Open Access

Baghdad Science Journal **Vol.13(1)2016**

DOI: http://dx.doi.org/10.21123/bsj.2016.13.1.0204

The Impact of Operating System on Bandwidth in Open VPN Technology

Husam Ali Abdulmohsin* ***Samer Sami Hasan****

Sharipah Setapa**

*Department of Computer Science, College of Science, Baghdad University, IRAQ
**Network & Communication Technology Lab, Software Technology and Management, Faculty of Information Science and Technology, University Kebangsaan Malaysia, 43600, UKM Bangi, Selangor Darul Ehsan, Malaysia

Received 24, December, 2014
Accepted 15, September, 2015

Abstract:

The internet is a basic source of information for many specialities and uses. Such information includes sensitive data whose retrieval has been one of the basic functions of the internet. In order to protect the information from falling into the hands of an intruder, a VPN has been established. Through VPN, data privacy and security can be provided. Two main technologies of VPN are to be discussed; IPSec and Open VPN. The complexity of IPSec makes the OpenVPN the best due to the latter's portability and flexibility to use in many operating systems. In the LAN, VPN can be implemented through Open VPN to establish a double privacy layer(privacy inside privacy). The specific subnet will be used in this paper. The key and certificate will be generated by the server. An authentication and key exchange will be based on standard protocol SSL/TLS. Various operating systems from open source and windows will be used. Each operating system uses a different hardware specification. Tools such as tcpdump and jperf will be used to verify and measure the connectivity and performance. OpenVPN in the LAN is based on the type of operating system, portability and straightforward implementation. The bandwidth which is captured in this experiment is influenced by the operating system rather than the memory and capacity of the hard disk. Relationship and interoperability between each peer and server will be discussed. At the same time privacy for the user in the LAN can be introduced with a minimum specification.

Key words: VPN Technology, OpenVPN, IPSec, Interoperability, Bandwidth, Tcpdump, Jperf.

Introduction:

Internets have been growing and becoming a highway of information. This can give the opportunity to others to retrieve any data which is sensitive through the highway. Information can be retrieved easily with the right tools and methods. Sometimes our colleagues can use a shoulder surfing [1] to get the information about the password which can retrieve the information. With that, it is time to think how to provide privacy and security the information.

Virtual Private Network (VPN) offers the method to prevent the sniffing, by providing privacy and security of data. It can also be defined as an electronic link which supports privacy and security to the data in the virtual tunnel. There are various types of VPN technology such are internet Protocol Security (IPSec), L2TP, PPTP, and SSL/TLS.

L2TP is using IPSec whereas PPTP has not been effectively secured. In Open System interconnection (OSI) IPSec falls under the network layer [2]. VPN based on SSL/TLS technology as an example operates above the transport layer.

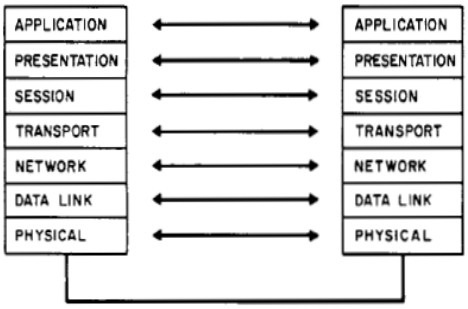

Fig. 1. Open Layer Interconnection

In order to establish a VPN in existing infrastructure, a virtual tunnel needed to be set-upped. The complexity during setup can cause a drawback in VPN. Other items which can influence the VPN network are operating system, interoperability, algorithm and physical devices used.

A lightweight VPN which is OpenVPN has been proposed to reduce the complexity of setup, documentation, portability, flexibility and scalability of IPsec. Local Area Network (LAN) which consists of a specific subnet will be designed to support client to server model for OpenVPN. This will also introduce a trusted domain [3] and double layer privacy. The performance and interoperability between various operating systems and related bandwitdhs will be examined. The validation, verification and bandwidth will be captured by using specific tools.

Methodology:

Skills in network and operating systems will help to reduce the troubleshooting occurring when the OpenVPN connection is established. The establishment of the testbed will involve the routing and the firewall. The UDP port and routing have to be established previously in the server. Different operating systems have different styles. Because the command to open a specific port is temporary, routing and firewall configuration will need to recreate again after booting. This can cause a problem when the connection cannot be established. The cause of error cannot be predicted. A start-up script has to be developed to capture both commands for the OpenVPN purposes. In a windows operating system, OpenVPN has to activate as a system administrator, if not, no changes will not be permitted in the configuration file. A lot of problems appeared because of lack of understanding routing and firewall. If the IP is using DHCP, that can also cause a problem because the OpenVPN remote server address is changing. The changing of IP will make the connection fail because it cannot find the remote server to validate and authenticate the key. It is wise to change the IP to static IP for the server. Tcpdump [4] and ping will be used to debug the connection. The measurement of bandwidth will be captured through Jperf [5]. This bandwidth will provide the performance and relationship to various operating systems.

I. RELATED WORK

A. IPSec

IPSec consists of various protocol which are:

- Internet Security association an key management protocol (ISAKMPD) [6]
- Internet key Exchange (IKE) [7] for key exchange
- Diffie-Hellman for deriving key material [8]
- Encryption and authentication algorithm

A protocol complexity, which bundles IPSec and network setup, has caused a high processing time for encryption and decryption. Two different networks are established, they are: 10.1.10.0 and 10.1.9.0 as shown in Figure 2. IPSec increased compared to normal TCP/IP connection. IKE is the main part which contributes to the overhead processing when using an automatic keying [9].

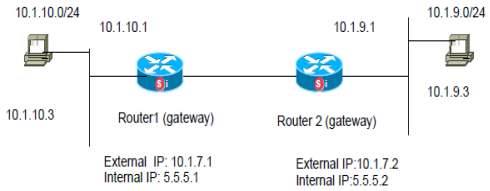

Fig. 2 VPN + IPSec Testbed [10]

This testbed racoon [11] is used to support IKE for the automatic keying. Both external and internal IP will be involved in tunnelling. A complex tunnelling causes a high processing time. The internal IP cannot be seen by other users or parties because the security level is high. The throughput value for IPSec is the lowest in fedora 6 compared to window server 2003 and window vista. But for overall, the VPN throughput initiation is higher in Linux [12].

The key can be configured manually or dynamically. Although IPSec supports a static key, it is impossible to implement in large network. With an automatic key exchange, the possibility of the key to be sniffed is decreased.

B. ***OpenVPN***

OpenVPN creates a virtual interface to the kernel and that will avoid dependency on it [13]. That interface operates in a used space that is easy to maintain and install. When the OSI level increases the security level decreases. It can be ported to various operating systems that are not involved in the kernel level. The portability, scalability and flexibility which are offered by OpenVPN have made it suitable to implement in Local Area Network (LAN), by creating a virtual interface to the kernel as shown in Figure 2 for opensource and window respectively. The external IP is transparent [14]. The External IP is the weakness of OpenVPN. Other user can know the IP which has been used by OpenVPN through scanning. Internet connection can influence the performance of OpenVPN [15]. Latency will be higher if the traffic has to go through various components in the network [16,17]. The window virtual interface is called tap as shown in Figure 3.

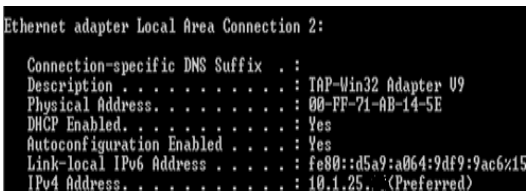

Fig. 3. Tap Interface in Window

In opensource it is usually decribed as shown in Figure 4.

Fig. 4. Virtual Interface in Open Source

In opensource the kernel interface is called tun0. A virtual machine can be used to create an identical configuration; it can also increase the

processing overhead. Strong hardware and memory are suggested for the physical machine to support the virtual machine. With an identical machine it easy to detect the similartity of two technologies. Various operating systems respond to tunnel and their reaction to the server will be noted. OpenVPN can be further used for any comparison example algorithm that has multiple protocols inside. OpenVPN on fedora 6 has produced a throughput which is higher than window server 2003 based on TCP throughput [18].

C. ***Key Management***

Generating and distributing the key will be automatic when using a key management. The gap between OpenVPN and IPSec is that IPSec has a key management which is called IKE. In OpenVPN, the key will be generated, distributed and configured manually. Once the authentication is successful, a key exchange will happen based on the SSL/TLS protocol. During rekeying, overlapping between the old and new key usage is permitted. With this technique, latency will be avoided during renegotiation [19].

Experimental:

The experiment is based on a client-server model which consist of Centos 6.4, Ubuntu 12.04 and windows vista as an operating system. The machine is not using the same specification as shown in Table 1. Notice that the memory in windows vista is higher compared to other machines. OpenVPN will be installed in each server and client. During the building of certificate and key by using OPENSSL command a certificate authority name ca.crt and ca.key will be generated. This key is only needed by the server for authentication and signing-in. Other keys such as the certification key and server key will be generated and named as server. key and server.crt. Generating certificates for the client will be named as client.crt and client. key. This experiment will be done on the specific subnet as shown in Figure 5. Two clients with different operating systems will communicate with the server through switch or hub.

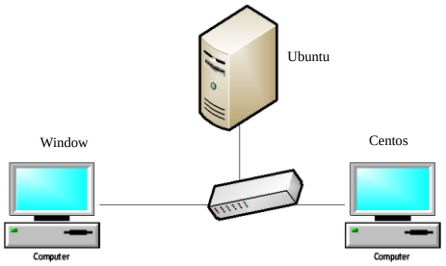

Fig. 5. Client Server

The machines have different specifications of hardware as shown in Table 1. The different specifications can also help to distinguish whether different hardwares can influence the bandwidth that has been captured.

Specification	Server	Client	Client1
Operating System	Ubuntu 12.04	Centos 6.4	Window Vista
Memory	1GB	1GB	4GB
Processing	32-bit	32-bit	32-bit
Hard disk	10GB	80GB	70GB
Software	OpenVPN 2.2.1	OpenVPN-2.2.1	OpenVPN GUI v1.0.3
	Tcpdump 4.2.1	Tcpdump 3.9.4	Wireshark 1.8.6/Wireshark 1.6.7

Table 1. Hardware and Operating System Specification

Once the installation of the OPENVPN is completed, a daemon will be started by using this command as shown below:

```
/etc/init.d/openvpn start
```

Fig. 6. Daemon to Start OpenVPN

Firewall will be open on port 1194 UDP and routing will be declared in

server. In the server a command, as shown in Figure 7, will run to open the port and routing for the client to connect:

```
# iptables -I INPUT -p udp -m udp --dport 1194 -j
ACCEPT
#route add –net 10.1.25.0 netmask 255.255.255.0
```

Fig. 7. Firewall and Routing

Once the server has fully completed, then both client such as Centos 6.4 and windows will be activated. Command line for centos 6.4 can be described as shown in figure 8.

```
/etc/init.d/openvpn start
```

Fig. 8. Daemon to Start OpenVPN

The debugging tool will monitor the connection and the results will be analysed. The performance received will help to evaluate the relationship between OpenVPN and the operating system. This experiment uses different specifications with a minimum memory, 1GB, whereas the maximum memory is 4GB. The bandwidth result will help to determine whether the memory has a low impact on the bandwidth compared to the type of the operating system. The type of the operating system is the main criterion which influences the performance of the bandwidth in the LAN.

EVALUATION

The connection between client and server will be successful once it communicates and vice versa as shown in Table 2.

Table 2. A Successful Connection

Time	Source	Destination	Protocol	Length
20:19:47	sha.mimos.local.openvpn	dhcp-10-1-25-123.a.local.54089	UDP	53
20:19:57	dhcp-10-1-25-123.mimos.local.54089	sha.a.local.openvpn	UDP	53

If the connection happens in one way, then the routing or firewall has not been configured and opened yet.

The client server model will be designed to capture the bandwidth. The data are collected for 10 seconds. Table 3 show the bandwidth of window vista decrease. Data transfer shows that windows vista bandwidth decrease is based on the time taken. The maximum data transfer is 7952 Kbytes with a maximum bandwidth 65143 Kbits/sec but the overall data transfer is 39520 Kbytes.

Table 3. Bandwidth for Windows Vista

Item	Interval	Transfer	Bandwidth
1	0.0- 1.0 sec	7864 Kbytes	64422 Kbits/sec
2	1.0- 2.0 sec	7952 Kbytes	65143 Kbits/sec
3	2.0- 3.0 sec	3488 Kbytes	28574 Kbits/sec
4	3.0- 4.0 sec	3176 Kbytes	26018 Kbits/sec
5	4.0- 5.0 sec	3176 Kbytes	26018 Kbits/sec
6	5.0- 6.0 sec	3176 Kbytes	26018 Kbits/sec
7	6.0- 7.0 sec	2088 Kbytes	17105 Kbits/sec
8	7.0- 8.0 sec	3232 Kbytes	26477 Kbits/sec
9	8.0- 9.0 sec	3184 Kbytes	26083 Kbits/sec
10	9.0- 10.0 sec	2176 Kbytes	17826 Kbits/sec
11	0.0- 10.0 sec	39520 Kbytes	32326 Kbits/sec

The data will be dropped when time is increased as shown in Figure 9. The graph shows that the bandwidth becomes fluctuated. At the end, the value is dropped into 17826 Kbit/sec.

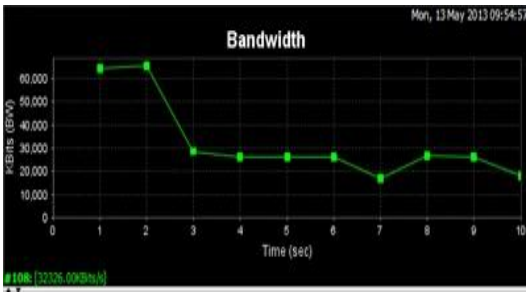

Fig. 9. Bandwidth for Windows Vista

OpenVPN initiation bandwidth is higher compared to windows vista as shown in Table 4. The processing of data in open source is higher and the maximum data transfer is 11.9Mbytes.

Table 4. Bandwidth for Windows Centos 6.4

Item	Interval	Transfer	Bandwidth
1	0.0- 1.0 sec	11.9MBytes	99.6 Mbits/sec
2	1.0- 2.0 sec	11.2 MBytes	94.4 Mbits/sec
3	2.0- 3.0 sec	11.2 MBytes	94.4 Mbits/sec
4	3.0- 4.0 sec	11.2 MBytes	94.4 Mbits/sec
5	4.0- 5.0 sec	11.1 MBytes	93.3 Mbits/sec
6	5.0- 6.0 sec	11.2 MBytes	93.3 Mbits/sec
7	6.0- 7.0 sec	11.1 Mbytes	93.3 Mbits/sec
8	7.0- 8.0 sec	11.1 Mbytes	94.4 Mbits/sec
9	8.0- 9.0 sec	11.2Mbytes	94.4 Mbits/sec
10	9.0- 10.0 sec	11.2 Mbytes	94.4 Mbits/sec
11	0.0- 10.0 sec	113 Mbytes	94.7 Mbits/sec

The encryption and decryption process will involve CPU and depend on the hardware specification to process the data. The performance of encryption and decryption will not be evaluated in this experiment.

The higher bandwidth shows the flexibility offered by Open VPN on the open source. This is because it does not interfere with the kernel level.

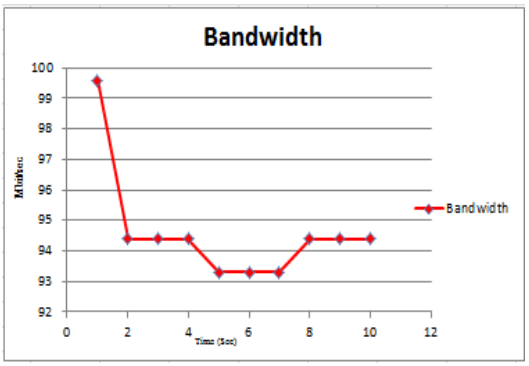

Fig. 10. Bandwidth for Centos 6.4

When time increases, the value of bandwidth is reduced between 0-10 seconds. The bandwidths become fluctuate until the interval time between 8-10 second becomes stable.

In order to verify the overall bandwidth, a value will be captured in the server. First, the bandwidth will generate from windows then it will be repeated with centos as shown in Table 5. The results show that bandwidth is always higher when centos is used as a media to transfer the data. This shows whether or not the specification of the hardware is higher such as memory or hard disk, it is not a key indicator of the performance of bandwidth and data transfer.

Table 5. Overall data at server with windows been captured first

Item	Operating System	Interval	Transfer	Bandwidth
1	Window	0.0- 10.1 sec	38.6 MBytes	32.4 Mbits/sec
2	Centos	1.0- 10.0 sec	90.0 MBytes	75.2 Mbits/sec

It shows that the value for the bandwidth in open source is higher than a windows operating system. As been mentioned previously operating systems have an impact on the VPN operation. Experience and familiarity with each operating system can contribute to establish a successful testbed. The authentication and verification, which have been implemented in VPN, will make sure whether only a key or certificate, which has been generated from the server, can successfully be connected.

Conclusion:

The complexity of installation and configuration is reduced because OpenVPN is involved at a user space. It is portable to other operating systems. Various operating systems in OpenVPN testbed are compatible and support interoperability between each other. Each user can have his own tunnel to communicate with others. With an easy installation and maintenance of OpenVPN, a double layer privacy can be achieved but it depends on the user and the organization need. A flexibility, user need, expertise, organization business and location need to be decided before choosing IPSec or OpenVPN.

Although the memory is higher in window vista yet the bandwidth is still low compared to centos 6.4. The specification of the hardware is not a key point of the performance when compared to the operating system. It is how the operating system reacts to the OpenVPN. Centos operating system is reliable, with fewer defects and suitable to any application. In the future, it can be expanded to compare speed of encryption and decryption of data based on the operating system. Another area that can be improved involves the distribution of key in a dynamic way which is not supported by the OpenVPN. It has been distributed manually to other peers. This is the area that can be improved. This experiment has shown that a double layer privacy can be established in the LAN with a hardware with minimum specification.

References:

[1] Ashley Podhradsky,Rob D'Ovidio, Pat Engebretson, Cindy Casey, 2013. Xbox 360 Hoaxes, Social Engineering and Gamertag Exploits. 46th Hawaii International Conference on System Sciences (HHICSS):3239-3250

[2] Radia Perlman, Charlie Kaufman. 2000. Key Exchange in IPSec: Analysis of IKE. IEEE Internet Computing

[3] Theis Solberg Hjorth, Rune Thorbensen, 2010. Trusted Domain: A security Platform for home Automation. Compute, 31: 940-955

[4] Tcpdump/Libpcap, 2013. Available: www.tcpdump.org

[5] Sourceforge, 2011, Available: http://sourceforge.net/projects/jperf

[6] D. Maughan, M.Schertler, M. Schneider, J. Turner, November 1998. Internet Security Association and Key Management Protocol (ISAKMP), RFC 2408, IETF.

[7] D. Harkins, D. Carrel, November 1998. The Internet Key Exchange (IKE). RFC 2409, IETF.

[8] E. Rescorla, June 1999. Diffie-Hellman Key Agreement Method. RFC 2631, IETF.

[9] Craig A. Shue, Minaxi Gupota, Steven A.Myers, June 2010. IPSec: Performance Analysis and Enhancements. IEEE International Conference on Communications (ICC), Glasgow, Scotland.

[10] Sharipah Setapa, Noraida Kamaruddin, Gopakumar Kurup, 2009. Securing VPN using IPSec. Proceeding for MMU International Symposium on Information and Communications Technologies (M2USIC).

[11] Sourceforge. net, "IPsec-tools", 2012. Available: http://ipsec-tools.sourceforge.net

[12] Shaneel Narayan, Kris Brooking,Simon de Vere, 2010. Network Performance Analysis of VPN Protocols: An empirical comparison on different operating systems. International Conference on Networks Security, Wireless Communications and Trusted Computing.

[13] I. Kotuliak, P. Rybár, P. Trúchly, 2011. Performance Comparison of IPSec and TLS Based VPN Technologies. 9th IEEE International Conference on Emerging eLearning Technologies and Applications • October 27-28, 2011, Stará Lesná, The High Tatras, Slovakia., page(s):217-221

[14] P. St. Juste, David Wolinsky, P. Oscar Boykin, Michael J. Covington, Renato J, 2010, Integrated Social and Over Lay Networks. Computer Networks. 54(2010) 1926-1938.

[15] Veeramuthu Rajaravivarma. Open Source Virtual Private Network Experience in Classroom.

Journal of Computing Sciences in Colleges, JCSC 24,3

[16] Jason Liu, Yue Li, Nathanael Van Vorst, Scott Mann,Keith Hellman, 2009.A real-time network simulation based on OpenVPN. The Journal of Systems and Software 82(2009) 473-485

[17] S. S. HASAN, et al., 2009.A New Binding Cache Management Policy for Nemo and Mipv6. Journal of Theoretical and Applied Information Technology, vol. 36.

[18] Ahmad A.Joha, Fathi Ben Shatwan, Majdi Ashibani, 2009. Remote Access VPNs Performance Comparison between window Server 2003 and Fedora Core 6. 8th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services. TELSIKS 2007. 26-28 Sept, 2007

[19] Yonan. J. Open VPN- an opensource SSL VPN connection. 2010, Available: http://openvpn.net

تأثير نظام التشغيل على حزمة البيانات بأستخدام تكنولوجيا (Open VPN)

حسام علي عبدالمحسن* **سامر سامي حسن*** **شريفة ستيبا****

* جامعة بغداد، كلية العلوم، قسم الحاسبات

**الجامعة الوطنية الماليزية، كلية العلوم و تكنولوجيا المعلومات، قسم تكنواوجيا المعلومات و الادارة، مختبر تكنواوجيا الاتصالات و الشبكات

الخلاصة :

أن الانترنت هو مصدر رئيسي للمعلومات لاختصاصات و استخدامات عديدة ومنذ وجوده تتضمن هذه البيانات معلومات حساسة و بذلك اصبح استرجاع البيانات من الوظائف الاساسية للانترنت. لسلامة هذه البيانات و ضمان عدم وصول المتطفلين اليها تم استحداث ما يسمى بال (VPN). من خلال هذا ال (VPN) يمكن زيادة خصوصية و امنية هذه البيانات. توجد طريقتان لتكنولوجيا ال (VPN) سوف يتم توضيحها و هي (IPSec) و (OpenVPN). التعقيد الذي تتمتع به طريقة (IPSec) جعل استخدام طريقة (OpenVPN) هي الافضل، حيث يتمتع الثاني بخاصية الانتقال و المرونة في استخدامها على عدة انواع من انظمة التشغيل. في حالة العمل على شبكة حواسيب من نوع LAN، يمكن تطبيق تكنواوجيا ال VPN من خلال استخدام (OpenVPN) لاستحداث مستويان من الخصوصية. شبكة ثانوية محددة سوف يتم استخدامها في هذا البحث. المفتاح و عملية التزكية سوف تتم من خلال الخادم. عملية التأكد من الهوية و استبدال المفتاح سوف تتم من خلال استخدام طرق معتمدة و هي SSL/TLS. سوف يتم استخدام عدة انواع من انظمة التشغيل منها الويندوز و انظمة التشغيل ذو المصدر المفتوح. تم استخدام عدة انواع من الحاسبات التي تختلف فيما بينها بالمواصفات و تم استخدام عدة انواع من انظمة التشغيل على هذه الحاسبات. اداتان سوف يتم استخدامها لفحص الاتصال و الاداء و هي (tcpdump) و(jperf). OpenVPN الموجود في الشبكة المستخدمة سوف يعتمد على نظام التشغيل و خاصية الانتقال و التنفيذ المباشر. حزمة البيانات المعتمدة من هذه التجربة تتأثر بنظام التشغيل بعيدا عن سعة الذاكرة الثانوية و الرئيسية. العلاقة و الفعالية بين اي حاسبة و الخادم سوف يتم مناقشتها و في نفس الوقت الخصوصية لكل مستخدم في الشبكة المستخدمة يمكن عرضها من خلال تعريف بسيط.

الكلمات المفتاحية: تكنولوجيا الشبكة الخاصة الظاهرية، الشبكة الخاصة الظاهرية المفتوحة، التشغيل البيني، عرض النطاق الترددي، برنامج التي سي بي دمب، برنامج الجي بيرف.