Factors Impacting the Performance of Data Transferred Via VPN

Dinesh Taneja, S S Tyagi

Abstract: As a cost effective measure to attain security and confidentiality of data, Virtual Private Network (VPN) is used to interconnect two networks. The research shows that the protocols and algorithms of VPNs adds the overhead and in turn affect the network performance. The two end point hardware appliances are configured with standard configuration to establish site to site VPN. There are different data formats transferred via these tunnels. A research was conducted in a simulation environment of open source technology to identify the various factors impacting the performance of data transfer via VPN tunnels. Empirical measurement shows that performance depends critically on nature of data and compressibility in different internet bandwidth conditions. This was also noticed that nested VPN architecture adds complexity in security at the cost of multifold transmission delays. VPN provide security at the cost of performance; hence application specific cost benefit analysis is essential to choose the optimal architecture.

Keywords—Cloud Computing, IPSEC, Nested Tunnel, SSL, VPN.

I. INTRODUCTION

Cloud computing is becoming popular and at the same time its adoptability may be faster if security aspects are addressed well. The security concern of the data in cloud computing can be broadly classified for data in rest, use and data in motion [1]. The data in motion has driven the need for secure access between geographically separated networks. As a cost effective measure to attain security and confidentiality of data, organizations use legacy site to site VPN solutions to interconnect two networks. The two most common architectures of VPN in the use today are: -

Site to Site VPN which is cost effective solution as compared to leased lines for connecting two different networks deployed across geographies. This VPN provide access to multiple hosts concurrently and it is a permanent connection between two networks.

Remote Access VPN is used to provide secured access to roaming individual users. This is established between a single machine and a network only on demand and connection is destroyed after the individual has completed its work.

PN technology uses different protocol suites such as MPLS, PPTP, L2TP, IPSEC, SSL and TLS. Out of this first three operate at OSI layer2 whereas IPSEC operates at Network Layer and SSL/TLS operate at higher layers.

The two most used VPN protocols are IPSEC and SSL. SSL has now been succeeded by new protocol TLS, however for discussion purpose, SSL name is still prevalent.

IPSEC is used for site to site VPN and remote VPN. IPSEC is a suit of protocols as defined in IETF to achieve secure communication over IP Packet switched shared medium. IPSec provides authentication, integrity, access control and confidentiality and the information exchanged is encrypted. For communication, this protocol uses three major steps including IKE phase1 used to negotiate PKS for next step, IKE phase-2 used to negotiate SA and then data is encrypted and decrypted using SA.

SSL protocol is mainly popular for remote access over browsers; however, some firewalls are now supporting interconnectivity of two networks using this protocol. SSL VPNs can also be classified for Application Layer Proxies, Protocol redirectors and Remote control enhancers. Flow exchange between the client machine include handshaking protocol to determine encryption parameters between client and servers, record protocol to exchange data and alert protocol to terminate the connections in case of errors [2].

To improve the privacy and anonymity of the user over internet, composite secure tunnels such as the onion routing (TOR) protocols have been proposed. TOR is based on Chaum’s notion of an anonymous channel [3]. Nested Tunnels or VPN chaining are other composite forms to increase security complexity, confidentiality and anonymity of the source of data. The group encrypted Transport VPN and Dynamic Multipoint VPN are the protocols to implement services in mesh and hub-spoke architecture respectively [4]. The existing mobile VPN solutions have certain advantages and disadvantages [5]. The Introduction of security protocols impacts overall quality of Service [6]. There is a need to classify traffic flow so as to achieve adaptive engineering [7]. The network monitoring system (NMS) tools also check the VPN connection availability, type of connection, data or packets transferred [8]. However, the performance impact or overhead due to VPN tunnel is not majorly addressed by NMS.

II. BACKGROUND

Organizations implement VPN tunnel as a cost effective measure to securely interconnect their organizations and or client spread across different geographies.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Dinesh Taneja*, Research Associate, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India.

Prof. S. S. Tyagi, Professor, Computer Engg. and Head of the Department of FCA, Manav Rachna International Institute of Research and Studies (MRIIRS), Faridabad, Haryana, India.

Conventions inside the IPSec suite make broad utilization of cryptographic calculations [9].

The VPN tunnels create overheads due to encryption and compression algorithms used in connecting two different network entities. Nested Tunnel and VPN chaining create more overheads as compared to a single tunnel. On the hand, it provides options to improve performance by means of compression of payload. To reduce the overheads, tunnel header compression has also been introduced by researchers [10].

Site to Site VPN Tunnels carry data of various kinds including but not limited to text, video, application specific binary formats which may or may not be compressed at application layer. Different verticals of the industry have varied type of data formats required for transmission. The Media and Healthcare Industry in particular has lot of data in Video formats along with contents in application specific formats. As a standard practice, firewall engineers configure virtual private networks with standard configuration. The overheads due to a single VPN or nested VPN tunnel interactions along with content type are overlooked. Different data formats may impact VPN performance. The internet bandwidths at different locations are either over utilized or under-utilized. The data transmission via VPN tunnels may be impacted due to single or nested tunnel, format of data, internet bandwidth utilization and configuration parameters of VPN.

III. Methodology

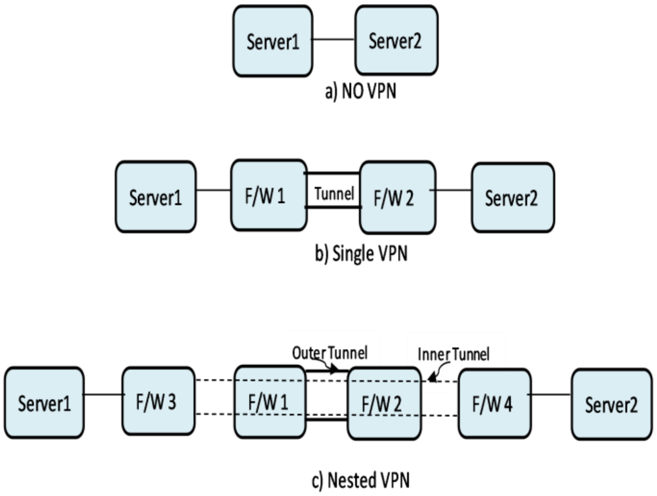
To study the awareness about the performance impact of VPN connections due to various factors, a survey was conducted amongst CIOs and IT leaders spread across geographies. Since different industry verticals have different format of data required for transmission, therefore survey was conducted across different Industry segments such as Telecommunication, healthcare, ITES, electronic media etc. Healthcare environment has major requirement to transfer patient data in DICOM format whereas electronic and media industry need to transfer video and images in raw format or standard known compressions formats such as mp4 or jpeg etc. Most of the industry verticals has mixed data format exchange requirements. An online survey form was used consisting of different questions. The responses confirming the usage of site to site VPN were considered for analysis.

A simulation environment was created using 6 servers having quad core 2.1 GHz processors and 8GB RAM specifications. Centos version 7.4 were used on all the servers. The experimental setups were created as depicted in the block diagram shown in Figure 1. Open VPN (ver. 2.4.6) was installed to create site to site VPN using SSL protocol and libreswan (ver. 3.25-2) was installed to create IPSEC VPN. All measurements were done in isolated environment dedicated for this purpose only so as to rule out any impact due to internet connection fluctuations, external devices and cloud service providers etc. One video file in MP4 format of 732188534 bytes (715MB) size and another plain text file of 727061038 bytes (710 MB) were used as sample data. The data was exchanged between two sides using vsftp (ver. 3.02-22). Video and text files were transmitted using different combinations of single and Nested Tunnels. To simulate the scenario over utilized internet bandwidth, the Ethernet speed between two internal servers was restricted to 100mbps and files of approximately 715 MB were transferred. To simulate the scenario of under-utilized internet bandwidth, the Ethernet speed of two inner servers were restricted to 1000mbps and files of approximately 715 MB were transferred.

In first step of testing, a benchmark was established using transfer of data without any VPN. As shown in Figure 1 (a), two servers were interconnected using direct cable and no vpn was configured on either side of the servers. The text and video files were transferred using file transfer protocol (ftp) and the results were recorded.

In the second step, the single VPN configurations were tested using IPSEC and SSL protocols one by one on both side firewalls. As depicted in Figure 1 (b), two servers were connected to each other and were simulated as firewalls. The tunnel was configured on both firewalls using Open VPN on both sides so as to simulate environment of site to site VPN using SSL protocol. Further, Libreswan was used on both simulated firewalls so as to create site to site VPN using IPSEC protocol. As shown in the Figure 1 (b), Server1 was connected to Firewall1 (F/w1) and Server2 was connected to firewall2 (F/w2). VSFTPD was configured on one of the server and ftp was used to exchange files between two servers.

In the third step of testing, as shown in Figure 1 (c), six servers were connected to each other to create the environment of nested VPN. Nested site to site VPN configurations were tested using two firewalls on each side. The outer Tunnel was configured on firewall1 and firewall2. The inner tunnel was created on firewall3 (F/w3) and firewall4 (F/w4). Table 1 shows the different protocols used on respective firewalls for simulating the environment of "No VPN", Single tunnel (IPSEC), single tunnel (SSL) and four different combinations of tunnel inside tunnel.



a) NO VPN

b) Single VPN

c) Nested VPN

Figure 1 Experimental setup block diagram

Table 1 VPN protocol configured in firewalls

Configuration	VPN Protocol on F/w1	VPN Protocol on F/w2	VPN Protocol on F/w3	VPN Protocol on F/w4
No VPN	NA	NA	NA	NA
IPSEC (Single Tunnel)	IPSEC	IPSEC	NA	NA
SSL (Single Tunnel)	SSL	SSL	NA	NA
SSL Inside SSL	SSL	SSL	SSL	SSL
IPSEC Inside IPSEC	IPSEC	IPSEC	IPSEC	IPSEC
SSL Inside IPSEC	IPSEC	IPSEC	SSL	SSL
IPSEC Inside SSL	SSL	SSL	IPSEC	IPSEC

All measurements were done using AES-128 encryption. Moreover, measurements were made with and without compression. The tests were conducted under 100mbps and 1000mbps bandwidth restriction on so as to simulate the environment of over-utilized and underutilized bandwidths. For this purpose, the bandwidth between F/w1 and F/w2 were restricted to 100mbps and 1000 mbps respectively.

All the tests conducted in simulation lab were repeated three times and it was observed that for each test scenario, the values were close to each other with no more than 1% variation. The average score value of the three tests for all respective scenarios were recorded and further considered for analysis. It was also observed that the resource utilization of the servers never crossed half margin. Therefore the impact due to compute resource (CPU and memory of firewall) utilization was not considered for analysis. This is to mention here that the results were collected in a simulation lab and may vary for different hardware resources. However, the analysis of the results may not vary due to hardware change. The results recorded for over utilized internet bandwidth simulated conditions are mentioned in Table 2 whereas results recorded for under-utilized bandwidth simulated conditions are mentioned in Table 3.

IV. RESULT

The result of the online survey of 18 IT leaders using site to site VPN from different organizations is shown in Figure 2.

The results as depicted in Figure 2 show that 72% were using same appliance / hardware for their perimeter security.

IPSEC is the preferred protocol for site to site VPNs for most of the CIOs participated in survey. Next question was based on ports permitted via tunnels. This was observed that 17 % of the IT managers were not aware of whether nested VPN is permissible in their set-ups while 22% allow nested VPN (all ports open in the IP range permitted via tunnel) to be used via their setup. Performance impact on data transmission and resource utilization of the firewall due to VPN is not being captured by network monitoring system. The type of data transferred via secured tunnels cannot be measured quantitatively from this survey however a clear qualitative picture emerged. It was found in 24% of the instances, Video format data was predominant while in 29% of the cases, other formats are more prevalent and rest have mixed data needs. The other format was referred as binary types, vmdk files of virtualization servers etc. It was also noticed that all respondents configured VPNs with compression ON by default. Survey shows limited awareness about the performance impact due to VPN architectures amongst IT leaders.

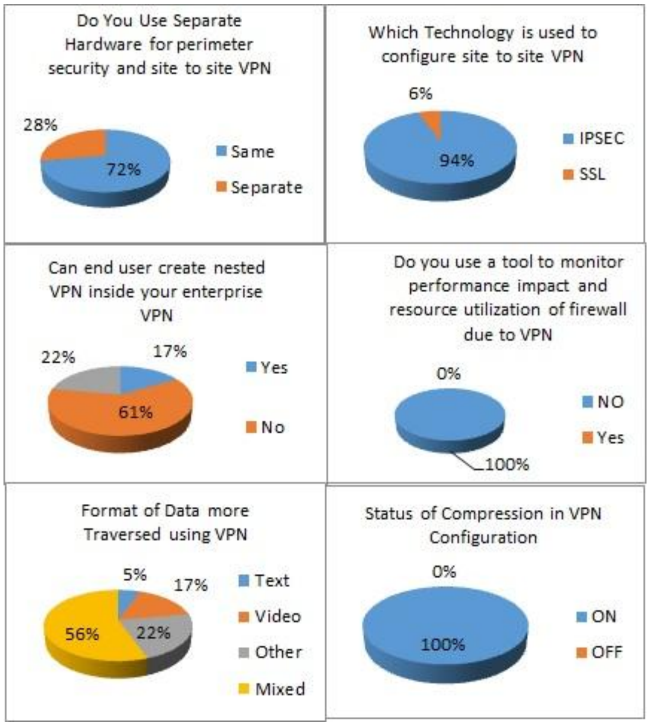


Figure 2 Online Survey Response.

The results collected in simulation lab environment for different combinations of tunneling, compression and bandwidth restrictions are recorded in Table 2 and Table 3. This is evident from the recorded results that there is a considerable impact on performance due to different combinations of VPN, compression and nature of data. The performance delay varied from 1.08 to 5 folds in various combinations with respect to the performance of data transfer without any VPN.

The performance analysis of the text file transmitted with different combinations of compression in over-utilized bandwidth conditions is depicted in Figure 3 and the performance analysis of video file in similar conditions is depicted in Figure 4. The performance analysis of the text file transmitted with different combinations of compression in under-utilized bandwidth conditions is depicted in Figure 5 and the performance analysis of video file in similar conditions is depicted in Figure 6. Following observations emerged from the analysis of the results presented in the respective tables and figures. First two analysis depicts the impact of single VPN tunnel as compared to data transmitted without tunnel.

In first two analysis stages, the impact of compression is not taken into consideration.

Table 2 Time Taken for file transfer with bandwidth restricted to 100mbps (over utilized bandwidth).

	Compression Status			
	OFF	***ON***	***OFF***	***ON***
Configuration	Time to transfer Video File (sec)		Time to transfer for Text File (sec)	
No VPN	186	NA	185	NA
IPSEC (Single Tunnel)	205	206	204	104
SSL (Single Tunnel)	217	218	216	93.5
SSL Inside SSL	399	400	403	286
IPSEC Inside IPSEC	574	570	566	334
SSL Inside IPSEC	678	694	680	382
IPSEC Inside SSL	609	626	580	352

Table 3 Time Taken for file transfer with bandwidth restricted to 1000mbps.

compression status	**OFF**	**ON**	**OFF**	**ON**
Times in seconds to transfer	***Time to transfer Video File (sec)***		***Time to transfer Text File (sec)***	
No VPN	6.22	NA	6.18	NA
IPSEC (Single Tunnel)	6.74	35.7	6.77	19.2
SSL (Single Tunnel)	10.7	10.9	10.9	10.2
SSL Inside SSL	225	228	217	221
IPSEC Inside IPSEC	248	288	248	260
SSL Inside IPSEC	216	222	216	220
IPSEC Inside SSL	235	269	242	262

The analysis due to compression is mentioned in point 3 and 4 whereas; impact due to nested VPN is mentioned in points 5 to 8.

1. Impact of Single VPN with compression OFF in over-utilized internet bandwidth conditions (For both text and video file) : As shown in Figure 3 and Figure 4, IPSEC VPN causes approximately 10% delay, whereas SSL VPN causes 16% delay as compared to the files transmitted without VPN.
2. Impact of Single VPN with compression OFF in Underutilized internet bandwidth condition (For both text and video file): As shown in Figure 5 and Figure 6, IPSEC VPN causes approximately 8% of delay, whereas SSL VPN causes 72% of delay as compared to the files transmitted without VPN.
3. Impact of compression (OFF vs ON) using single VPN in over-utilized internet bandwidth condition: As shown in Figure 3 and Figure 4, it has been observed that there is no impact on the speed of video file transmission done using IPSEC and SSL VPN due to compression. However, transmission of text file done using IPSEC and SSL with compression ON is impacted.

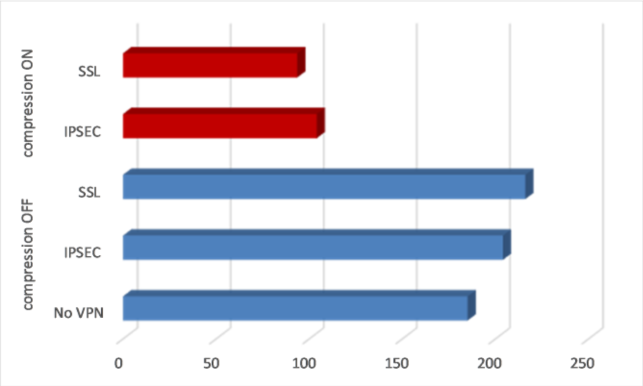


Figure 3 Analysis of Text File transmitted using over-utilized bandwidth condition

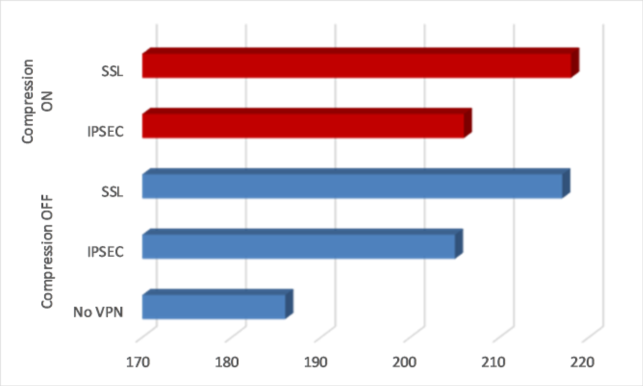


Figure 4 Analysis of Video File transmitted in over-utilized bandwidth condition

The transmission of text file is approximately 1.96 and 2.3 times faster respectively as compared with compression OFF using same protocol.

4. Impact of compression (OFF vs ON) using single VPN in under-utilized internet bandwidth condition: As shown in Figure 5 and Figure 6, it has been observed that the speed of video file transmission done using IPSEC with compression ON is delayed by approximately 5 times as compared to compression OFF condition whereas the speed of Text file is delayed by approximately 2.8 times in similar conditions. This result was in contradiction to the general perception that compression enhances the transmission speed. It has also been observed that the transmission speed of both text and video files has no impact due to compression while using SSL VPN.
5. Impact of nested VPN in over-utilized internet bandwidth condition: It has been observed that the file transmission was delayed by approximately 1.83 to 4 times for different combinations of nested VPN as compared to single tunnel.
6. Impact of nested VPN in under-utilized internet bandwidth condition: This was further observed that the file transmission was drastically delayed due to nested VPN in under-utilized internet bandwidth conditions.

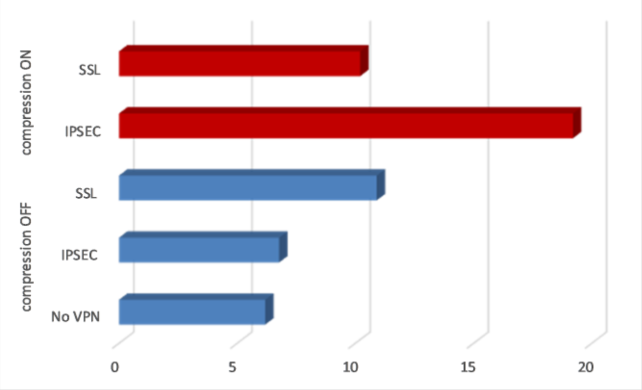


Figure 5 Analysis of Text File transmitted in under-utilized bandwidth condition

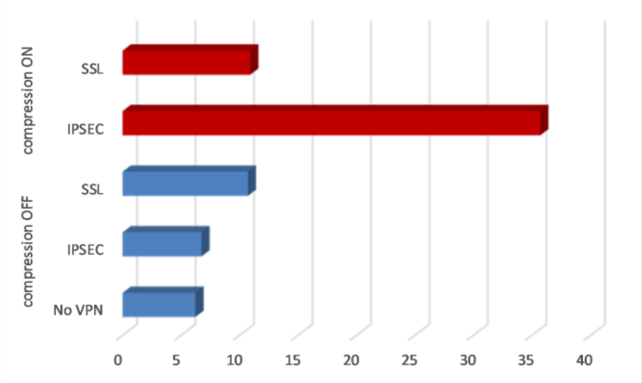


Figure 6 Analysis of Video File transmitted in under-utilized bandwidth condition

7. Impact of compression (OFF vs ON) using nested VPN in over-utilized internet bandwidth condition: It has been observed from the results mentioned in Table 3 that the transmission speed of video file is not majorly impacted due to compression. However, the compression has increased the speed of text file approximately 1.4 to 1.8 times for different nested VPN combinations.
8. Impact of compression (OFF vs ON) using nested VPN in under-utilized internet bandwidth condition: It has been observed from the results mentioned in Table 3 that the transmission of both video and text files was slightly delayed by enabling the compression.

V. Conclusion and Future Work

The survey shows that IPSEC protocol is preferred for site to site VPN to interconnect two networks. The empirical measurement shows that the data transfer performance depends critically on internet bandwidth utilization, format of data and compressibility configuration of VPN implementation. It was found that for incompressible content types like MP4 video, enabling compression in VPN algorithm adds to the delays. The compression of text file by VPN algorithms in under-utilized bandwidth conditions was generating major delays rather than reducing transmission time. Therefore, as shown in the survey, the general practice of enabling compression by default in VPN configuration is counterproductive. Achieving acceptable performance with such configurations would require superfluous expenditure on firewall appliance resources. Thus, it is recommended that VPN configuration may be tailored to the nature of data transmitted via tunnels for different internet bandwidth conditions.

In the survey, it was found that significant proportion of organizations transmits mixed data and for such cases, static configuration (compression ON) may not be optimal. VPN provide security at the cost of performance; hence application specific cost benefit analysis is required to choose the optimal architecture. Packet inspection and the correlated decision of data compression may be a better choice before transferring the data. Therefore, it is recommended that the future VPN solutions may be self-adaptive to these factors which may impact the performance.

Nested VPN may add complexity to improve the security of the data in motion. The performance impact due to nested VPN is very high. It can also be assessed that for improved security, the larger encryption key size may be a better option as compared to nested VPN.

Analyzing the latency due to VPN tunnels and correlating the impact to end-user experience may be the focus of network monitoring tools. The network monitoring tools are required to address the impact analysis due to overheads generated by VPN encryption and compression algorithms.

REFERENCES

1. D. Taneja and S. S. Tyagi, “Information Security in cloud computing: A Systematic Literature Review and analysis,” International Journal of Scientific Engineering and Technology, pp. 50-55, 2017.
2. H. Mao, L. Zhu and H. Qin, “A Comparative research on SSL VPN and IPSec VPN,” International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-4, 2012.
3. J. Hur and d. D. K. Noh, “Efficient and Secure Identity-Based Onion Routing,” International Journal of Applied Engineering Research, vol. 12, no. 6, pp. 1069-1074, 2017.
4. M. Pólkowski, D. Laskowski and P. Łubkowski, “Application of Data Encryption for Building Modern Virtual Private Networks,” Theory and Engineering of Complex Systems and Dependability, vol. 365, 2015.
5. A. Alshalan, S. Pisharody and D. Huang, “A Survey of Mobile VPN Technologies,” IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1177-1196, 2016.
6. J. P. Thomas and Z. Shen, “Security and QoS Self-Optimization in Mobile Ad Hoc Networks,” IEEE Transactions on Mobile Computing, vol. 7, pp. 1138-1151, 2007.
7. C. Yu, J. Lan, J. Xie and Y. Hu, “QoS-aware Traffic Classification Architecture Using Machine Learning and Deep Packet Inspection in SDNs,” Procedia Computer Science, vol. 131, no. C, pp. 1209-1216, 2018.
8. T. Malinowski and A. Arciuch, “The procedure for monitoring and maintaining a network of distributed resources,” Federated Conference on Computer Science and Information Systems, pp. 947-954, 2014.
9. A. A. Alhaj, “Performance Evaluation of Secure Data Transmission Mechanism (SDTM) for Cloud Outsourced Data and Transmission Layer Security (TLS),” International Journal of Cloud Applications and Computing, vol. 4, no. 1, 2014.
10. S. Vanjire and S. Vanjire, “Nested Tunnel header compression Protocol in wireless network with .NET technology,” International Conference on Communication and Signal Processing, pp. 882-886, 2014.
11. R. K. Chauhan and S. S. Tyagi, “Performance Analysis of Proactive and Reactive Routing Protocols for Ad hoc Networks,” International Journal of Computer Applications, vol. 1, no. 14, pp. 27-30, 2010.

12. D. Zhang and D. Ionescu, "Online Packet Loss Measurement and Estimation for VPN-Based Services," IEEE Transactions on Instrumentation and Measurement, vol. 59, no. 8, pp. 2154-2166, 2010.

AUTHOR PROFILE

Dinesh Taneja is research associate at Manav Rachna International Institute of Research and Studies, Faridabad. He has keen interest in Information Security and performance analysis for data in motion with respect to the data security. He has designed campus IT Infrastructure and data centers consisting of heterogeneous equipment. His main areas of interest are cloud computing, low cost high available clusters and information security. He has vast experience of more than 20 years in the domain of enterprise solution architecture. He did his Master of Engineering in computer technology and applications from Delhi College of Engineering in 1999.

Prof. S. S. Tyagi is presently working as a Professor, Computer Engg. and Head of the Department of FCA, Manav Rachna International Institute of Research and Studies (MRIIRS), Faridabad. He is former HOD-Department of Computer Sc. & Engg. and also of Deptt. of Information Technology. He completed his Ph.D in Computer Science and Engineering from Kurukshetra University, Kurukshetra in the year 2010. He did his M.E from BITS Pilani in the year 2002 and B.Tech in Computer Technology from Nagpur University, Nagpur in 1992. He is having an experience of more than 25 years including 4 years of industrial and 21 years of academic/teaching experience. He has been holding various academic and administrative positions during his career. He is having a vast experience of teaching for the students of B.Tech, M.Tech, MCA and Ph.D.