International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 13 No. 2 Feb. 2015, pp. 398-413

http://www.ijisr.issr-journals.org/

Investigating the Relationship between Firewall Security and Network Performance in a Distributed System

Francis Kwadzo Agbenyegah[1], Michael Asante[2], and Alexander Osei-Owusu[3]

[1]Lecturer, school of Computer Science,
Data link University College,
Tema, Ghana

[2]Senior Lecturer, Head of Department,
Department of Computer Science, Kwame Nkrumah University of Science and Technology,
Kumasi, Ghana

[3]Research Coordinator, Graduate School,
Ghana Technology University College,
Accra, Ghana

ABSTRACT: This research work investigated the firewall security and performance relationship for distributed systems. The relation between the security and performance efficiency is presented through different scenarios and the relationship between security and performance in firewalls is evaluated. Emphasis is on the relationship between network security and performance; the effects of firewalls on network performance. Various scenarios were evaluated through simulations using OPNET IT Guru Academic Edition 9.1 to show the effects of firewalls on network performance. The result shows that the network security does not have a direct correlation to network performance.

KEYWORDS: Firewalls, network security, network performance, OPNET.

1 INTRODUCTION

Internet connectivity is growing massively and most enterprises are migrating to the use of web based services for services provision [6]. As enterprises take on the Internet as a new business tool whether to sell, to collaborate or to communicate – web applications have become the new weakest link in the organization's security strategy [12]. Technological innovations are fundamentally changing the way people live, work, play, share information and communicate with each other [12]. This is seen to be sharpening organizations competitive edge as it provides customers, rapid access to information. Firewalls provide a mechanism for protecting these enterprises from the less secure internet over which customers or collaborating partners transfer packets destined for the corporate network [1].

Network Firewalls protect a trusted network from an untrusted network by filtering traffic according to a specified security policy. A firewall is often placed at the entrance of each private network in the Internet. The function of a firewall is to examine each packet that passes through the entrance and decide whether to accept the packet and allow it to proceed or to discard the packet. A firewall's basic task is to regulate some of the flow of traffic between computer networks of different trust levels. Typical examples are the Internet which is a zone with no trust and an internal network which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter network" or Demilitarized zone (DMZ) [12].

2 RELATED WORK

[5] defined a security policy as a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide. According to the authors this is an ongoing process, with regular reviews and auditing of security policies and mechanisms, providing feedback to improve the security policy.

[4] Postulate that it is extremely important to involve the users in the implementation of a security policy. Understanding of security problems by users, and giving them clear and easy to follow rules, can be a key factor in the successful implementation of the policy.

According to [9] Security policies protect the confidentiality, integrity, and availability of the assets of an organization. To enforce this, security services should be deployed, such as authentication, encryption, antivirus software and firewalls

[11] Argued that the access control part of the security policy deals with making sure that authorized individuals can perform the tasks they are authorized to and those others cannot. It is typically referred to as the 'access control policy'. According to [3], in terms of networks, the most commonly used access control mechanisms are firewalls and filtering routers.

[3] Argues that firewalls control access to resources by filtering network traffic, only allowing access that is specified by the security policy.

According to [9], the protection that these firewalls provide is only as good as the policy they are configured to implement. The policy should be clear, concise, and easy for the administrator to follow. [7], argued that if a policy is not well designed, then it will not be enforced properly and the security goals will not be met

[10], state that the configuration of a firewall is probably the most important factor in terms of the security a firewall provides

According to [2] ,[8], firewall policies are made up of rule sets, and these rule sets are ever expanding due to new rules continually being added and very few removed, so device access policies tend to be large and always increasing in size.

[8], showed that, for most firewalls, the ordering of the rules in a rule set are important, as in the common 'first match' filtering mechanism, the position of the rules in the rule set dictate if they are matched against traffic or not. The earlier in the rule set the higher the priority the rule has when matching against traffic

3 METHODOLOGY

The main aim of this study was to evaluate the performance of a distributed system against firewall security policy. The relationship between performance and security under three (3) different scenarios were evaluated:in particular the research sought to evaluate the performance of a network incorporating firewalls, some networks were modeled with and without firewalls and different firewall functionality and simulated such networks with an eye on their performances.

NO FIREWALL SCENARIO

The internet used across this simulation is done for 300 workstations and it is simulated in a way that, the 150 workstations access the database application and 100 workstations use file transfer Protocol (FTP) to download and upload file onto the file server. Following are the performance metrics used for the performance evaluation of internet when there is no security across the internet.

- DB query time and response time for the database application are estimated
- Ftp download response time and upload response time
- Node level statistics like server DB query response time and load are also estimated for the database application
- Link level and utilization statistics are also estimated across the simulation process
- Data throughput which is the amount of data transferred in the network per time unit is evaluated through statistics like Traffic Received and Traffic Sent (bits/sec) which indicates the value of throughput. A more efficient network should allow more traffic to pass that leads to larger throughput.
- Packet Delay
- Traffic drop
- Task processing time of the server is also evaluated

- Jitter: Packets arrive at destination with variable delay. Jitter depends on the congestion of the network. In computer networks, the term jitter means variations in delay of packets received. Jitter is an essential quality of service (QoS) factor in evaluation of network performance

The same performance metrics were used for the two scenarios. A packet size of 32MB (low), 100MB (medium) and 200MB (high) were imposed across the network and a link speed of 10Mbps, 1Gbps and 10Gbps were set between the router and the cloud and each of the above performance metrics was used to evaluate the behavior of each packet size with regard to the data rate to investigate applications performance.

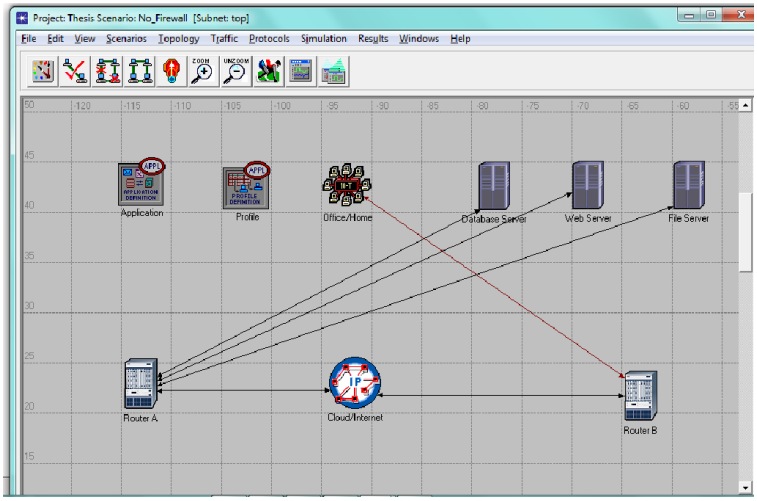

Fig.1 Network Layout (M. Asante ,F.K. Agbenyegah,A. Osei-Owusu (2014))

FIREWALL SCENARIO

The first scenario as shown in fig.1 is duplicated and the required firewall scenario was created. In this particular scenario a firewall router was created and a constant packet latency of 0.05 seconds was imposed for packet filtering. Similar performance metrics were used as in the first scenario.

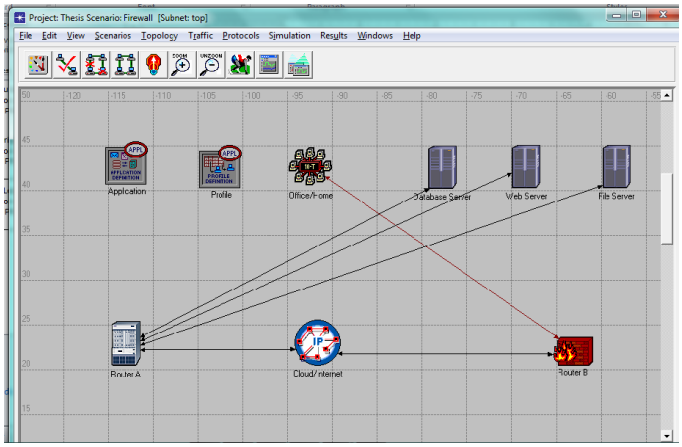

Fig.2 Firewall Scenario setup Network Layout (M. Asante ,F.K. Agbenyegah,A. Osei-Owusu (2014))

FIREWALL: WITH PACKET FILTERING CAPABILITIES SCENARIOS

This scenario is created by duplicating the fig. 2 scenario and the main aim of this scenario was to block the unauthorized applications access. After the three scenarios were created the simulation was run for two hours and the corresponding performance of the network was evaluated.

RUNNING THE SIMULATION

Once all the three scenarios had been set up, the simulation was run for two hours. It was run from the scenarios menu by choosing the manage scenarios option as shown below in fig. 3

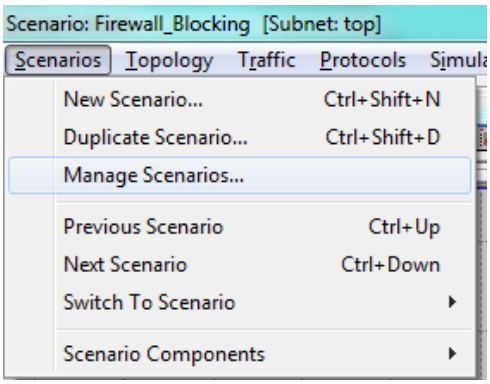

Fig. 3 Manage Scenario

With this option selected, a new window was opened and the simulation was run for two hours as illustrated in fig. 4 shown below

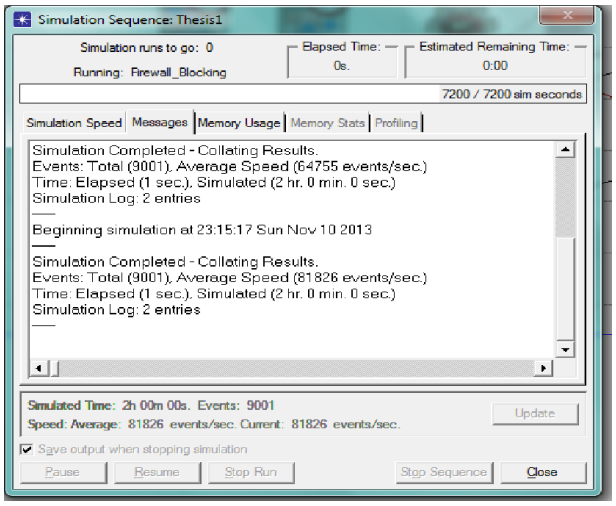

Fig.4 Running Simulation

Once the simulation was completed, the results were evaluated for all the three scenarios based on the performance metrics chosen and were compared with each other.

4 RESULTS AND EVALUATIONS

In this section, the result of the simulation of the three scenarios are presented and analyzed.

The evaluation was done based on;

- No Firewall scenario where there is no firewall security imposed on the network, so all the applications that generated the required traffic across the distributed system are allowed to pass through the router.
- Firewall scenario where a firewall is imposed to filter some packet of the other application
- The third scenario like the firewall with blocking capability where the ftp applications are blocked and only allowed the database application to pass through.

The performance of the database, and ftp applications were evaluated in this section based on the performance metrics chosen at all the three levels namely, global level, node level and link level. All the obtained graphs were compared against the performance metrics and a detailed analysis was given.

RESULT FOR DATABASE APPLICATION

The database application is one of the applications that generated traffic used in this simulation and the performance of the database application is estimated against the database query response time. A packet size of 32MB (low), 100MB (medium) and 200MB (high) were imposed across the network and link speeds of 10Mbps, 1Gbps and 10Gbps were set in-turn between the router and the cloud and the database query response time was evaluated in each packet size and data rate to investigate applications performance.

Database Query Response Time is the elapsed time between the end of an inquiry, query or demand on a computer system (e.g. Database server) and the beginning of a response; for example, the length of the time between an indication of the end of an inquiry and the display of the first character (result) of the response at a user terminal. The lower the query response time of a database operation, the higher the performance of the database application

DATABASE QUERY RESPONSE TIME - NO FIREWALL SCENARIO

This scenario allows all the applications to pass through the router without any filtering or restriction to the flow of traffic.

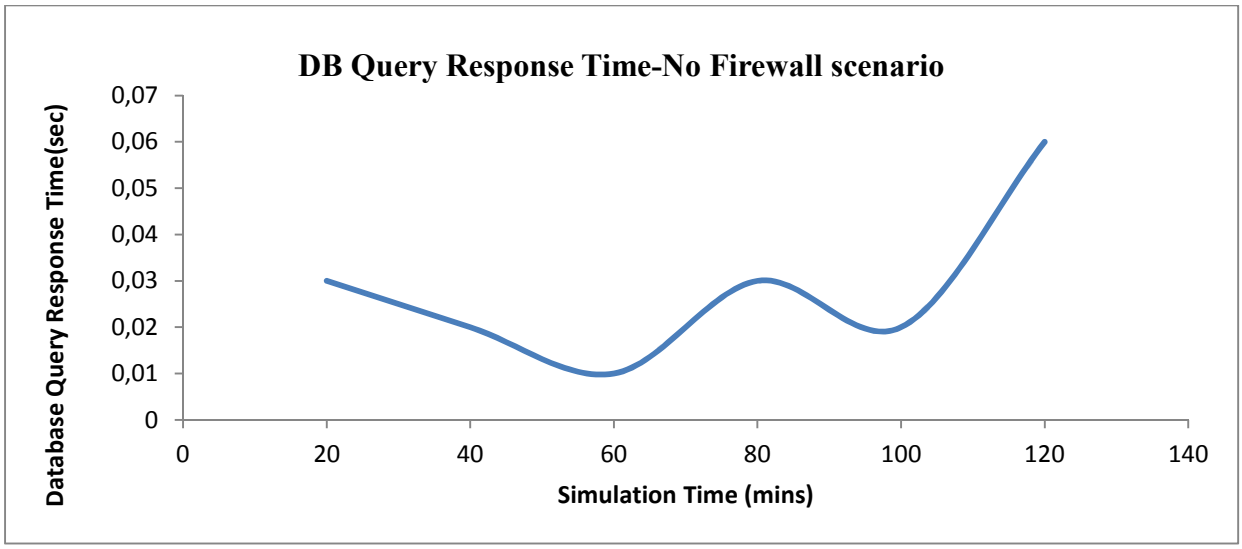

Fig. 5: Database Query Response Time - No Firewall Scenario

From Fig.5, the response time was constant throughout the simulation time with a value between 0.01 seconds and 0.06 seconds. As expected, since there is no restriction to the flow of traffic across the network, response time was smaller. When no security is implemented on the network, there is an easy flow of traffic through the router. As the packets gets to the router interface, there is no inspection of packets so the user request gets served quickly hence the low response value of 0.01 seconds.

DATABASE QUERY RESPONSE TIME - FIREWALL SCENARIO

In this scenario, a packet latency of 0.05 was imposed on the network to filter the packets. Latency is the time required by a system to complete a single transaction from start to finish. In this scenario, a latency of 0.05 introduces a delay of 50ms into the network.

The figure below shows the database response time when firewall was imposed on the network.

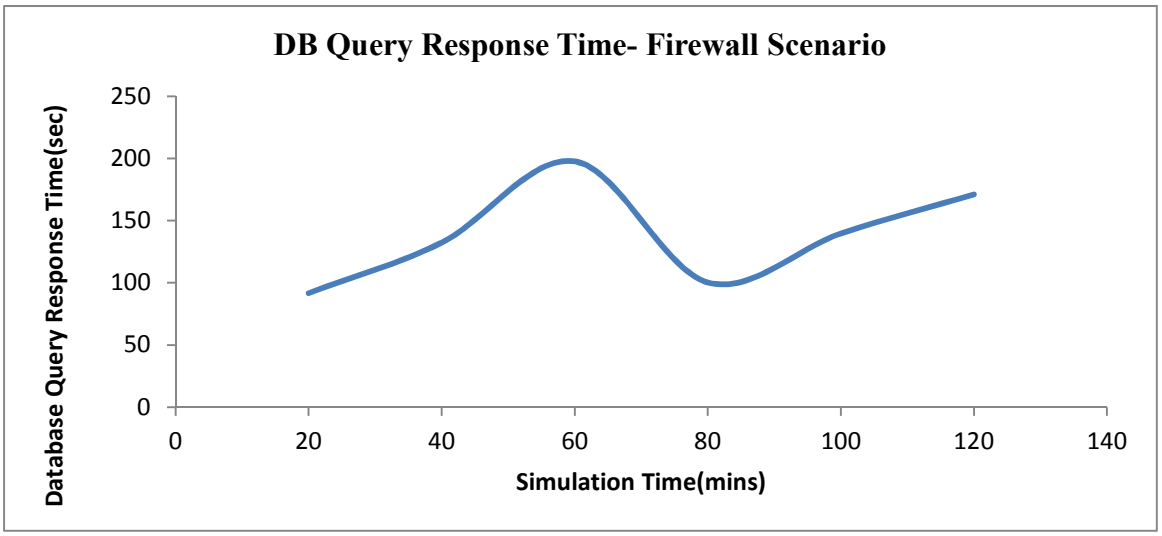

Fig. 6: Database Query Response Time - Firewall Scenario

From the fig. 6 above, the database query response time is as high as 197.60 seconds. This is due to the packet filtering imposed on the distributed system. When the distributed system has firewall protection, everything that goes in and out of it is monitored. The firewall monitors all this information traffic to allow 'good data' in, but block 'bad data' from entering computer network. Firewalls use packet filtering methods to control traffic flowing in and out of the network. Firewall software uses pre-determined security rules to create filters – if an incoming packet of information (small chunk of data) is flagged by the filters, it is not allowed through. Packets that make it through the filters are sent to the requesting system and all others are discarded. All these activities delay the response of the systems hence a high value in the database query response time.

DATABASE QUERY RESPONSE TIME - FIREWALL BLOCKING SCENARIO

In the third scenario, the functionality of the firewall is further increased incorporating filtering FTP traffic entering the system. The graph below in fig. 7 shows the database query response time when other application (ftp) is blocked. It has a high response time of 73.33 seconds. This is due to the fact that all other applications are blocked and only the database application goes through. As the packets reaches the firewall interface, the firewall looks at its filter table before making the decision to allow only the database packet to pass through hence the higher value of 73.33 sec since some packet filtering also occurs before decision are taken.

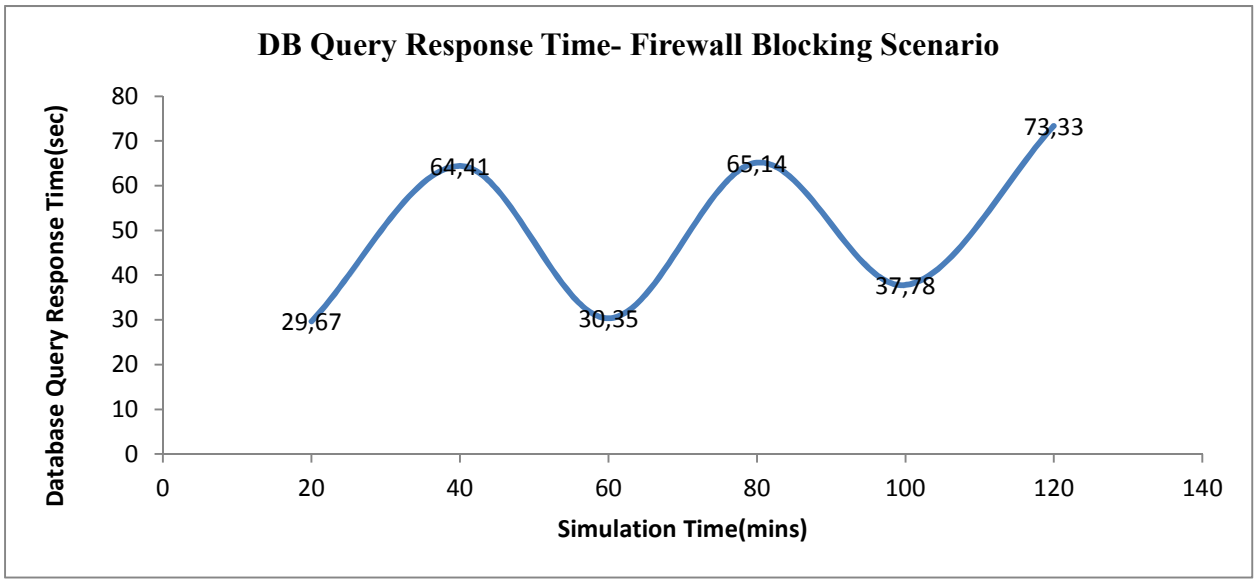

Fig. 7: Database Query Response Time - Firewall Blocking Scenario

SERVER DATABASE QUERY LOAD

The load on the database server was evaluated and analyzed in this section. The server database query load is in request per seconds. The higher the value of the server database query load, the longer user request from the database server waits and this degrades the performance of the server.

SERVER DATABASE QUERY LOAD - NO FIREWALL SCENARIO

The fig.8 shows the server loads across the network when no security policy is enforced.

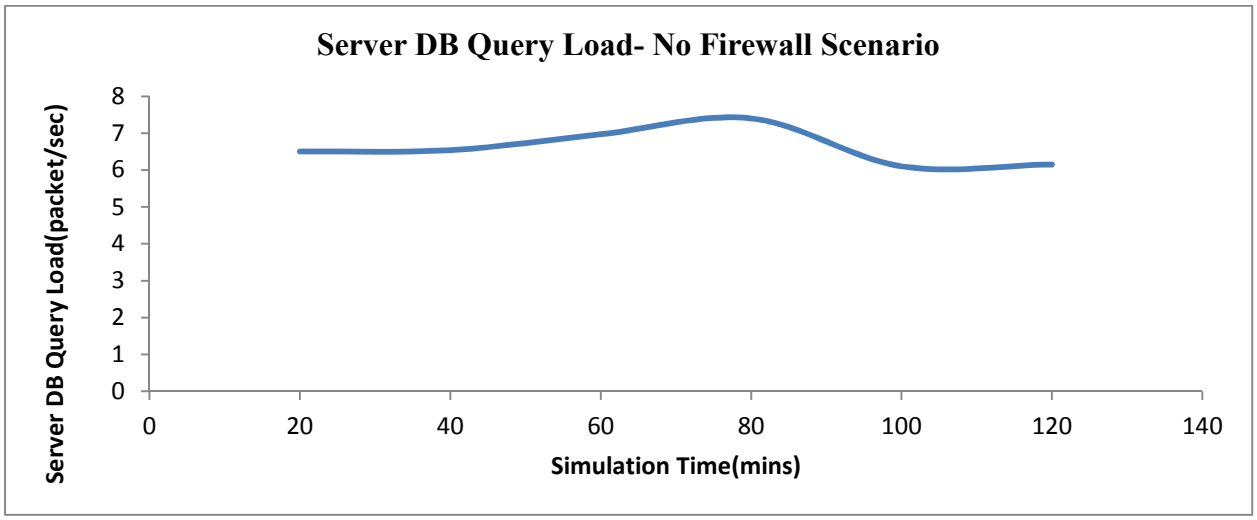

Fig. 8: Server Database Query Load - No Firewall Scenario

The higher load on the database server is as a result of a lot of request that goes through the router into the server. A database server (program) has defined load limits, it can handle only a limited number of concurrent client connections per IP address (and TCP port) and it can serve only a certain maximum number of requests per second. When a web server is near to or over its limit, it becomes unresponsive and this leads to a delay in user request.

When no security is applied, almost all the clients are connecting to the database server in a short interval, and this increases the load on the server since the server tries to process each request. The network slowdowns, so that client requests are served more slowly and the number of connections increases so much that server limits are reached.

SERVER DATABASE QUERY LOAD - FIREWALL SCENARIO

The fig.9 shows the load on the server when firewall is imposed on the network. As expected, the load on the server is very low when security is enforced across the network. Since most of the unwanted traffic have been blocked, only the legitimate packets goes into the server, so it quickly response to the user request hence the low value.

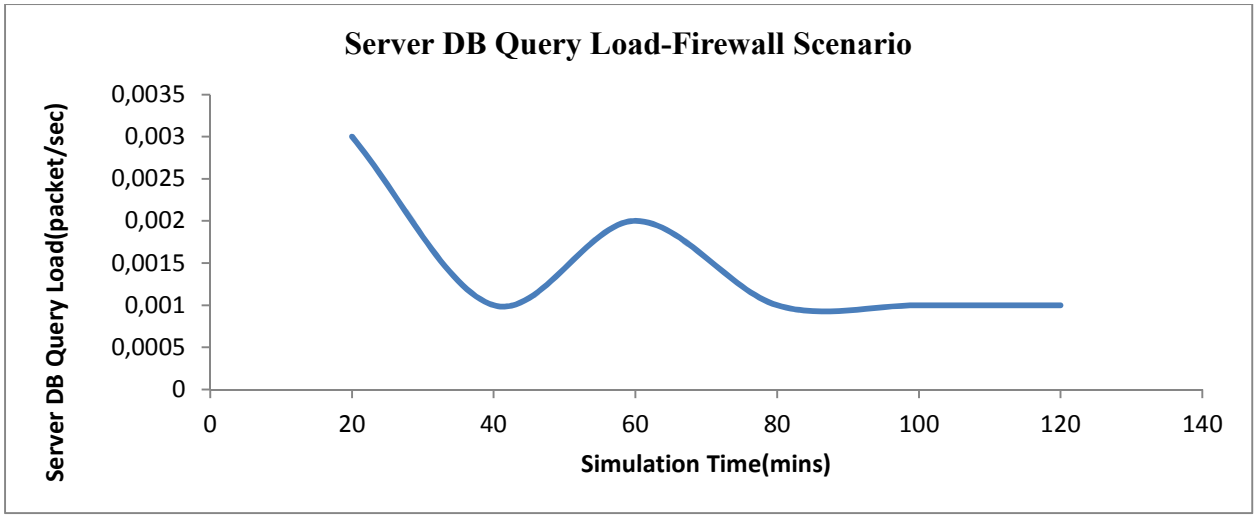

Fig. 9: Server Database Query Load - Firewall Scenario

From the graph, it has a higher value of 0.003 seconds during the iniatial stage and drops to 0.002 seconds and finally with 0.001 seconds. This shows that when firewall is imposed, because of the filtering of the unwanted packets, only some small legitimate packets goes to the server, hence the low load. When firewall is imposed, it limits the number of request that goes to the server for processing hence the lesser load on the server.

SERVER DATABASE QUERY LOAD - FIREWALL BLOCKING

In the third scenario, the FTP applications are blocked and only the database application is allowed access through the router.

The load on the server is high and almost equals the value when no firewall is imposed. In this scenario, all the applications are blocked and only the database application gets to the server, hence the higher load.

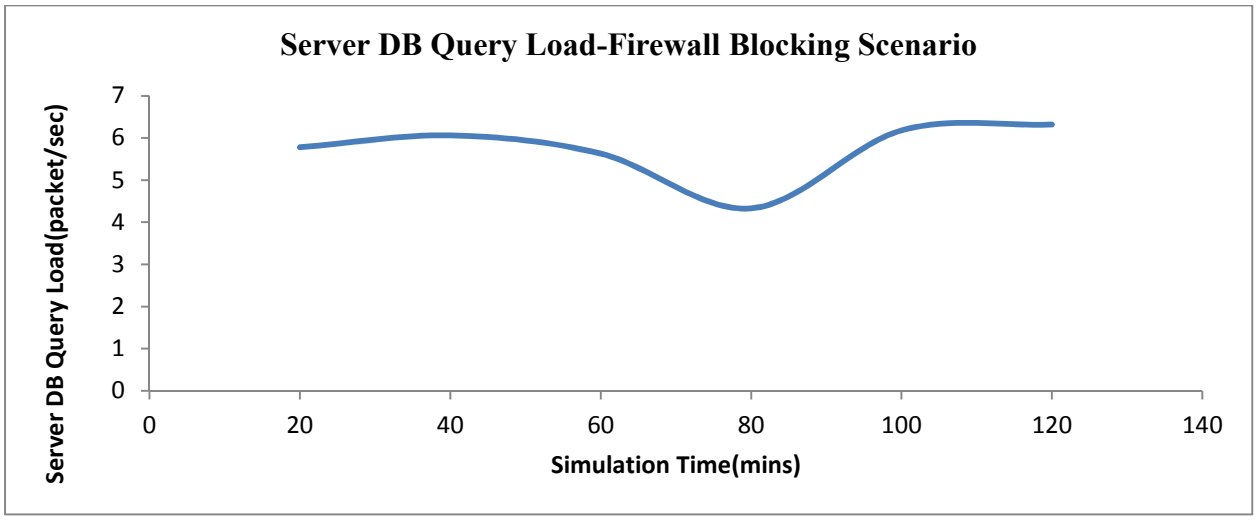

Fig.10: Server Database Query Load- Firewall Blocking Scenario

From the figure 10 above, it has an initial load of 5.78 seconds and later increase to 6.06 seconds and later has a value of 6.32 seconds. As expected, the load on the server in this case is high because the database application goes into the server without any restrictions hence the higher value. Combining the behaviour of graphs for figure.8, 9, and 10, the resultant graph is shown below in fig.11

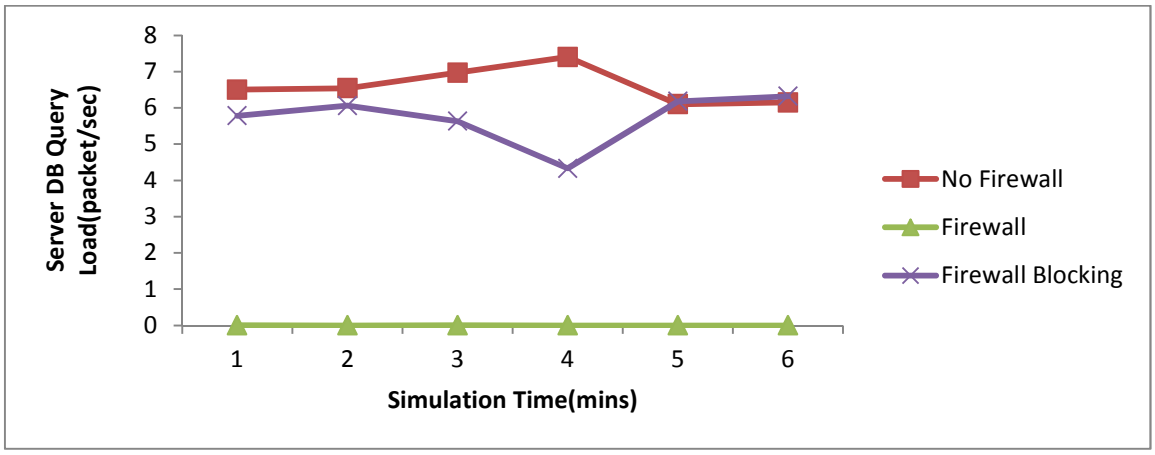

Fig 11: Server Database Query Load

From the graph, it can be seen that the load on server is almost equal in the case of firewall blocking and no firewall scenario. It has a low constant value when firewall is imposed on the networked. Since the firewall allows only legitimate packets access into the server, only packets that conforms to the security policy of the organization get pass through the firewall hence the low load on the database server when security is implemented

RESULT FOR FTP APPLICATION

This section discusses about the ftp application, which is one of the applications that generated traffic used in the simulation experiment. Ftp application is evaluated against download response time and upload response time. The load on the ftp server is also evaluated to investigate the performance of the network under the three different scenarios.

FTP DOWNLOAD RESPONSE TIME – NO FIREWALL SCENARIO

The fig. 12 below shows the ftp download response time when no firewall is imposed on the network. The result shows a low/quick download response time when no security is imposed on the network. Since there are no restrictions to the flow of traffic across the network, it leads to a faster response time. It can again be observed that the ftp download response time is not constant but varies along the simulations. It has a initial value of 0.11 seconds and then rise to 0.12 seconds and then drops again to 0.12 seconds.

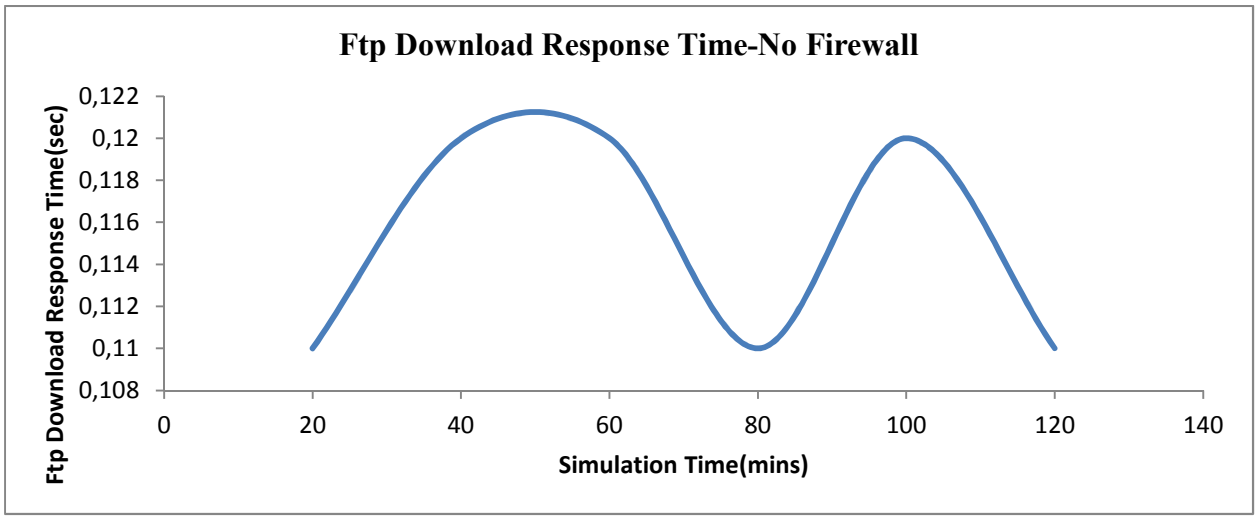

Fig.12: Ftp Download Response Time – No Firewall Scenario

FTP DOWNLOAD RESPONSE TIME - FIREWALL SCENARIO

When firewall was implemented, the download response time has a high value of 28.23 seconds when a packet size of 200MB is considered. The higher value is as a result of the overhead encounter by the firewall when processing the request and also the packet latency of 0.05 imposed to induce some delay into the system as in fig.13.

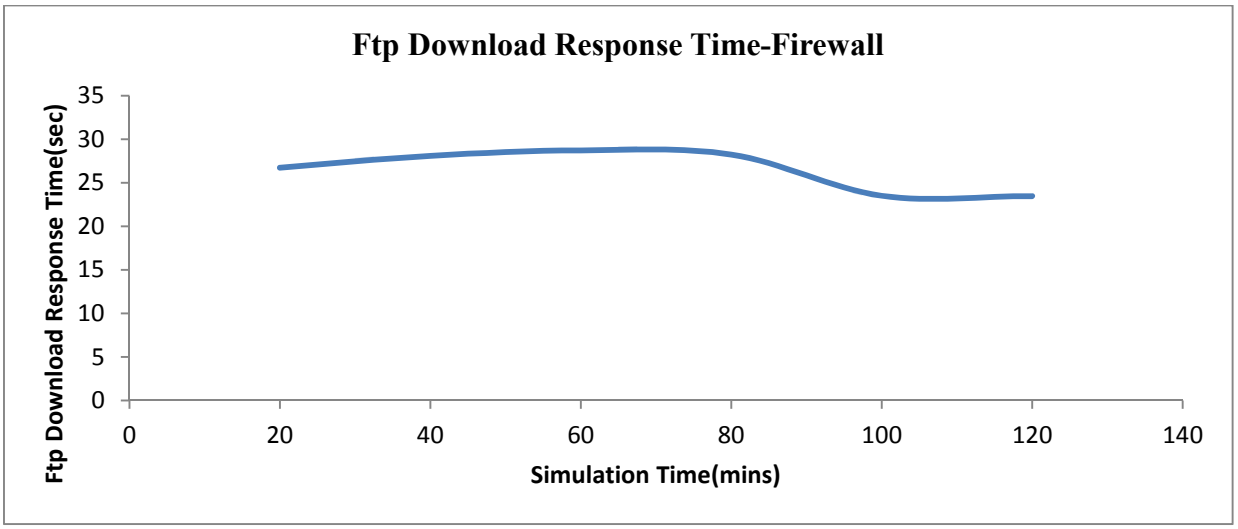

Fig13: Ftp Download Response Time – Firewall Scenario

A firewall is a piece of hardware or software that is capable of filtering network traffic. This is generally performed strictly based upon the origin and/or destination of the data packets. A packet is a container used to break up large messages into smaller more manageable segments. Each packet contains a header and data. The header contains its origin address, destination address and other information about the packet itself. Firewalls go through a simple three step process to determine whether a packet should be accepted or rejected. The firewall first analyzes the packet header. It then uses this information to determine if the packet matches any open connections within the state filter. Finally, if it does not match any state, a predetermined rule set is used to determine the action that should be taken. All these decisions by the router implementing the firewall take a considerable time on the processors hence the higher value.

FTP DOWNLOAD RESPONSE TIME – FIREWALL BLOCKING SCENARIO

In the third scenario, the ftp application is blocked from passing through the router. From the figure14 below, it can be observed that the response time is constant through out the simulation exercise. It has a value of 0.004 seconds across since the ftp application has been blocked access.

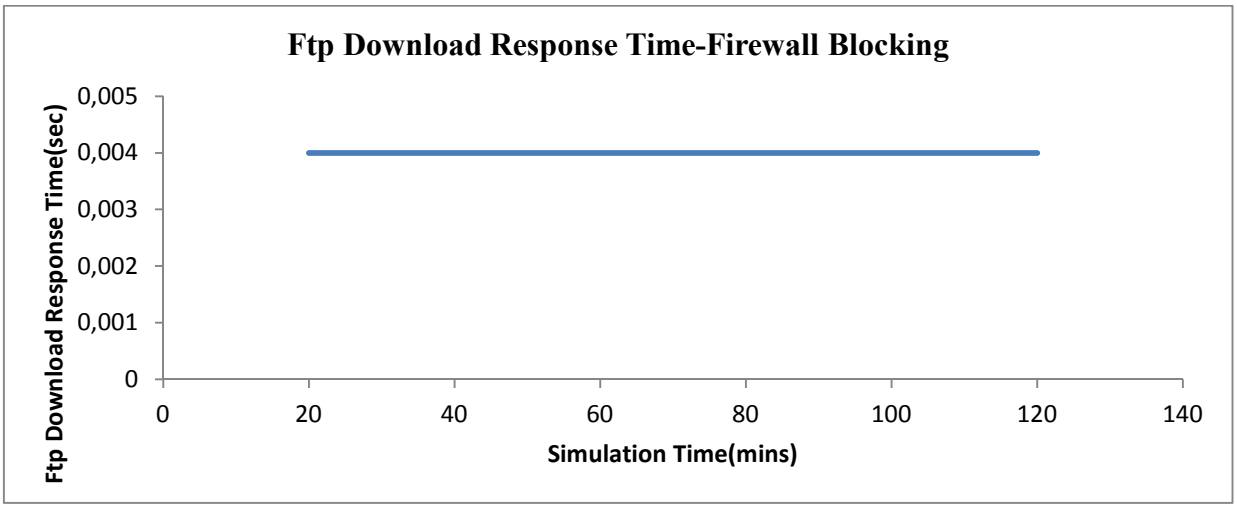

Fig.14: Ftp Download Response Time – Firewall Blocking Scenario

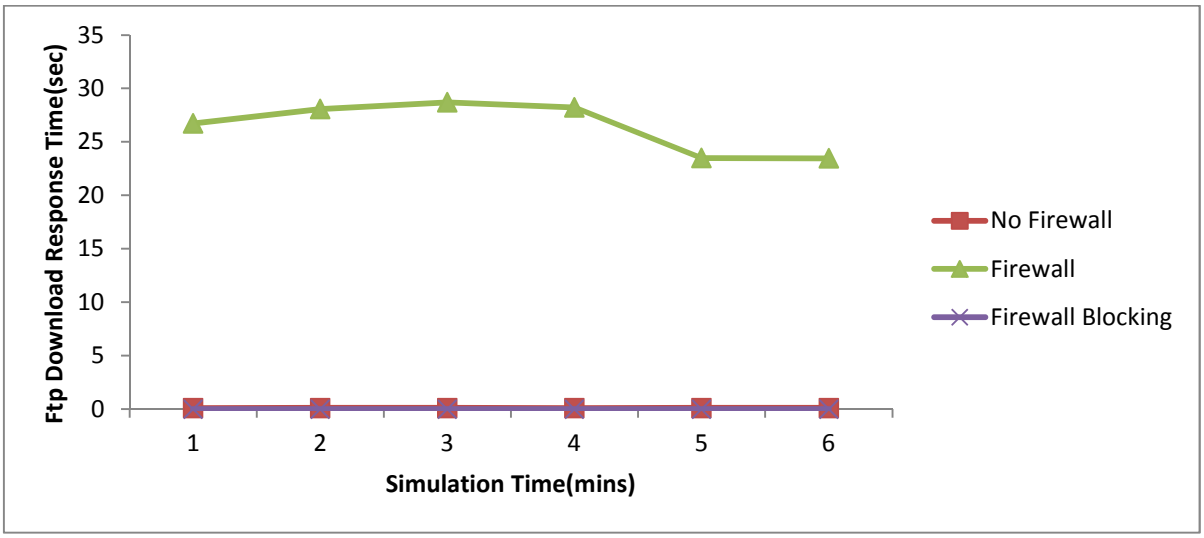

Fig.15: Ftp Download Response Time

When all the three scenarios were considered, the resultant graph is shown figure15. From the figure15 it can be seen that, the download response time is high when security is imposed on the network as in the second scenario. It can also be observed that the ftp download response time increases with an increase in the data packet. In the case where no security is implemented on the network, and some applications are blocked, the download response reduced considerably. The reduction in the download response time is as a result of no restriction across the network.

FTP UPLOAD RESPONSE TIME – NO FIREWALL SCENARIO

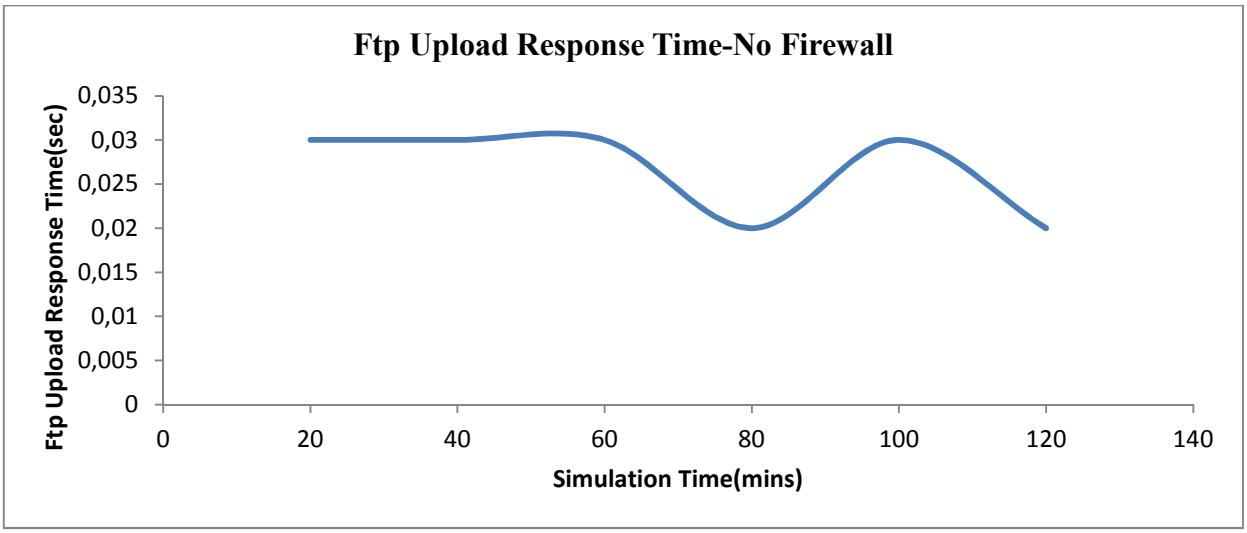

Fig.16: ftp upload response time – No firewall scenario

The figure16 shows the graphical display when no firewall was implemented.

The low value as seen from the graph is as a result of the no restriction to the flow of traffic across the router. When no security is implemented on the network, there is an easy flow of traffic through the router. As the packets gets to the router interface, there is no inspection of packets so the user request gets served quickly hence the low response value of 0.02 seconds.

FTP UPLOAD RESPONSE TIME – FIREWALL SCENARIO

The figure 17 shows a high value when security is imposed on the network. The upload response time is high meaning users experience some delay when uploading their files onto the ftp server. This high value degrades the system performance since users have to wait a considerable amount of time before their request can be granted by the server. The high value in the upload response time when firewall is imposed is as a result of the extra processing being done by the router to filter out any illegitimate packets from accessing the router. Due to this overhead of the router, users get some delay in the system.

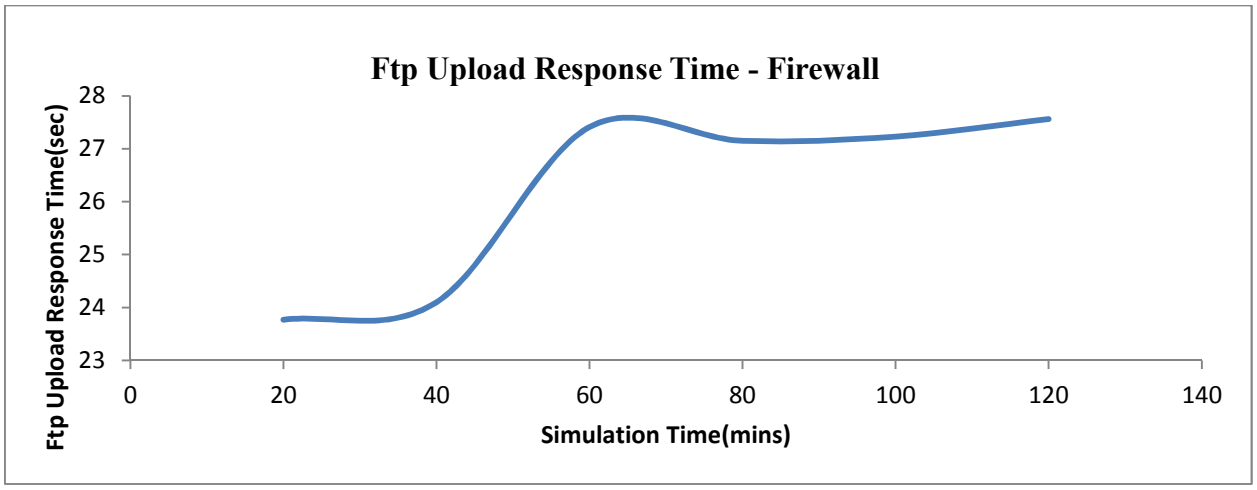

Fig.17: ftp upload response time – Firewall scenario

FTP UPLOAD RESPONSE TIME – FIREWALL BLOCKING SCENARIO

In the third scenario, the ftp application was blocked at the router. The upload response time was 0.004 seconds when trying to upload 200MB of data onto the server. The figure 18 shows the graphical display of the upload response time when the ftp application is blocked. Since the router takes some time to check its policy (filter) table before taking action on the packet, hence the value even though ftp is blocked

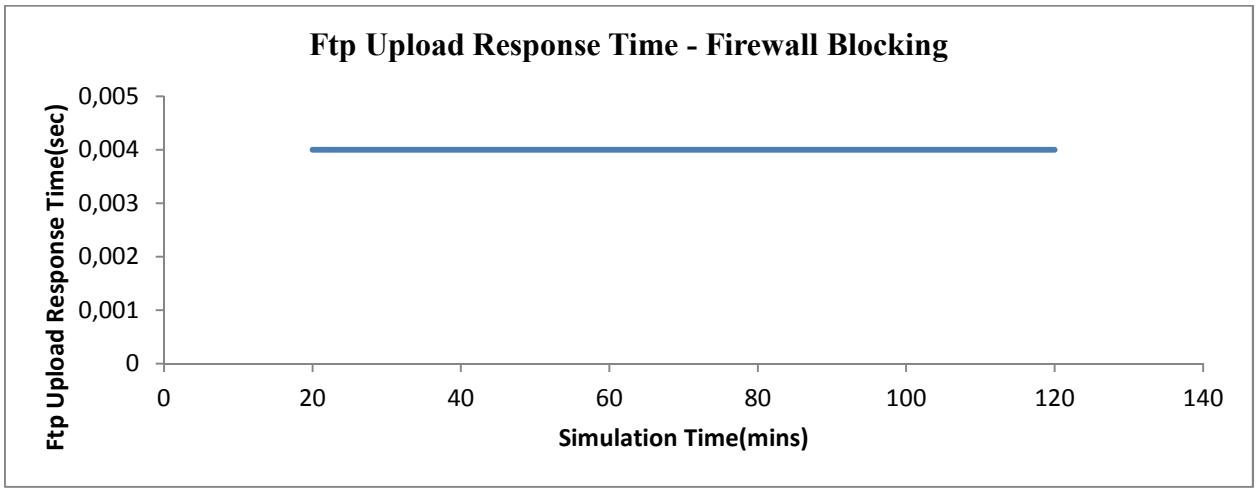

Fig.18: ftp upload response time – Firewall blocking scenario

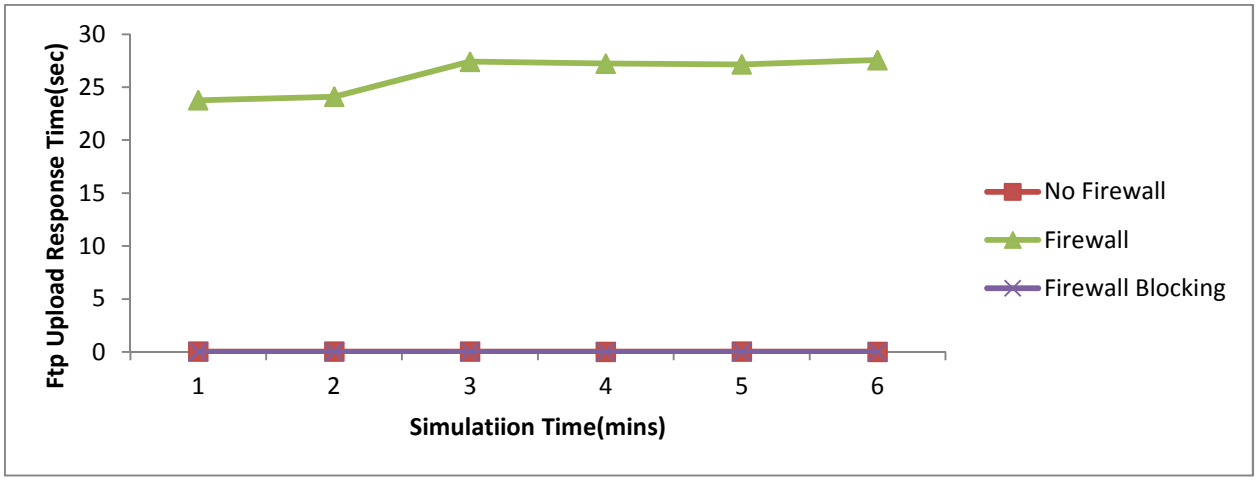

Fig.19: ftp upload response time

Taking the three scenarios into consideration resulted in the figure 19.

It is evident from the figure19 that, when some applications were blocked from accessing the ftp server, it led to a low response time. When no firewall was imposed,it resulted in a decrease in the upload response time. But the upload response time is very high in the case of the presence of a firewall as a result of packet filtering occuring on the router.

SERVER FTP LOAD

The load is more when no firewall is imposed on the network. It has a high value of 0.14 seconds. In the second scenario where security is implemented on the system, the load reduces to 0.001 seconds. But in the third case, since the ftp application is blocked, it has a value of 0. In the second scenario, a value of 0.001 seconds is the load on the server, meaning only small amount of packets gets to server for processing hence the server spend only 0.001seconds processing user request. It can therefore be inferred that imposing firewall on the network increases response time for a user request. This unresponsive nature of the system degrades the system performance since users request are not granted quickly.

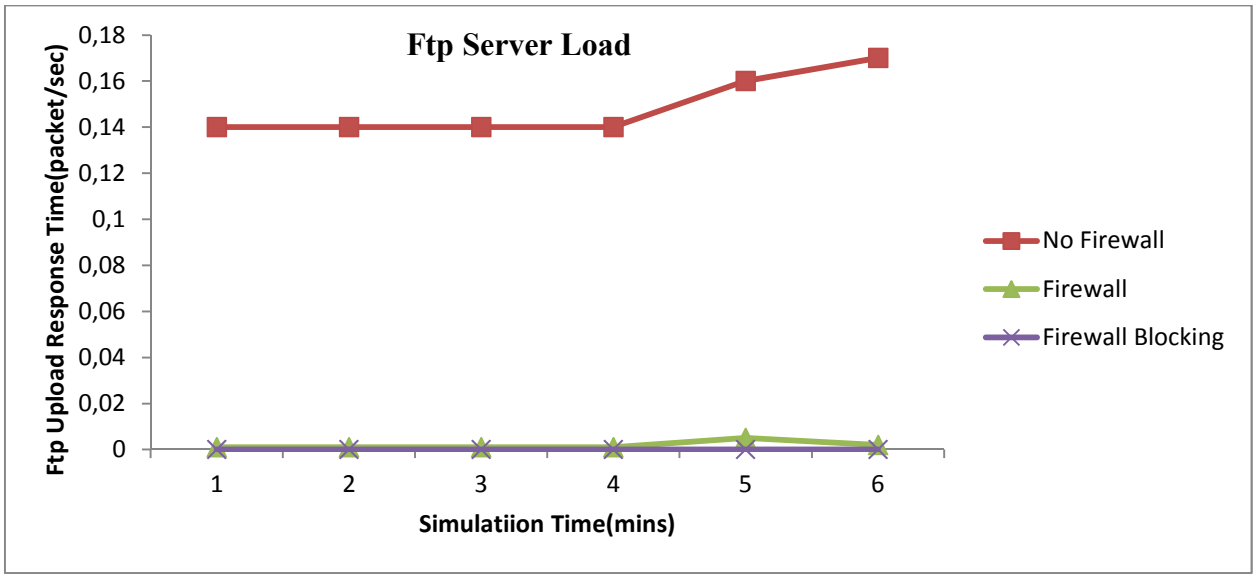

Fig.20 Ftp Server Load

CLOUD PERFORMANCE

This section discusses the cloud utilization. It is evaluated against the point to point utilization. Network utilization is the ratio of current network traffic to the maximum traffic that the port can handle. It indicates the bandwidth use in the network. While high network utilization indicates the network is busy, low network utilization indicates the network is idle.

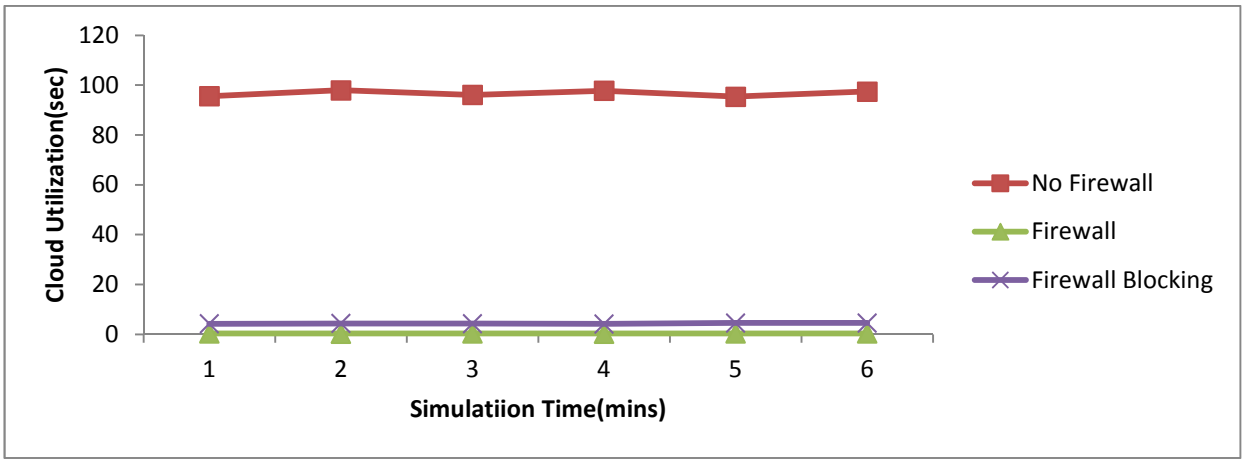

Fig.21: Cloud Point to Point utilization

It can be observed from figure 21 that the overall point to point utilization of cloud is more when there is no firewall across the network as the cloud needs to process the database, and ftp packets continuously. As the firewalls imposes some security policies and also delays the packets due to packet filtering, the cloud utilization is decreased. In the third scenario where the ftp traffics were blocked the overall utilization of the cloud is further reduced as shown in the figure 21. As the traffic is blocked, the cloud has ample space to process the database packets and the overall utilization is reduced. Thus from the overall analysis it can be estimated that the overall utilization of the cloud can be optimized when firewall is imposed on the network.

5 SUMMARY

The simulation experiment was used to measure the following:

- database query response time
- ftp upload and download response time
- Point-to-point link utilizations.

Simulation results given in figure.5, figure.6 and figure.7, shows the database response to user requests under the three different scenarios. Response time is low in the first scenario and the third scenario. Introduction of a firewall increases response times, however, when other applications traffics are filtered; the database response time improves over no firewall scenario. The low response time corresponds to a higher network performance.

Similarly, figure.15 and figure.19 shows the result for the ftp application. Again the download/uploads response time is very close and low for the ftp application when no firewall is imposed and some applications blocked. Also it was evident from the results that the chosen performance metrics increases with an increase in data size but almost the same with different data rates. This increases the network performance since users see a quick response to their request. The chosen performance metrics have a higher value when firewall is imposed on the network. This means that when security is imposed on a network, the network performance degrades.

The general conclusion is that network security and network performance are inversely related, which implies that imposing more security on the network, results to decrease in the network performance.

6 CONCLUSION

The need for firewalls has led to their ubiquity. Nearly every organization connected to the Internet has installed some sort of firewall. The result of this is that most organizations have some level of protection against threats from the outside. This study has found out that network security and network performance are inversely related. As seen from the result of the simulation, network performance is adversely affected when firewall is implemented. There is performance degradation when security policies of the organization are implemented. Nevertheless firewalls do not only secure a network but also contribute to network performance by stopping attacks, improving network availability, and reducing unnecessary processing of illegitimate requests.

7 RECOMMENDATION

Based on the result of the study we recommend that organizations turning to implement security on their network should be prepared to experience a little decrease in network performance. Implementation of firewall should however be subjected to organizational decision

The first and most important decision reflects the policy of how the organization wants to operate the system; is the firewall in place explicitly to deny all services except those critical to the mission of connecting to the internet, or is the firewall in place to provide a metered and audited method of queuing access in a non-threatening manner? There are degrees of paranoia between these positions.

The second is what level of monitoring, redundancy, and control do you want? Having established the acceptable risk level, you can form a checklist of what should be monitored, permitted, and denied.

On the technical side, there are a couple of decisions to make, based on the fact that for all practical purposes what we are talking about is a static traffic routing service placed between the network service provider's router and your internal network. The traffic routing service may be implemented at an IP level via something like screening rules in a router, or at an application level via proxy gateways and services.

The decision to make is whether to place an exposed stripped-down machine on the outside network to run proxy services for telnet, FTP, news etc., or whether to set up a screening router as a filter, permitting communication with one or more internal machines. There are benefits and drawbacks to both approaches, with the proxy machine providing a greater level of audit and, potentially, security in return for increased cost in configuration and a decrease in the level of service that may be provided (since a proxy needs to be developed for each desired service).

REFERENCES

[1] Al-Shaer E. and Hamed, H. (2004) “Discovery of policy anomalies in distributed firewalls”, in Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, vol.4

[2] Caldwell, D., Gilbert, A., Gottlieb, J., Greenberg, A., Hjalmtysson, G., and Rexford, J. (2003) “The cutting edge of ip router configuration”, in Proceedings of 2nd ACM Workshop on Hot Topics in Networks Hotnets-II.

[3] Corbitt, T. (2002) “Protect your computer system with a security policy,” Management Services, vol. 46(5), pp.20–21,[Online].Available:http://findarticles.Com/p /articles/mi_qa5428 /is_200205/ ai_n21313131/ pg_2? Tag =artBody;col1 [2002.]

[4] Danchev, D., (2003) “Building and implementing a successful information security policy,” [online] Available: http:// www.windowsecurity.com [2003]

[5] Fraser, B., Aronson, J. P., Brownlee, N., and Byrum, F. (1997) “Site security handbook (rfc2196),” [Online] Available: http://www.ietf.org/rfc/rfc2196.txt? Number =2196 [Sep 1997]

[6] Hunt, R., and Verwoerd, T.(2003) “reactive firewalls - a new technique” Computer communications, Elsevier, UK. Vol. 26, No 12

[7] Madigan, E. M., Petrulich, C., and Motuk, K. (2004) “The cost of non-compliance: when policies fail’’ in SIGUCCS 04 in proceeding of the 32nd annual ACM SIGUCCS

[8] Mayer, A., Wool, A., and Ziskind, E. (2006) “Offline firewall analysis”, International Journal of Information Security vol.5 no.3 pp. 125-144

[9] Richard. J. Macfarlane (2009) “An Integrated Firewall Policy Validation Tool”

[10] Rubin, A. D., Geer, D., and Ranum, M. J. (1997) Web Security Sourcebook. Wiley

[11] Samarati, P. and de Vimercati, S. C. (2000) “Access control: Policies, models, and mechanisms”, Lecture Notes in Computer Science, vol.2171, pp.137–196.

[12] Sheth, C., and Thakker, R. (2011) Performance Evaluation and Comparative Analysis of Network Firewalls