International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Impact of Firewalls on IEEE.802.11a, b, g, n WiFi Releases Networks

Mudathir Babiker Idris Babiker[1], Dr. Amin Babiker A/Nabi Mustafa[2]

[1,2]Faculty of Engineering, Neelain University, Khartoum –Sudan

Abstract: ***Networks security has been a serious issue in recent years, especially in WLANs which is more vulnerable to attack than other wired networks. Now a days WLANs cannot be avoided so studies must be taken to find the best security solutions to protect the WLANs and try to minimize the negative effect of these solutions on the network performance.This paper analyzes the impact of firewall on IEEE 802.11a, b, g & n wifi releases regarding the delay and throughput in traffic between the wireless nodes and the server using OPNET 17.5 WLAN utility. Two scenarios for each release have been introduced and simulated, with firewall and without firewall.***

Keywords: Firewall, OPNET 17.5, Security, WLAN, Delay, Throughput

1. Introduction

Background

The word "firewall" was used firstly by Lightoler in 1764 not for network protection but to describe the part of the building which use fire in it (e.g. a kitchen). The primary reason for implementing firewalls is to protect and enforce policy of business networks. Different methods and types have been used since the creation of firewalls. The way firewalls works is to filter data packets by using different levels of the ISO network model like application, transport, network and data layers.

Firewalls Techniques

The techniques used by firewalls can be divided into four categories, Service Control, Direction Control, User Control and Behavior Control. Service control means that which type of internet services are allowed to be used by network users, direction control means that in which direction predefined services are allowed to go through the firewall, user control activated to control and determine which user is allowed to use the service, this one is always used for local users. The last feature is behavior control which monitors how specific services are being used and controlled.

Types of firewalls

Packet Filtering Firewall

The perception of packet filtering firewall depends on setting many rules to each packet going inside or outside the network, then according to these rules the firewall forward or discard the packet. These rules depend on a group of information's inside the packet like source ip address which is the ip address of the device the packet comes from, destination ip address which is the ip address of the device the packet goes to, the transport layer protocol type and source and destination port number which indicate the type of the application used like HTTP, SNMP or FTP.

Stateful Inspection Firewalls

This type of firewall adds another security feature to packet filtering firewall by making a directory for each outgoing TCP connection as shown in table 1. Now stateful inspection firewall will permits incoming packets only to those how comply with one of the already established connections or directory. That means this kind of firewall records information about TCP connection.

Table 1

Source Address	*Source Port*	*Destination Address*	*Destination Port*	*Connection State*
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established

Application-Level Gateway

It is also called "application proxy" , it works for example when the user makes a request to access an application in the remote server, like FTP or SMTP using TCP/IP connection, then the proxy ask the user to provide a valid user ID and authentication information, after that the connection is established. There is a code that must be delivered by the proxy to the firewall for each application requested if not the service will not be allowed. The proxy also has another feature, it can be configured by network administrator to allow only specific features of the application and deny the others.

Circuit-Level Gateway

This type of gateway works similar to application level gateway and it can be dependent system or a part of a proxy function for specific applications. The way it works is to establish two different TCP connections, the first one is between the gateway and the inside user and the other one is between the gateway and outside user and it does not examine the contents of packets. The security policy comes in determining which connection is to be allowed. The ideal use of this type of gateways is in the situation in which the system administrator trusts the internal users

2. Methodology

OPNET 17.5 has been used to simulate four different methods of IEEE 802.11a, b, g & n releases to analyze the impact of firewall to the traffic. Two scenarios are used, one with firewall and the other without firewall, tow parameters, delay and throughput have been considered to evaluate the network performance for each 802.11 releases.

3. Network Components

This section discusses the network components used in this simulation which is shown in figure 1 & figure 2. The components used in the suggested networks model is running on OPNET 17.5, the devices in figure 1 are 40 WLAN stations ,SIP server, HTTP server, 2 ip phones, switch Ethernet 16,Firewall,router,IP backbone. Figure 2 has the same devices of figure 1 except the firewall. We use web browser HTTP and FTP heavy traffic applications in the Application_ Config .

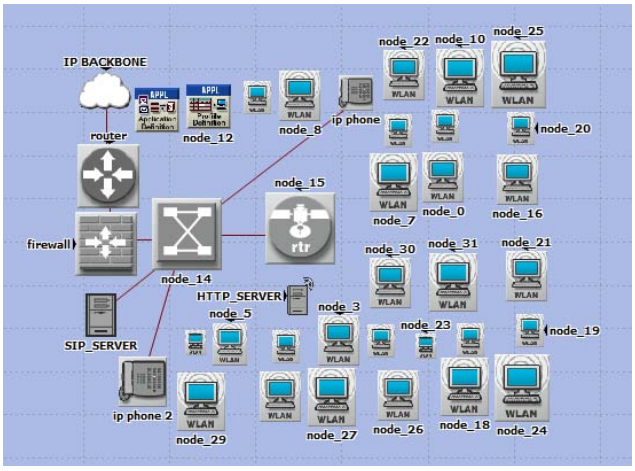

Figure 1

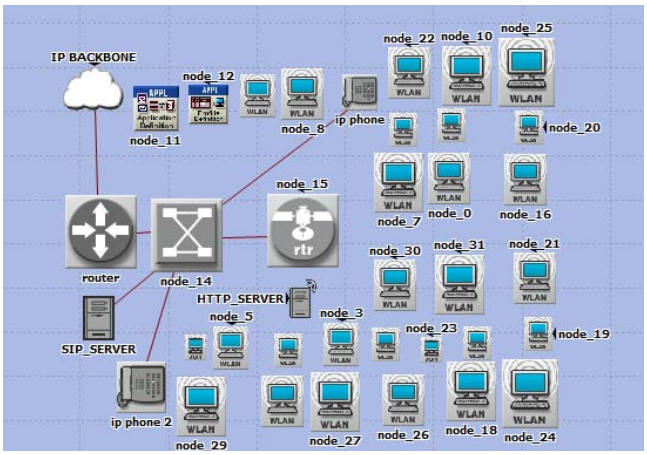

Figure 2

4. Results and Analysis

The analysis of the results for firewall impact on Wi-Fi releases a,b,g and n will be based on figures 3,4,5,6,7,8,9,10 which represent the delay and throughput in WLAN network shown above.

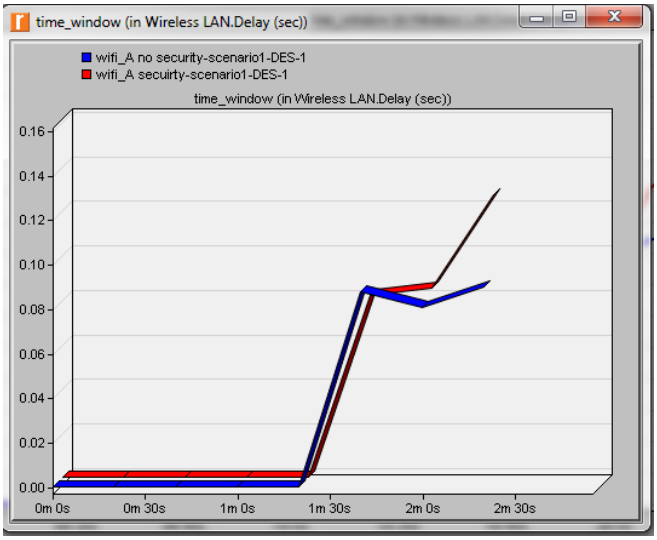

Figure 3: Delay

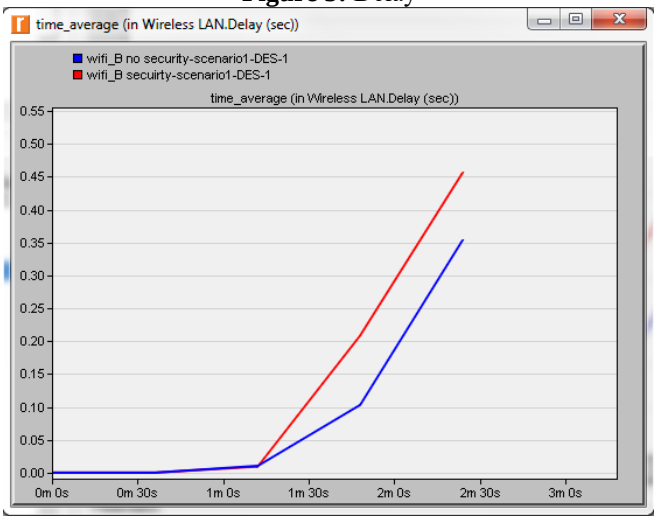

Figure 4: Delay

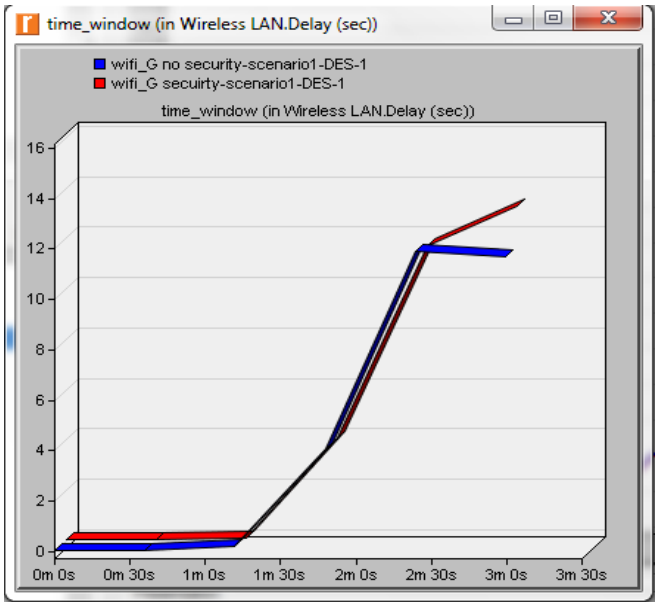

Figure 5: Delay

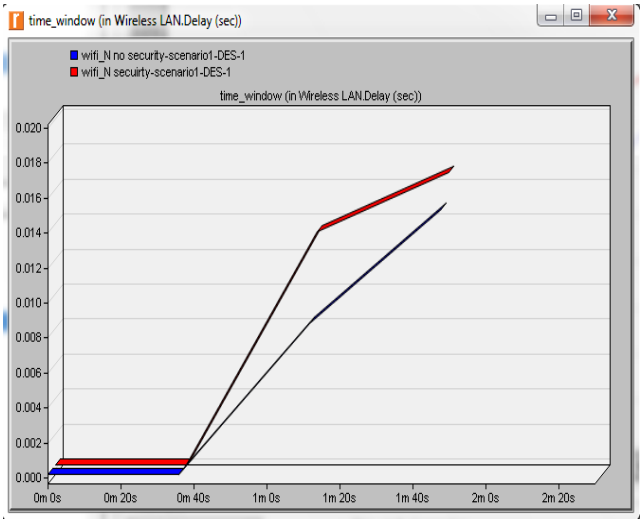

Figure 6: Delay

Figure 3 and 7 represents the comparison of the above wifi network with the use of IEEE 802.11 a release, with and without firewall, the result shows that the delay is increased when using firewall device because of security procedures implemented by the firewall for every packet going in or out of the network but the throughput will decrease for the same reason. Figure 4 and 8 shows the result of using IEEE 802.11 b release, Figure 5& 9 shows the result of using IEEE 802.11 g release, Figure 6 & 10 shows the result of using IEEE 802.11 n release. The results show clear impact of firewall wifi network especially in release b. The use of firewall cannot be avoided but we need to use it with less security features to decrease its impact on network performance.

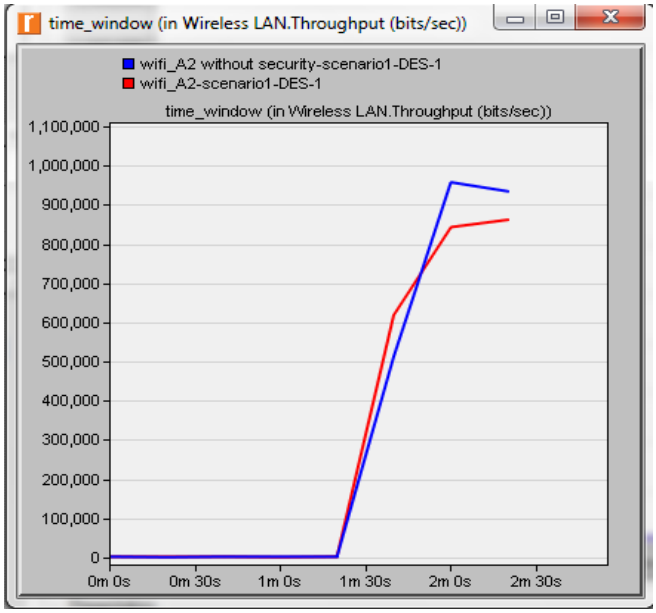

Figure 7: Throughput

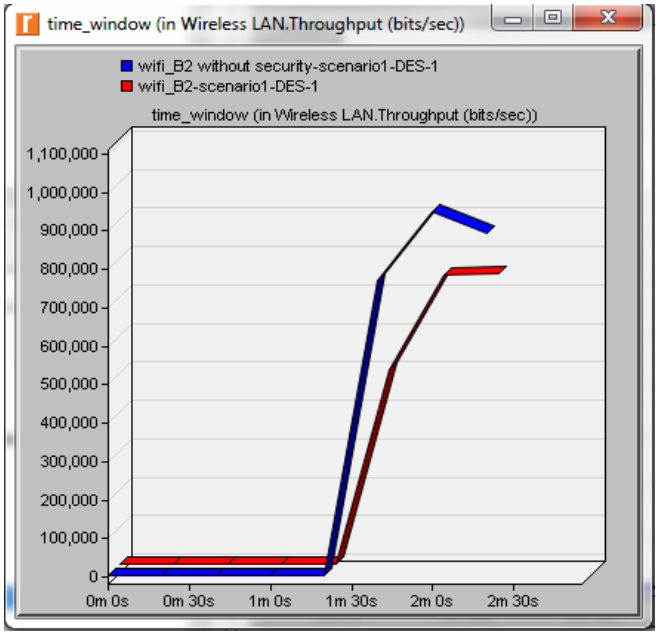

Figure 8: Throughput

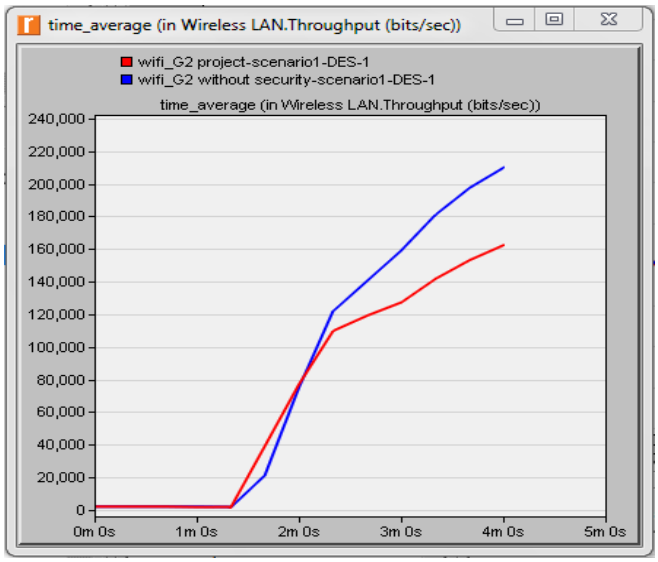

Figure 9: Throughput

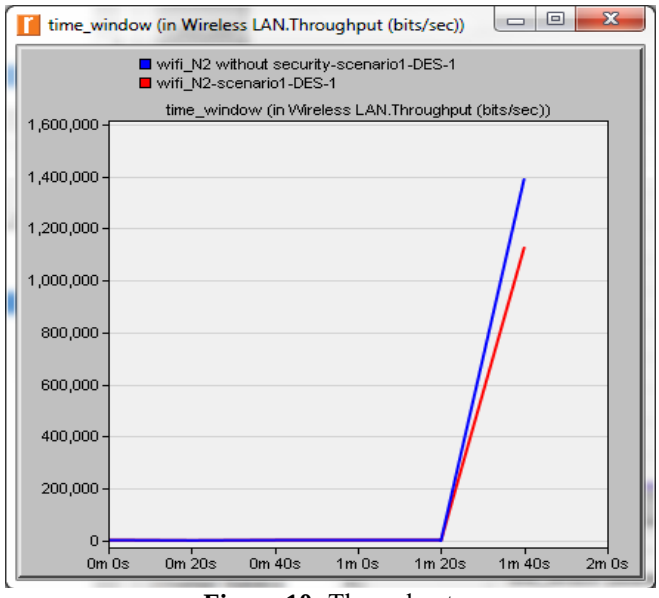

Figure 10: Throughput

References

[1] William Stalling," Network Security Essentials" fourth edition.
[2] Aruna Malik, Harsh K Verma, Raju Pal " Impact of Firewall and VPN for securing WLAN" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 5, May 2012.
[3] S P Maj, W Makasiranondh, D Veal," An Evaluation of Firewall Configuration Methods", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010.
[4] Manila Bohra1, Laghvi Aloria2, Neha Gupta,"Distributed Firewall Application for Policy Management and Network Security "**International** Journal of Innovative Research in Computer and Communication Engineering *Vol. 1, Issue 2, April 2013.*
[5] Seny Kamara, Sonia Fahmy, Eugene Schultz, Florian Kerschbaum, and Michael Frantzen "Analysis of Vulnerabilities in Internet Firewalls" Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University.
[6] RUCHIR BHATNAGAR &VINEET KUMAR BIRLA," WI-FI SECURITY: A LITERATURE REVIEW OF SECURITY IN WIRELESS NETWORK" IMPACT: International Journal of Research in Engineering & Technology, Vol. 3, Issue 5, May 2015.