The Impact Of Using Security Protocols In Dedicated Private Network And Virtual Private Network

Dr. Sabah Nassir Hussein FCMI, Abdul HadiQais Abdul Hadi

Abstract: With the development of computer networks techniques and the increased use of private networks, the intrusion and attack on these networks also increased, so the use of the protection protocols became necessary, but using these protocols will reduce the quality of the performance of these networks. This research highlights the impact of using security protocols on two types of private networks. The OPNET version 14.0 has been used to simulate the two networks and to apply the different types of security protocols such as (L2TP,PPTP, and IPsec).

Keywords: VPN; Security protocols; dedicated private network.

1. Introduction.

Attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of attacks are release of message contents and traffic analysis. The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. Attacks are very difficult to detect because they do not involve any alteration of the data. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.So to protect data transfer through network will useVPN (Virtual Private Network) is an overall term used to define a network that uses any mixture of techniques to safeguard a connection via a tunnel through the network. VPN transmits data through the tunnel. Before transmission package, it is encapsulated (wrapped) in a new package, with a new header. This header offers routing information so that you can pass a shared or public network, before it reaches its end of the tunnel point. VPN need both tunnel endpoints to support Tunneling Protocol itself [1, 2]. The disadvantages of VPNs Tunneling increase the length of IP packets;this may result in inefficient use of bandwidth, especially for short packets. Potential performance impact at end routers as they need to do more workRemove headers, decrypt packet body. Administrative overhead and cost associated with managing the VPN server.

- *Dr. Sabah Nassir Hussein FCMI, Abdul HadiQais Abdul Hadi*
- *Computer Techniques Engineering Department Computer Techniques Engineering Department, College of Electrical & Electronic Techniques College of Electrical & Electronic Techniques, Baghdad, Iraq Baghdad, Iraq*
- *drsabah2004@yahoo.com, mofa_hadi@yahoo.com*

In 2007 Muhammad Aamir1, Mustafa Zaidi and HusnainMansoor [3],presented the concept of Performance Analysis of Diff Serve based Quality of Service in a Multimedia Wired Network and VPN effect using OPNET . Thenetwork includes Internet based communication and VPN was configured to allow the access of 'Data Server' to the external user for Database service. It was observed when the server was accessed internally as well as by the external user, average data rate of Database traffic received by internal network users (bytes/sec) decreased due to external load. **In 2009 H. Bourdoucen, A. Al Naamany and A. Al Kalbani [4],**presented simulation of wireless LAN for IEEE802.11g protocol has been done, and analyzes impact of integrating Virtual Private Network technology to secure the flow of traffic between the client and the server farm using OPNET WLAN utility has been carried out. Two Wireless LAN scenarios have been considered and the results compared. These are Normal Extension to a wired network and VPN over Extension to a wired network. The results collected from the two scenarios, indicate the impact of performance, mainly Response Time and Load, of Virtual Private Network over wireless LAN.

2. Type of VPN:

Usually the VPN can be classifying as a*remote access* and *site-to- site* as shown in the fig (1) [5].

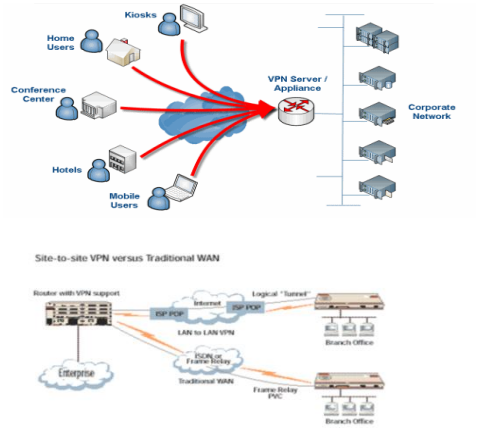


Figure (1**):** Theremote access, and site-to-site VPNs.

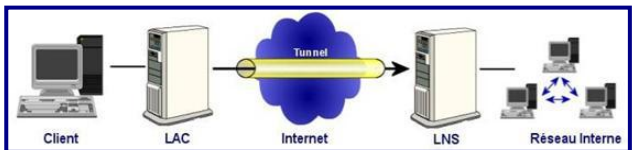
3. The security protocols of a VPN:

3.1- PPTP (point to point tunnel protocol).The PPTP is an extension of PPP, whichencapsulates PPP frames in IPdatagrams for transmission over an IP - based network, such as the Internet or an ATMnetwork. The PPTP control connections, to create, maintain, and terminate the tunnel. PPTPuses a modified version of Generic Routing Encapsulation (GRE).The payloads of the encapsulated PPP frames can be encrypted, compressed or both [6].Tunnel Maintenance with the PPTP Control Connection between PPTP client and PPTP server using reserved TCP. The PPTP control connection carries the PPTP call control and management message that is used to maintain the PPTP tunnel. This includes transmission of periodic PPTP Echo-Request and PPTP Echo -Reply messages to detect a connectivity failure between the PPTP client and PPTP server [7]. As shown in the Fig (2).

Figure (2): The PPTP connection.

3.2- L2TP(LAYER 2 TUNNEL PROTOCOL).

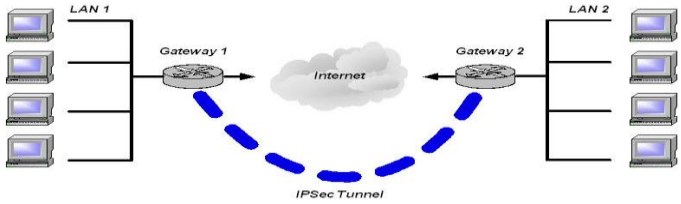
The L2TP Protocol is used for mixing multi-protocol dial-up services into current ISP (Internet Service Provider). PPP defines an encapsulation contrivance for transferring multiprotocol packets across layer 2 (L2) (PTP) links. Usually, a user gets a L2 connection to a Network Access Server (NAS) using one of techniques (e.g., ISDN,ADSL, etc.) and then runs PPP over that connection[8].L2TP uses UDP messages over IP networksfor both tunnel maintenance and tunneleddata. The payloads of encapsulated PPPframes can be encrypted, compressed or both.Fig (3) [9] shows that L2TP architecture divides the functions between L2TP Access Concentrator (LAC) that handles the physical communication to the remote client, and L2TP Network Server (LNS) that terminates remote clients' PPP session and acts as a gateway into the enterprise network



Figure(3): The L2TP Architecture

3.3 IPsec security

IPsec security is network layer protection and offer protection to the data traffic between two connecting entities in proposed networks. IPsec essential to be implemented with the support of two protocols authentication header AH and encapsulated security payload (ESP). These protocols can be appliedindividually or in a combinationway in two different modes; transport mode and tunneled mode. Both of these modes have different methods towards security behavior [10]. Fig(4) shows the IPsectunnel, the tunnel is create betweenthe Gateway-1router and the Gateway-2router.



Figure(4): The IPsec tunnel

IPsec use Encapsulated Security Payload (ESP)[11] protocol for data integrity, source authentication and data encryption. As declaredprevious that IPsec have two modes; transport mode and tunnel mode .IPsec use the tunnel mode of ESP to secure the complete IP datagram packet instead of only guarding IP header. If authentication of data source is particular to be a part of the security association. The security associations,is a virtual relationship between two sites containing of anestablished of arrangements about security parameters to be used to protect the traffic flow [12]. In IPsec security associations are the most important aspect and both AH and ESP protocols use SAs for transport and implementation of security policies. [13].

4. Software Implementation.

The design and implementation of a private network using the OPnetsimulator has been done assuming that private network serves productive factory sprawling spread throughout Iraq, that connect five sites one of them are in Mosul for two marketing group, other two marketing groups sites are in Basra and Baghdad, as well as two sites one for factory productive and the other to communicate with rawmaterials and equipment suppliers.Required from this network is to provide a secure private communication environment and protected from intrusion and interference then test the efficiency of the secure performance and protection for the two types of private networks. The types of application have been set from edit attributes as (FTP, EMAIL, VIDEO, DATABASE, HTTP and VOICE).

4.1- Implementation of a private network using Leased lines of ATM Networks.

The Asynchronous Transfer Mode (ATM) is a connection-oriented, telephone packet-switched, it provides quality of service QoS capabilities through its different service classes, such as CBR (constant bit rate) that is well-suited for voice traffic that usually requires circuit switching, and sources transmit stream traffic at a fixed rate, and UBR, unspecified bit rate. The leased line of the ATM has been used to set the private network that carries applications: Voice, video, Email, Data from data Base resources and FTP of the private network as shown in fig (5).

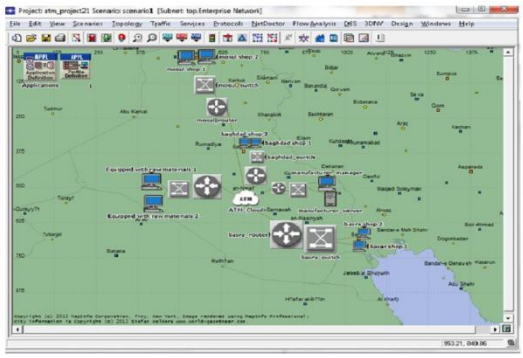


Figure (5): The ATM Leased line private network

4.2- Implementation of a Virtual Private Network over internet network

In this implementation the subnet has been changed from ATM to IP cloud as shown in fig (6), the VPN consist of the following devices; nine of workstation connected using Ethernet protocols, five switches of 16 ports, five sites routers, and one Ethernet server.

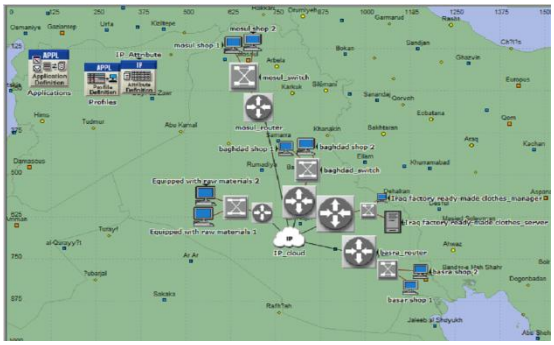


Figure (6): The Implementation of a Virtual Private Network

4.2.1 Implementation of L2TP.

The configure L2TP will be in the routers gateway and the configuration of L2TP will be the same in ATM network and internet network. all sites will be the same configuration but the defriend will be in the site (ID) and name of the site but the main site of the manufacture will defriend a lot because it must connect to many site so it must to connect to each sites in secure connection and the destination will be 4 sites as shown in the fig (7),the interface information will be 4 sites.

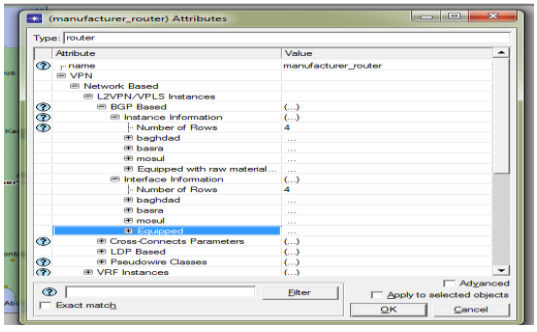


Figure (7): The manufacture site

Layer 2 protocol used for traffic from the customer edge (CE) router To use L2TP select encapsulation Remote site IDs are particularly important to connect sites and set it to 6.

4.2.2 Implementation of point to point tunneling protocol . Before configuration the PPTP must duplicate the scenario and use the same parameters that use in L2TP scenario to PPTP scenario but only change the encryption type to PPTP as show in the fig (8). The Mosul router gateway is using the same parameters the use in L2TP but change the encapsulations type to PPTP.

4.2.3 Implementation of Internet security protocol. To configure IPsec protocol must duplicate scenario and first need to remove all parameters that used in PPTP and L2TP from all routers then select Mosul router click right on it chose edit attribute will open list and chose form it security. The IPsec Parameters can be used to configure the security related parameters on this node. IKE parameter this content internet Key Exchange (IKE) automatically negotiates, IPsec security associations (SAs) and enables IPsec secure communications without costly manual reconfiguration. Fig (9), shows the attributes needed for that connection.

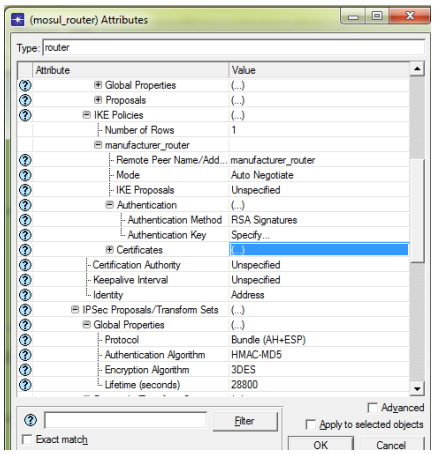
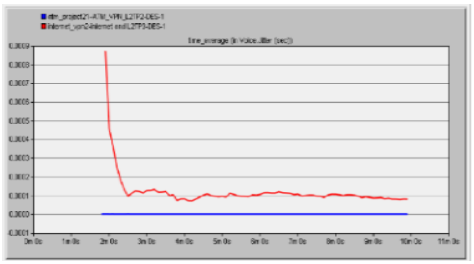


Figure (9): the ipsec configureation.

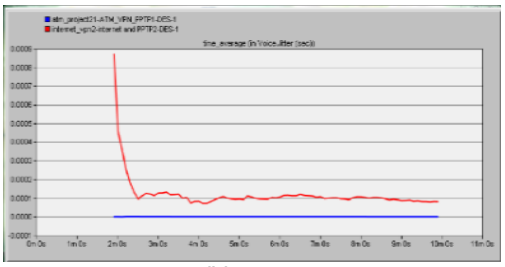
5. The Performance test results of the private networks that implemented using OPNET simulation.

OPNET simulator has measurement criteria that can be used to measure the efficiency of the performance and quality of service (Qos) of the implemented networks, the Qos measure can be used with services of voice ,Email, video, Ftp and DB some of these criteria are:Traffic Sent and receive ,Response time (sec) ,Email or file transfer Download response time ,Email or file transfer upload response time , Jitter (sec): Jitter is defined as a variation in the delay of received packets. and MOS is called Mean Opinion Score (MOS). MOS gives a numerical indication of the perceived quality of the media received after being transmitted and eventually compressed using codecsAs shown in the fig (10),the jitter (variation in the delay) during theVoice conferencing of the two types of networks the first one is that shown in fig (5), the ATM leased line private network and it's jitter drawn in green lines and other

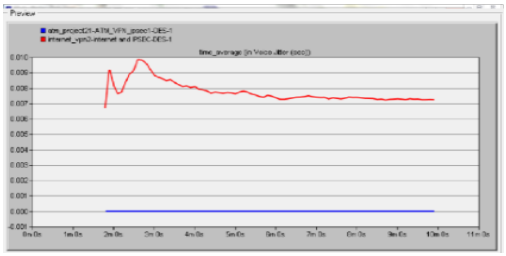
network is as in fig (6), the Virtual Private Network and it's jitter drawn in red lines .The jitter has been measure with three types of security protocols (PPTP, L2TP, and IPSEC). A higher value of jitter will be in the virtual network due to using a public routers and the extra redundancy bits in the IPsec protocol Impose upon further delay unwanted as shown in red line of part (c).



(a)PPTP



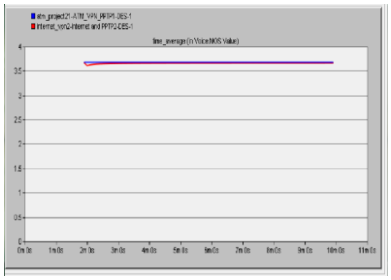
(b)L2TP



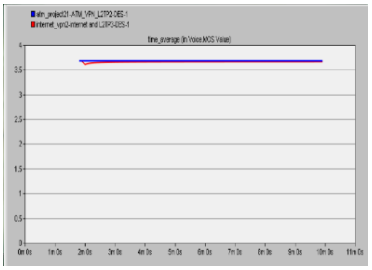
(c)IPsec

Figure (10): The Voice conferencing Jitter

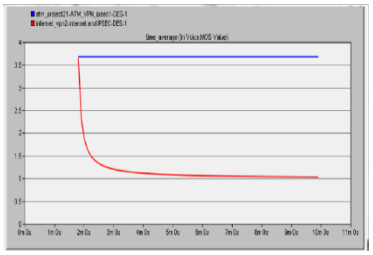
Figure (11) illustrates that **MOS** is high in the **DPN(using ATM leased line)** Than **VPN** (**usinginternet network)**. So the best network is **DPN(using ATM leased line).**



(a)PPTP



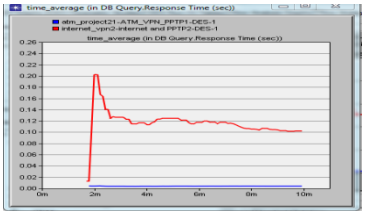
(b)L2TP



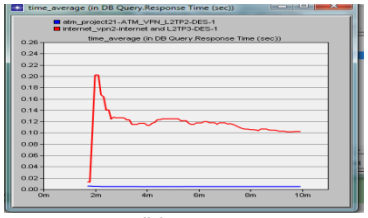
(c)IPsec

Figure (11): Mean Opinion Score (MOS).

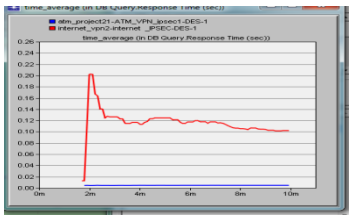
Download Response Time refers to the time that is taken server to accept to request through. As shown in figure (12), DB Download Response Time **DPN(using ATM leased line)** is comparatively less than **VPN (using internet network)**.



(a)PPTP



(b)L2TP

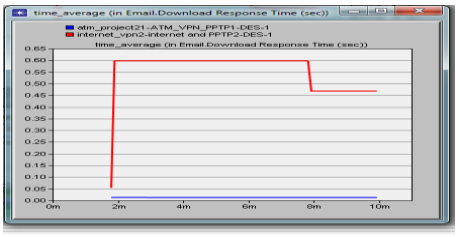


(c)IPsec

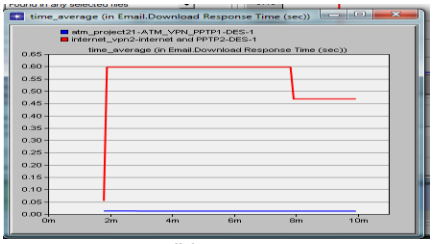
Figure (12): DB Download Response Time across the networks DB.

Email and FTP Download Response Time refers to the time that is taken server to accept to request through. As shown in figures(13,14), Email Download Response Time **DPN(using ATM leased line)** is comparatively less than

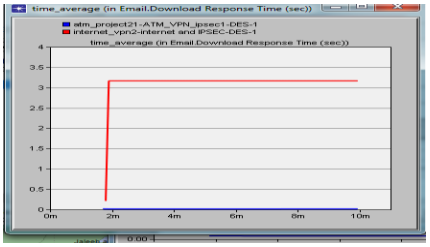
VPN (using internet network)and **VPN remote access (using internet)**.



(a)PPTP

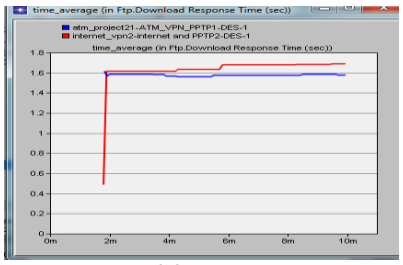


(b)L2TP

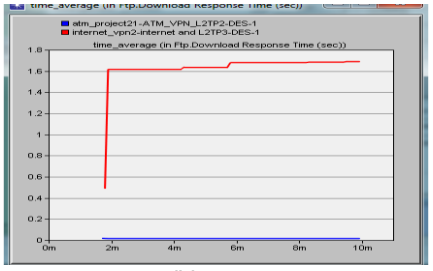


(c)IPsec

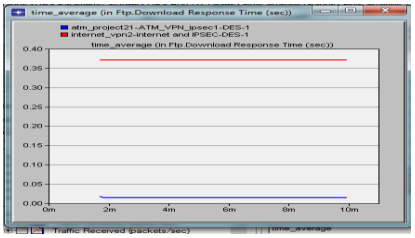
Figure (13): Email download response time.



(a)PPTP



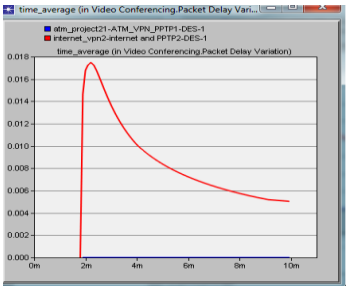
(b)L2TP



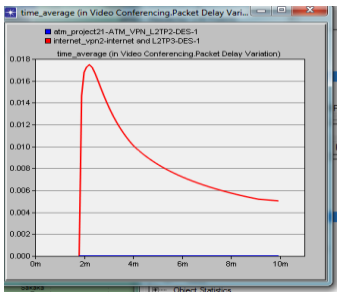
(c)IPsec

Figure (14): FTP download response time

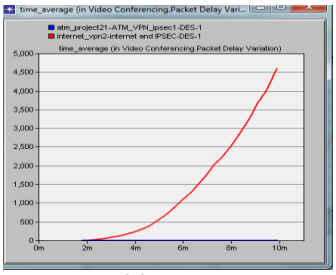
Delay variation is measured by the difference in the delay of the packets. It is observed from the figure (15) thatApparently, the IPsec is comparatively less than the PPTP AND L2TP.



(a)PPTP



(b)L2TP



(c)IPsec

Figure (15): video conferencing packet delay variation.

6. CONCLUSIONS.

Creating a WAN with VPN technology might not be as simple as it sounds. There are many different VPN solutions and deciding which one to choose . comparative between ATM network and internet network then apply all type security protocols (PPTP,L2TP,IPsce) that use to create VPN (virtual private network) to connect many sites to gather. the comparative will do form the quality of service (QOS) and the service used is FTP, VOICE ,DATABASE , EMAIL , WEB browser and VIDEO after

comparative will now the best network and best security protocol and use the OPNET network simulation version 14.0 program to configuration the tow network.

FUTURE WORK. The investigated different VPN solutions and could be used to help any enterprise to choose a proper VPN solution so that the future work of the work use the realip to connect sites via Internet world .

7. REFRENCES

[1]. Shah Deval and Helen Holzbaur, “Virtual Private Networks: Security With an Uncommon Touch,” Data Communications,Sept. 1998.

[2]. “VPN Technologies: Definitions and Requirements”, Paper, VPN Consortium, July 2008.

[3]. Muhammad Aamir1, Mustafa Zaidi and HusnainMansoor“the concept of Performance Analysis of Diff Serve based Quality of Service in a Multimedia Wired Network and VPN effect using OPNET”, in 2007

[4]. H. Bourdoucen, A. Al Naamany and A. Al Kalbani “Impact of Implementing VPN to Secure Wireless LAN ” International Journal of Computer and Information Engineering 3:1 2009

[5]. N. Edde, Security Complete, Second Edition, 2002.

[6]. R. Malhotra, R. Narula, "Techno-Evaluation and Empirical Study of VirtualPrivate Networks Using Simulations," Journal of Computing, Volume 3, Issue 7, July 2011.

[7]. R. Fisli, “Secure Corporate Communications over VPN-Based WANs,” Master’s Thesis in Computer Science at the School of Computer Science and engineering, Royal Institute of Technology, Sweden, 2005..

[8]. R. Malhotra, R. Narula, "Techno-Evaluation and Empirical Study of Virtual Private Networks Using Simulations," Journal of Computing, Volume 3, Issue 7, July 2011.

[9]. M. Finlayson ,J. Harrison ,R. Sugarman, "VPN TECHNOLOGIES - A COMPARISON" February 2003, updated June 2004.

[10]. Security Architecture for the Internet Protocol (RFC 2401)

[11]. IP Security Document Roadmap (RFC 2411)

[12]. V. Manral, “Cryptographic Algorithm Implementation Requirements for (ESP) and (AH)” RFC 4835, April 2007.

[13]. S. Kent, “IP Authentication Header”, RFC4302, December 2005.

[14]. A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs), RFC 4110,July 2005.