Domineering Analysis & Mitigation of IP-SEC VPN Using GNS3

Engr. Maria Abdullah[†] and Najeed Ahmed Khan[††], Shariq Mahmood Khan[††]

[†]Computer Systems Engineering Department Dawood University of Engineering & Technology
Karachi, Pakistan
[††]Computer Science & Software Engineering Department, NED University of Engineering & Technology
Karachi, Pakistan

Abstract
The needs of Internet have been expanded, a definitive test for system architects is to permit the focused on systems to get to delicate corporate data in a protected way by means of Internet. VPN engineering is an innovation that remains stood in presence for certain time and it exists a demonstrated innovation that permits organizations to transmit corporate information safely and financially over an expansive separation. IP Security is a typical set of rules for acquiring the Internet Protocol (IP) communication by Verification and encryption of transmission of an information stream. The aim of this research is to find out the effect of implementing the IP Security tunnel on edge routers. AES - Encryption algorithm, SHA - Hashing algorithm and Pre-shared - Authentication keys are used in the proposed framework. Also focus is on the TCP and ICMP execution assessment on a VPN environment with distinctive IPsec with tunnel & without tunnel to identify Security, Delay & CPU utilization as an overheads.

Key-words:
VPN; IP Security; ICMP; TCP; SHA1; AES algorithm.

1. INTRODUCTION

Organize security is one of the inclining themes in present days. As world is more powerless, VPN significance has expanded. Business association these days is not restricted to one place. Along these lines, they need security in shoddy value which can satisfy by utilizing VPN and its present day burrowing convention which has been outlandish for anybody the experience it. It has been brilliant cake for the individuals who work more out in the open bistro organize than sitting in same put consistently. It is giving new name to the security and information exchange through the web [1]. A VPN connection can be represent as a pipe carrying enclosed private data via a public network VPN is the extensively used tunnel, and it uses different protocols that guarantee protected data communication among multiple locations linked with public telecommunication networks such as Internet. VPN .VPN innovation has been concentrated over an extensive variety of its event, from execution perceptions of VPN conventions, payload and working frame works, to IP variants. Working frameworks, conventions and system media are at the center of the VPN frameworks that significantly encourage better execution and Security. As per prior research VPN gives distinctive execution on various scenarios [2]. VPN procedures deliver locked communication channels with information encryption and integrity, and they are implemented with various encryption algorithms. Encryption algorithms are Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard 128 bit (AES128) Advanced Encryption Standard 256 bit (AES256). Authentication and data integrity algorithms are Message-Digest 5 (MD5) and Secure Hash Algorithm (SHA1) [3]. Web Protocol Security (condensed IPsec) is a convention suite for securing the Internet Protocol (IP) correspondences by the verification and encryption of every IP parcel transmission of an information stream. The IPSEC private system layer security and it is more appropriate for VPN innovation. IPsec convention is utilized to build up high force security procedure to the parcel at the IP layer. It help the root validation, information classification connectionless information respectability, and the different other security administrations. IPsec convention incorporates three things that is Internet Key Exchange (IKE) convention, Encapsulation Security [4]. This research paper solely clarify the superiority of IPsec base VPN for information transmission over a protected links, Distinctive parameters like Security is elaborated, and evaluates postponement and CPU usage as an overheads.

2. VIRTUAL PRIVATE NETWORK

VPN is a isolated data and speech network that uses public communication infrastructure while maintaining privacy by using security and tunneling protocol. In past years, undertakings, medium organizations and individual use of Internet are expanded drastically. The wide differences of VPN ad ministrations and items are possible by contending vendors. This made associations tangled about the determination of association with Different Features like system insurance and fool proof. The VPN conventions can likewise be sorted in two significant gatherings, site to site VPN & Remote Access

Manuscript received April 5, 2017
Manuscript revised April 20, 2017

VPN. Site to-site VPN Protocols are the company's network and are utilized to secure system association between two or more association's business locales utilizing imparted medium, for example, Internet, to transmit system movement safely. Remote access VPN: Remote Access VPN is likewise termed virtual private dial-up networks (VPDNs) between portable clients and associations and are utilized to create association Network by utilizing imparted medium, for example, Internet for secured transmission [1].

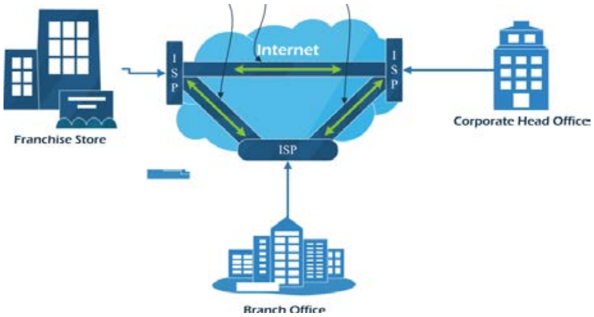


Fig. 1 Site to Site IP Security VPN

3. CRYPTOGRAPHY

Each framework that is created can be hacked or assaulted. Every diverse hack or assault speaks to a different risk against the framework. For each risk a danger investigation is passed to focus the suitability of that risk and what harm is possible if that danger is acted upon. Contingent upon the treat investigation countermeasures are taken such that the outflow of propelling the assault is more noteworthy than the normal gain from the assault. The different strategies are additionally called cryptographic building block. In information and broadcast communications, cryptography is fundamental when imparting over any untrusted medium, which incorporates pretty much any system, especially the Internet [3]. Each single piece can deal with a specific issue. Encourage, these pieces can be joined realizing cryptosystem like An ES IPsec gives security relies on upon the level of security required by the clients and application with utilized Different Cryptographic Algorithm. The main concern of using an encryption algorithm is to deliver better security to a network which prevents unauthorized attacks. There is an extensive variety of cryptographic algorithm that can be used in VPN with IPsec [3, 4].

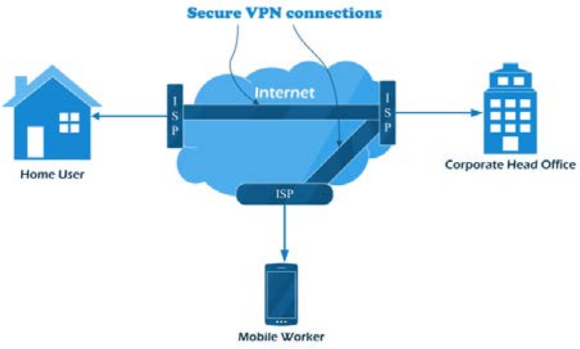


Fig. 2 Remote Access using Point to Point Tunneling Protocol

4. IP SECURITY

IPsec gives the ability of securing any sort of activity over IP-based systems like for instance the Internet. . IPsec can secure the whole way between two elements on the other hand a particular part of the transmission way giving information uprightness, information classification, anti-replay insurance and numerous additional security administrations. Moreover, IPsec executes an internet Key Exchange (IKE) system which permits two substances to arrange and select the required assurance systems, cryptographic changes and to exchange keys. The security arrangements are based upon the open schema of IP Security Architecture (IPsec), characterized by the IPsec Working Group of the IETF. It is known as a framework that it gives a steady and enduring base for giving Network Layer security [5]. The vital IPsec protocols are IP Authentication Header (AH) which provides data source authentication, data truthfulness, and replay security. IP Encapsulating Security Payload (ESP) gives information privacy, data source authentication, information trustworthiness, and replay insurance [6]. Internet Security Association and Key Management Protocol (ISAKMP) give a technique for automatically setting up Security Associations and managing their cryptographic keys [7]. Internet Key Exchange (IKE) that performs the key exchanges. It is vital to see how these conventions communicate with each other in request to have the capacity to actualize and utilization IPsec [8, 9]. IPsec incorporates convention for setting up common validation between operators at start of session and arrangement of cryptographic keys to be utilized amid session [10]. Keeping in mind the end goal to keep the transmission secure you have to select how the encryption will occur, what sort of encryption calculations to utilize etc. There are two paramount realities in regards to key trade. Key trade is in a broad sense a confounded business. Key trade gets more entangled as the gathering of conveying parties increment Key Exchange Protocols Developed for IP. IKE is a hybrid convention and is dedicated around a arrangement categorized by the Web Security Association and Key Management Protocol (ISAKMP).

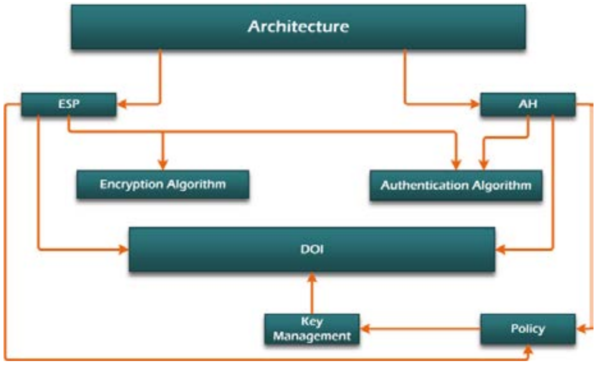


Fig. 3 IP Security Roadmap

IPsec gives two separate modes of operations namely Transport mode and tunnel mode. In Transport mode, the endpoint of the entire correspondence are additionally the IPsec Conventions and uses the IP addresses of the correspondence endpoints. The AH, ESP both ensure the transport header. In this mode AH furthermore ESP catch the bundles dropping out of the Transport Layer into the internet Layer and give the arranged security. Transport mode encodes the information divide (payload) of every bundle, leaves the header untouched and is most regularly used to secure information correspondence inside a system.

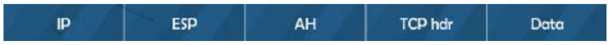


Fig. 4 Confidentiality to be applied after Integrity

Whereas Tunnel mode encrypts both header and payload. It is extra protected, used to protect data that crosses strange third gathering networks. It is also used for network-to-network communication. IPsec packet level security is provided mainly by two protocols: AH and ESP. AH provides guaranteed connectionless integrity and data source authentication of the IP datagram.

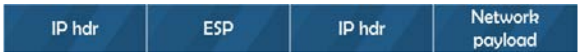


Fig. 5 ESP in Tunnel Mode

Datagrams and it protects beside replay packets. ESP provides origin authenticity, confidentiality protection, integrity of a packet, authentication-only implementation and encryption-only implementation.

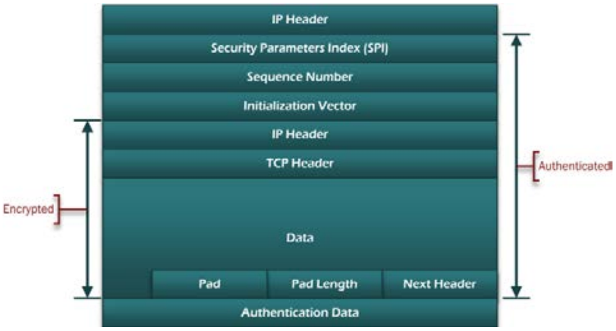


Fig. 6 ESP Header in Tunnel Mode

5. ANALYSIS

This section defines the analytical approach of same topology with two different configurations i.e. without tunnel and with IPsec tunnel. The two approaches are examined on the following parameters:

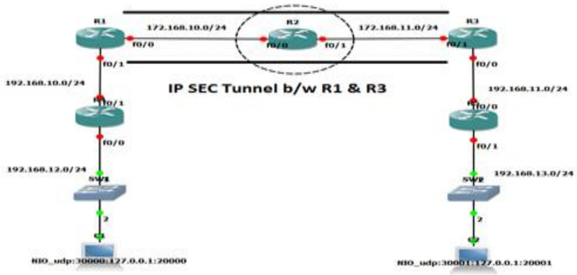
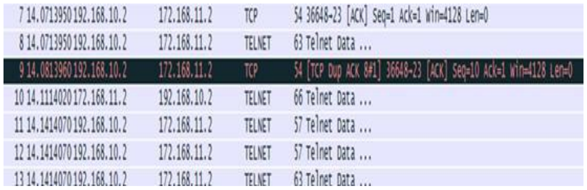


Fig. 7 IPSEC Tunnel between R1 & R31

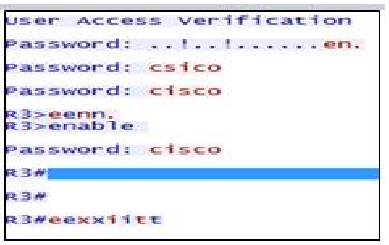
A. Security without tunnel

Packets are captured using Wire shark when traffic (i.e. TCP & ICMP) is generated from R4 to R5 or vice versa. When TCP follow stream is being checked, it shows that password is passing in clear text form which is purely a security flaw. If anyone captures the packets traversing from R1 to R3 and vice versa, passwords can easily be seen in the capture. Figure 8 shows different communication parameters including passwords.



```
 7 14.0713950 192.168.10.2   172.168.11.2   TCP      54 36648→23 [ACK] Seq=1 Ack=1 Win=4128 Len=0
 8 14.0713950 192.168.10.2   172.168.11.2   TELNET   63 Telnet Data ...
 9 14.0813960 192.168.10.2   172.168.11.2   TCP      54 [TCP Dup ACK 8#1] 36648→23 [ACK] Seq=10 Ack=1 Win=4128 Len=0
10 14.1114020 172.168.11.2   192.168.10.2   TELNET   66 Telnet Data ...
11 14.1414070 192.168.10.2   172.168.11.2   TELNET   57 Telnet Data ...
12 14.1414070 192.168.10.2   172.168.11.2   TELNET   57 Telnet Data ...
13 14.1414070 192.168.10.2   172.168.11.2   TELNET   63 Telnet Data ...
```

Fig. 8 Communication Parameters including Passwords

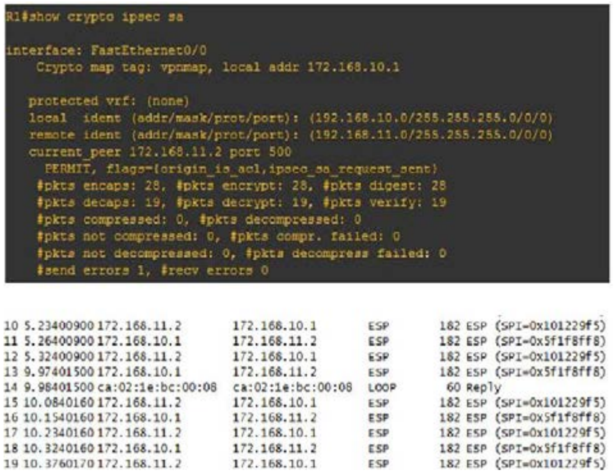


```
User Access Verification
Password: ..!..!.......en.
Password: csico
Password: cisco
R3>eenn.
R3>enable
Password: cisco
R3#
R3#
R3#eexxiitt
```

Fig. 9 Communication Parameters with Passwords

B. With IPsec Tunnel

The figure 9 shows packets are encapsulated by ESP when traffic passing from R1 to R3. The following report shows an example that packets are encrypting as well as decrypting when traffic is going through IPsec tunnel.



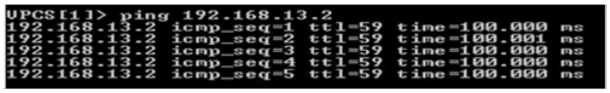
```
R1#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: vpnmap, local addr 172.168.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.11.0/255.255.255.0/0/0)
   current_peer 172.168.11.2 port 500
     PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
    #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify: 19
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
```

```
10 5.23400900 172.168.11.2        172.168.10.1        ESP      182 ESP (SPI=0x101229f5)
11 5.26400900 172.168.10.1        172.168.11.2        ESP      182 ESP (SPI=0x5f1f8ff8)
12 5.32400900 172.168.11.2        172.168.10.1        ESP      182 ESP (SPI=0x101229f5)
13 9.97401500 172.168.10.1        172.168.11.2        ESP      182 ESP (SPI=0x5f1f8ff8)
14 9.98401500 ca:02:1e:bc:00:08   ca:02:1e:bc:00:08   LOOP      60 Reply
15 10.0840160 172.168.11.2        172.168.10.1        ESP      182 ESP (SPI=0x101229f5)
16 10.1540160 172.168.10.1        172.168.11.2        ESP      182 ESP (SPI=0x5f1f8ff8)
17 10.2340160 172.168.11.2        172.168.10.1        ESP      182 ESP (SPI=0x101229f5)
18 10.3240160 172.168.10.1        172.168.11.2        ESP      182 ESP (SPI=0x5f1f8ff8)
19 10.3760170 172.168.11.2        172.168.10.1        ESP      182 ESP (SPI=0x101229f5)
```

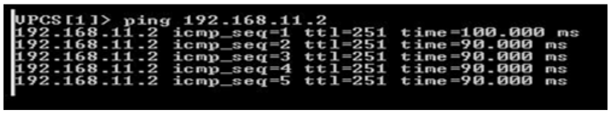
Fig. 10 Encrypted/decrypted Packets when Traffic Passed through IPSEC Tunnel

B.1. Delay

Below mentioned reports are generated when random traffic is generated from PC1 to R5 & PC1 to PC2 respectively.



```
VPCS[1]> ping 192.168.13.2
192.168.13.2 icmp_seq=1 ttl=59 time=100.000 ms
192.168.13.2 icmp_seq=2 ttl=59 time=100.001 ms
192.168.13.2 icmp_seq=3 ttl=59 time=100.000 ms
192.168.13.2 icmp_seq=4 ttl=59 time=100.000 ms
192.168.13.2 icmp_seq=5 ttl=59 time=100.000 ms
```



```
VPCS[1]> ping 192.168.11.2
192.168.11.2 icmp_seq=1 ttl=251 time=100.000 ms
192.168.11.2 icmp_seq=2 ttl=251 time=90.000 ms
192.168.11.2 icmp_seq=3 ttl=251 time=90.000 ms
192.168.11.2 icmp_seq=4 ttl=251 time=90.000 ms
192.168.11.2 icmp_seq=5 ttl=251 time=90.000 ms
```

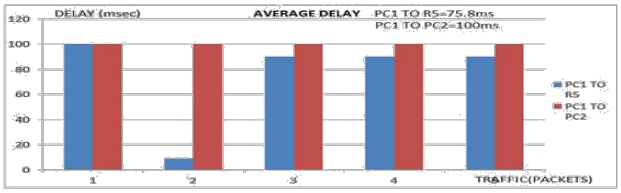
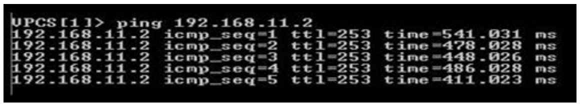


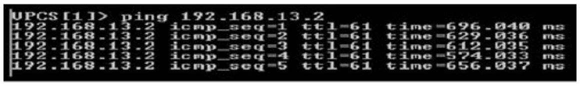
Fig. 11 Packets flow delay in milli-seconds.

C. With IPsec Tunnel

Below mentioned reports are generated when random traffic is generated from PC1 to R5 & PC1 to PC2 respectively.



```
VPCS[1]> ping 192.168.11.2
192.168.11.2 icmp_seq=1 ttl=253 time=541.031 ms
192.168.11.2 icmp_seq=2 ttl=253 time=478.028 ms
192.168.11.2 icmp_seq=3 ttl=253 time=448.026 ms
192.168.11.2 icmp_seq=4 ttl=253 time=486.028 ms
192.168.11.2 icmp_seq=5 ttl=253 time=411.023 ms
```



```
VPCS[1]> ping 192.168.13.2
192.168.13.2 icmp_seq=1 ttl=61 time=696.040 ms
192.168.13.2 icmp_seq=2 ttl=61 time=629.036 ms
192.168.13.2 icmp_seq=3 ttl=61 time=612.035 ms
192.168.13.2 icmp_seq=4 ttl=61 time=574.033 ms
192.168.13.2 icmp_seq=5 ttl=61 time=656.037 ms
```

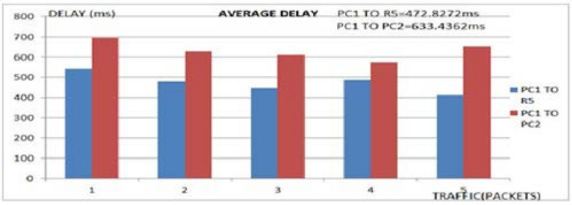


Fig 12 Packets flow delay in milli-seconds from PC1 to R5 & PC1 to PC2

D. CPU Utilization

Below mentioned reports are generated when random traffic (i.e. TCP & ICMP) is passed from R1 to R3 and vice versa. The traffic is generated from R4 to R5 & vice versa.

E. Without tunnel

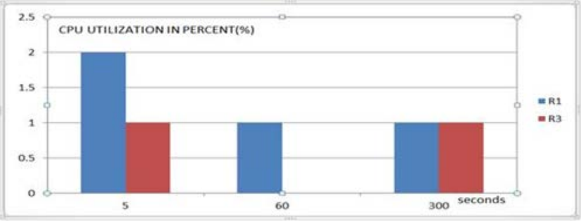


Fig. 13 CPU utilization without tunnel in R1& R3.

F. With IPsec tunnel

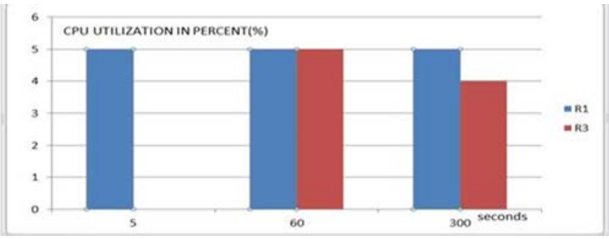


Fig. 14 CPU utilization with tunnel in R1& R3

The graph state that IPSEC Tunnel Topology has higher CPU Utilization as compare to simple topology (without tunnel).

6. CONCLUSION

From the Analysis we conclude that:

A. Security

VPNs securely associate distant customers and offices in a corporate network. The objective of a VPN is to add a level of security to the exchange of data.

Notwithstanding when organization is utilizing a rented line, they can convey a VPN system to ensure their information. It is a virtual system; due to the association between any two hubs of the entire VPN is not a physical connection which essentially private system utilizes Instead, it develops a rationale organize on top of the stage which an Internet Service Provider gives. What's more, the customer information is transmitted in the consistent connection .VPN utilizes the burrowing innovation, encryption and decoding procedure, and key administration, client and gadget character validation advances.

By analyzing the figures it is concluded that VPN is a secure technique to transfer data. IPSEC Tunnel provides greatest way to secure the data as it encrypts all the packets passing from the tunnel. Different algorithms used to encrypt and authenticate the packets. While in simple topology (without tunnel) packets are going in clear text form.

B. Delay

As VPN is a secure technique to transmit the data from branch to another or from one branch to the head office. Router 1st encrypts the packet going from source to endpoint and decrypts the packets while receiving therefore it takes more time than a simple packet passing from router to another. The expansion of passage headers and encryption overhead builds the bundle sizes of all encoded applications. IPsec VPN administrations are worked by overlaying an indicate point work over the Internet utilizing Layer 3 encrypted passages. This engineering requires security apparatuses, for example, (equipment or programming) routers that bolster IPsec passages, to be introduced at both closures of each passage. Encryption/decryption is performed at these tunnel endpoints, and the protected traffic is carried across the common network.

From graphs shown above, packet takes more delay in IPSEC tunnel as compare to the simple topology (without VPN).

C. CPU Utilization

IPsec and key exchange impacts performance when active. Key connections, public key verification, and encryption/decryption take a substantial quantity of resources. There is a little reduction in execution for non-encoded bundles that experience an interface that does crypto. This is because all packets have to be checked against the crypto map.

The above graph state that IPSEC Tunnel Topology has higher CPU Utilization as compare to simple topology (without tunnel). Since the packet is encrypted and decrypted in IPsec tunnel therefore it takes more CPU utilization.

VPN is an absolute new network technology. IPsec permits VPN arrange a standard security for the corporate system. IPsec is the most trusted and secure VPN arrangement accessible in the present market. The dispute of VPN is agreeably solved by IPSEC enable VPN by compromise certain level of overheads.

7. FUTURE WORK

This research experiment was undertaken only under the wired Platform by analyzing various metrics. However, this research possibly will be protracted to various interesting studies as below.

- Conduct the similar study on a wireless network.
- Conduct the similar study on hardware routers
- Conduct the same study for UDP and other types of traffic and calculate different parameters like: jitter, QoS and packet loss.
- Conduct the same study with different client/server operating system

And, as there are vast variations on the VPN research area, there is a need for further research on the evaluation of the performances, to include a greater range of operating systems, protocols and metrics.

References

[1] Saugat Bhattarai,’’VPN (Term Paper) Research’’,Kathmandu University. 2016. [Online] January 2016 - Available: www.researchgate.net/publication/289120789_VPN_research_Term_Paper>.[Accessed 26.02.17].

[2] Rashikala Werawerna, “TCP/UDP Network Performance Evaluation of Various IPsec Algorithms An Empirical Test-bed Analysis of a Virtual Private Network Protocol”. UNITEC Institute of Technology, New Zealand 2013

[3] Gary C. Kessler,’’An Overview of Cryptography’’. [Online]. Available:, http://www.garykessler.net/library/crypto.html#why3>. [Accessed 26.02.17].

[4] Pankaj Kumar Singh, Pawan Parkash, “A Novel Approach for the analysis and issues of IPsec VPN”, .IJSR, ISSN: 2319-7064, July 2013.

[5] RFC 2401, Security Architecture for Internet Protocol, provide an overview of IPsec. [Online]. Available: http://www.ietf.org/rfc/rfc2401.txt>.[Accessed 26.02.17].

[6] Kent & Atkinson, IP Authentication Header, pg 10. AH is IP protocol number 51. The AH version 2 is defined in RFC 2402, IP Authentication Header. [Online]. Available at http://www.ietf.org/rfc/rfc2402.txt>.[Accessed 26.02.17].

[7] Kent & Atkinson, IP Authentication Header, pg 12. ESP is IP protocol number 50. The ESP version 2 is defined in RFC 2406, IP Encapsulating Security Payload (ESP). [Online]. Available at http://www.ietf.org/rfc/rfc2406.txt>.[Accessed 26.02.17].

[8] D.Harkins and D.Carrel, “The Internet Key Exchange (IKE)”RFC 2409 (Proposed Standard), internet Engineering Task Force, Nov, 1998

[9] Miteshkumar Shaileshbhai Parmar, Arvind D Meniya, “Imperatives & issues of IPsec based VPN”. International Journal of Science and Modern Engineering (IJISME), ISSN: 2319-6386, Volume-1, Issue-2, and January 2013.

[10] Mr.Hitesh Dallam’s Dolly Dallam’s Sonia Batra,Ms Poooja Rani “Implementation of IPsec Protocol 2012, Second International Conference on Advanced Computing & Communication Technologies 978-0-7695-4640-7/12