I.J. Wireless and Microwave Technologies, **2012, 5, 19-27**
Published Online October 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2012.05.03

Available online at http://www.mecs-press.net/ijwmt

Empirical Network Performance Evaluation of Security Protocols on Operating Systems

Shaneel Narayan[a,*], Michael Fitzgerald[a]

[a] *Department of Computing, Unitec Institute of Technology, Auckland, New Zealand*

Abstract

Securing data transmission is currently a widely researched topic. There are numerous facades in data security. Virtual Private Network (VPN) is one such strand that provides security for data that is in motion. Performance of a network that has VPN implementation is at the forefront of network design and choice of the operating systems and cryptographic algorithms is critical to enhancing network performance. In this research undertaking, three VPN techniques, namely DES, 3DES and AES, which are commonly used to implement IPSec VPNs, are performance analyzed on test-bed setup. These are implemented on a network with Linux Fedora and a router and Windows desktop operating systems on another node. The VPN algorithms tested show that there may be performance differences when implemented with different operating system combinations.

Index Terms: VPN, AES, 3DES, DES, Windows 7, Windows Vista, Windows XP, Linux Fedora, Network Performance

1. Introduction

Internet Protocol Security (IPSec) is a commonly implemented protocol used for securing Virtual Private Networks (VPNs). VPN technology is a cost effective technique to securely transfer data on or via third party networks. The protocol's increasing prevalence within the business world has lead to questions regarding its performance when interacting with different operating systems. To implement IPSec, various cryptographic algorithms, for example, Advanced Encryption Standard (AES), Data Encryption Standard (DES) or Triple DES (3DES) can be utilized. This research evaluates performance of IPSec algorithms on Fedora operating systems. In [1], the authors evaluated various protocols on Windows operating system – that work is now extended to include Linux Fedora distribution. Research related to VPN has been undertaken since the early days of its introduction and there exist multiple threads of research on this topic. Research related specifically to VPN performance evaluation is tabulated in Figure 1. The novelty of this research is that the operating system combinations being tested have not been attempted before by any other researcher.

* Corresponding author:
E-mail address: snarayan@unitec.ac.nz

Researcher(s)	**Platform(s) - VPN protocol(s)/algorithm(s)**
Narayan, Fitzgerald, Ram (2010) [1]	Windows 2008, 7, Vista, XP
Narayan, Kolahi, Brooking, de Vere (2008) [2]	Windows 2003 - PPTP, SSL, IPSec
Joha, Satwan & Ashibani (2007) [3]	Windows XP Client, Windows Server 2003 & Fedora Core 6 as VPN Servers - PPTP, L2TP, IPSec
Berger (2006) [4]	Cisco Pix501, Netscreen 5XP, Soho WG2500, Symantec FW/VPN 100 - IPSec, L2TP, PPTP
Nadeem & Javed (2005) [5]	Java JDK 1.4 simulation - DES, 3DES, AES, Blowfish
Khanvilkar & Khokhar (2004) [6]	Linux 15 open-source VPN solutions
Khanvilkar & Khokhar (2004) [7]	Linux RedHat 8.0/9.0 - Blowfish, 3DES, SHA1, MD5, SSH, SSL, IPSec
Lin, Chang & Chung (2003) [8]	Windows 2000 - MD5, SHA1, DES, 3DES
Khayatt, Shaikh, Akhgar & Siddiqi (2002) [9]	Novell BorderManager & Windows 2000 - IPSec
Pena & Evans (2000) [10]	Linux kernel 2.2.10, Linux kernel 2.0.36 with FreeS/Wan – PPTP, IPSec
McGregor & Lee (2000) [11]	System model - IPSec, MD5, SHA1, RC5, 3DES

Fig. 1. Related Research

The rest of the paper is organized as follows: Section II outlines the experimental setup used in this research. We present the results and discuss the findings in Section V. Finally, the research is concluded

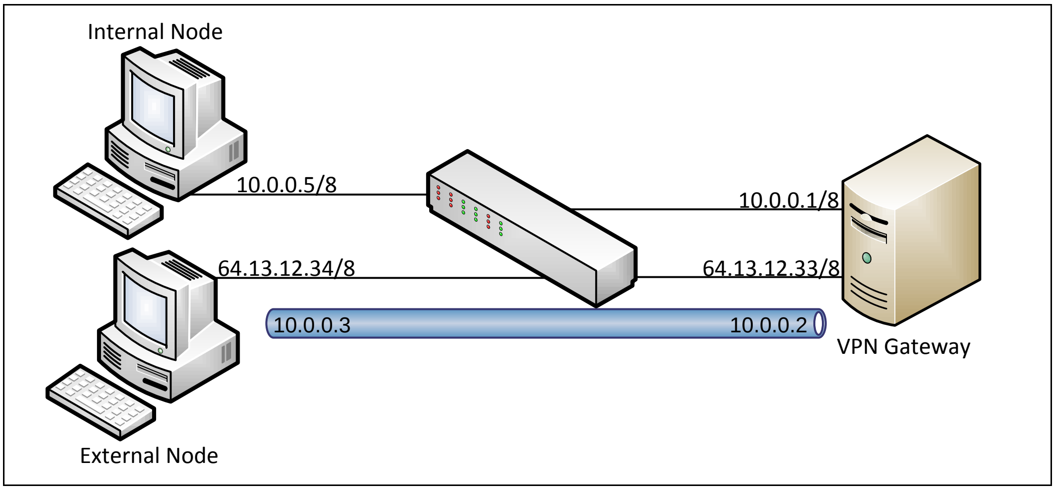

Fig. 2. Network Diagram

2. Experimental Setup

To evaluate the performance of the three IPSec protocols on Fedora and Windows operating system combinations, a test network with TCP/IP was setup as shown in Figure 2. The network's nodes are all Intel Pentium 4 C2D with 2.86GHz CPU and 2GB RAM. They are connected to a 10/100 Ethernet switch with 100Mbps UTP links. The network consists of two subnets joined by Fedora acting as a router. Two end computers act as the end points of the VPN tunnel and operating systems on them will be varied as required in the tests. The traffic generation and monitoring tool used was D-ITG [12]. This tool measured the throughput and similar performance metrics. One operating system at a time (from Windows 7, Windows Vista and Windows XP) will be installed on the end computers and a VPN tunnel with different IPSec algorithms will be created. To ensure high data accuracy, all tests were executed 20 times, and to get the maximum throughput for a given packet size, each run had duration of 30 seconds. The results are presented and discussed next.

3. Results and Discussion

We now present and discuss the results. In Figure 3, TCP throughput values for Fedora as a router operating system with various combinations of operating systems are shown. From this graph, it is evident that in some scenarios, throughput for TCP traffic type is almost twice that of other operating system combinations. The common factor in all high throughput operating systems is encryption algorithm AES. Evidently AES, the newest of all encryption protocols tested, give the best performance, in term of throughput, irrespective of the combination of operating system with Fedora. Average throughput for AES encryption protocol is approximately 70Mbps while that of all others is approximately 40Mbps. In Figure 4, Windows Server 2008 as a router throughput values are presented (mostly taken from [1]). Here it is again seen that AES is the gives better performance than the rest of the test encryption algorithms.

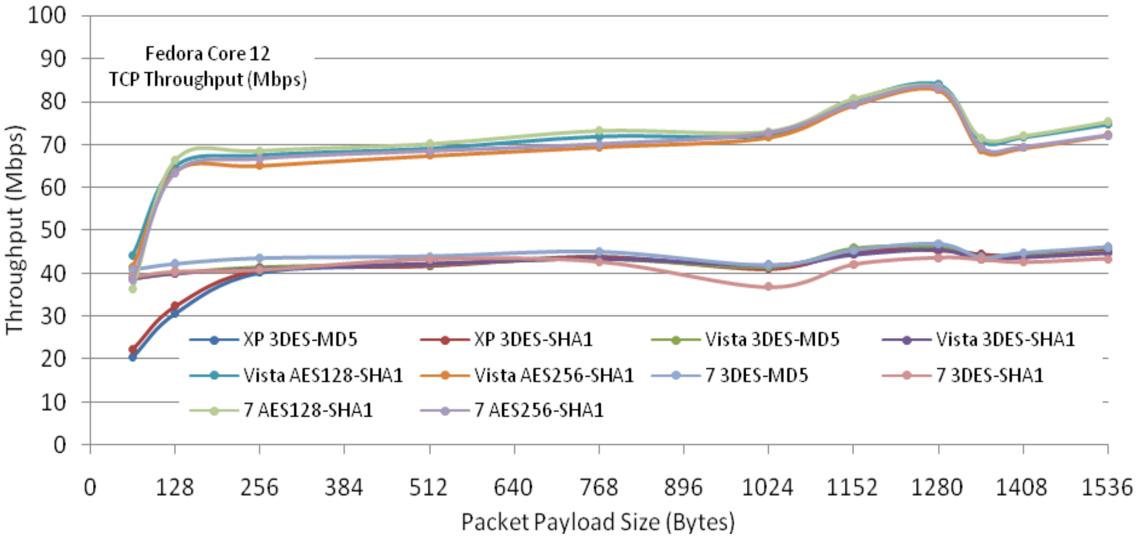

Fig. 3. TCP Throughput

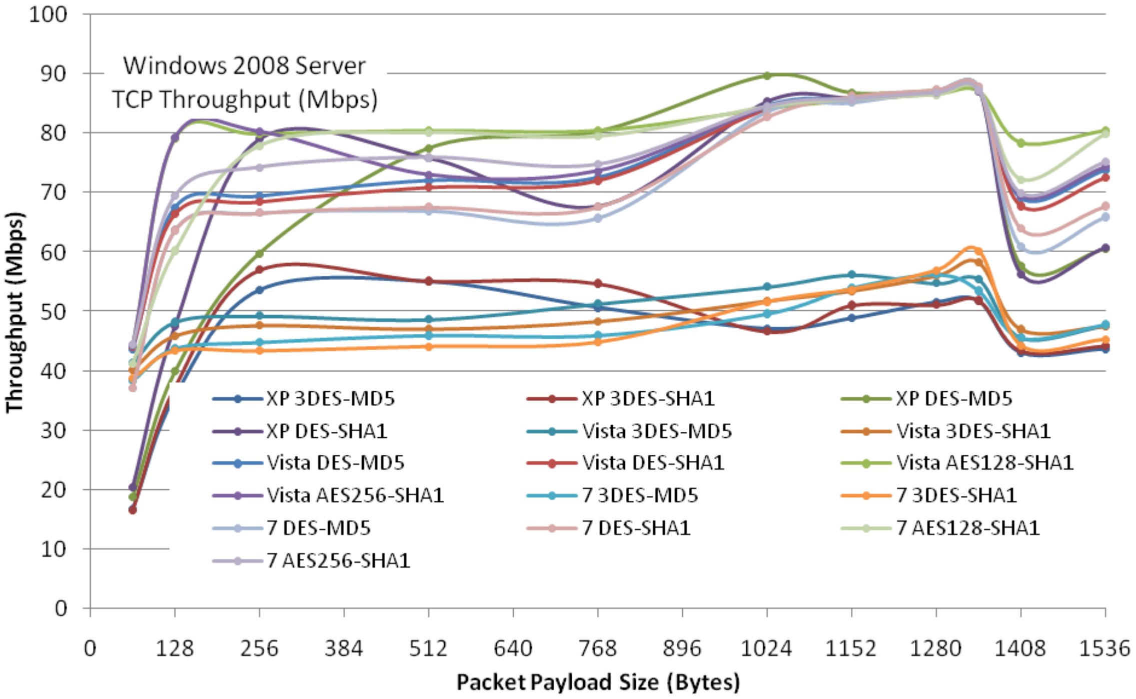

Fig. 4. TCP Throughput – Windows Server 2008

TCP jitter values are presented in Figure 5. Not much can be differentiated between the operating systems except Windows 7 with AES256-SHA1 consistently gives the lowest jitter for all packet sizes. All jitter values are below 0.8ms and there seems to be a slight incline as packet sizes increase, that is, larger packets give slightly higher values than smaller counterparts. Round trip time values (Figure 6) shows clear distinction between all operating systems scenario and Windows XP combinations. Windows XP with AES gives the highest round trip time values – for some packet sizes, these values are more than double that of other operating system combinations. The others all band together and give round trip time values averaging around 20ms.

UDP performance metric values are presented and discussed now. UDP throughput values, shown in Figure 7, give a clear distinction between two groups of performers. Higher throughput values are attained on operating systems combinations that use AES as the encryption algorithm, while the other encryption algorithms all give consistently low throughput values. AES values average to almost 85Mbps while that of other is approximately 30Mbps (difference of almost 3 fold). Comparing these with Windows Server 2008 values (Figure 8 and mostly taken from [1]), a different pattern is evident. In that, mostly Windows Vista based operating system combinations give low throughput, however AES combinations still give the best throughput values. Comparing TCP and UDP throughput values, highest value for TCP traffic type is approximately 70Mbps while that of UDP is 85Mbps. It is also evident that most other values for the two traffic types are similar.

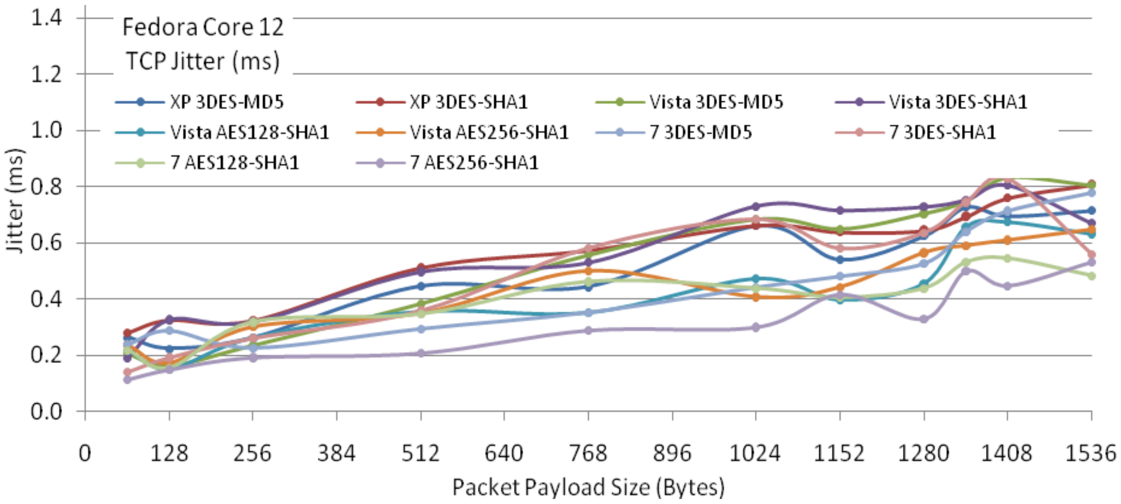

Fig. 5. TCP Jitter Values

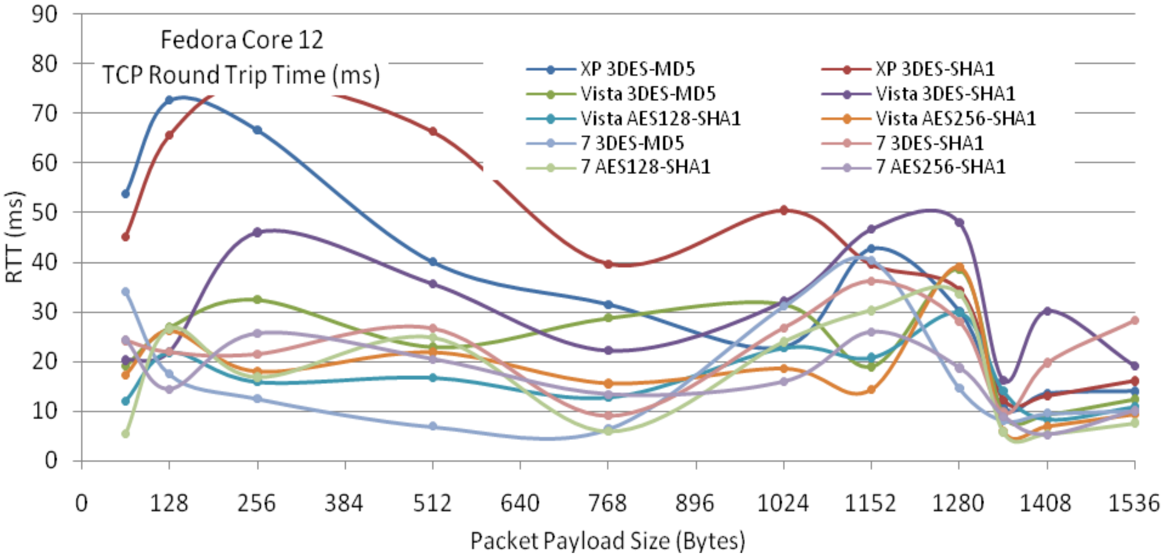

Fig. 6. TCP Round Trip Time

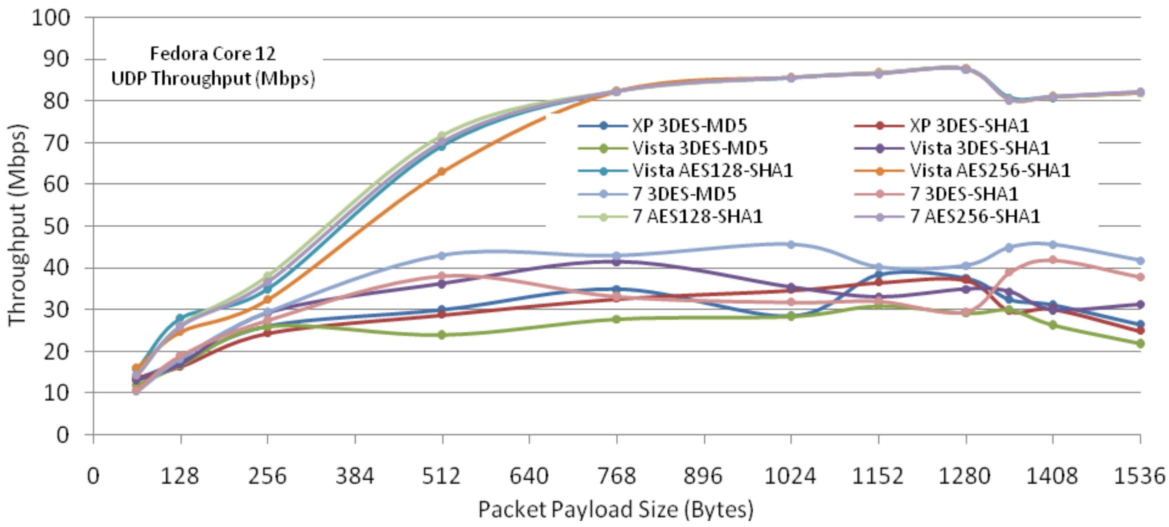

Fig. 7. UDP Throughput

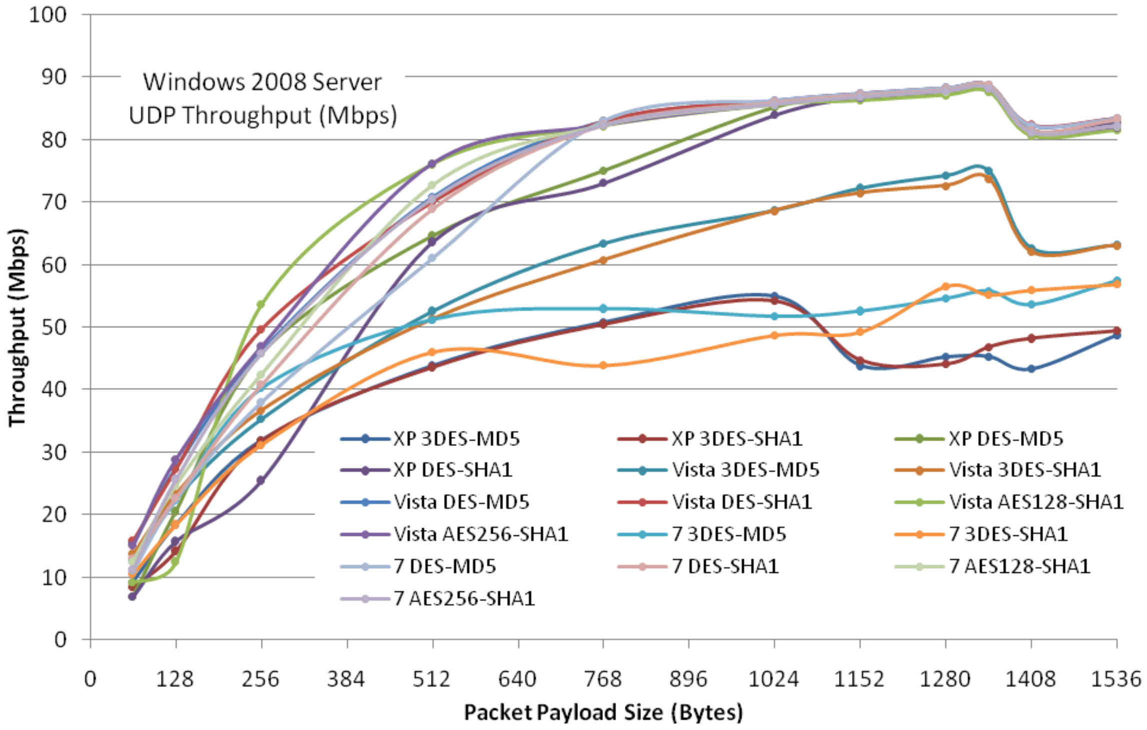

Fig. 8. UDP Throughput – Windows Server 2008

UDP jitter values (Figure 9) shows that for all packet sizes less than 1024Bytes, there is hardly any distinction between the operating systems/encryption algorithm combinations. These values are below 0.6ms, while that of larger packet sizes are greater than 0.6ms. For larger packets Windows Vista combinations give significantly lower jitter values than that of Windows 7. Comparing Round Trip Time values, presented in Figure 10, operating systems with AES as the encryption protocol give significantly lower values than the rest of the combinations. For some packet sizes (mostly in the range 640-1024Bytes) the difference is almost 3fold. It is also observed that for packets larger than 1152, round trip values are comparatively lower than that of other packet sizes for all combinations of operating systems and the encryption algorithms.

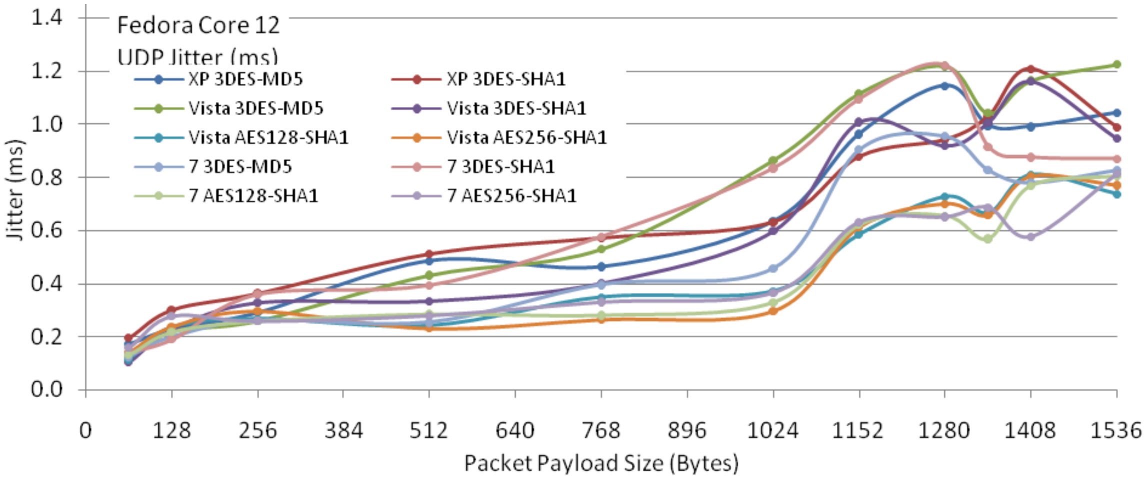

Fig. 9. UDP Jitter Values

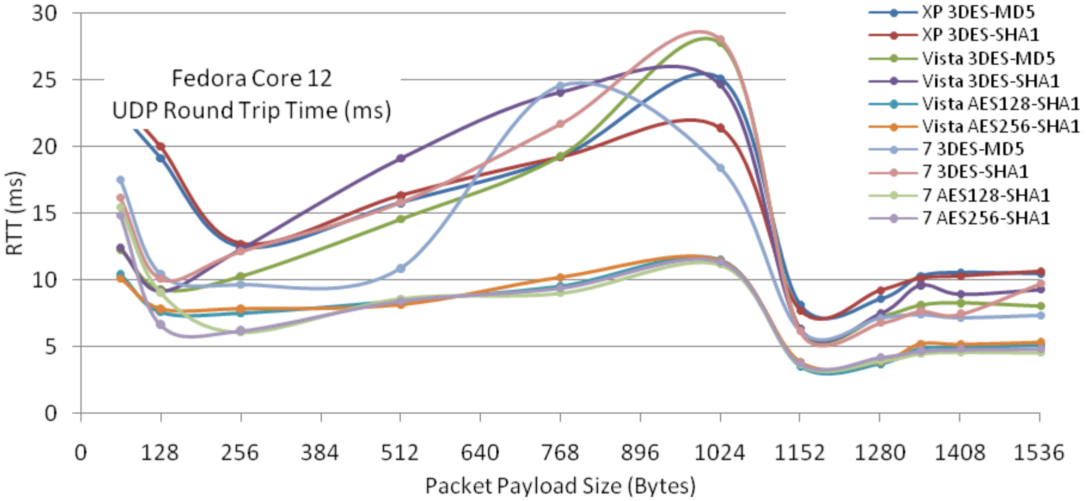

Fig. 10. UDP Round Trip Time Values

Comparing TCP performance metric values with UDP, slightly greater throughput is achieved for UDP traffic type. UDP also gives the highest jitter attained, however for most scenarios, TCP and UDP jitter values are comparable. UDP Round Trip Time values are much less than that attained for TCP traffic type.

4. Conclusion

In this research, we empirically evaluated performance of VPN IPSec methods AES, DES and 3DES each implemented with various algorithms. These tests were conducted Linux Fedora and Windows desktop operating system combinations, with one node as Linux Fedora router and the other with Windows 7, Vista or XP Professional. From this empirical test-bed evaluation, the following specific conclusions can be drawn:

1. AES as the encryption algorithm, the newest of all algorithms that were tested, gave the best throughput irrespective of the operating system combination with Linux Fedora. This was evident for both TCP and UDP traffic types.
2. Linux Fedora throughput values and that obtained with Windows Server 2008 as a router are comparable. The former values are the subject of this research and the latter was obtained in [1].
3. Comparatively AES encryption algorithms gives slightly lower jitter values than other algorithms tested. This is true for both TCP and UDP traffic types.

The research team aims to extend this study to incorporate more operating systems including more Windows operating systems and Linux distributions.

References

[1] S. Narayan, M. Fitzgerald, and S. Ram, "Empirical Network Performance Evalaution of IPSec Algorithms on Windows Operating Systems Implemented on a Test-bed", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), December 2010.

[2] S. Narayan, S. S. Kolahi, K. Brooking, and S. de Vere, " Performance Evaluation of Virtual Private Networks in Windows 2003 Environment", IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE), December 2008.

[3] A. A. Joha, F. B. Shatwan, and M. Ashibani, "Performance Evaluation for Remote Access VPN on Windows Server 2003 and Fedora Core 6", IEEE 8th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS), Serbia, pp. 587-592, September 2007.

[4] T. Berger, "Analysis of Current VPN Technologies", The First IEEE International Conference on Availability, Reliability and Security (ARES), April 2006.

[5] A. Nadeem and M. Y. Javed, "A Performance Comparison of Data Encryption Algorithms", IEEE First International Conference on Information and Communication Technologies (ICICT), pp. 84-89, August 2005.

[6] S. Khanvikar and A. Khokhar, "Experimental evaluations of Open-Source Linux-based VPN solutions", IEEE 13th International Conference on Computer Communications and Networks (ICCCN), pp. 181-186, October 2004.

[7] S. Khanvikar and A. Khokhar, "Virtual Private Networks: An Overview with Performance Evaluation", IEEE Communications Magazine, vol. 42, issue 10, pp. 146-154, October 2004.

[8] J. Lin, C. Chang, and W. Chung, "Design, Implementation and Performance Evaluation of IP-VPN", IEEE 17th International Conference on Advanced Information Networking and Applications, pp. 206-209, March 2003.

[9] S. Al-Khayatt, S. A. Shaikh, B. Akhbar, and J. Siddiqi, "A Study of Encrypted, Tunneling Models in Virtual Private Networks", IEEE International Conference on Information Technology: Coding and Computing, pp. 139-143, April 2002.

[10] C. J. C. Pena and J. Evans, “Performance Evaluation of Software Virtual Private Networks (VPN)”, 25th Annual IEEE Conference on Local Computer Networks (LCN), pp. 522-523, November 2000.

[11] J. P. McGregor and R. B. Lee, “Performance Impact of Data Compression on Virtual Private Network Transactions”, 25th Annual IEEE Conference on Local Computer Networks (LCN), pp. 500-510, November 2000.

[12] Botta, A Dainotti, A Pescapè, "Multi-protocol and multi-platform traffic generation and measurement", INFOCOM 2007 DEMO Session, May 2007, Anchorage (Alaska, USA).