ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

How Firewall Keeps The Signal Save In Local LAN?

[1] Teeb Hussein Hadi , [2] Raddam Sami Mehsen
[1][2] Baqubah Technical Institute, Middle Technical University, Baghdad, Iraq

***Abstract*— With the grown of internet, the transfer of package should be secured and grantee that availability, integrity, and confidentiality of data are met. Firewalls are multihomed server node models with gateway capabilities. The firewall rejects all remote-login traffic while accepting other applications. Based on the characteristics of their proxy servers, datagrams of some applications experience additional latency while being forwarded. This paper analyzed the use of firewall node model that connected as external network with different QoS parameters like: IP Traffic Dropped, Download Response Time, IP Processing Delay and Traffic Received. By applying the specified security policies, firewalls aim to protect the local network against the unauthorized access attempts from outside world.**

***Index Terms*— Firewall, Proxy servers, Local LAN, Security, Packet filtering**

I. INTRODUCTION

The important and essential process in the Internet is how to transfer the data packets with higher security. Applying some security policies by firewalls satisfy the safety access requirements of network packets in blocked mode [1]. Firewall is a set of components that aim to protect the inner network against the unauthorized access attempts from outer network; filtering manner; depending on set of rules called "security policies" that control the firewall management [2]. Firewall applies its rules on some of attacks also but not all like: Denial-of-service, Eavesdropping, Host Attacks, Password Guessing, Protocol-based attacks, Social Engineering and War Dialing. To control these attacks, firewall could be hardware or software [3]. Firewall has important policies that managing firewall rules such as: Firewall policy editor, automated correction of policy fault, Fault localization, Anomaly detection and Policy modeling [4]. This paper analyzed the use of firewall node model that connected as external network with different QoS parameters like: IP Traffic Dropped, Download Response Time, IP Processing Delay and Traffic Received. By applying the specified security policies, firewalls aim to protect the local network against the unauthorized access attempts from outside world.

2. RELATED WORK

Akbas et al. (2012), simulated and verified an enterprise network by using firewall and some security characteristics in real and virtual networks. Krit et al. (2018), suggested new application "QudsWall" using C# that make the use and manage of firewall easier. Mudathir et al. (2016), simulated WLAN environment to show the effect of firewall on IEEE 802.11a, b, g by analyzing the performance parameter such as: delay and throughput. Graves et al. (2017), suggested new network "Distributed Secured Network (DSN)" by combining the firewalls with Intrusion Detection System (IDS) dynamically. Appelt et al. (2017), proposed an automated approach that combines machine learning with multi-objective genetic algorithms to fix vulnerable WAFs problems bypassing SQL injection attacks. Agbenyegah et al. (2017), used OPNET IT Guru to simulate different scenarios results that worked under firewall control or without and analyzed the impact on network performance.

3. THE PROPOSED NETWORK

The simulation model for our network is built with OPNET modeler to study the use of firewall node model as shown in fig 1 that contains a local protected network with four nodes: Remote customer application client, Remote HTTP client, Remote FTP client and Hacker. Fig 2 presented the structure model of a local protected network that consists of firewall and internal router connected with two hubs one for servers and one for client. Server hub connected with Remote-login server, Customer application server and FTP server while client hub connecter with Local remote-login client, Local customer application client and Local FTP client.

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

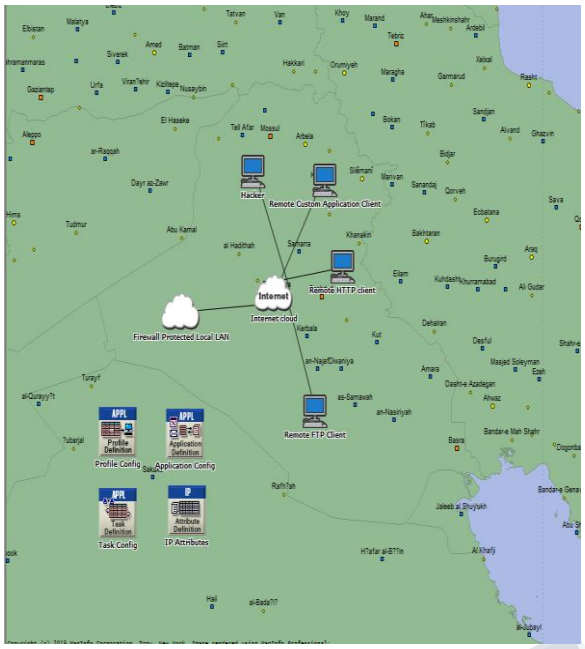

Fig 1: Simulation the Proposed Network

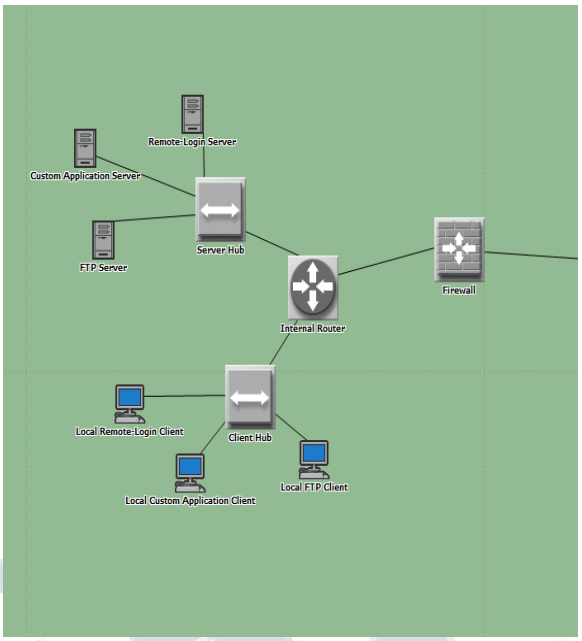

Fig 2: Schematic View of Firewall Protected Local LAN

Firewalls are multihomed server node models with gateway capabilities. By applying the specified security policies, they aim to protect the local network against the unauthorized access attempts from outside world. Because of this purpose, a firewall must be the only connection to outside for the nodes of protected LAN. The scenario models a LAN and an outside network separated with a firewall. Firewalls contain proxy servers which determine the firewalls security policies for the corresponding applications. If a firewall does not have the proxy server of a certain application then this application is not allowed through the firewall. Proxy servers may introduce some additional processing delay to the forwarded packets, or just forward them without any proxy server latency (circuit level filtering) depending on the application that the datagrams belong to. The firewall in this scenario is also deployed as an HTTP server. This is also a common configuration approach in the real life networks since, most of the time, HTTP servers provide public data to the outside world.

4. NETWORK SIMULATION RESULTS AND DISCUSSIONS

In this section, different QoS parameters like: IP Traffic Dropped (packet/sec), Download Response Time (sec), IP Processing Delay (sec) and Traffic Received (byte/sec) are analyzed by applying the specified security policies. The duration of simulation is 3600 minutes and 512 for seed.

4.1 IP Traffic Dropped

This graph shows the dropped packets of the Hacker in fig 3, and the timestamps of these drops indicate when s/he attempted to remote login. Security policies of firewall models can be specified by modifying the compound attribute "Proxy Server Information". The table of this attribute determines which applications are accepted and which ones are rejected. It also specifies whether there is an additional latency introduced to the datagrams by the proxy servers, and which characteristics it has.

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

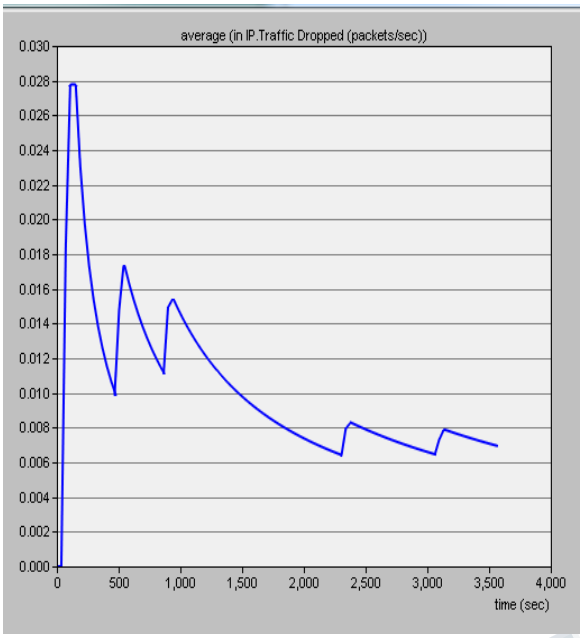

Fig 3: IP Traffic Dropped

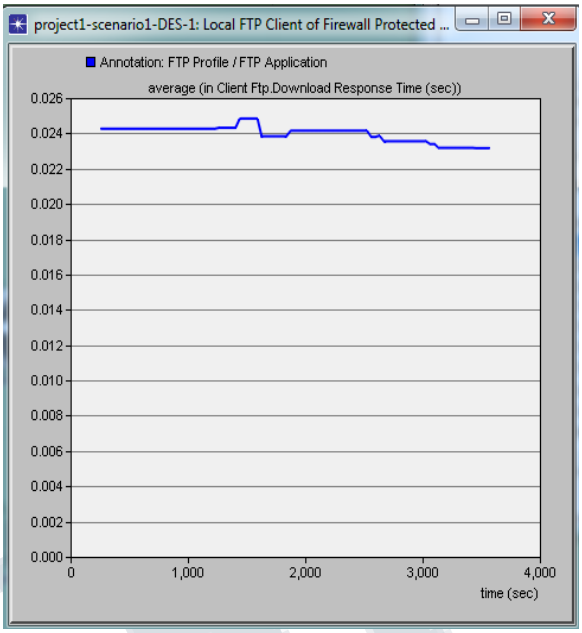

Fig 5: Download Response Time in Local FTP Client

4.2 Download Response Times

FTP is allowed through the firewall with additional proxy server latency. Though this latency is a very insignificant part of the difference between the FTP download response times for local and remote FTP clients of firewall protected LAN as shown in fig 4 and 5; most of the difference still based on the different distances to the server and different number of hops on the route.

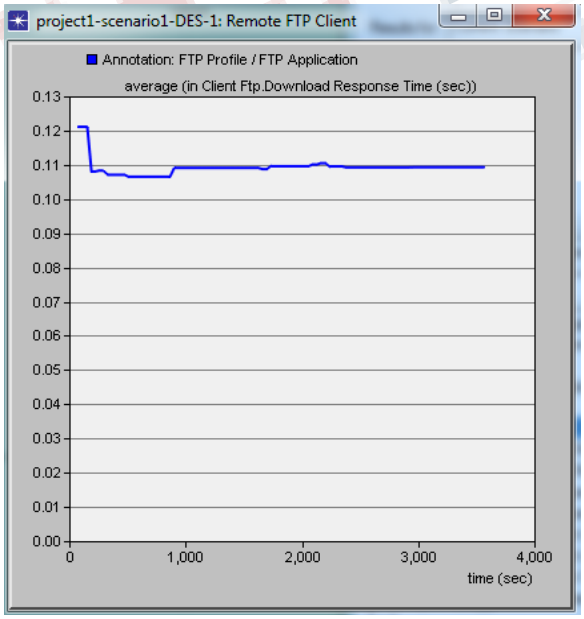

Fig 4: Download Response Time in Remote FTP Client

4.3 IP Processing Delay

This graph of firewall node indicates two concentration value ranges as shown in fig 6, where the high one contains the processing delays of the datagrams that also experienced additional proxy server latency. The datagrams with low delays have just experienced routing delays and maybe queuing delays if the server was busy initially.

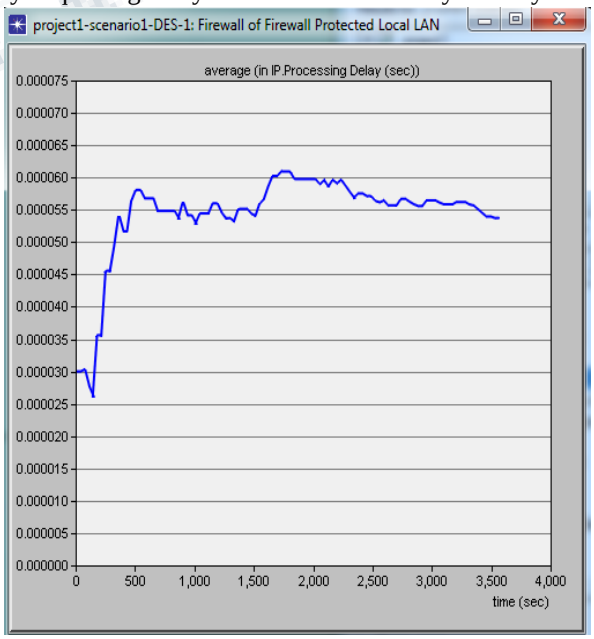

Fig 6: IP Processing Delay

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

4.4 Traffic Received

In this scenario, the firewall is configured in order to reject all the remote-login through traffic as shown in fig 7 and 8. Hence, as also seen in the results; the Hacker, who is actually a remote-login client; cannot receive any responses from the server, in contrast to the local remote-login client who can communicate with the server since the server is at the same side of the firewall.

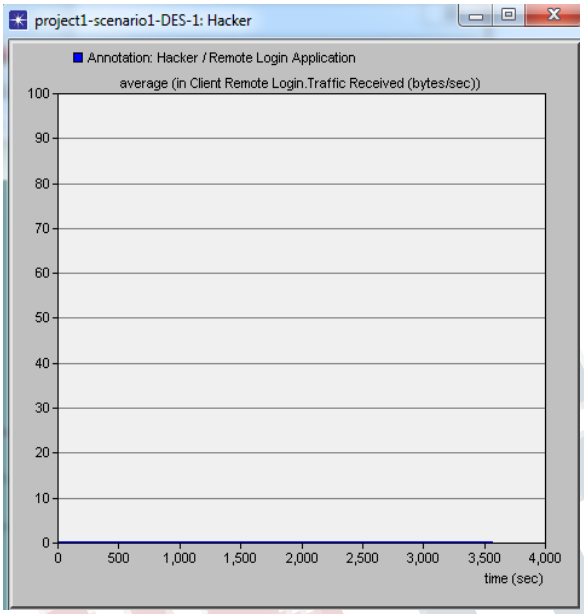

Fig 7: Traffic Received in Hacker/ Remote Login

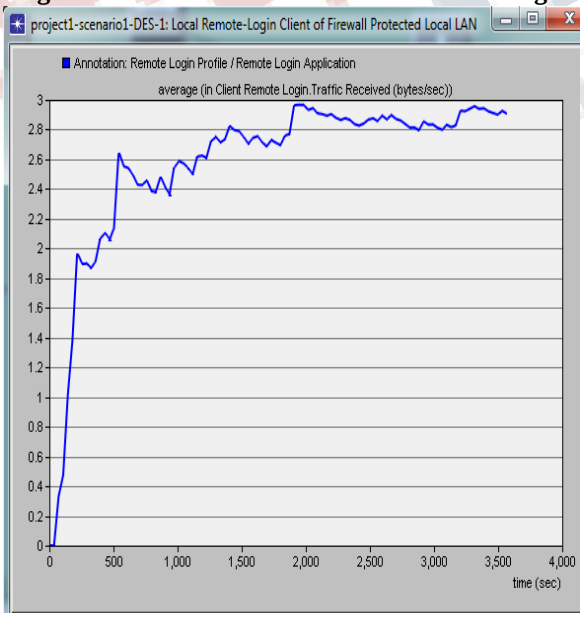

Fig 8: Traffic Received in Local Remote Login

5. CONCLUSION

OPNET modeler has been used in this paper to simulate and analyze the use of firewall node model that connected as external network with different QoS parameters like: IP Traffic Dropped (packet/sec), Download Response Time (sec), IP Processing Delay (sec) and Traffic Received (byte/sec). By applying the specified security policies, firewalls aim to protect the local network against the unauthorized access attempts from outside world. Security policies of firewall models can be specified by modifying the compound attribute "Proxy Server Information". The table of this attribute determines which applications are accepted and which ones are rejected. It also specifies whether there is an additional latency introduced to the datagrams by the proxy servers, and which characteristics it has. The datagrams with low delays have just experienced routing delays and maybe queuing delays if the server was busy initialy.

REFERENCES

[1] M. Chandrashekhar and K. Raghuveer, “Performance evaluation of data clustering techniques using KDD Cup-99 Intrusion detection data set”, International Journal of Information and Network Security (IJINS), ISSN: 2089-3299, Vol-1, No.4, October 2012, pp. 294-305.

[2] W. R. Cheswick, S. M. Bellovin and A. D. Rubin. Firewalls and Internet security: repelling the wily hacke. Addison-Wesley Longman Publishing Co., Inc, 2003.

[3] Zeng-gang, X. and Xue-min, Z. Research and Design on distributed Firewall based on LAN, Computer and Automation Engineering (ICCAE), DOI: 10.1109/ICCAE.2010.5451596, Publisher: IEEE, Singapore, pp. 517-520, 2010.

[4] Er. Smriti Salaria and Er. Nishi Madaan, "Firewall and Its Policies Management", IJCSMC, Vol. 3, Issue. 4, p 366, April 2014.

[5] Deniz Akbas and Halûk Gümüskaya, Real and OPNET modeling and analysis of an enterprise network and its security structures, Procedia Computer Science 3, Published by Elsevier Ltd, doi:10.1016/j.procs.2010.12.170, pp. 1038–1042, 2010.

[6] Salah-ddine Krit and Elbachir Haimoud, “Overview of firewalls: Types and policies: Managing windows embedded firewall programmatically,” International Conference on Engineering & MIS (ICEMIS), 2017.

[7] Mudathir Babiker Idris Babiker, Amin Babiker

and Nabi Mustafa "Impact of Firewalls on IEEE.802.11a, b, g, n WiFi Releases Networks," International Journal of Science and Research, vol. 5(2), pp. 2205-2208, 2016.

[8] Thomas Graves and Chetan Jaiswal, "Smart cooperative firewalls: An aid to a safer and secure cyber world," IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), Oct. 2017.

[9] Dennis Appelt, Annibale Panichella and Lionel Briand, "Automatically Repairing Web Application Firewalls Based on Successful SQL Injection Attacks" IEEE 28th International Symposium on Software Reliability Engineering (ISSRE), Oct. 2017.

[10] Francis Kwadzo Agbenyegah and Michael Asante, "Impact of Firewall on Network Performance", International Journal of Scientific & Technology Research, ISSN 2277-8616, Volume 6, Issue 03, March 2017.