Volume 2, Issue 5, May 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Impact of Firewall and VPN for securing WLAN

Aruna Malik*
National Institute of Technology
Jalandhar, Punjab 144011, India

Harsh K Verma
National Institute of Technology
Jalandhar, Punjab 144011, India

Raju Pal
National Institute of Technology
Jalandhar, Punjab 144011, India

Abstract— ***Many corporations are seriously concerned about security of networks and therefore, their network supervisors are still reluctant to install WLANs. In this regards, the IEEE 802.11i standard was developed to address the security problems, even though the mistrust of the wireless LAN technology still exists. The thought was that the best security solutions could be found in open standards based Technologies that can be delivered by Virtual Private Networking (VPN) being used for long time without addressing any security holes for the past few years. This paper analyzes impact of integrating Virtual Private Network technology and firewall to secure the flow of traffic between the client and the server using OPNET WLAN utility. Three scenarios without firewall, with firewall and Firewall_VPN have been introduced and simulated. The simulation results of three scenarios are compared over WLAN and analyse the impact of Firewall and VPN on network performance.***

Keywords— *VPN, Firewall, OPNET 14.5, Security, WLAN*

I. Introduction

WIRELESS LAN technologies such as IEEE802.11 provide end users and network professionals with a good degree of flexibility and cost reduction in terms of cost of saving cables. The Access Point (AP) is a wireless LAN transceiver that serves as a focal point of a stand-alone wireless network or as the connection point between wireless and wired networks. Several wireless 802.11 technologies are now available [1]. IEEE 802.11b is the most well known technology. Its bit rate can be up to 11 Mbps in the 2.4 GHz band. IEEE 802.11g is an extension of 802.11b; and works in the same 2.4GHz band, its data rate can be up to 54 Mbps. IEEE 802.11a operates in the 5 GHz band up to 54 Mbps [2]. As WLANs provide mobility and convenience to users, the efficiency of today's WLANs are still far from satisfactory. Communications may be cut off when mobile stations travel between cells Wireless data connections have high bit error rates, low bandwidth and long delays [3].

With the rapidly growing adoption of the wireless networking technology, for many implementers, security is the issues of utmost priority. The main reasons for growing concerns in security are the insufficiencies of the basic security services offered by the IEEE 802.11 standard. Then again, security is increasingly becoming important for delivering next generation wireless multimedia applications. This motivated research into exploring alternate avenues for the enhancement of the required security solutions [4].Security can be provided by using Firewall as well as VPN. A firewall is a specially programmed router that sits between a site and the rest of the network. It is a router in the sense that it is connected to two or more physical networks and it forwards packets from one network to another, but it also filters the packets that flow through it [5].

A virtual private network can establish secured virtual links among different organizations, such as branch offices. Tunnelling by appending additional headers facilitates the virtual lease line while cryptographic technologies prevent private information passing through the public Internet from being intercepted, modified, or fabricated. However, when complex cryptographic algorithms are employed, encryption and decryption within VPN tunnels becomes the performance bottleneck.Hence, dedicated hardware has been proposed to maximize the throughput and minimize the latency. Modern VPN technologies include PPTP, L2TP, and IPsec. PPTP and L2TP work at the data link layer and are suitable for secure remote access between mobile users and enterprises.In contrast, IPsec works at the network layer and can provide secured tunnels among subnets. IPsec provides encryption and authentication mechanisms for the IP protocol suite. Encryption prevents intruders from reading information by sniffing traffic among hosts. Authentication prevents intruders from spoofing the hosts of a connection. Nowadays, IPsec has become a must for the VPN service in a security gateway [6]. This paper is organized as follows: Section 2 presents background information. Section 3 describes the network topology studied. Section 4 analyses results and discussion. Section 5 concludes this paper.

II. Background Information

The wired network protected in both ways using VPN as well as Firewall. In case VPN a dedicated link (Tunnel) from source Router to Destination Router so there are minimum chance for interruption by proxy. But traffic sent and received is minimum than firewall because in firewall case proxy sent packet continuously to server for synchronizations the data. Since SND/REC may synchronize the data from server but in the case of VPN there is no chance for that's one. In other way we think security about WLAN networks since our aim to compare the two networks so all scenario contains same infrastructure as is in wired networks. The use of WLAN networks raises a critical problem in security like the abolition of the physical barrier the first activity that we could notice in practice is simply the search for an Internet access. The best complement in the WEP [7] stays a solution of VPN (Virtual Private Network). Various technologies allow going up a tunnel VPN, which consists in calculating the data passing in transit between two machines, to insure the integrity and the authentication users.

III. Network Topology

This section describes the network topology used for the simulations. In this network we are using three departments namely entertainment, research, education and three servers namely voice, video and data. All departments are connected to router1 (Ethernet4_slip8_gtwy) via switch Ethernet16_switch_adv).Servers are connected to router 2. A firewall is implemented between router 1 and router 2 via IP Cloud. Each subnet contains wireless workstations and one access point. Entertainment department support voice application and video applications while research department support video and data applications and education department support video, voice and data applications. Firewall is connected to the IP cloud which in turn connected to Router 2 using PPP DS1 at Data rate 1.544Mbps. Servers are connected to Router 2 using 100 base T with data rate of 100 Mbps. Subnets are connected to switch which in turn connected to Router 1 using 100baseT at data rate of 100Mbps. The network model is shown in the Fig 1.

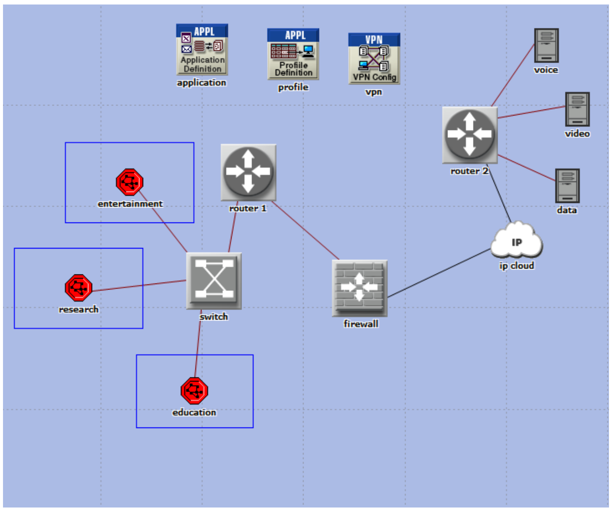

Fig 1. Network Topology Used

In our network we are using three Scenarios namely:

Without Firewall

In this scenario we allowed all the clients in the subnets to access all the traffic i.e. voice, video and data from the servers.

With Firewall

We assume that we need to protect the video applications in the data server from external access, including the entertainment department, so we used a firewall in order to do this.

Firewall_VPN

In the firewall scenario, we protected the video traffic in the server from any external access using the firewall router. Suppose we want to allow the video clients in the entertainment department to have access to the video applications in the server, since the firewall filters all video related traffic regardless of the source of the traffic, we need to consider the VPN solution [8, 9]. The firewall will not filter the traffic created by video clients because the IP packets in the tunnel will be encapsulated inside an IP datagram.

A. Parameters used in the network

1) Workstation:

Throughout our simulation we used wlan_wkstn_adv node model it represents a workstation with client-server applications running over TCP/IP and UDP/IP. The workstation supports one underlying WLAN connection at 1Mbps, 2Mbps, 5.5Mbps and 11Mbps.This workstation requires a fixed amount of time to route each packet, as determined by the "IP forwarding Rate" attribute of the node. Packets are routed on a first-come-first serve basis and may encounter queuing at the lower protocol layers, depending on the transmission rates of the corresponding output interfaces.

2) Server:

In our network we use Ethernet Server. This Ethernet Server model represents a server node with server applications running over TCP/IP and UDP/IP. This node supports one underlying Ethernet connection at 10Mbps, 100Mbps, or 1 Gbps.

3) Switch:

In our network we use ethernet16_switch.This node model support up to 16 Ethernet interfaces. The switch implements the spanning tree algorithm in order to ensure a loop free network topology. The number of interconnections is limited to 16 for this type of switch. In addition, the connections can be at 10Mbps, 100Mbps, or 1000Mbps.

4) Subnet:

It is a single network object that contains other network objects (links, nodes, and other subnets). Sub-networks allow us to simplify the display of a complex network through abstraction. It also helps us in logically organize network model.

5) Firewall:

The firewall, which can also be seen such as as concentrator VPN follows the model OPNET "ethernet2_slip8_firewall". It thus contains two interfaces ethernet, those who interest us here, but also 8 interface series, unused in our case. It is characterized by the same parameters (CPU/Workstations, ARP/Wireless Router, IP: Ethernet /Server). Since the most common WLAN usage is considered, the wireless speed was configured at 11Mbps with the random CSMA/CA DCF access mode [10].

6) IP Cloud:

In our network we use ip32_cloud node model. It represents an IP cloud supporting up to 32 serial line interfaces at a selectable data rate through which an IP traffic can be can be modelled. IP packets arriving on any cloud interface are routed to the appropriate output interface based on their destination IP address.

7) Access Point:

Throughout our simulation we use wlan_ethernet_router_adv. This is a wireless LAN based router with one ethernet interface.

8) Router:

The ethernet4_slip8_gtwy node is used as router in our network. This model represents an IP based gateway supporting four ethernet hub interfaces, and eight serial line interfaces. IP packets arriving on any interface are routed to the appropriate output interface based on their destination IP address. This gateway requires a fixed amount of time to route each packet as determined by the "IP Routing Speed" attribute of the node.

IV. Results And Discussion

1) *Throughput*

It can be defined as total data traffic in bits/sec successfully received and forwarded to the higher layer by the Wlan Mac layer.It can be easily seen from the fig 2 that throughput is high in case of with firewall as compared with vpn .It is found that the throughput value in case of with firewall, without firewall and VPN is 1240425.185bps, 848001.7203bps and 732454.9737bps respectively.

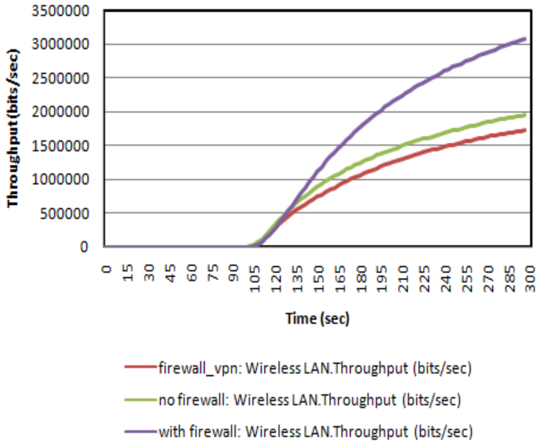

Fig 2. Results for Throughput

2) *Delay*

It represents the end to end delay of all the packets received by the wireless LAN Macs of all Wlan nodes in the network and forwarded to the higher layers. Delay is maximum in case of Firewall_vpn while it is found minimum in case of with firewall. Delay values in case of firewall_vpn is found 0.6158 sec while it is found .3836sec in case of no firewall and in case of with firewall this value found to be 0.1078 sec as shown in fig 3.

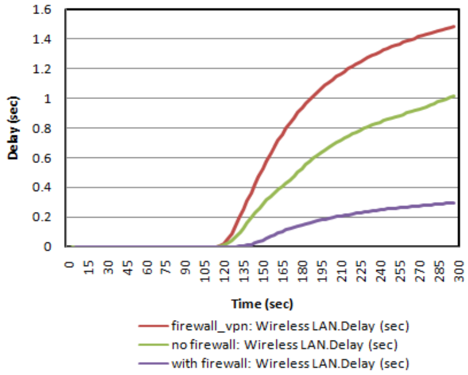

Fig 3. Results for Delay

3) *Retransmission Attempts*

It can be defined as total no of retransmission attempts by all WLAN Macs in the network until either packet is successfully transmitted or it is discarded as a result of reaching short or long retry limit. Retransmission attempts are high in case of with firewall and minimum in case of no firewall. It is found that values for retransmission attempts in case of with firewall is 0.66 while this value change to 0.06 in case of no firewall while in case of firewall _vpn this value changes to 0.07 as shown in fig 4.

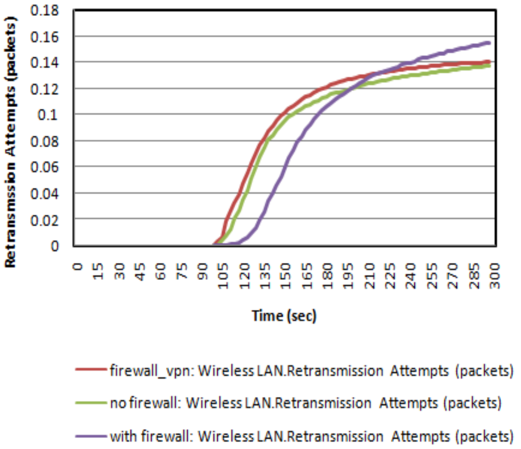

Fig 4.Results for Retransmission Attempts

V. Conclusion

In this paper we use three different scenario namely without firewall with firewall and firewall _vpn .It is analyzed that throughput is high in case of with firewall and minimum in case of firewall_vpn. There is maximum delay is found in case of firewall_vpn. It is found that retransmission attempts is high in case of with firewall.Thus it is concluded that using firewall and vpn the security of the network is increased while on the other hand there is reasonable decrease in the performance of network which may be due to the encryption process and added authentication headers for packets.

ACKNOWLEDGMENT

The author is thankful to the Department of Computer Science and Engineering, Dr.B.R. Ambedkar National Institute of Technology, Jalandhar for providing the computing facilities to carry out this work.

REFERENCES

[1] M. M.A. Ghazala, M. F. Zaghloul, and M. Zahra, "Performance Evaluation of Multimedia Streams over Wireless Computer Networks (WLANs)", International Journal of Advanced Science and Technology Volume 13, December, 2009.

[2] Sapna, M. Sharma and H. Kaur "Performance Evaluation of Hybrid network Using RIP &IGRP for Different Applications", 2010 IEEE.

[3] W. Hneiti, N.Ajlouni "Performance Enhancement of Wireless Local Area Networks", 2006 IEEE.

[4] S.Kumudu and A.Seyed Shahrestani "Wireless VPNs: An Evaluation of QoS Metrics and Measures" 2005 IEEE.

[5] Y.P Kosta, U. D. Dalal and R.Jha "Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN)", 2010 IEEE.

[6] Y.D. Lin, H.Yunwei and S.T. YU, N. C. Tung "Building an integrated security gateway mechanism performance evaluation implementation & research issue" IEEE Communications Surveys http://www.comsoc.org/pubs/surveys

[7] IEEE Std. 802.11, "IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification," Edition 1999, [10] ISO/IEC 8802-11: 1999.

[8] http://www.opnet.com/products/opnet-products.html.

[9] http://www.opnet.com/products/modeler/home-1 html.

[10] M.S.Gast, "802.11 Wireless Networks: The Definitive Guide", Editor O'Reilly, April, 2002.