A Security Solution for Wireless Local Area Network (WLAN) Using Firewall and VPN

Sourabh Kumar Vishali Sharma
Department of Electronics and Communication Engineering,
Lovely Professional University, Phagwara, Punjab-144401

Abstract
In the era of internet millions of users share resource for different purpose. The chances of security risks are more when a user connected with internet. Internet technology plays an important role in every aspect of human life. We can create virtual connectivity with-in seconds with anyone in the world and can exchange or share the information through internet. Sometimes these information is very useful for Defense, and personal use. Sometimes this information is stolen on the internet or we can say destroyed so that receiver cannot receive that information, so for successful communication on internet our connection should be protected. For this protection we can use Firewall protection, VPN Network. These Networks is much more protected than normal Network. Network with VPN and Firewall is faster and efficient rather than normal connection. In normal Network user may faces unexpected delay due to malware and virus. In this paper we have described and analyze impact of Virtual Private Network technology and firewall with normal network. We have simulated three scenarios without firewall, with firewall and Firewall_VPN. The simulation results of three scenarios are compared over WLAN and analyze the impact of Firewall and VPN on network performance. OPNET 14.5 is used for simulator work.

Keywords: VPN, Firewall, Security, WLAN, OPNET 14.5.

I. INTRODUCTION

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.Security can be provided by using Firewall as well as VPN [2].

Firewall is a barrier between Local Area Network (LAN) and the Internet. It allows keeping private resources confidential and minimizes the security risks. It controls network traffic, in both directions. Figure 1 depicts a sample firewall between LAN and the internet. The connection between the two is the point of vulnerability. Both hardware and the software can be used at this point to filter network traffic.

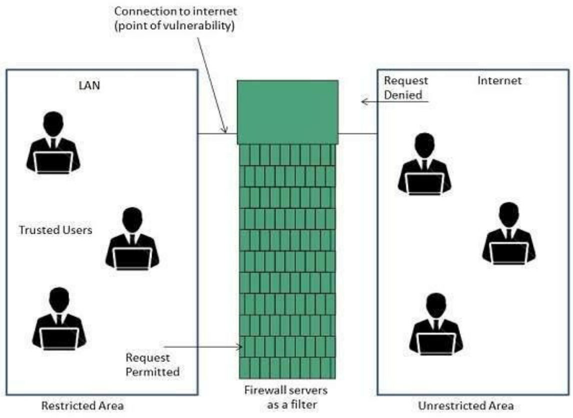

Fig 1 Firewall protections

A virtual private network (VPN) provides a secure connection between a sender and a receiver over a public non-secure network such as the Internet. A secure connection is generally associated with private networks. (A private network is a network that is owned, or at least controlled via leased lines, by an organization). A VPN can transform the characteristics of a public non-secure network into those of a private secure network. VPNs reduce remote access costs by using public network resources. Compared to other solutions, including private networks, a VPN is inexpensive.

This paper is organized as follows: section II describes the proposed work, section III describes the network topology studied, section IV analysis results and discussions, section V concludes this paper and section VI describes about the future work.

II. PROPOSED WORK

Fire wall play an important role when we communicate with others on internet .The chances of security risks are more when a user connected with internet. The Thought was that the best security solutions could be found with the help of firewall security. A firewall establishes a barrier between a trusted, secure internal network and another network that is, the Internet which is assumed not to be secure and trusted. It is basic need of user to work under the protection of firewall .But the question here is that is firewall security capable to handle the security risk, if capable then how firewall provide the protection and which level of protection provided by Firewall to us and how much chances of risk we can handle under the protection of firewall. in today time malware and virus is too strong that it can damage the protection level of firewall and also the vpn protection but it is necessary for safe communication on internet to work under these kind of protection level it reduce the threats chances level or you can say it increase the protection level which provide us that environment in which we can share information which may be personal or defense use.

To full fill our objective we need to implement the three different network of wlan so we can analysis or can check the security level of each network which will be firewall protected, vpn protected ,and without protected .

1. To Get Network performance without firewall using Remote-login, Http, and Data Base server.
2. To Get Network performance with firewall Using Remote-login, Http, and Data Base server.
3. To Get Network performance with Firewall _VPN Using Remote-login, Http, and Data Base server.

III.NETWORK TOPOLOGY

This section describes the network topology created of the three scenarios Without Firewall, With Firewall and Firewall and VPN.

1. *WITHOUT FIREWALL*

In this section the network topology for without firewall scenario is described which is used for the simulations. In this network we are using three servers which are HTTP, DataBase Server, and Remote Login also three Switched LAN networks which are HTTP LAN, DataBase LAN and Remote Login LAN are being used. All servers are connected to Router D via Ethernet 10baseT wire. All three

LAN networks are connected with Router A, Router B and Router C respectively via Ethernet 10baseT wire. Router A, Router B and Router C are connected to IP cloud which inturn is connected to Router D using PPP DS3 wire. The network model is shown in the Fig 2.

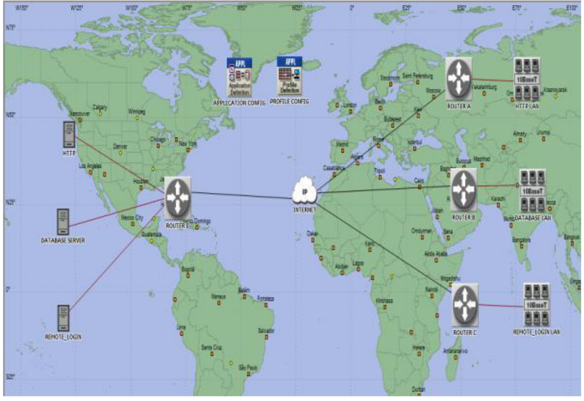

Fig. 2 Network Topology without Firewall

2. *WITH FIREWALL*

In this section the network topology for with firewall scenario is described which is used for the simulations. In this network also we are using three servers namely HTTP, DataBase Server, and Remote Login and three Switched LAN networks namely HTTP LAN, DataBase LAN and Remote Login LAN are also being used. All servers are connected to Router D via Ethernet 10baseT wire. All three LAN networks are connected with Router A, Router B and Router C respectively via Ethernet 10baseT wire. Router A, Router B and Router C are connected to IP cloud which inturn is connected to Router D_0 using PPP DS3 wire. A firewall is implemented between Router D and Router D_0. The network model is shown in the Fig 3.

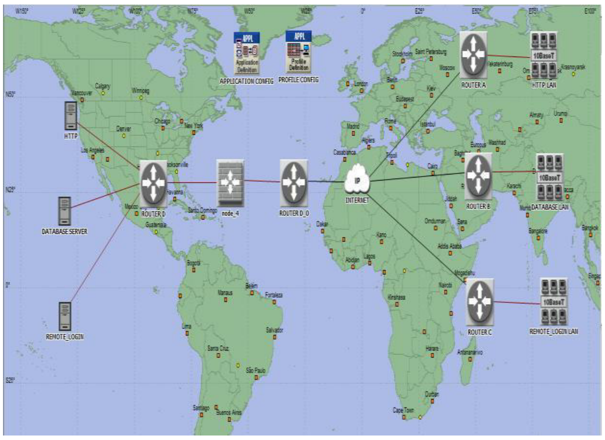

Fig. 3 Network Topology Using Firewall

3. *FIREWALL AND VPN*

In this section the network topology for with firewall and VPN scenario is described which is used for the simulations. In this the whole network is same as with firewall scenario but a vpn configuration is provided in the network.

IV. RESULTS AND DISCUSSION

This section compares and analysis the response time for all three scenarios without firewall, with firewall and with firewall & vpn for three different servers which are Data Base, HTTP and Remote Login.

1 *DB QUERY RESPONSE TIME:*

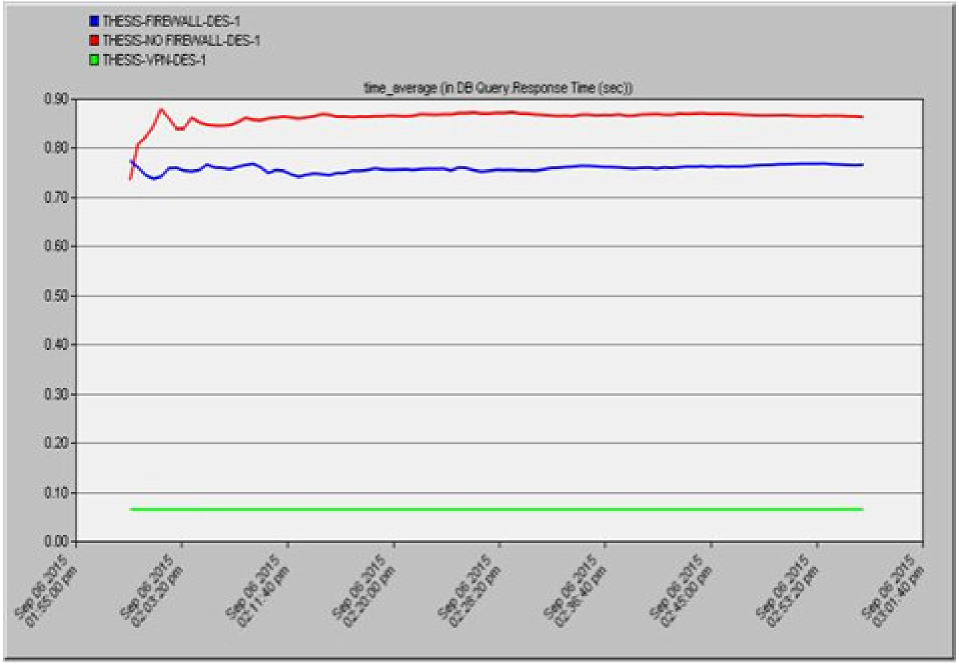

Fig. 5 DB QUERY RESPONSE TIME

Table 1. DB Query Response Time

Scenario Name	RESPONSE TIME (sec)
WITHOUT FIREWALL	0.6174
WITH FIREWALL	0.4028
FIREWALL & VPN	0.0286

From the figure 5, it can be seen that the DB Query Response Time of firewall & VPN is less than without firewall and with firewall. So we can say that when we use network protected with firewall & VPN then the DB Query Response Time is best as it is shown in figure that the response time in case of firewall & VPN is 0.0641 sec and we can also see that network with firewall is giving us DB Query Response Time of 0.7653 sec. But if we use network without firewall then the DB Query Response Time hike upto 0.8624 sec which is worst response time. So we can conclude that the network with firewall & VPN is faster as compared to with firewall and without firewall networks.

2. *HTTP PAGE RESPONSE TIME:*

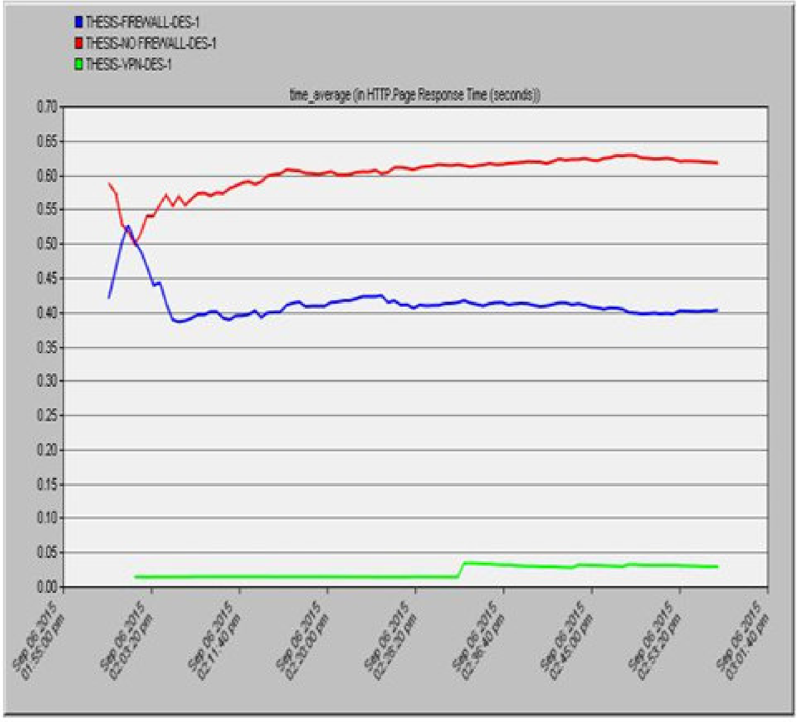

Fig. 6 HTTP PAGE RESPONSE TIME

Table 2 HTTP Page Response Time

Scenario Name	RESPONSE TIME (sec)
WITHOUT FIREWALL	0.8624
WITH FIREWALL	0.7653
FIREWALL & VPN	0.0641

From the figure 6, it can be seen that the HTTP Page Response Time of firewall & VPN is less than without firewall and with firewall. So we can say that when we use network protected with firewall & VPN then the HTTP Page Response Time is best as it is shown in figure that the response time in case of firewall & VPN is 0.0286 sec and we can also see that network with firewall is giving us HTTP Page Response Time of 0.4028 sec. But if we use network without firewall then the HTTP Page Response Time hike upto 0.6174 sec which is worst response time. So again we can conclude that the network with firewall & VPN is faster than the other two networks.

3. *REMOTE LOGIN RESPONSE TIME:*

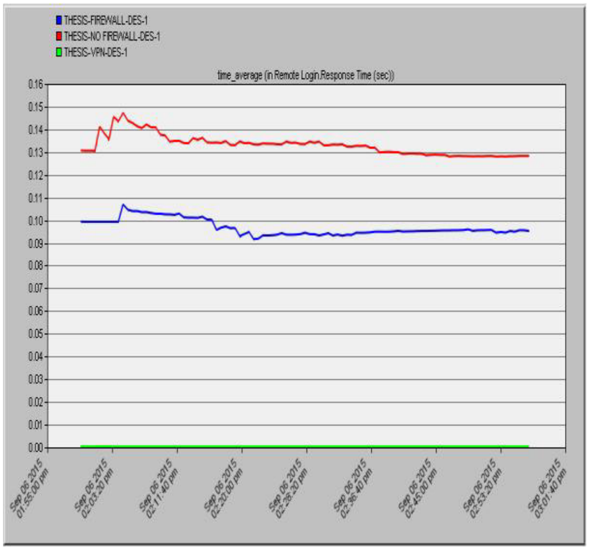

Fig. 7 REMOTE LOGIN RESPONSE TIME

Table 3 Remote Login Response Time

Scenario Name	RESPONSE TIME (sec)
WITHOUT FIREWALL	0.1283
WITH FIREWALL	0.0953
FIREWALL & VPN	0.0004

From the figure 7, it can be seen that the Remote Login Response Time of firewall & VPN is less than without firewall and with firewall. So we can say that when we use network protected with firewall & VPN then the Remote Login Response Time is best as it is shown in figure that the response time in case of firewall & VPN is 0.0004 sec and we can also see that network with firewall is giving us Remote Login Response Time of 0.0953 sec. But if we use network without firewall then the Remote Login Response Time hike up to 0.1283 sec which is worst response time. So here also we can conclude that the network with firewall & VPN is faster as compared to other two networks.

V. CONCLUSION

In this thesis we have simulated three scenarios without firewall, with firewall and Firewall_VPN. We have taken three different servers Http, Database and Remote login. For analysis we have taken different performance metrics on the behalf of each server like Http Page Response time, Database Response time, and Remote login Response time in which we obtained that network with Firewall_VPN is giving better Response time in comparison of other two scenarios. Firewall_VPN network performance is much better than with firewall network performance and with firewall network performance is better than without firewall network performance as network without firewall is giving us unexpected delay. So we can say that network with Firewall_VPN is faster and efficient rather than others networks.

VI. FUTURE WORK

In this paper we have taken Firewall_VPN and Firewall Network for faster and efficient .In future we can simulate different networks under advance security system. Also we can simulate PPTP, L2TP, Open VPN. Then we will analysis how much PPTP, L2TP, Open VPN is faster and how much efficiency it is providing to a network.

REFERENCES

[1] Hailu Tegenaw, Mesfin Kifle, "Application Aware Firewall Architecture to Enhance Performance of Enterprise Network", 2015 IEEE
[2] Aruna Malik, Harsh K Verma, and Raju Pal, "Impact of Firewall and VPN for securing WLAN",

International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, May 2012, IJARCSSE

[3] Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov, "Secure Virtual Private LAN Services: An Overview with Performance Evaluation", 2015 IEEE

[4] Anupriya Shrivastava, M A Rizvi, "External Authentication Approach for Virtual Private Network using LDAP", 2014 IEEE

[5] Hamid Alipour, Youssif B. Al-Nashif, Pratik Satam, and Salim Hariri, "Wireless Anomaly Detection Based on IEEE 802.11 Behavior Analysis", IEEE transactions on information forensics and security, vol. 10, no. 10, October 2015

[6] Meng Zhang, Anand Raghunathan, and Niraj K. Jha, "MedMon: Securing Medical Devices Through Wireless Monitoring and Anomaly Detection", IEEE transactions on biomedical circuits and systems, vol. 7, no. 6, December 2013

[7] Cataldo Basile, Antonio Lioy, Christian Pitscheider, Fulvio Valenza and Marco Vallini, "A novel approach for integrating security policy enforcement with dynamic network virtualization", 2015 IEEE

[8] Marco Baldi, Marco Bianchi, Nicola Maturo, and Franco Chiaraluce, "A Physical Layer Secured Key Distribution Technique for IEEE 802.11g Wireless Networks", IEEE Wireless Communications Letters, Vol. 2, No. 2, April 2013, IEEE

[9] Atri Mukhopadhyay and Goutam Das, "A Ring-Based Wireless Optical Network to Reduce the Handover Latency", Journal of Lightwave Technology, Vol. 33, No. 17, September 1, 2015, IEEE

[10] Fan Yan, Yang Jian-wen, Cheng Lin, "Computer Network Security and Technology Research", 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, 2015 IEEE

[11] Zouheir Trabelsi, Liren Zhang, Safaa Zeidan, "Dynamic rule and rule-field optimisation for improving firewall performance and security", The Institution of Engineering and Technology, 2014

[12] Hammad Kabir, Raimo Kantola, Jesús Llorente Santos, "Security Mechanisms for a Cooperative Firewall", 2014 IEEE International Conference on High Performance Computing and Communications (HPCC), 2014 IEEE 6th International Symposium on Cyberspace Safety and Security (CSS) and 2014 IEEE 11th International Conference on Embedded Software and Systems (ICESS), 2014 IEEE