Impact Of Firewall On Network Performance

Francis Kwadzo Agbenyegah, Michael Asante

Abstract: This research work investigated the firewall security and performance relationship for distributed systems. Internet connectivity is growing with most enterprises migrating to the use of web based services for services provision. As organization grab the Internet as another business tool whether to sell, to team up or to communicate - web applications have turned into the new weakest connection in the organization's security technique. 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. The connection between the security and execution proficiency is exhibited through distinctive scenarios and the relationship between security and performance in firewalls is assessed. We demonstrated distinctive networks (with and without firewalls and diverse firewall functionality and simulated such systems with an eye on their performance). The simulation was done for 300 work stations and simulated in a way that all the 300 work stations access an email and web application under three different scenarios. Attention is on the relationship between system security and performance; the impacts of firewalls on system execution. Different scenarios were assessed through simulations utilizing OPNET IT Guru Academic Edition 9.1 to demonstrate the impacts of firewalls on system performance. The result shows that maintaining security which involves the utilization of numerous applications and the use of firewall has an effect on network performance.

Index Terms: Firewall, Security, Network Performance, Packets, Opnet

1. INTRODUCTION

Innovative developments in the area of IT are in a broad sense changing the way individuals live, work, play, offer data and speak with one another [13]. Internet connectivity is one of the major driving forces behind today's technological innovation. As of January 2008, the internet connected an expected 541.7 million PCs in more than 250 nations on every landmass [9]. The web is not a solitary system, but rather an overall gathering of approximately connected systems that are open by individual PC, in a mixture of routes, to anybody with a PC. "Serving as the first line of guard against noxious attacks and unapproved traffic, firewalls are critical components in securing the private systems of most organizations, establishments, and home systems. A firewall is ordinarily a barrier between a private system and the outside web such that all system traffic needs to go through" [5]. "In a distributed network, messages are embodied into packets, which regularly go through different access route in a system and firewalls are in charge of filtering, checking, and securing such packets" [6]. Most deployed firewalls frequently take countless guidelines, resulting in execution bottlenecks in the system [13].

2. RELATED WORK

Security is a major issue for organizations, both the legal issues associated with computer and network security as well as its implementation. Threats such as malware and Denial of Service (DoS) constantly test organizations security. [1], have described a security scheme as a formal proclamation of the guidelines by which individuals who are offered access to an organization's technology and data resources must tolerate.

- *Francis Kwadzo Agbenyegah: Lecturer, Faculty of Informatics Ghana Technology University College Accra – Ghana*
- *Michael Asante: Senior Lecturer, Head of Department Department of Computer Science, Kwame Nkrumah University of Science and Technology Kumasi- Ghana*

As indicated by the authors, this is a progressing procedure, with customary audits and reviewing of security arrangements and components, giving criticism to enhance the security strategy. [4], "hypothesize that it is amazingly vital to include the clients in the usage of a security policy. Comprehension of security issues by clients, and issuing them clear and simple to take after principles, can be a key figure in the fruitful execution of the security arrangement". According to[10] "Security policy secures the confidentiality, honesty, and accessibility of the resources of an organization. To uphold this, security administrations ought to be deployed, for example, authentication, encryption, utilization of antivirus program and firewall". [12], "contended that the access control part of the security policy manages verifying that only approved people can perform the assignments they are approved to and those others can't. It is regularly alluded 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], "contends that firewalls control access to resources by filtering system traffic, just permitting access that is specified by the security plan". According to [8], "the assurance that these firewalls give is just comparable to the policy they are configured to execute. The policy ought to be clear, succinct, and simple for the administrator to follow". [7]," postulate that if a policy is not all around composed, then it won't be implemented legitimately and the security objectives won't be met" [11], "state that the configuration of a firewall is presumably the most critical factor in terms of the security a firewall offers" According to [2], [14], firewall strategies are comprised of principle sets, and these standard sets are perpetually extending because of new standards constantly being included and not very many evacuated, so device access policy have a tendency to be extensive and continually expanding in size [14], states 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

In this paper, the impact of firewall on network performance was evaluated. We created three scenarios namely networks with firewall, without firewalls and different firewall functionality with OPNET IT Guru Academic Edition 9.1 as a simulation tool. The simulation was then run for two hours.

SET UP OF THE VARIOUS SCENARIOS

No firewall Scenario

In this scenario, no security was implemented on the network. This scenario was modeled as shown in fig.1.1 in such a way that all the 300 workstation used in the simulation access the internet. 150 workstations access web application and 100 workstations use email to download and upload file onto the file server Taking after are the performance measurements utilized for the performance assessment when there was no security forced over the network.

i. Http page response time was assessed
ii. Email download response time and upload response time was estimated
iii. Link level and utilization statistics were also estimated across the simulation process
iv. Data throughput which is the amount of data transferred in the network per time unit was 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 which will result in a larger throughput.
v. Packet Delay
vi. Traffic drop
vii. Task processing time of the server is also evaluated

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 was set between the router and the cloud and the above performance metrics were measured in each packet size and data rate to investigate applications performance.

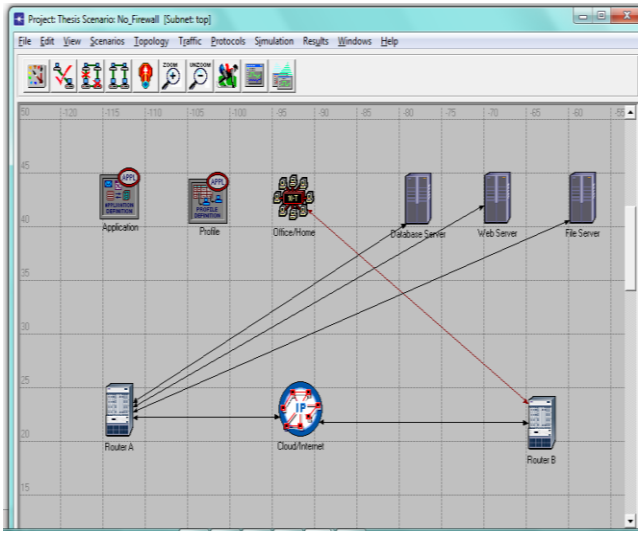


Fig.1.1 *Network Layout (M. Asante,F.K. Agbenyegah(2014))*

Firewall Scenario

The first scenario (i.e. No firewall Scenario**)** shown in fig.1.1 was replicated and the requisite firewall scenario was created. In this specific setup a firewall router was produced and a persistent packet latency of 0.05 seconds is enforced for packet filtering. Analogous performance metrics were used as in the first setup.

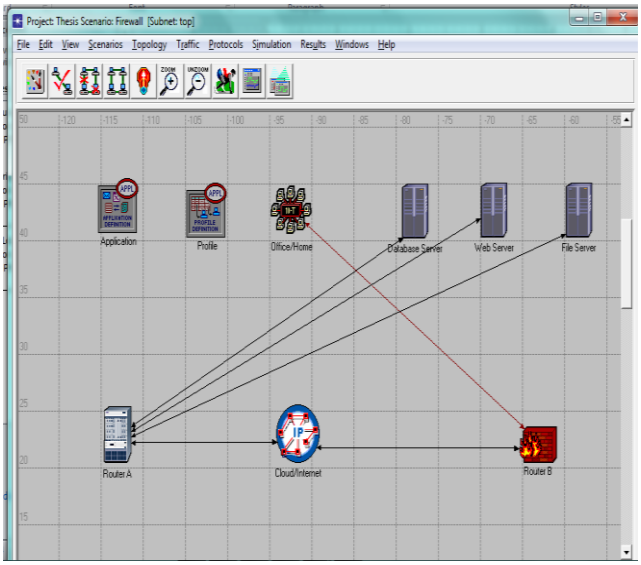


Fig.1.2 *Firewall Scenario setup (M. Asante and F.K Agbenyegah(2014))*

Firewall: With Packet Filtering Capabilities scenarios

This scenario was generated by replicating the second scenario (with firewall) shown in fig.1.2 and the main aim of this scenario was to block the unauthorized applications access. After the three scenarios have been created, the simulation was allowed to run for two hours and the corresponding performance of the network was evaluated based on the stated performance metrics. After a complete run of the simulation, the results were recorded for the three scenarios and the results were compared based on the performance metrics used

4. RESULTS AND ANALYSIS

The three scenarios simulated in this research were evaluated based on:

i. 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.
ii. Firewall scenario where a firewall is imposed to filter some packet of the other application
iii. The third scenario like the firewall with blocking capability where the ftp applications are blocked and only allowed the web application to pass through.

The performances of the web and email applications were analyzed based on the performance metrics chosen for three levels namely; global level, node level and link level. The results obtained, were compared against the performance metrics and a detailed analysis was given.

Result for Email Application (Email Download Response Time)

E-mail application was evaluated in this section against the email downloads and uploads response time when the three scenarios were considered. E-mail with packet size of 32MB, 100MB and 200MB were used and link speed of 10Gbps, 1Gbps and 32Mbps were used and evaluated against the performance metrics and the email download response time was recorded in each case and the response time was plotted against the simulation time as illustrated in figure 1.3. It can be observed that the download response time has a low value of 0.12 seconds and 0.11 seconds when a packet of 100MB and 200MB were downloaded. Since there is no limitation to the flow of packets through the router, the download time was very low. It can therefore be inferred that if there is no blockage to the packets, the resulting download time will be faster.

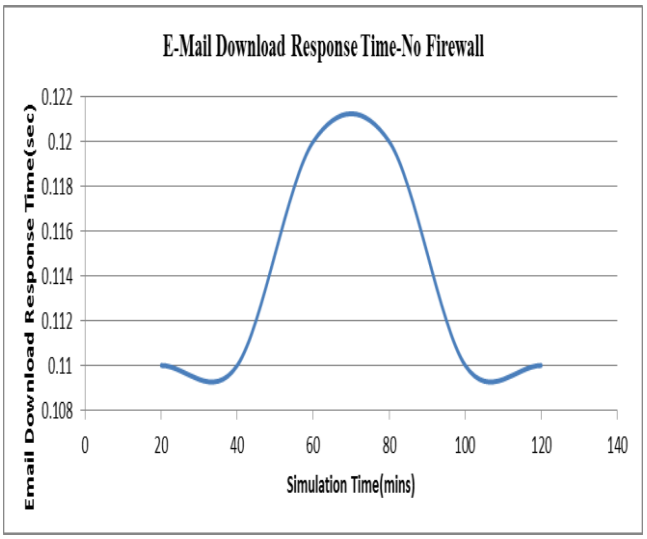


Fig.1.3 *Email downloads response time- no firewall scenario*

E-mail Download Response Time – Firewall Scenario

The figure1.4 illustrates the download response time against simulation time in a firewall scenarios. The figure shows a high value in the download response time. Firewalls sorting traffic is a relatively simple process. First, they examine the packet headers. Then, they check the active state table for matches. Finally, they search through the predefined rule set until a match is found. Every packet will either match a state or rule and therefore be blocked or admitted. If a packet is to be blocked, it is simply not forwarded. The next packet to be examined will overwrite it and it will disappear. If a packet is allowed to pass, it is pushed through the firewall towards its destination before the packet behind it inline can overwrite it. All this add on to the overhead of the router hence a large value of 11.29 seconds when downloading data from the email server.

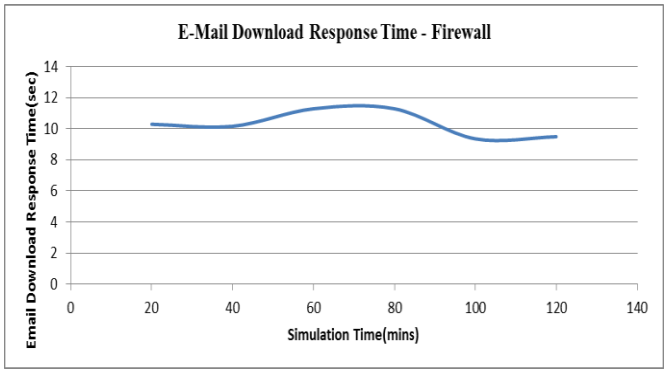


Fig.1.4 *E-mail downloads response time - Firewall Scenario*

E-mail Upload Response Time – No Firewall Scenario

The figure1.5 shows a graph of the upload response time against simulation time in a no Firewall scenario. It has a peak value of 0.13 seconds and minimum value of 0.119 seconds when the simulation was run for 2 hours. The low value is due to absence of restriction to the flow of traffic. As expected, since there is no blockage to the flow of traffic, the user experience low response time when uploading files to the email server.

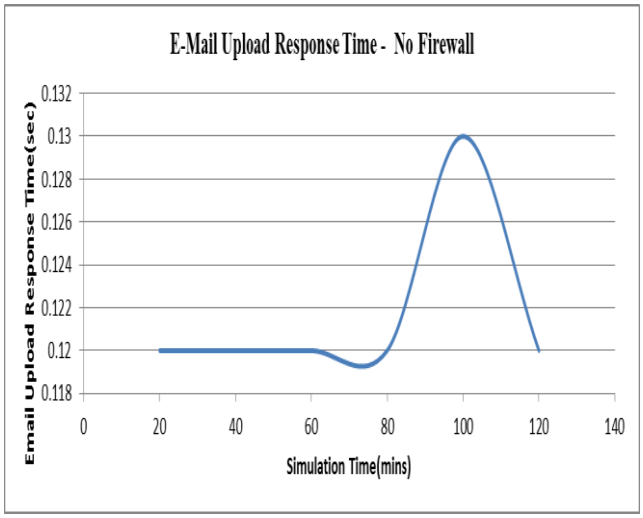


Fig.1.5 *Email Upload Response Time – No Firewall Scenario*

E-mail Upload Response Time – Firewall Scenario

A packet latency of 0.05 was imposed to induce delay into the system. 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. Due to the filtering of packet at the router, users experience a delay when uploading file into the server, hence the higher value of 10.91seconds in the upload response time.

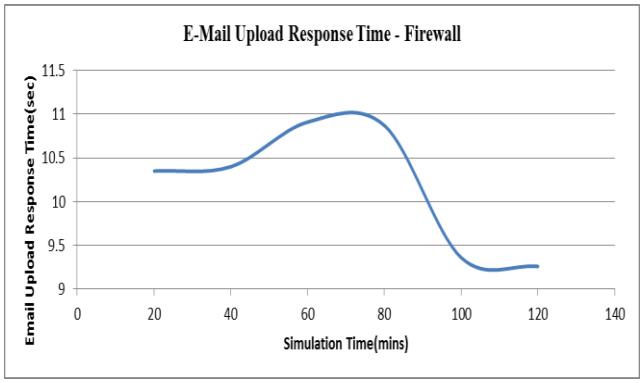


Fig.1.6 *E-mail uploads response time - Firewall Scenario*

Due to the extra processing incurred on the router, it takes time to process each packet that tries to access the email server, hence the higher value of 10.91 sec in the response time. In order to filter traffic, firewalls use predefined rule sets. These are ordered lists that contain packet qualities matched to an action. The actions a firewall can take are to block a packet from crossing or to allow it to do so. Rules separate packets based on several qualities within the header. Many rules distinguish packets based on their origin and destination. Rule lists are written sequentially. The firewall iterates through rules and stops at the first rule that matches the packet being held. Many rules may apply to a packet. If a packet does not match any rule, it is filtered based on the default rule. Most firewalls allow outbound packets by default and block inbound packets by default. When security is imposed on the router, the router takes an extra time processing the incoming request against its policy and deciding whether to allow a packet through or drop it. This therefore increases the time it takes to upload hence users experience some delay in uploading their files.

E-mail Upload Response Time – Firewall Blocking Scenario

In the third scenario, the email application is blocked by the router. In this scenario, the email application is blocked and the router takes 0.003 seconds before returning a denial request to the user since it must take some time to check its security policy before deciding which packet to pass through.

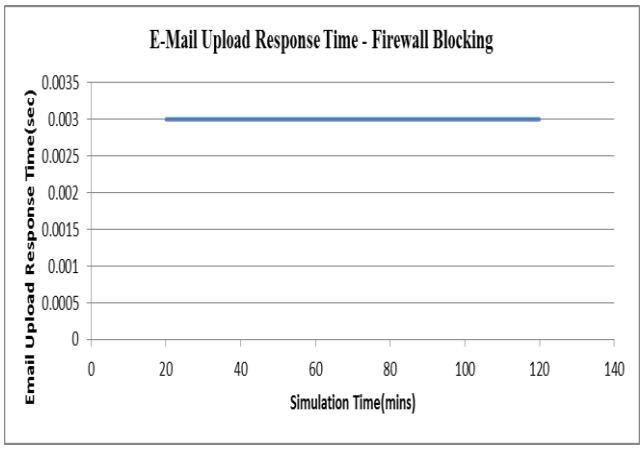


Figure.1.7 *E-mail uploads response time - Firewall Blocking Scenario*

The figure1.8 shows the result when all the three scenarios were combined. It can be seen that the upload response time is high when firewall was imposed on the network. Due to the extra processing time taken by the router to process all packets that required access, the router took more time to examine its policy table before allowing access hence the high response time. In the no firewall scenario, the response time is low since there was no processing done to the packet at the router. With no firewall, the system performance is enhanced. But the system degrades as more security is imposed on the network

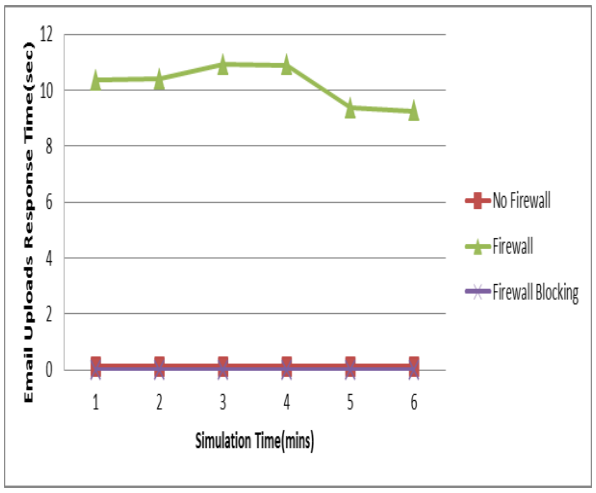


Fig.1.8 *E-mail uploads response time*

Server E-mail Load

It can be observed from figure 1.9 that the load on the server is high when no firewall was implemented. A lot of user request gets to the server, so the server takes time to grant each request hence the high load on the server. When firewall was imposed, the load on the server reduced drastically as can be seen from the figure 1.9. Due to the overhead of the router processing packets and deciding on which one to allow access or deny, only small legitimate packets gets to the server for processing hence the low load. In the third scenario, the email application was blocked so there was no processing on the server.

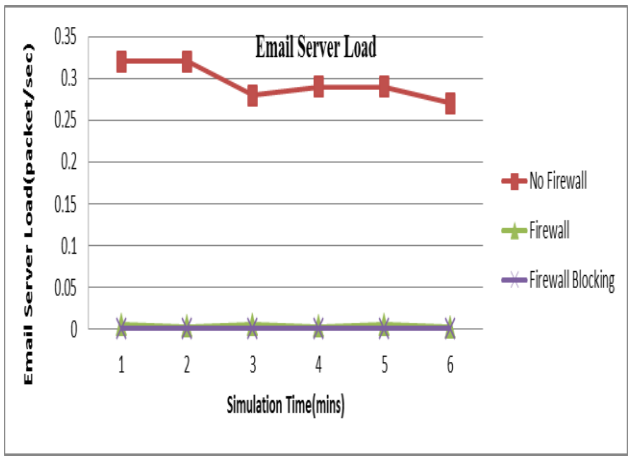


Figure.1.9 *Server E-mail Load*

Result for Web Application

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

Http Page Response Time - No Firewall Scenario

The figure1.10 shows the page response time when no firewall was imposed across the network. The lower response time shows that there is no restriction to the flow of traffic across the network. It has low constant values between 0.03 seconds and 0.05 seconds.

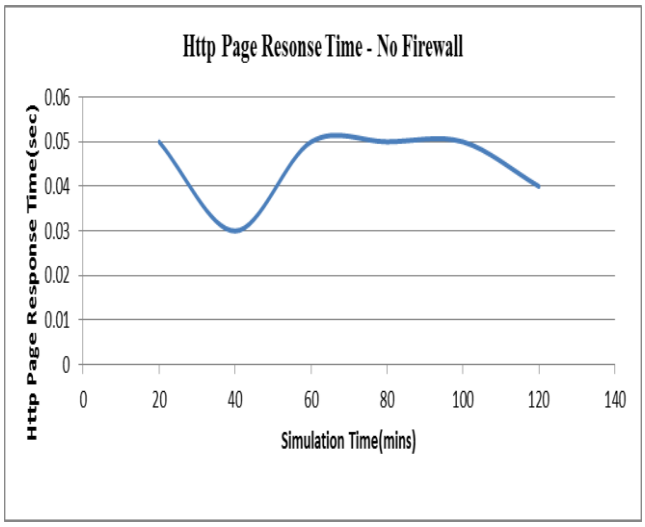


Fig.1.10 *Http Page Response Time – No firewall Scenario*

Http Page Response Time - Firewall Scenario

From the figure1.11 it can be inferred that the average page response time is more when there is a firewall. This is due to the packet filtering, and the packet latency of 0.05 set across the firewall router and thus the delay is incurred in the system Page response time is very high when there is a firewall implementation over the cloud and when packet size increases. Due to the security policies and the packet latency time imposed over the firewall, the overall page response time increases as it has a value of 9.40 sec as shown in fig.1.11

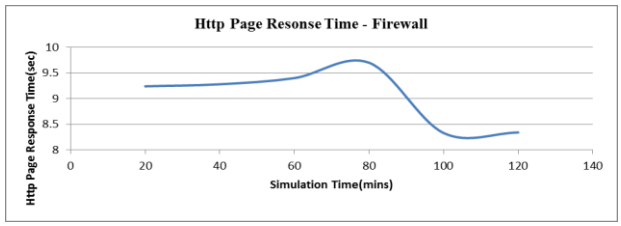
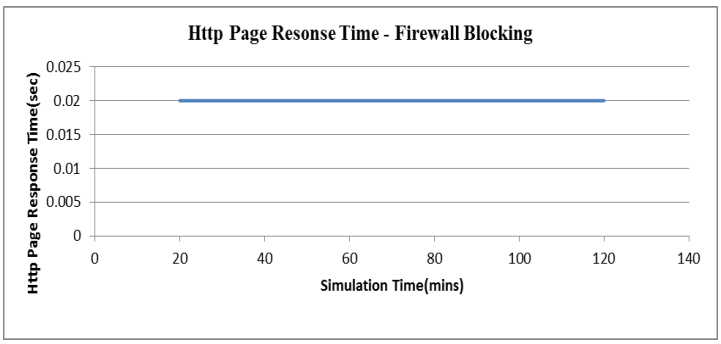


Fig.1.11 *Http Page Response Time – Firewall Scenario*

Http Page Response Time - Blocking Firewall Scenario

The figure 1.12 shows the page response time when other applications are blocked. As expected, the page response time is very low when the other application is blocked. It has a low value of 0.02 seconds.



Figiure.1.12 *Http Page Response Time - Firewall Blocking*

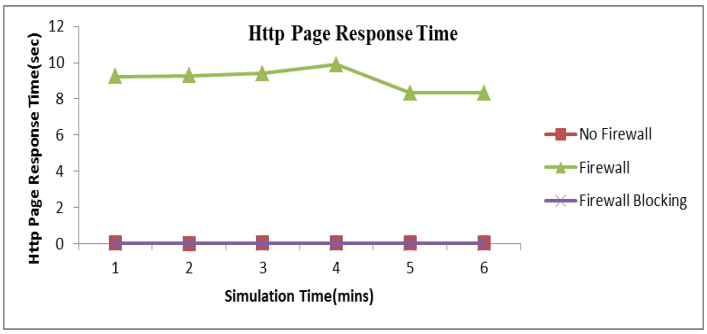


Figure.1.13 *Http Page Response Time*

From the figure 1.13, it can be inferred that the page response time is more when firewall is imposed on the network. Due to the overhead of firewall filtering on the router, it introduces extra processing which leads to an increase in page response time, i.e. degrade system performance. In the case where there was no firewall, the page response time is reduced. The third scenario blocks the web application from the network hence the low response time.

Server Http Load

From the figure1.14, it is evident that the load on the web server is more when no firewall was imposed on the network as compared to when a firewall was implemented. In the third scenario the web application was blocked hence the values 0 on the server load. In no firewall scenario, all packets that traverse the network went through hence the server spends a lot of time processing the user request. This accounted for the high value in the web server load. In the case where the firewall was imposed, the firewall filtered all the packets and only legitimate packets that conforms to the security policy of the organization was allowed through. It can be concluded that when firewall is imposed on the network it degrades network performance since there is packet filtering taking place on the router. This overhead of the firewall impedes system performance.

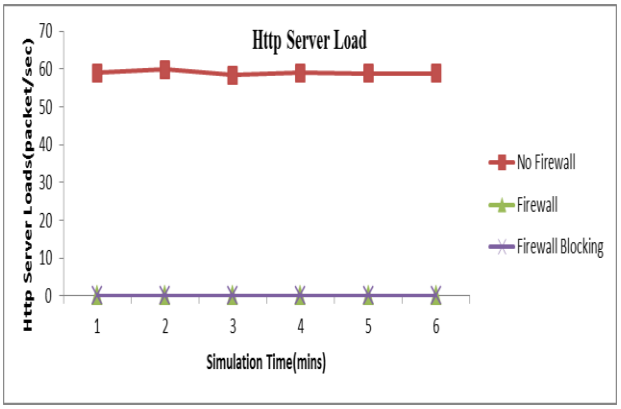


Fig.1.14 *Http Server Load*

Cloud Performance

This section discusses the cloud utilization. It is evaluated against the point to point utilization. Network utilization is the proportion of current system traffic to the greatest traffic that the port can deal with. It shows the transmission capacity use in the system. While high system usage shows the system is occupied, low system use demonstrates the system is idle. It can be observed from figure 1.15 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 web application, and email packets continuously. As the firewalls imposes some security policies and also delays the packets due to packet filtering, the cloud utilization is decreased. When the third scenario where the email traffics are blocked the overall utilization of the cloud is further reduced as shown in the above graph. As the traffics are blocked, the cloud has ample space to process the web 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.

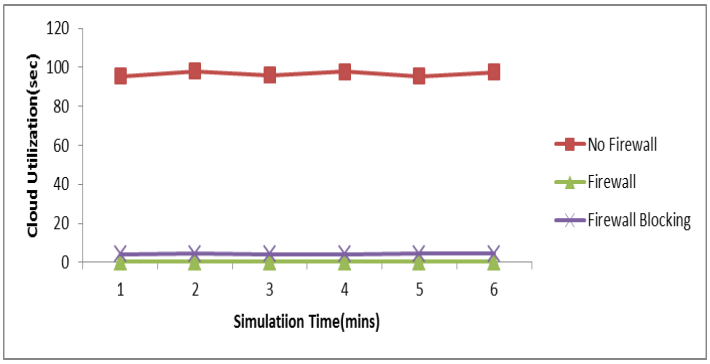


Fig.1.15 *Cloud Point to Point utilization*

5. FINDING, CONCLUSION, AND RECOMMENDATION

Findings

The simulation experiment was used to measure the following:

i. Http page response time
ii. Email upload and download response time
iii. Point-to-point link utilizations.

Simulation results given in figure.1.13, shows the http page response to user requests under the three different scenarios. Response time was low in the first scenario and the third scenario. Introduction of a firewall increases response times, however, when traffic from other applications was filtered; the page response time improves under 'no firewall scenario'. The low response time corresponds to a higher network performance. Similarly, figure.1.8 shows the result for the email application. Again the download/uploads response time was very close and low for the email 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 the network, the network performance degrades. It can therefore be inferred that network security and network performance are inversely related, which implies that imposing more security on the network, correlates to decrease in the network performance.

6. Conclusion

The requirement for firewalls has prompted their omnipresence. Almost every organization connected with the Internet has introduced a firewall. The after effect of this is that most organizations have some level of assurance against dangers 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 don't just secure a system, additionally add to system performance by ceasing assaults, enhancing system accessibility, and lessening superfluous preparing of illegitimate solicitations.

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.

REFERENCES

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

[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] Hwang, J. H., Tao X., Chen, F., and Liu, A. X. (2011) “Systematic Structural Testing of Firewall Policies”

[6] Lodin, S. W. and Schuba, C. L. (1998) “Firewalls fend off invasions from the net”, IEEE Spectrum, vol. 35, no. 2, pp. 26–34.

[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] Pesante, L.,(2008) “Introduction to Information Security”

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

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

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

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

[14] Wool, A. (2006) Packet Filtering and Stateful Firewalls Wiley, Firewall Architectures,p.526