Bandwidth-IPSec Security Trade-off in IPv4 and IPv6 in Windows 7 Environment

Samad Salehi Kolahi, Yuqing (Rico) Cao, Hong Chen
Department of Computing, Unitec Institute of Technology, New Zealand
skolahi@unitec.ac.nz
caoyuqing.nz@hotmail.com
hongchen1127@gmail.com

***Abstract*—Due to overheads of security algorithms used in IPSec, transferring data using IPSec is known to be significantly slow compared with open system. In this paper, we present new results on performance of IPSec using 7 encryption systems for both IPv4 and IPv6 using Windows 7 and wireless network access. For the system studied, enabling IPSec results in approximately 60% (IPv4) and 48% (IPv6) less TCP throughput compared to open system. Among encryption mechanisms, 3DES-SHA provides the highest TCP bandwidth for IPv4, while 3DES-MD5 gives the best result for IPv6. We also provide the results for UDP.**

Keywords—IPSec Security, Encyption, Bandwidth, Windows 7

I. INTRODUCTION

Information on the Internet is carried using the Internet Protocol (IP), which does not inherently provide privacy or other securities. In today's IT environment, it is critical to protect user's data during data transmission via the Internet. As a result, IP Security (IPSec) is developed to provide secure communication on the Internet. IPSec (IP Security) has been the most robust technique for securing communications over the Internet. The architecture of IPSec compliant system is defined in RFC 4301 (Security Architecture for the Internet Protocol) by the Network Working Group of the IETF [1]. IPSec is a point-to-point protocol. On one side of network, IPSec encrypts the packet; the other side decrypts the packet and both sides share encryption key(s). IPSec is a collection of open standards that work together to establish data confidentiality, data integrity and authentication for users [2].

According to the registers that allocate network addresses around the world, the current Internet Protocol version 4 (IPv4) has already run out of network addresses. Internet Engineering Task Force (IETF) therefore developed a new version of Internet Protocol named IPv6 that not only provides the network addresses to 2^{128}, but also provides many additional benefits that lacks in IPv4, such as auto-configuration, mobility, secure communication and backward compatibility. New versions of operating systems have capability for IPv6 and hardware vendors, software developers and Internet Service Providers (ISP) are moving towards supporting IPv6 [3].

The main objective of this paper is to produce new results for bandwidth for IPSec site-to-site VPN (using 7 encryption techniques) for both IPv4 and IPv6 using wireless networks access and Windows 7 operating systems. The encryption systems we compared are open system, DES-MD5 (Data Encryption Standard –Message-Digest 5), 3DES-SHA (Triple Data Encryption Standard –Secure Hash Algorithm), AES128-SHA (Advanced Encryption Standard-Secure Hash Algorithm), 3DES-MD5, AES256-SHA, DES-SHA, and AES192-SHA. We measured throughput for both TCP and UDP using IPv6 and IPv4.

The organization of this paper is as follows. In the next section, the related work of IPSec, IPv4 and IPv6 are discussed. Section three covers the experimental setup. Section four covers information regarding the traffic measurement tool and the data generating. Section five covers the results produced and the last sections include the conclusions and future works.

II. RELATED WORK

Performance evaluation and comparison of IPSec VPN on different operating systems has been conducted by a number of researchers.

In 2002, Wei and Srinivas [4] presented a study of a secure wireless LAN based on the IPv4 of IPSec VPN tunneling protocol. Host to host IPSec was created between an Apple computer and an IPSec gateway. Their results demonstrated that the TCP throughput without IPSec was roughly three times than that with IPSec.

In 2003, Jin-Cherng and colleagues [5] conducted an investigation on router performance when using various services and hash/encryption algorithms such as AH-MD5, AH-SHA, ESP-3DES using IPSec. They tested the throughput of router before and after implementing IPSec. Their results showed that the throughput decreased 90.02% when 3DES-SHA of IPSec was implemented and decreased 88.23% when DES-SHA was implemented.

In 2004, Zeadally and colleagues [6] conducted an empirical performance comparison of IPv4 and IPv6 protocol stack implementations of three operating systems including Windows 2000, Solaris and Linux. Their results showed that there was a decrease in throughput and round-

trip time performance for IPv6 compared to IPv4 on those three operating systems.

In 2004, Khanvilkar and Khokhar [7] investigated the influence of different types of VPN technologies on network performance using 100Mb/s fast Ethernet. Their results demonstrated that IPSec had only 25% bandwidth utilization.

In 2009, Narayan and colleagues [8] conducted a study of network performance of IPsec VPN on Windows server 2003, Windows vista and Linux operating systems. Two VPN severs acted as software routers were used to connect to networks. Their studies concluded that throughput values varied from 15 to 95 Mbps for IPSec in Windows environment.

There has been no work done to date on performance of open system, IPSec for both IPv4 and IPv6 under Windows 7 using networks connected by hard routers. The lack of available research on impact of IPSec was the main motivation behind this paper.

III. Experimental Setup

The test-bed diagram for site to site VPN is displayed in Figure 1. IPSec VPN is commonly setup site to site, which will establish the VPN tunnel between two routers.

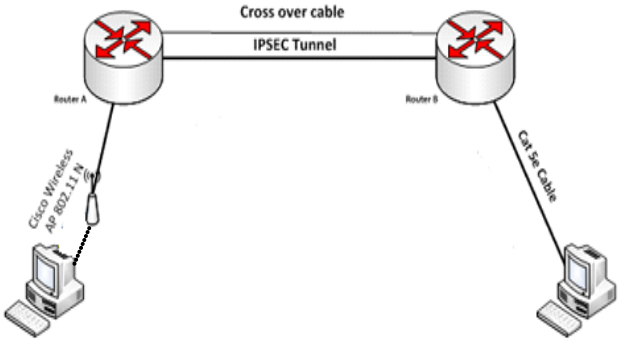

Figure 1: Network test-bed.

Two hard routers were connected via Cross over Cat 5e cable, one client machine was connected wirelessly via Cisco Linksys WAP4410N 802.11n Access Point (AP). The anther machine was directly connected to the Cisco 2811 router via Cat5e Cable. The test-bed hardware setup remained constant for all experiments conducted and:

The hardware benchmark was comprised of two computers with Intel® Core™ i5 2.80 GHz, 8.00 GB of RAM and two Cisco 2811 routers. For the efficient operation of Windows 7, an Air Live Wn-5000 wireless PCI NIC and a Western Digital Caviar 160 GB hard-drive were installed on the two workstations.

In test-beds, Microsoft Windows 7 professional 64bit with SP1(Service Pack 1) was installed on the computer of left side and Microsoft Windows 2008 standard 64bit with SP1(Service Pack 1) was install on the receiving computer of right side.

For each test bed we implemented open system, IPSec for both IPv4 and IPv6 measuring TCP and UDP throughput. In all options, the wireless link had WPA2 (Wireless Protected Access 2) security.

Throughput (the number of bits transmitted per unit time) depends on several factors in a network, such as process limitations and hardware design. In order to eliminate the effect of such conditions, hardware with same characteristics was used in all of the tests.

IV. Data Generation and Traffic Monitoring Tool

Netperf 2.4.5 [9] was selected as the tool to analyze the performance of IPv4 and IPv6 on Windows **7** operating systems over 802.11n WLAN. Netperf can be used to measure the performance of many different types of networks. It creates and sends TCP and UDP packets in either IPv4 or IPv6 networks and provides tests for throughput. Most performance evaluation tests were executed for 30 seconds, which usually generated 1 million packets per run. To ensure high data accuracy, each test was repeated at least 30 times and data average and runs continued until standard deviation of results was below 0.5% of average.

V. Results

The experiments were conducted to evaluate and compare the throughput for TCP and UDP on open system, IPv4 and IPv6 in IPSec for DES-MD5, DES-SHA, 3DES-MD5, 3DES-SHA, AES128-SHA, AES192-SHA and AES256-SHA encrypted systems.

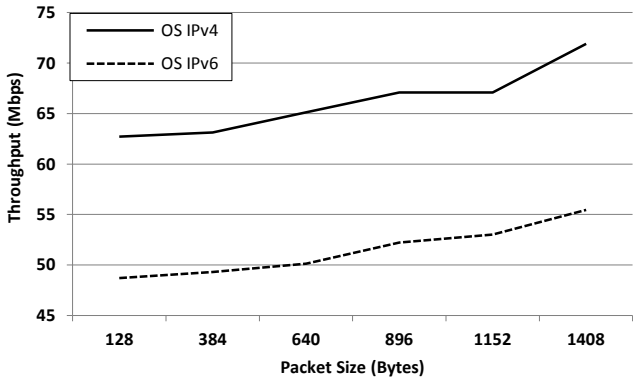

Figure 2: TCP Throughput Comparison for Open System using IPv4 and IPv6.

Figure 2 shows the TCP throughput comparison for open system (OS) of both IPv4 and IPv6 on Windows 7 over 802.11n WLAN. From TCP throughput values, for all packet sizes, there were performance differences between IPv4 and IPv6 OS.

As can be seen from Figure 2, TCP throughput of open system with IPv4 and IPv6 both increased as the packet size increased. IPv4 had higher TCP throughput than IPv6 for all packet sizes. The maximum difference between IPv4 and IPv6 on open system was 16.44 Mbps for packet size of 1408 Bytes and the minimum difference was 13.8 Mbps for packet size of 384 Bytes.

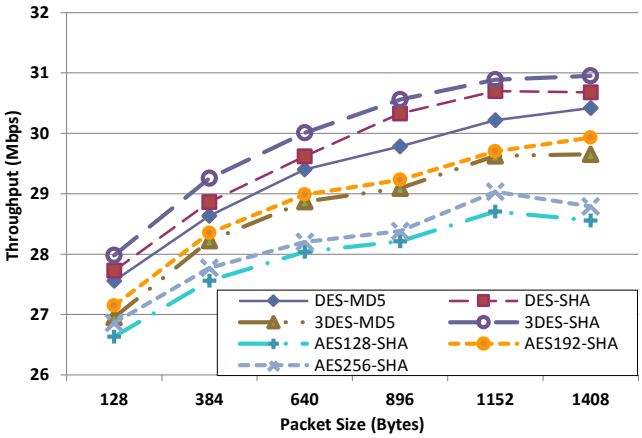

Figure 3: TCP Throughput Comparison for IPv4 IPSec systems.

Comparing the different encryption systems of Figure 3, 3DES-SHA system has the highest TCP throughput (30.95 Mbps) than others while AES128-SHA system has the lowest TCP throughput (26.63 Mbps).

From Figure 3, we can also see that the highest point of difference between the 7 encrypted IPSec systems can be noted at the packet size of 1408 Bytes where DES-MD5 system provided the TCP throughput of 30.68 Mbps and AES128-SHA system provided the TCP throughput of 28.56 Mbps. The lowest point of difference was noted at the packet size of 128 Bytes where 3DES-SHA system provided the TCP throughput of 27.98 Mbps and AES128-SHA system provided the lowest TCP throughput of 26.63 Mbps.

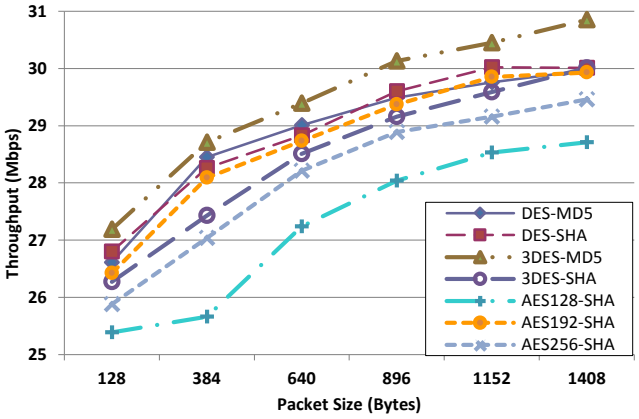

Figure 4: TCP Throughput Comparison for IPv6 IPSec systems.

Figure 4 shows the TCP throughput comparison of IPv6 IPSec for different encrypted systems. Comparing the different encryption systems, 3DES-MD5 encryption system had the highest TCP throughput while AES128-SHA encryption system had the lowest TCP throughput for all packet sizes. The difference between the performance of some encryption systems is little (eg AES192-SHA and DES-SHA). The range of bandwidth is 25.3 Mbps to 30.9 Mbps for various encryption systems.

From Figure 4, we can also see that the maximum difference between the bandwidth of the 7 IPSec systems was approximately 3 Mbps at the packet size of 384 Bytes and the minimum difference was approximately 1.7 Mbps at the packet size of 128 Bytes.

Analyzing the impact of IPSec (Figures 3 and 4), it can be seen that the throughput of both IPv4 and IPv6 was reduced when IPSec was enabled. For IPv4 network, compared to open system, the throughput of IPSec encrypted systems was decreased by a maximum of 43.34 Mbps (decrease rate of 60.28%) for the packet size 1408 Bytes and by a minimum difference of 36.07 Mbps (decrease rate of 57.53%) for the packet size 128 Bytes. For IPv6 network, compared to open system, the throughput of IPSec encryption systems was decreased by a maximum of 26.75 Mbps (decrease rate of 48.23%) for the packet size 1408 Bytes and by a minimum difference of 22.88 Mbps (decrease rate of 45.65%) for the packet size 640 Bytes.

Figures 2, 3 and 4 also show the TCP throughput increased as the packet size increased for all packet sizes with few exceptions.

UDP results obtained from the test-bed for IPv4 and IPv6 are presented in Figures 5 and 6.

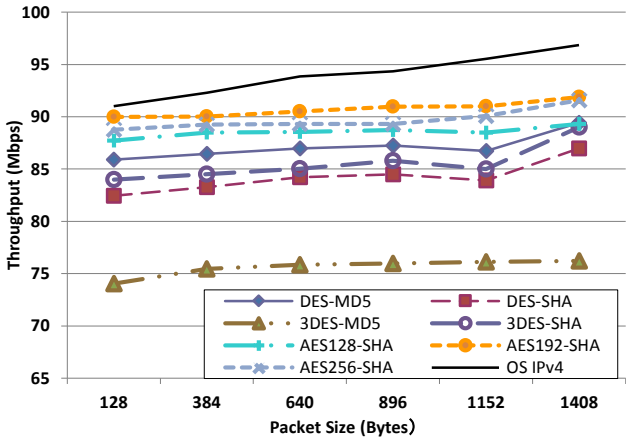

Figure 5: UDP Throughput Comparison for Open system and IPv4 IPSec systems.

Figure 5 shows the UDP throughput comparison of open system (OS) and IPSec encryption systems for IPv4. From UDP throughput values, for all packet sizes, the performance was reduced when IPSec was enabled.

The UDP throughput was generally increased as the packet size increased for all packet sizes with the exceptions at packet size 1152 Bytes.

Comparing the 7 IPSec encrypted systems, AES192-SHA system gave the best UDP throughput performance while 3DES-MD5 system gave the worst UDP throughput performance.

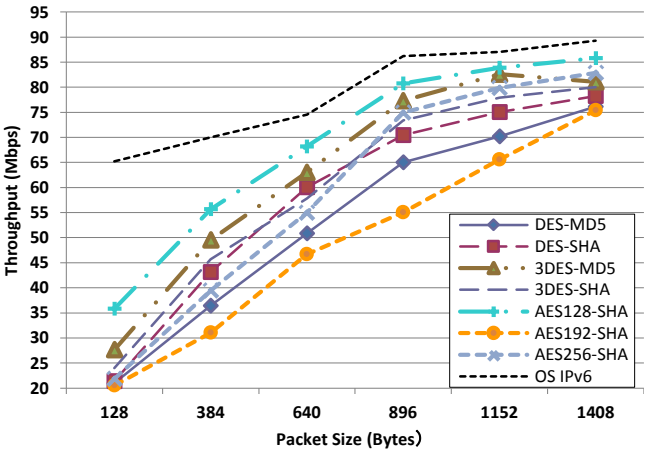

Figure 6: UDP Throughput Comparison for Open system and IPv6 IPSec systems.

Figure 6 shows the UDP throughput comparison for open system (OS) and IPSec using IPv6. From UDP throughput values, for all packet sizes, the performance was reduced when IPSec was enabled. In addition, the UDP throughput was increased as the packet size increased for all packet sizes with the exception of 3DES-MD5 system at packet size 1408 Bytes where the UDP throughput dropped a little.

Comparing the 7 IPSec encrypted systems, AES128-SHA system gave the best UDP throughput performance while AES192-SHA gave the worst UDP throughput performance.

Analyzing the UDP throughput impact of IPv4 and IPv6 in IPSec, as shown in Figures 5 and 6, it can be seen that the throughput of both IPv4 and IPv6 is reduced when IPSec is enabled. For IPv4 network, compared to open system, the UDP throughput of IPSec encrypted systems was decreased by a maximum of approximately 20 Mbps (decrease rate of 21%) for packet size of 1152 Bytes and by a minimum difference of approximately 9 Mbps (decrease rate of 9.8%) for packet size of 128 Bytes. For IPv6 network, compared to open system, the throughput of IPSec encrypted systems was decreased by a maximum of 45 Mbps (decrease rate of 68%) for packet size of 128 Bytes and by a minimum difference of 10 Mbps (decrease rate of 11%) for packet size of 1408 Bytes.

Analyzing the 7 different IPSec encrypted systems in both IPv4 and IPv6 network for TCP and UDP, it can be observed that if one encryption IPSec system performed well in IPv4 network, it might have a bad performance in IPv6 network. For example, for TCP throughput, the 3DES-SHA system performed the best in IPv4 network, whereas TCP throughput performance of this encrypted system ranged fifth in IPv6 network.

It can be observed that IPv4 had the higher TCP and UDP throughput than IPv6 for both open system and the 7 encrypted systems. The lower throughput gained in IPv6 than in IPv4 is resulted by the drawback of having a larger overhead in IPv6 (which has a 40-bit header while IPv4 has a 20-bit header) over IPv4 [10, 11]. The overhead increase in IPv6 is an implication of the performance degrade, resulting in lower bandwidth.

The UDP throughputs are higher than TCP on both open system and IPSec security enabled systems. This is due to UDP being a connectionless protocol and does not use any form of error correction and therefore does not send any acknowledgements. The source does not have to wait to receive any acknowledgements [11].

The gain in TCP and UDP throughput as the packet size increase is likely due to the amortization of overheads associated with larger user packet sizes [12].

The lower throughput results obtained when IPSec security is enabled (compared to open system with no security) is due to two reasons. First, the encryption and decryption takes up the CPU and memory; and second, the data packets become longer because of overheads associated with encrypting. Different algorithms use various overheads sizes and therefore the results for various encryptions were different. Although IPSec guarantees the security of data transmission, it leads to the decrease of throughput for both TCP and UDP [13].

VI. Conclusion

Results showed that, due to higher overhead, IPv6 provided lower bandwidth than IPv4 for open system and using IPSec encryption methods. There was a bandwidth trade-off when IPSec security was enabled for both IPv4 and IPv6. For the system studies, enabling IPSec resulted in approximately up to 43.34 Mbps less TCP throughput than open system for IPv4 and up to 26.75 Mbps less TCP throughput than open system for IPv6. For IPv6, among 7 IPSec encryption methods studied, 3DES-MD5 encryption system had the highest TCP throughput, while for IPv4, 3DES-SHA system gave the best result. For both IPv4 and IPv6, AES128-SHA system had the lowest TCP throughput.

VII. Future Works

In future, we plan to extend this study by incorporating Solaris, Fedora and Windows 8 systems. In addition, the performance of other VPN technologies, such as SSL, PPTP and L2TP will be investigated.

References

[1] R. Molva., "Internet Security Architecture" http://www.eurecom.fr/~nsteam/Papers/pap04.pdf

[2] Roland, J.F., and Newcomb, M.J., 2003, CSVPN Certification Guide, CISCO Press.

[3] N. Baghaei and R. Hunt, "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients," in Proceedings of the 12th IEEE International Conference on Networks, Vol. 1 Nov. 2004, pp.299-303.

[4] Q. Wei and S. Srinivas (2002). "IPSec-based secure wireless virtual private network. MILCOM 2002. Proceedings.

[5] L. Jin-Cherng, C. Ching-Tien, et al. "Design, implementation and performance evaluation of IP-VPN". 17th International Conference on Advanced Information Networking and Applications, 2003. AINA 2003, pp. 206-209.

[6] S. Zeadally, R. Wasseem, and I. Raicu, “Comparison of End-System IPv6 Protocol Stacks,” IEE Proc. Communications, vol. 151, no. 3, 2004, pp. 238 – 242.

[7] Khanvilkar, S.; Khokhar, A.;"Virtual private networks: an overview with performance evaluation," Communications Magazine, IEEE , vol.42, no.10, pp. 146- 154, Oct. 2004.

[8] S.Narayan, K. Brooking, et al. “Network Performance Analysis of VPN Protocols: An Empirical Comparison on Different Operating Systems.” International Conference on Networks Security, Wireless Communications and Trusted Computing, NSWCTC '09, pp. 645-648.

[9] R. Jones. Netperf 2.4.5 Available: http://www.netperf.org/netperf/NetperfNew.html

[10] R. Murugesan, S. Ramadas. R. Budiarto, “Improving the Performance of IPv6 Packet Transmission over LAN,” 2009 IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009), October, 2009, pp. 182-187.

[11] S.S. Kolahi and P. Li, “Evaluating IPv6 in Peer-to-Peer 802.11n Wireless LANs,” IEEE Internet Computing, Vol. 15 Issue 4, 2011, p70-74.

[12] S. Zeadally and L. Raicu, “Evaluation IPv6 on Windows and Solars,” Internet Computing, IEEE, vol.7, no. 3, 2003, pp. 51-57.

[13] E. Barka; K. Shuaib; H. Chamas, "Impact of IPSec on the Performance of the IEEE 802.16 Wireless Networks," New Technologies, Mobility and Security, 2008. NTMS '08. , vol., no., pp.1-6.