementing two parallel firewalls this average time decreased by noticeable amount.

Figure 7 show the average utilization of the router-internet link in the two directions. From the figures we note that applying a single firewall give an improvement in the link utilization in the two directions because of the firewall prevents the un-useful traffic from saturating the internet-router link and our approach of parallel firewalls will give more decrease in router-internet utilization compared to single firewall which increase the improvement of link utilization.



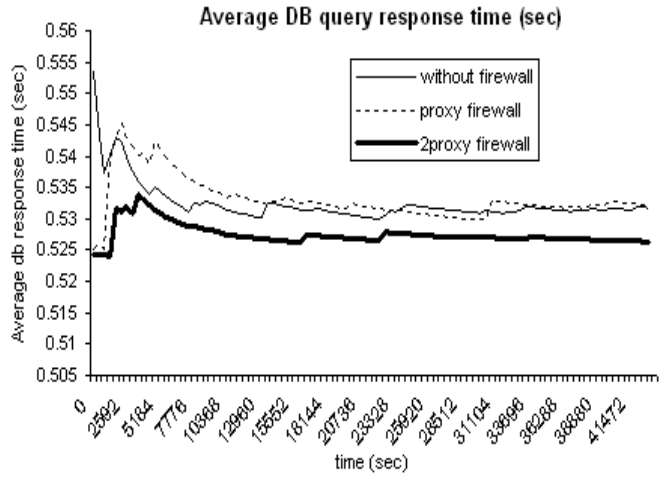
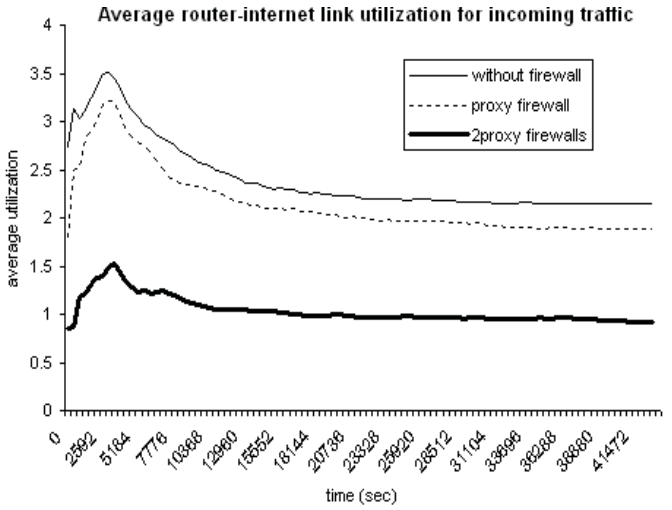


Fig. 6. the average database query response time

Figure 8 show the point to point throughput (bits/sec) in two direction of router-internet link.

In this paper the throughput means the amount of traffic which passes through the link in a specific period of time. And we measure the average throughput of router internet link so small values of average throughput of link are preferable. From the figures we note that applying single firewall will give a noticeable decrement in the average link throughput in the two directions which leads to improvement of link performance and our approach of parallel firewalls will give more decrease in the average link throughput in the two directions compared to single firewall which increase the improvement of link performance.



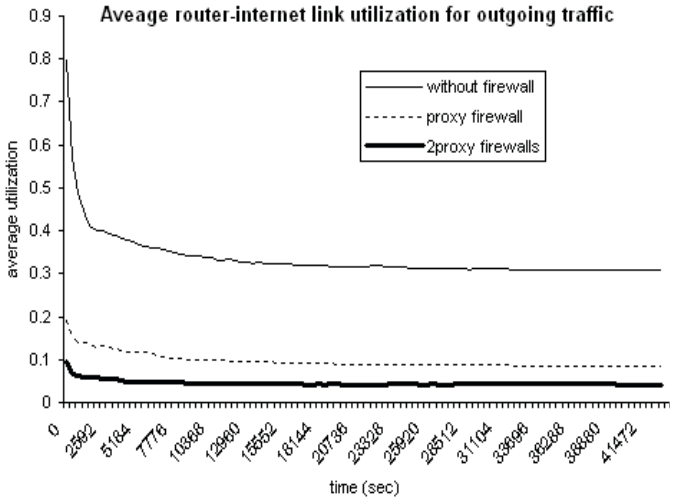


Fig. 7. The average utilization of the router-internet link in the two directions.

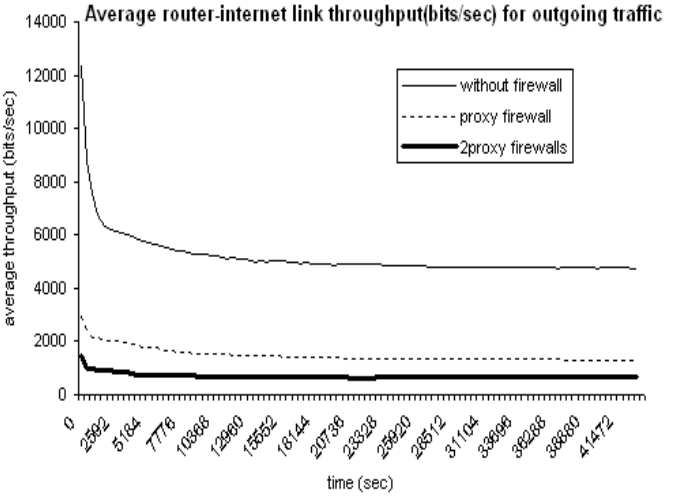


Fig. 8. Average point to point throughput in two directions.

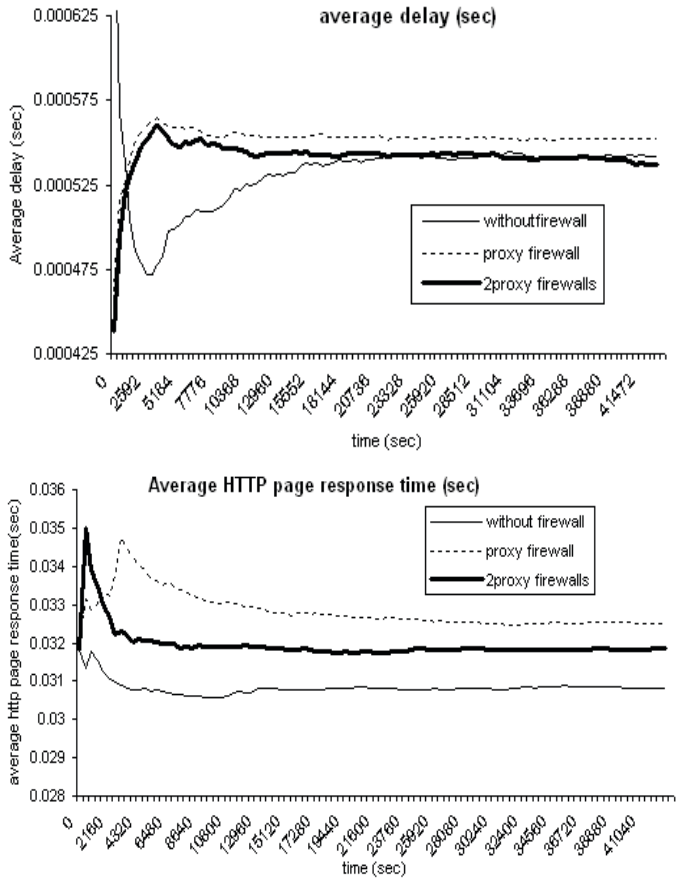


Fig. 9. the average Ethernet delay and the average page response Time.

Figure 9 shows the average Ethernet delay in the network From the figure we note that applying single firewall to the network will increase the average delay because of the application proxy firewall take or spends much more time in a "full inspection process" for each packet which increases the total average network delay which represents a problem especially in networks which have applications more sensitive to time as e-business, financial. Also the average page response time of http server shown in figure 10 increased by a noticeable value due to the firewall overhead added caused by full inspection process of packets which also represent a problem. So we can say that adding a single firewall to the network will give an improve in some performance parameters at the same time it has some drawbacks with other performance parameters as increasing delay (latency) and page response time which is not a simple problem.

Our approach of parallel firewalls will solve this problem as shown in Figures 9. The amount of delay caused by a single firewall is decreased by noticeable value also the increment in page response time decreased by a noticeable value.

From a reliability point of view, the parallel firewall architecture provides an increased amount of reliability because it overcomes the single point of failure in a single firewall device configuration [13], if the firewall fails then the Internet connection becomes unavailable. In a parallel configuration, having a single device fail does not block Internet access totally.

VI. CONCLUSION

In this paper we studied the firewall principles and types. Also we reported the experimental results of simulation of application proxy firewall using OPNET simulator. From these results we can conclude that the firewall deployment has some benefits and drawbacks with respect to network performance. Some of firewall benefits are improvement link utilization and throughput. The main drawbacks of applying firewall (application proxy) are the delay produced due to full inspection process. The parallel firewalls technique used in this paper is not only solving some problems of traditional firewall as delay and average response time of http server but also improve the most of network performance parameters. Finally we can say that the parallel firewall is cost effective from the performance point of view and the firewall only cannot provide all security requirements of a modern network but it can be considered as the first step toward a network security solution.

REFERENCES

[1] W. Stallings, Cryptography and Network Security, Fourth Edition, Pearson, Prentice Hall, 2009.

[2] Horvath, M.R. Fulp, E.W. Wheeler, "Policy Distribution Methods for Function Parallel Firewalls," international conference on computer communication and networks, US Virgin Islands, 2008.

[3] Yusuf Bhaiji, CCIE Professional Development Network Security Technologies and Solutions, Cisco Press, 2008.

[4] Koht-arsa, K. Sanguanpong, "A practical approach for building a parallel firewall for ten gigabit Ethernet backbone," Security Technology, 2008, ICCST 2008. 42nd Annual IEEE International Carnahan Conference, Prague, 2008.

[5] Ryan J. Farley, Errin W. Fulp, "Effects of processing delay on function-parallel firewalls," international conference on Parallel and distributed computing and networks, Austria, 2006.

[6] Kowk T. Fung, Network Security Technology, CRC Press, August 2005.

[7] Errin W. Fulp , Stephen J. Tarsa, Trie-Based Policy Representations for Network Firewalls, Proceedings of the 10th IEEE Symposium on Computers and Communications (ISCC'05), p.434-441, June 27-30, 2005.

[8] David W Chadwick, "Network Firewalls Technology," IS Institute, University of Salford, Salford, England, 2004.

[9] Steve McQuerry, Interconnecting Cisco Network Devices, 2nd Edition, Cisco Press, November, 2003.

[10] John E. Canavan, Fundamentals of network security, Artech House telecommunications library, 2001.

[11] Alaiddin M. Tayeh, "Effectiveness of Information Security Management at the Palestinian Information Technology Companies," Master thesis, Islamic University of Gaza, Palestine, 2008.

[12] Carsten Benecke, "A Parallel Packet Screen for High Speed Networks," acsac, pp.67, 15th Annual Computer Security Applications Conference (ACSAC '99), 1999.

[13] NIST SP 800-41, Guideline s on firewalls and firewall policy, (Jul. 2008).

[14] OPNET online documentation 8.0.C, OPNET Technologies, Inc., Washington DC.

[15] Shabana Razak, Mian Zhou, and Sheau-Dong Lang," Network Intrusion Simulation Using OPNET," University of Central Florida, Orlando.

[16] H. Garantla, and O. Gemikonakli," Evaluation of Firewall Effects on Network Performance," School of Engineering and Information Sciences, Middlesex University, London, 2009.