The Impact of Firewall Security for Wireless Performance

Tagwa Ahmed Bakri Gali[1], Amin Babiker A/Nabi Mustafa[2]

Depatment of Communication Engineering – AL–Neelain University, Khartoum – Sudan

Abstract: ***This paper evaluates firewalls, their importance in protecting networks and their functions such as performance, efficiency and security. The intercourse between the security and performance efficiency is created through different scenarios and the relationship between security and performance in firewalls is evaluated. Several scenarios were evaluated through simulations using OPNET to show the effects of firewalls on network performance.***

Keywords: Firewalls, network security, network Performance

1. Introduction

Network security becomes an ever increasingly vital part of any network designs and executions. A typical network security involves the planning and design of an organization’s network and information technology (IT) security infrastructures, so as to protect its valuable Applications, sensitive data, and network resources from Unauthorized access.

Researchers and developers work round the clock to combat security risks. Firewalls are all important ingredients in improving network security. Antivirus developers always recommend the usage of a separate firewall.

2. Methodology

2.1 Firewall

A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules. [1]

Performing as a barrier between a trusted network and other untrusted networks -- such as the Internet. A firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network defined in the firewall policy is; all other traffic is denied. [2]

2.2types of firewalls

1) Packet firewalls: examine incoming and outgoing packets and apply a fixed set of principles of the packages to determine whether they will be permitted to go. The packet filter firewall is typically very fast because it does not examine the data in the package. It only examines the type of the Packet along with the source and destination addresses, including URLs, domain names, and so on .[3]
2) Stateful firewalls: improves on the functions of packet filters by going after the state of connections and blocking packets that deviate from the required state. This is accomplished by incorporating greater awareness of the transfer layer. As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are countenanced by an existing firewall rule, but unlike packet filtering, stateful inspection keeps track of each liaison in a state table. [4]

   While the privileged information of state table entries varies 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, use, and termination. [5]
3) Application-layer firewalls: As attacks against Web servers became more coarse, so likewise did the demand for a firewall that could protect servers and the applications running along them, not merely the network resources behind them. Application-layer firewall technology first emerged in 1999, enabling firewalls to inspect and filter packets on any OSI layer up to the application layer. The underlying benefit of application-layer filtering is the ability to block specific content, and know when certain applications and protocols -- such as HTTP, FTP and DNS -- are being misapplied. Firewall technology is immediately integrated into a diversity of devices; many routers that pass information between networks contain firewall components and most home computer operating systems include software-based firewalls. Many hardware-based firewalls also provide additional functionality like basic routing to the internal network they protect. [6]
4) Proxy firewalls: Firewall, proxy servers also operate at the firewall's application layer, acting as an intermediary for requests from one network to another for a specific network application. A proxy firewall prevents direct links between either sides of Firewallwall; both sides are forced to accept the session through the proxy, which can choke up or allow traffic based on its rule set. A proxy service must be run for each type of Internet application the firewall will support. [7]

3. Network Models and Results

We made out the wireless network simulation scenario, once the existence of the Firewall and the other without Firewall. We put several determinants of performance: delay – Traffic Received - UDP - Load on the mesh. Where we put up when comparing the presence of Firewall and not present of Firewall for the delay that is receiving high-delay data which is not relatively desirable in many cases. For data received, the network without a firewall the data received in so tight. For UDP we note that the presence of firewall we get the highest value and access to the information. The load in the network shall be great when there is a firewall, causing congestion in the network and the lack of access of efficiency is demanded.

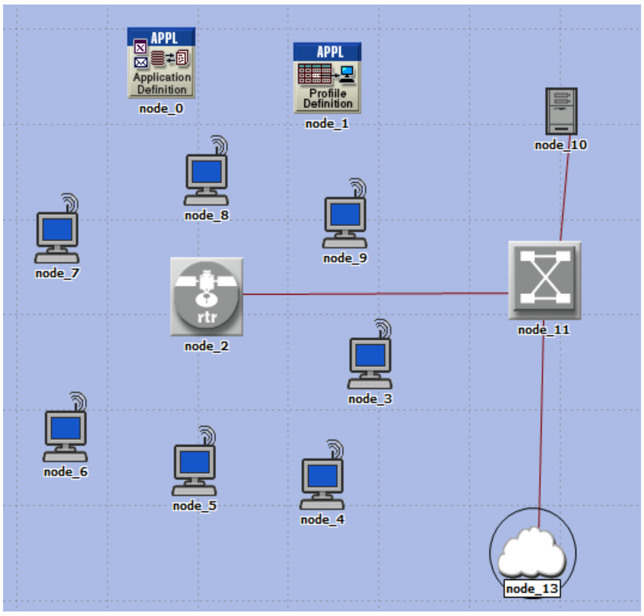

Figure 1: wireless network without firewall

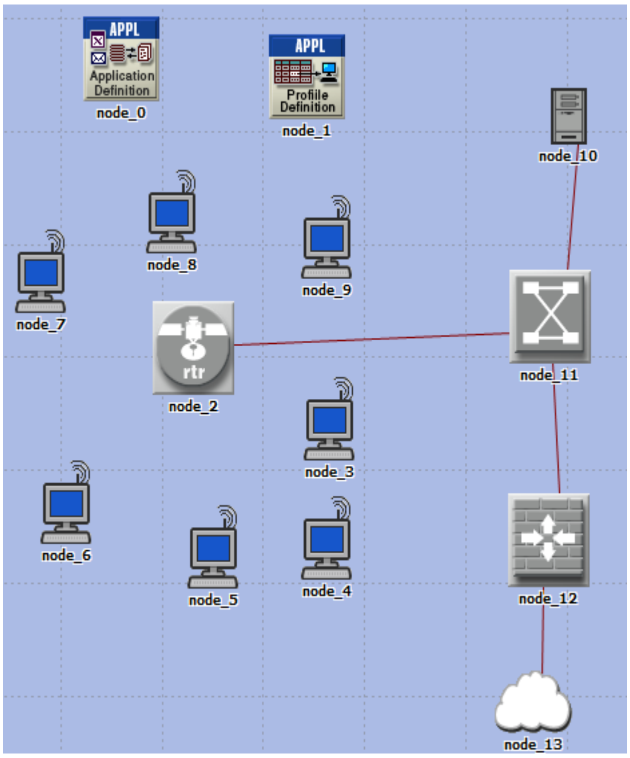

Figure 2: wireless network with firewall.

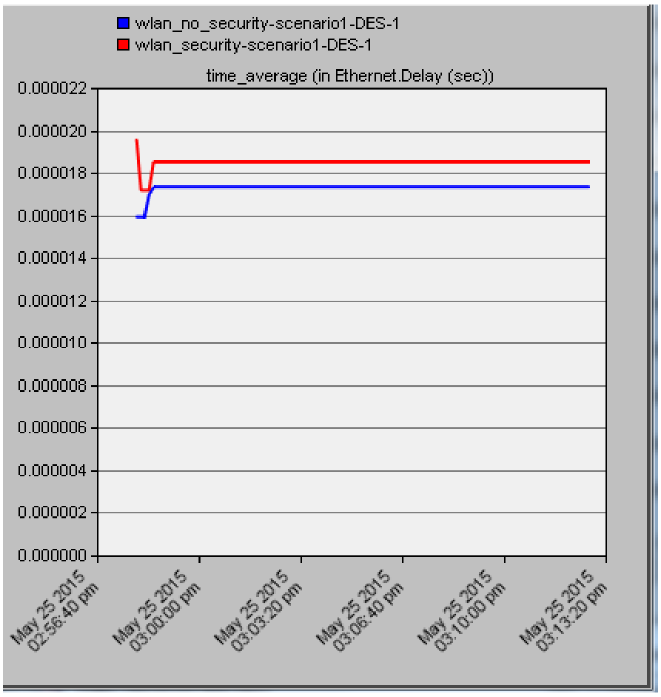

Figure 3: comparison between the firewall and without a firewall on Delay.

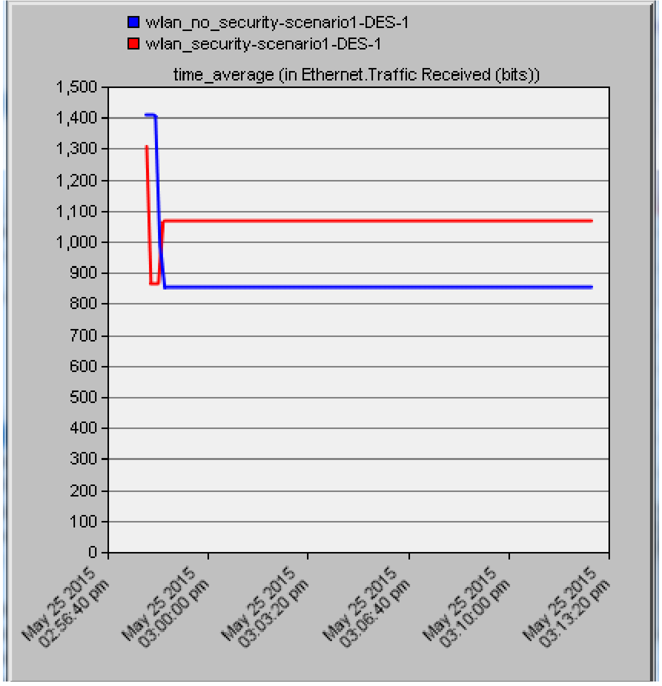

Figure 4: comparison between the firewall and without a firewall on Traffic Recived.

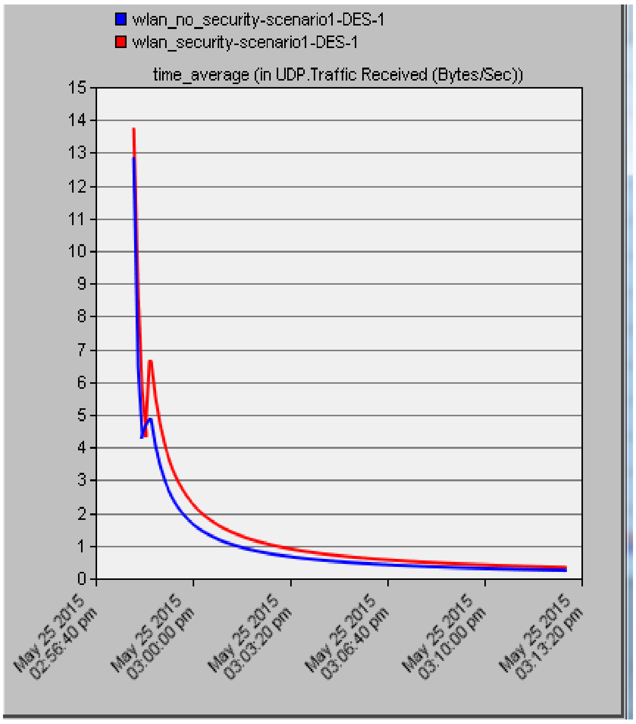

Figure 5: comparison between the firewall and without a firewall on UDP.

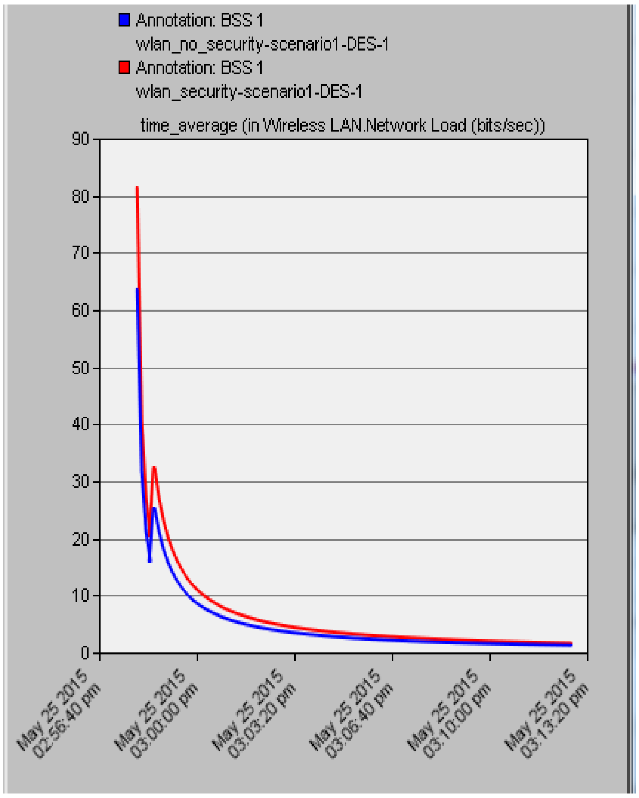

Figure 6: comparison between the firewall and without a firewall on Network Load

4. Conclusion

In this paper, Importance of firewalls in securing network communications and resources is essential. Still, more processing of networked information may contribute to performance degradation of networks. Hence, it is important that as firewalls are scrutinized in terms of their contribution to network security, they should also be investigated in terms of their effects of web protection. In this paper, various scenarios incorporating firewalls are analyzed with regard to their effects on the network performance.

For this, simulation models were created and implemented on OpNET for calculating network performance with and without firewalls.

Our finding that, the intuitive belief about firewalls that security and performance efficiency are inversely proportional does not necessarily hold in every situation, and certainly not in today's cyber world where threats are not myths but the reality of the daily life. This work supports and underscores the importance of firewalls in the world of networking. However, there a tremendous need to look further into firewalls and their enhancements.

Referances

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

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

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

[4] Conway, Richard (204). Code Hacking: A Developer's Guide to Network Security. Hingham, Massachusetts: Charles River Media. p. 281. **ISBN 1-58450 314-9**.

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

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

[7] Oppliger, Rolf (May 1997). "Internet Security: FIREWALLS and BEYOND".Communications of the ACM 40 (5): 94. doi:10.1145/253769.253802