Remote Access VPNs Performance Comparison between Windows Server 2003 and Fedora Core 6

Ahmed A. Joha, Fathi Ben Shatwan, Majdi Ashibani

The Higher Institute of Industry

Misurata, Libya

goha_99@yahoo.com

Abstract - A Virtual Private Network (VPN) can be defined as a way to provide secure communication between members of a group through use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. This work examines and empirically evaluates the remote access VPNs, namely Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP/IPSec), and Secure Socket Layer (SSL). We explore the impact of these VPNs on end-to-end user application performance using metrics such as throughput, RTT, jitter, and packet loss. All experiments were conducted using a window XP SP/2 host (VPN Client) connected to a windows server 2003 host (VPN Server) and to a fedora core 6 host (VPN Server).

Keywords- VPN; PPTP; L2TP; IPSec; SSL; OpenVpn; tunneling; encapsulation; performance evaluation

1. INTRODUCTION

In the past, organizations or enterprises would physically install lines over large distances to ensure secure data transfer. However, this system is impractical for every enterprise and everyday users due to the cost, space, and time required for such installations. The concept of Virtual Private Network (VPN) is not new – technologies such as Frame Relay (FR) or Asynchronies Transfer Mode (ATM) have been used over the last decades as a basis for the implementation of this concept. Whatever the format or the technology behind it, a VPN provides a service functionally equivalent to a private network using resources of a public network. In recent years, with the exponential growth of the Internet, the landscape of telecommunications has changed radically and the Internet has become part of almost every aspect of the developed world including education, banking, business, and politics. Over the past two decades the public Internet has been found to be vulnerable to attackers seeking sensitive information. The most recent solution to this problem has been IP-based Virtual Private Network (IPVPN). A Virtual Private Network (VPN) can be defined as a way to provide secure communication between members of a group through use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. VPN systems provide users with the illusion of a completely private network. An IP Virtual Private Network (IPVPN) can be

K. Al Agha et al. (eds.), *Home Networking*

defined as a VPN implementation that uses public or shared IP network resources to emulate the characteristics of an IP-based private network.

2. Tunneling Basics

Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork. The encapsulated packets are then routed between tunnel endpoints over the internetwork. The logical path through which the encapsulated packets travel through the internetwork is called a tunnel. Once the encapsulated frames reach their destination on the internetwork, the frame is decapsulated and forwarded to its final destination. Tunneling includes this entire process (encapsulation, transmission, and decapsulation of packets) as shown in "Figure. 1".

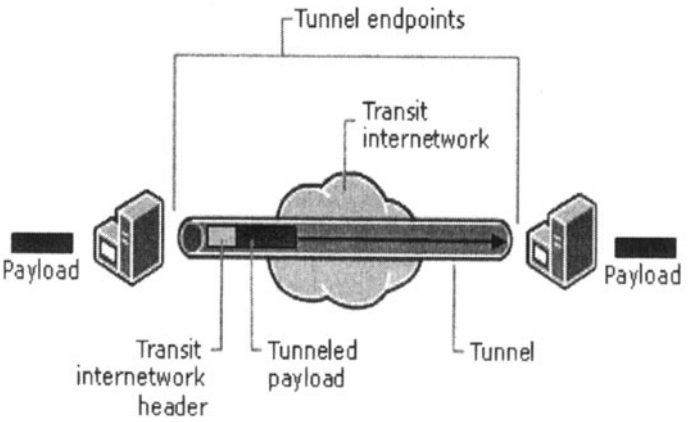

Figure1. Tunneling

3. Security of VPN

A VPN should provide the following critical functions to ensure security of the data.

3.1 Authentication

AUTHENTICATION ENSURES THAT THE DATA IS COMING FROM THE SOURCE FROM WHICH IT CLAIMS TO COME.

3.2 Access Control

Access control concept relates to the accepting or rejecting of a particular requester to have access to some service or data in any given system. It is

therefore necessary to define a set of access rights, privileges, and authorizations, and assign these to appropriate people within the domain of the system under analysis.

3.3 Confidentiality

Confidentiality ensures the privacy of information by restricting an unauthorized users from reading data carried on the public network.

3.4 Data Integrity

Data Integrity verifies that a data has not been altered during its travel over the public network.

3.5 Non-Repudition

Non-repudiation ensures that the originator of a message cannot deny having sent the message.

4. THE BENFITES OF VPN

The main purpose of a VPN is to give enterprises the same capabilities, or even better in some cases as the list below shows, as in private networks, but at a much lower cost. Enterprises benefit from VPN in the following ways [1]:

4.1 Cost

When using VPN, cost is reduced in many ways. Most importantly, VPN eliminate the fixed monthly charge of dedicated leased lines. The cost is even higher if the lines are purchased.

4.2 Scalability

VPN offers better scalability. An enterprise with only two branch offices can connect the two offices with just one leased line. But as the enterprise grows, full-mesh connectivity might be required between the different offices. This means that the number of leased lines, and the total cost associated with deploying them, increases exponentially. In addition, if an enterprise wants to scale globally, the cost associated with deploying leased lines will be even higher, if it is even possible to reach the same global connectivity with leased lines. VPN that utilizes the Internet avoid this problem by simply using the infrastructure already available.

4.3 Security

Security is not impaired when using VPN since transmitted data is either encrypted or, if sent unencrypted, forwarded through trusted networks.

4.4 Productivity

In addition to cost savings, VPN increases profits by improving productivity. The improved productivity results from the ability to access resources from anywhere at anytime (i.e. more business can be conducted).

5. ARCHITECTURE OF VPN

A VPN should typically support the following architecture "Figure. 2". A main LAN at the headquarters of an enterprise, other LANs at remote offices, partner or customer company LANs, and individual users connecting from out in the field. There are basically two types of VPNs, remote access VPN and site-to-site VPN. Site to site VPN can be further divided into intranet VPN and extranet VPN.

5.1 Remote Access VPN

The remote access VPN is a user-to-LAN connection used by enterprises that have employees who need to connect to their private network from various remote locations (e.g. homes, hotel rooms, airports). Since users access the network over the Internet, the remote access VPN is a low-cost solution, compared to the dial-up solution which often results in costly phone bills.

5.2 Site to Site VPN

By using dedicated equipment, enterprises can connect multiple sites over a public network such as the Internet, thus creating a site-to-site VPN. Site-to-site VPNs can be one of two types.

5.2.1 Intranet Site to Site VPN

If an enterprise has one or more branch offices that they wish to join in a single private network, they can create an intranet VPN. This is a low-cost solution compared to maintaining dedicated leased lines.

5.2.2 Extranet Site to Site VPN

When an enterprise has a close relationship with another enterprise (for example, a partner, supplier or customer), it can build an extranet VPN which connects LANs together. By doing so, the partner companies can work in a shared environment.

5.3 VPN within an Intranet

Intranets can also utilize VPN technology to implement controlled access to subnets on the private network. Even though a public network is not involved in this case, the security features (e.g. encryption, authentication) of secure VPN technology are taken advantage of.

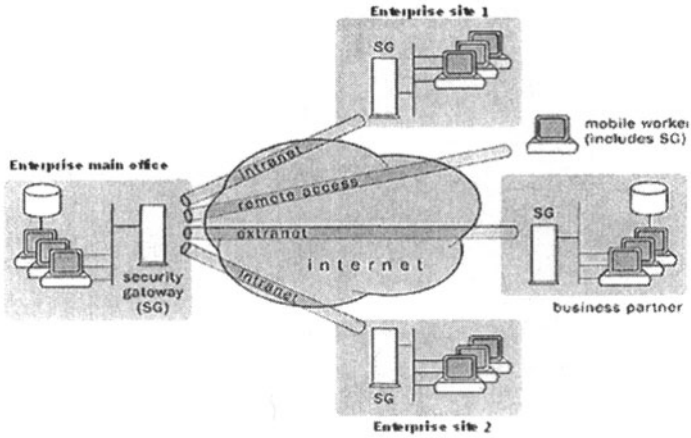

Figure2. VPN architecture

6. Remote Access VPN Protocols

For a connection to be established, both the client and the server must be using the same VPN protocol [2].

6.1 Point to Point Tunneling Protocol (PPTP)

PPTP is a standard tunneling protocol developed by PPTP Forum which consists of Microsoft and some other remote access vendors. Basically, PPTP is an extension of Point to Point Protocol (PPP), which encapsulates PPP frames in IP datagrams for transmission over an IP-based network, such as the Internet or over a private intranet. PPTP is described in RFC 2637 in the IETF RFC Database [3]. Microsoft has included PPTP clients in all versions of Windows since Windows 95 and PPTP servers in all its server products since Windows NT 4.0, PPTP clients and servers are supported in Linux. PPTP has been very popular, especially on Windows systems, because it is widely available, free and easy to set up.

6.2 Layer Two Tunneling Protocol (L2TP)

L2TP is a combination of PPTP and Layer Tow Forwarding (L2F). Rather than having two incompatible tunneling protocols competing in the marketplace and causing customer confusion, the IETF mandated that the two technologies be combined into a single tunneling protocol that represents the best features of both. L2TP is described in RFC 2661 in the IETF RFC Database [4]. L2TP alone does not provide any security. In order to have strong security in place the L2TP must be run over IPSec.

6.3 Internet Protocol Security (IPSec)

IPSec is a framework of IETF open standards aim at securing traffic on the network layer. It does not specify the authentication and encryption protocol to use. This makes it flexible and able to support new authentication and

encryption methods as they are developed. IPSec is described in RFCs 2401-2411 and 2451 in the IETF RFC Database [5]. IPSec is supported in Windows XP, 2000, 2003 and Vista, in Linux 2.6 and later. Many vendors supply IPSec VPN servers and clients.

L2TP/IPSec combines L2TP's tunnel with IPSec's secure channel. Microsoft has provided a free L2TP/IPSec VPN client for Windows 98, ME and NT since 2002, and ships an L2TP/IPSec VPN client with Windows XP, 2000, 2003 and Vista. Windows Server 2003 and Windows 2000 Server include L2TP/IPSec servers. There are several open-source implementations of L2TP/IPSec for Linux

6.4 Secure Socket Layer (SSL)

SSL is a higher-layer security protocol developed by *Netscape*. SSL is commonly used with HTTP to enable secure Web browsing, called HTTPS. Most browser and servers currently use SSL 3.0. However, SSL can also be used to create a VPN tunnel. For example, OpenVpn is an open-source VPN package, which uses SSL to provide encryption of both the data and control channels.

7. Experimental Test Bed and Measurement Procedures

The work in this paper is based on the test bed, that was built to evaluate the performance of remote access VPNs on both windows server 2003 VPN server and fedora core 6 VPN server. The hardware components of this test bed are listed in the "Table 1.", The software components of this test bed are listed in the "Table 2.", and the connections of these components are shown in the "Figure 1".

Table1. TEST BED HARD WARE COMPONENTS

Node	Description
dc01Server	Desktop equipped with double Genuine Intel 2600 MHz processor, 512 Mbytes of RAM, and VIA Rhine II Compatible Fast Ethernet Adapter built-in NIC. It is act as a domain controller server.
vpn01Server	Desktop equipped with double Genuine Intel 3000 MHz processor, 512 Mbytes of RAM, Broadcom Extreme Gigabit Ethernet built-in NIC, and VIA VT6105 Rhine III Compatible Fast Ethernet Adapter NIC. It is act as a domain client and VPN server.
vpn01Client	Laptop equipped with Genuine Intel 1866 MHz processor, 512 Mbytes of RAM, and Broadcom 440x 10/100 Integrated controller built-in NIC. It is act as a VPN client.
HUB	LANTECH, Ethernet 10 BASE-T HUB.

Table2. TEST BED SOFTWARE COMPONENTS

Node	Description
dc01Server	This node is loaded with windows server 2003. Configure your server wizard is used to configure this node to act as a domain controller server [6].
vpn01Server	This node is loaded with windows server 2003. Configure your server wizard is used to configure this node to act as PPTP and L2TP/IPSec VPN servers [6] and OpenVpn-2.0.9.exe is installed to configure this node to act as SSL VPN server [7]. In addition, this node is loaded with fedora core 6. Pptpd-1.3.3-1.fc6.i386.rpm is installed to configure this node to ac as PPTP VPN server [8], xl2tpd-1.1.09-1.i386.fc6.rpm and OpensWan-2.4.5-2.1 are installed to configure this node to act as L2TP/IPSec VPN server [9][10], and OpenVpn-2.0.9.tar is installed to configure this node to act as SSL VPN server [7].
vpn01Client	This node is loaded with windows XP SP/2. New connection wizard is used to configure this node to act as PPTP VPN client that is connected to vpn01Server node with MS-CHAPv2 authentication algorithm, MPPE encryption algorithm, and no compression algorithm [6]. New connection wizard is used to configure this node to act as L2TP/IPSec VPN client that is connected to vpn01Server node with preshared key, MS-CHAPv2 authentication algorithm (windows server 2003) or MD5-CHAP authentication algorithm (fedora core 6), ESP-3DES encryption algorithm, and no compression algorithm [6]. OpenVpn-2.0.9.exe is installed to configure this node to act as SSL client that is connected to vpn01Server node with preshared key, SHA1 authentication algorithm, 3DES encryption algorithm, and no compression algorithm [7].

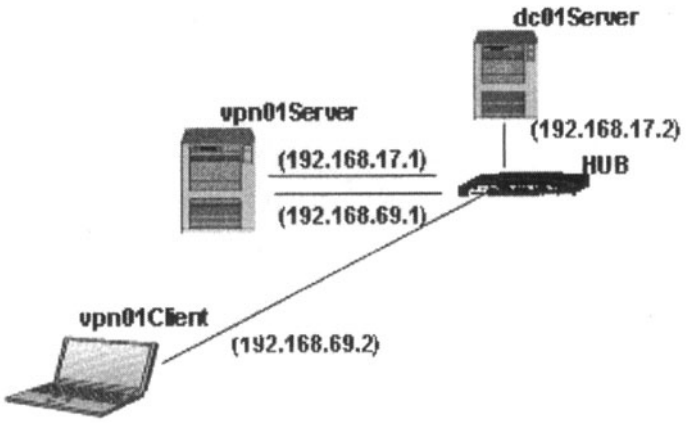

Figure3. Test bed connections

We measure some performance metrics like Throughput, RTT, Jitter, and packet loss in both TCP and UDP mode. These metrics are used in our experiments as they have a direct impact on the ultimate performance perceived by end user applications. During our experiments, the following parameters were used to quantify the QoS services provided [11]:

- Throughput is the rate at which bulk of data transfers can be transmitted from one host to another over a sufficiently long period of time.
- Round Trip Time (RTT) is the amount of time it takes one packet to travel from one host to another and back to the originating host.
- Packet delay variation (Jitter) is measured for packets belonging to the same packet stream and shows the difference in the one-way delay that packets experience in the network. Jitter occurs when packets are sent and received with timing variations. Jitter is effectively a variation of packet delay where delays actually impact the quality of service.
- Packet loss is measured as the portion of packets transmitted but not received in the destination compared to the total number or packets transmitted.

8. Experimental Results

Iperf tool is used to measure TCP Throughput in TCP mode and UDP throughput, jitter, and packet loss in UDP mode [12]. Hrping tool is also used to measure RTT [13].

The following results were collected from the test bed was illustrated in section 7.

8.1 TCP Throughput

TCP throughput is measured according to tcp window size, time of test, and the number of flows (parallel streams). The same experiments were repeated number of times to find the average TCP throughput.

The results of these experiments are presented in "Figure 4", "Figure 5", and "Figure 6".

These figures indicate clearly that the PPTP on windows server 2003 has produced the best TCP throughput value, the PPTP on fedora core 6 has produced the second TCP throughput value, the OpenVpn on fedora core 6 has produced the third TCP throughput value, the L2TP/IPSec on fedora core 6 has produced the forth TCP throughput value, the L2TP/IPSec on windows server 2003 has produced the fifth TCP throughput value, and the OpenVpn on windows server 2003 has produced the lowest TCP throughput value.

8.2 Round Trip Time (RTT)

RTT can be measured by sending packets with a variant packet size from a client to the server. The same experiments were repeated a number of times to find the average RTT. The results of these experiments are presented in "Figure 7". This figure indicates clearly that the PPTP on windows server 2003 has produced the best RTT value, the PPTP on fedora core 6 has produced the second RTT value, the L2TP/IPSec on windows server 2003 has produced the third RTT value, the OpenVpn on fedora core 6 has produced the forth RTT value, the OpenVpn on windows server 2003 has produced the fifth RTT value, and the L2TP/IPSec on fedora core 6 has produced the last RTT value.

8.3 UDP throughput

UDP throughput is measured according to transmission rate of packets. The same experiments were repeated a number of times to find the average UDP throughput. The results of these experiments are presented in "Figure 8". This figure indicates clearly that the UDP throughput values of the PPTP on windows server 2003, the PPTP on fedora core 6, the L2TP/IPSec on windows server 2003, and the L2TP/IPSec on fedora core 6 are equal to the transmission rate if the transmission rate is less than 8000 kbits/sec and less than the transmission rate if the transmission rate is more than 8000 kbits/sec. In addition, this figure indicates clearly that the UDP throughput values of the OpenVpn on windows server 2003 and the OpenVpn on fedora core 6 are equal to the transmission rate if the transmission rate is less than 200 kbits/sec and less than the transmission rate if the transmission rate is more than 200 kbits/sec. Also, this figure indicates that the UDP throughput values of the OpenVpn on windows server 2003 and the OpenVpn on fedora core 6 are always less than 500 kbits/sec.

8.4 Jitter

Jitter is measured according to the transmission rate of packets. The same experiments were repeated a number of times to find the average Jitter. The results of these experiments are presented in "Figure 9". This figure indicates clearly that the PPTP on windows server 2003, the PPTP on fedora core 6, the L2TP/IPSec on windows server 2003, and the L2TP/IPSec on fedora core 6 have produced a low Jitter values. Also, this figure indicates clearly that the OpenVpn on windows server 2003 and the OpenVpn on fedora core 6 have produced a high Jitter values if the transmission rate is more than 200 kbits/sec.

8.5 Packet loss

Packet loss is measured according to the transmission rate of packets. The same experiments were repeated a number of times to find the average Packet loss. The results of these experiments are presented in "Figure 10". This figure indicates clearly that both PPTP and L2TP/IPSec on both windows server 2003 and fedora core 6 have produced a low Packet loss values. Also, this figure indicates clearly that the OpenVpn on both windows server 2003 and fedora core 6 have produced a high Packet loss values if the transmission rate is more than 200 kbits/sec.

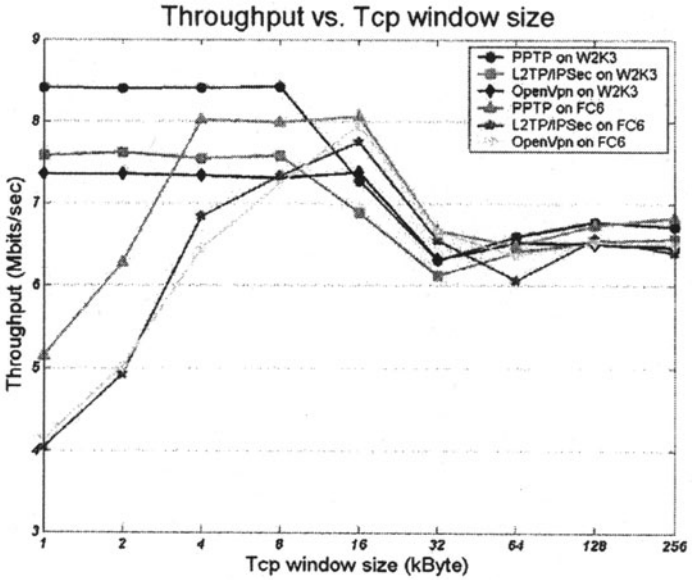

Figure4. TCP throughput according to the window size

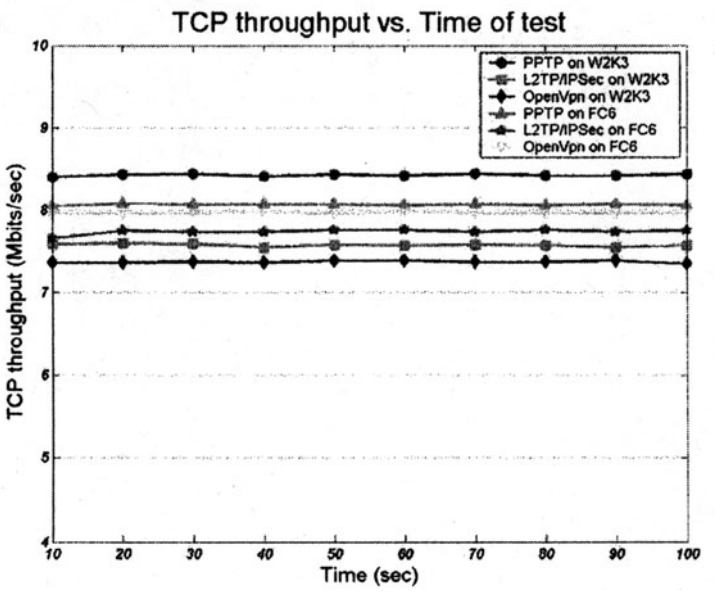

Figure5. TCP throughput according to thetime of test

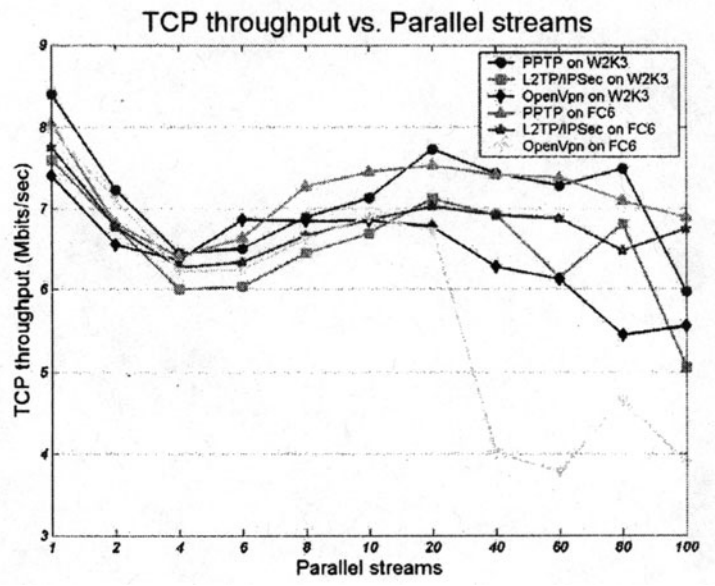

Figure6. TCP throughput according to the parallel streams

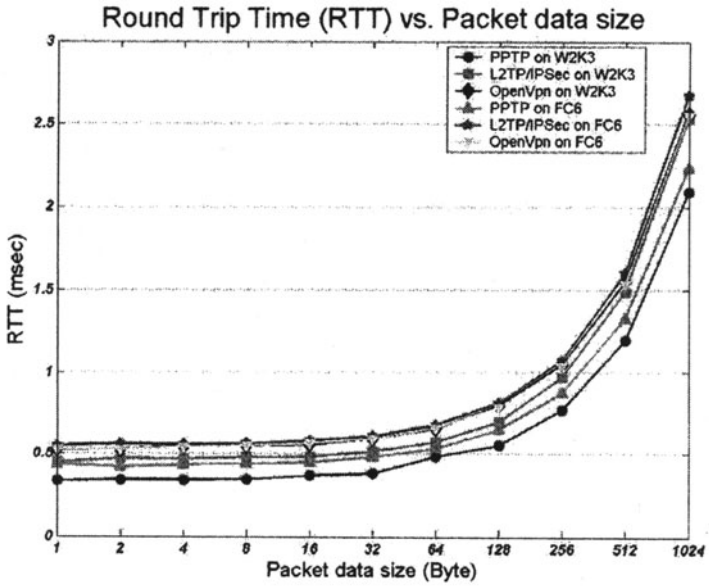

Figure7. RTT according to the packet data size

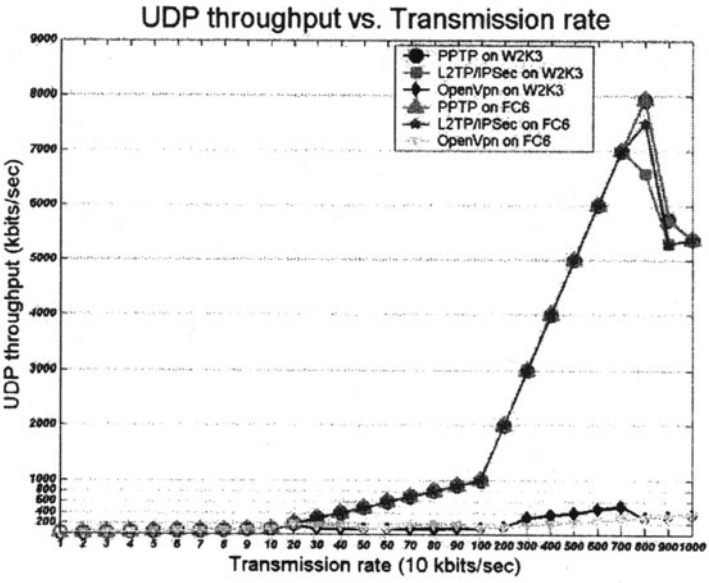

Figure8. UDP throughput according to the transmission rate

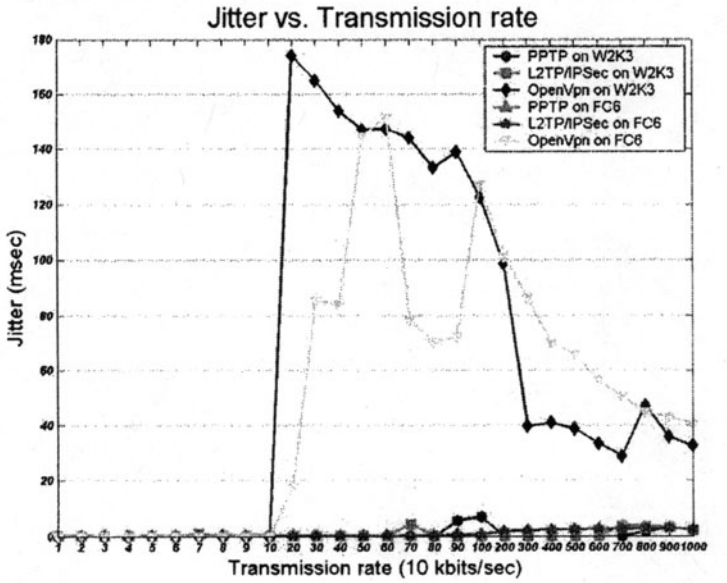

Figure9. Jitter according to the transmission rate

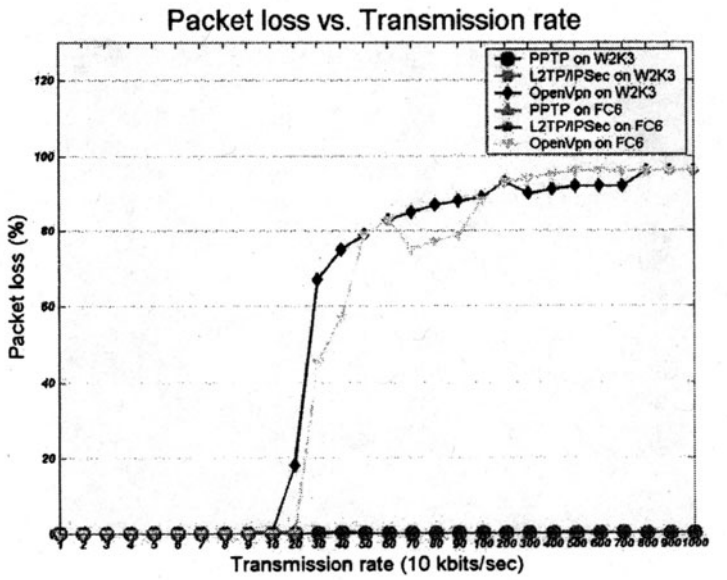

Figure10. Packet loss according to the transmission rate

The test bed experimental results are summarized in the "Table III.".

Table3. SUMMARY OF THE EXPERIMENTAL RESULTS

TCP throughput					
Best	**2nd**	**3rd**	**4th**	**5th**	**lowest**
PPTP on W2k3	PPTP on FC6	OpenVpn on FC6	L2TP/IPSec on FC6	L2TP/IPSec on W2K3	OpenVpn on W2K3
Round Trip Time (RTT)					
Best	**2nd**	**3rd**	**4th**	**5th**	**last**
PPTP on W2k3	PPTP on FC6	L2TP/IPSec on W2k3	OpenVpn on FC6	OpenVpn on W2K3	L2TP/IPSec on FC6
UDP throughput					
High				**Low**	
PPTP on W2k3	PPTP on FC6	L2TP/IPSec on W2K3	L2TP/IPSec on FC6	OpenVpn on W2K3	OpenVpn on FC6
Jitter					
Low				**High**	
PPTP on W2k3	PPTP on FC6	L2TP/IPSec on W2K3	L2TP/IPSec on FC6	OpenVpn on W2K3	OpenVpn on FC6
Packet loss					
Low				**High**	
PPTP on W2k3	PPTP on FC6	L2TP/IPSec on W2K3	L2TP/IPSec on FC6	OpenVpn on W2K3	OpenVpn on FC6

9. CONCLUSION AND FUTURE WORK

This paper has presented an experimental performance evaluation for the remote access VPNs, namely PPTP, L2TP/IPSec, and OpenVpn on both windows server 2003 and fedora core 6 VPN servers. From the results that were collected from the test bed and the user applications requirements, the following conclusion remarks are gained:

- Due to the smallest overhead packets that have been introduced by PPTP, PPTP on both windows server 2003 and fedora core 6 have produced the best performance values for both TCP and UDP-based user applications.
- In order to have strong security, L2TP/IPSec combines L2TP's tunnel with IPSec's secure channel which increases the overhead packets. So, L2TP/IPSec on both windows server 2003 and fedora core 6 have produced a good performance values for both TCP and UDP-based user applications.
- Because OpenVpn was written as a user space daemon rather than a kernel module, OpenVpn on both windows server 2003 and fedora core

6 have produced a low performance values in high traffic environments for the UDP-based user applications.

- The performance values of both PPTP and L2TP/IPSec on windows server 2003 are better than the performance values of both PPTP and L2TP/IPSec on fedora core 6.

This work should be extended to include performance evaluation of the remote access VPNs on other software and hardware VPN servers.

The OpenVpn needs to be manipulated to improve it's performance with UDP-based user applications.

REFERENCES

[1] Rezan 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.

[2] Jon C. Snader, "VPNs ILLUSTRATED: Tunnels, VPNs, and IPSec," Addison-Wesley, 2006.

[3] RFC 2637, "PPTP," IETF, ftp://ftp.isi.edu/in-notes/rfc2637.txt, 1999.

[4] RFC 2661, "L2TP,"IETF, ftp://ftp.isi.edu/in-notes/rfc2661.txt, 1999.

[5] RFCs 2401-2411, and 2451, "IPSec," IETF, ftp://ftp.isi.edu/in-notes/, 1999.

[6] http://www.microsoft.com, 2007.

[7] http://openvpn.net/download.html, 2007.

[8] http://sourceforge.net/project/showfiles.php?group_id=44827, 2007.

[9] http://www.xelerance.com/software/xl2tpd, 2007.

[10]http://www.openswan.org,2007.

[11]IP Performance Metrics (IPPM) Working Group, IETF, http://www.ietf.org /html.charters/ippm-charter.html.

[12]http://dast.nlanr.net/projects/IPerf, 2007.

[13]http://www.cfos.de, 2007.