IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. II (Jan – Feb. 2015), PP 79-84
www.iosrjournals.org

The Impact of Security Overhead Traffic on Network's Resources Performance

Esam Suliman Mustafa Ahmed[1], Dr.Amin Babiker A/Nabi Mustafa[2]
[1, 2](*Faculty of Engineering / AL-Neelain University, Sudan)*

Abstract: *Security of transferred data is a big concern for data networks users .One of the best security solutions is the IPSec Virtual Private Networking (IPSec VPN).In this paper, The Impact of additional traffic generated by IPSec protocol on the network's resources performance is discussed. Network simulation is a major part of this Paper. OPNET simulation software is used. Analyzing the impact of applying IPSec VPN to secure a flow of traffic from a remote sites connected through IPSec Tunnels to one Server is the methodology of the study, using OPNET. Three scenarios have been simulated. The results are compared by measuring the utilization of the server in the three scenarios.*
Keywords*: VPN, IPSec, Opnet, Security, ESP, AH.*

I. Introduction

IPSec Tunnel One of the most important and widely-used security technologies, it uses encryption and Authentication to provide secure access over the public internet. Data sent from one site to another passes securely across the Internet. When the data travels from source to destination it passes across intermediate networks that may be shared, unwanted users may access the flow of data. VPN provides mechanisms to ensure that the data transferred securely.

1.1 Types of IPSec VPN

Two forms of VPN:

1- Site to Site VPN

Site -to -Site VPN (Figure 1). Fixed VPNs devices that link various office locations together and provides a secure connection between the corporate network and its branches. The VPN devices encrypt the packet and send the encrypted version over the Internet. When a packet arrives, the organization VPN device decrypts the packet and transmits the result to the user's computer.

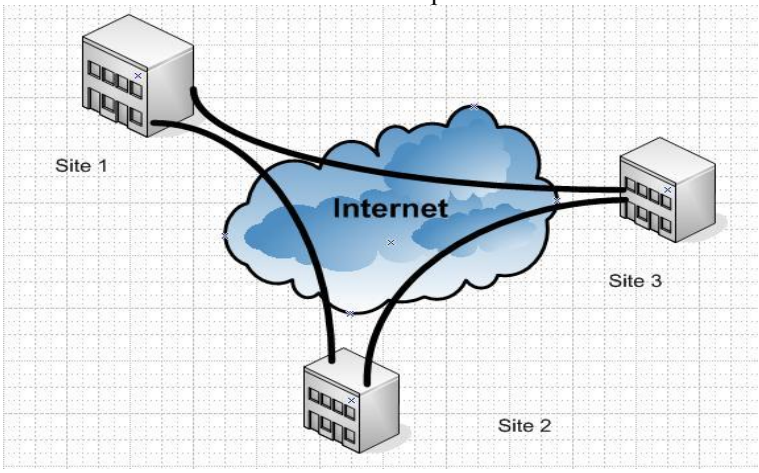

Figure 1: Site-to-Site VPN

2- Client Server VPN

Client Server VPN (Figure 2). Each user has Client Software to allow them to connect to the VPN Server. a user connects to the Internet and then launches the VPN application. the VPN software encrypt all packets and sends the encrypted packet to the corporate VPN server.

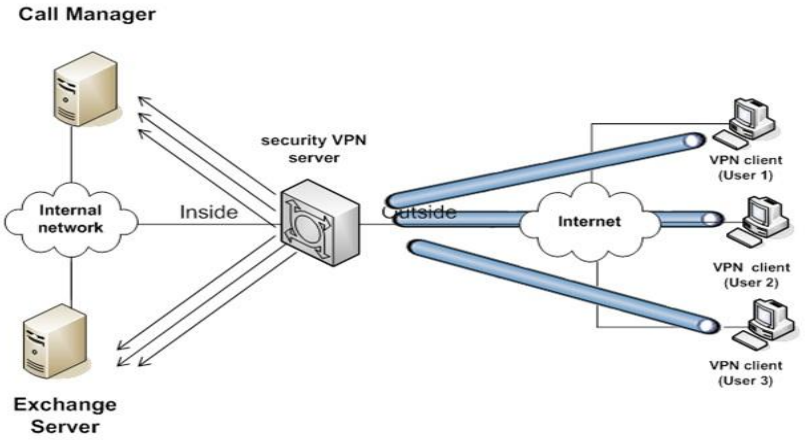

Figure 2: Client Server VPN

1.2 IPSec Overview

IPSec is set of security algorithms that allow a pair of communicating devices to transfer data securely by offering strong encryption and authentication .IPSec protects what is delivered from the transport layer to the network layer. In other words, the transport mode protects the network layer payload, the payload to be encapsulated in the network layer.

1.3 Two Security Protocols

1- Authentication Header (AH)

The Authentication Header (AH) Protocol is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet. The protocol uses a hash function and a symmetric key to create a message digest; the digest is inserted in the authentication header. The AH is then placed in the appropriate location based on the mode (transport or tunnel). Figure 4 shows the fields and the position of the authentication header. A field inside the authentication header (the next header field) holds the original value of the protocol field (the type of payload being carried by the IP datagram).

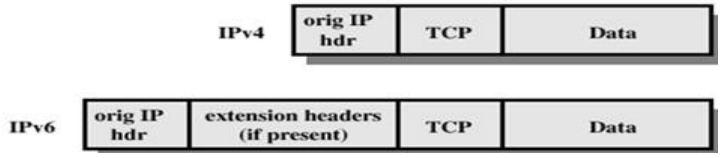

Figure 3: Ipv4 and Ipv6 Datagram without AH

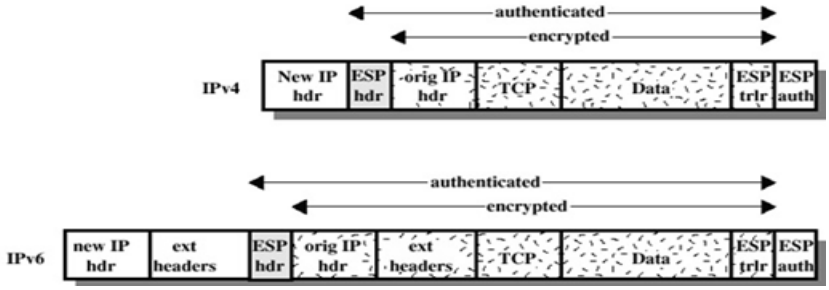

Figure 4: ESP Encryption and Authentication

1.4 Encapsulating Security PAYLOAD (ESP)

The AH Protocol does not provide privacy, only source authentication and data integrity. IPSec later defined an alternative protocol that provides source authentication, integrity, and privacy called Encapsulating Security Payload (ESP). ESP adds a header and Trailer. Note that ESP's authentication data are added at the end of the packet which makes its calculation easier. Figure 5 shows the ESP header.

When an IP datagram carries an ESP header and trailer, the value of the protocol field in the IP header is 50.A field inside the ESP trailer (the next-header field) holds the original value of the protocol field (the type of payload being carried by the IP datagram, such as TCP or UDP). The ESP procedure follows these steps:

1. An ESP trailer is added to the payload.
2. The payload and the trailer are encrypted.
3. The ESP header is added.
4. The ESP header, payload, and ESP trailer are used to create the authentication data.
5. The authentication data are added to the end of the ESP trailer.
6. The IP header is added after the protocol value is changed to 50.

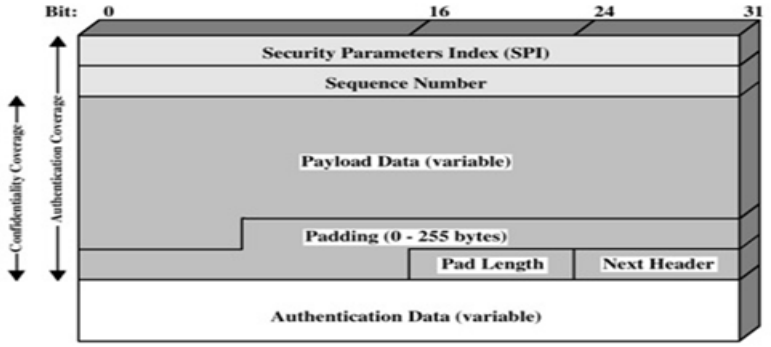

Figure 5: Encapsulating Security Payload

1.5 Services Provided by IPSec

IPSec overhead traffic affect on the overall throughput of the network. The congestion occurred in the network increase the response time for each application and increase the CPU utilization of the network resources .some applications like Real-time Applications are so sensitive to network delay and congestion which may lead to audio gaps and drop calls .

II. An OPNET Simulation

OPNET is a very usefully simulation program with a vast range of features. Used to create a virtual environment to simulate real networks. After a virtual network is created it can be possible to add many network components for example routers switches, servers, work stations and protocols. After creation of the scenario we can apply the configuration that we need to test and run the simulation. Finally we can analyze the result and make a comparison between the different scenarios to get the impact of applying different protocols and parameters. OPNET permits not only the building of a virtual network but also provides tools for dynamically investigating the network.

III. The Design

Three scenarios are used to measure the utilization of the server before and after applying IPSec.

In the first scenario the network is configured where the server is accessed by Clients from different three sites connected through DS1 channels to the HQ router without applying a VPN tunneling as it shown in fig 6. in the second scenario a VPN tunneling are configured between the three sites and HQ router. The server acts as FTP, DB, and HTTP server for the clients in the three sites as it shows in fig 7. Channel's bandwidth increased from DS1 to DS3 in the third scenario

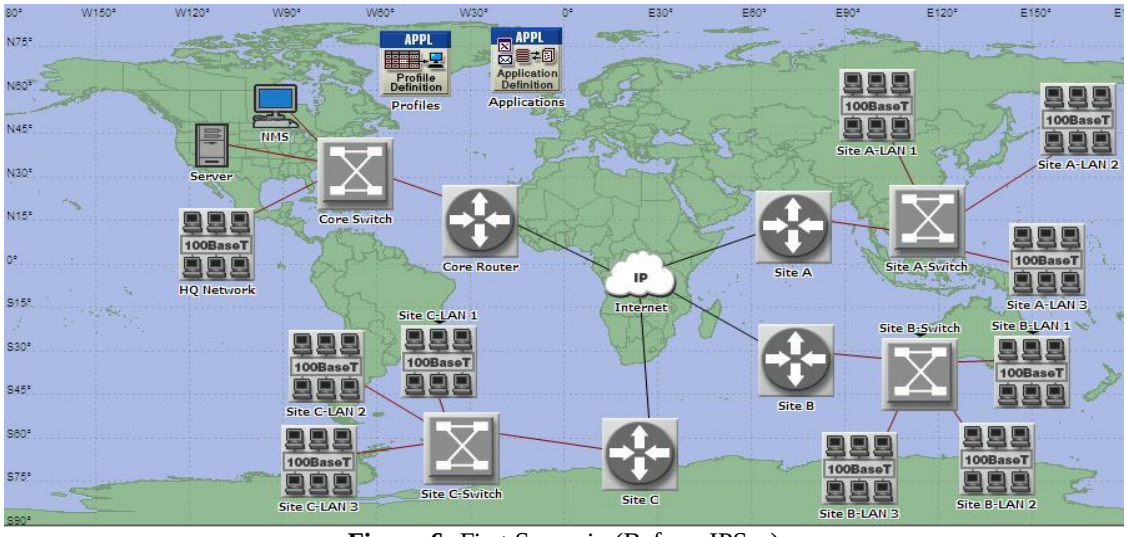

Figure 6: First Scenario (Before IPSec)

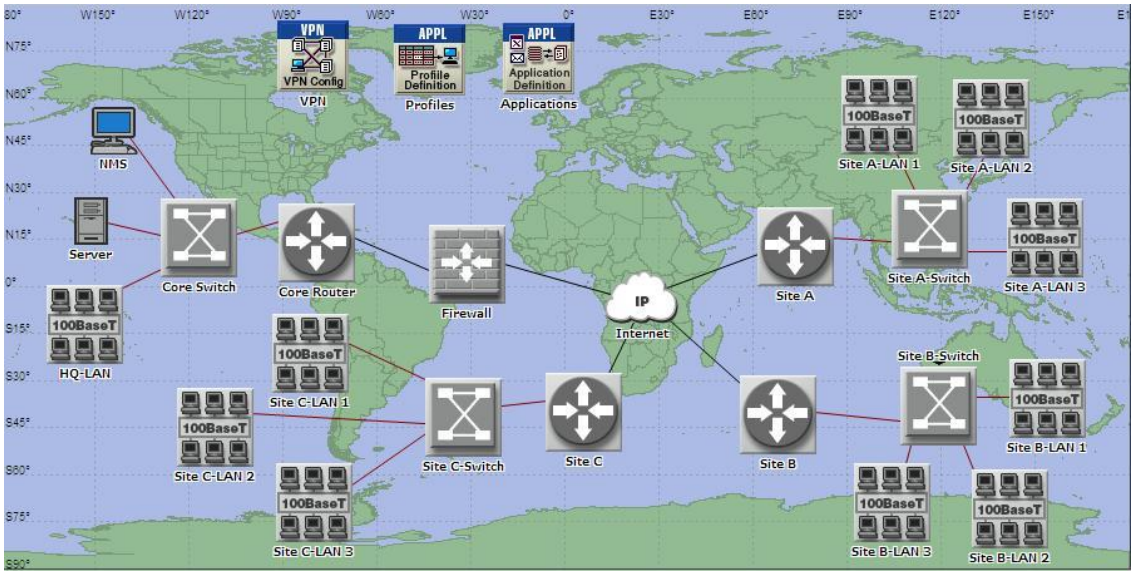

Figure 7: Second Scenario (After IPSec)

IV. The Results

The simulation runs for 1 hour. An event is defined as File Transfer (Light), Web Browsing (Light HTTP), and Database Access (Light). Results were collected after the simulation was run. Statistics of each scenario presented in a graph that detailed the activity throughout the simulation. Graph 8 illustrates the Utilization of the server's CPU in the three scenarios. The graph shows that the CPU utilization becomes very high after applying the IPSec due to Encapsulating security payload. Utilization decreased when increasing the Bandwidth of the links between the remote sites and HQ (IPSec with more Bandwidth scenario). Graphs 9 and 10 illustrate time average in server performance load (tasks/second and requests/second) in the two scenarios (before and after IPSec). the number of tasks and requests handled by the server increased after applying IPSec Graph 11 shows the delay-element (in the client DB Traffic Received (bytes/second)).
Graph 12 shows the incoming packets to the core router in the two scenarios (Before and After IPSec).

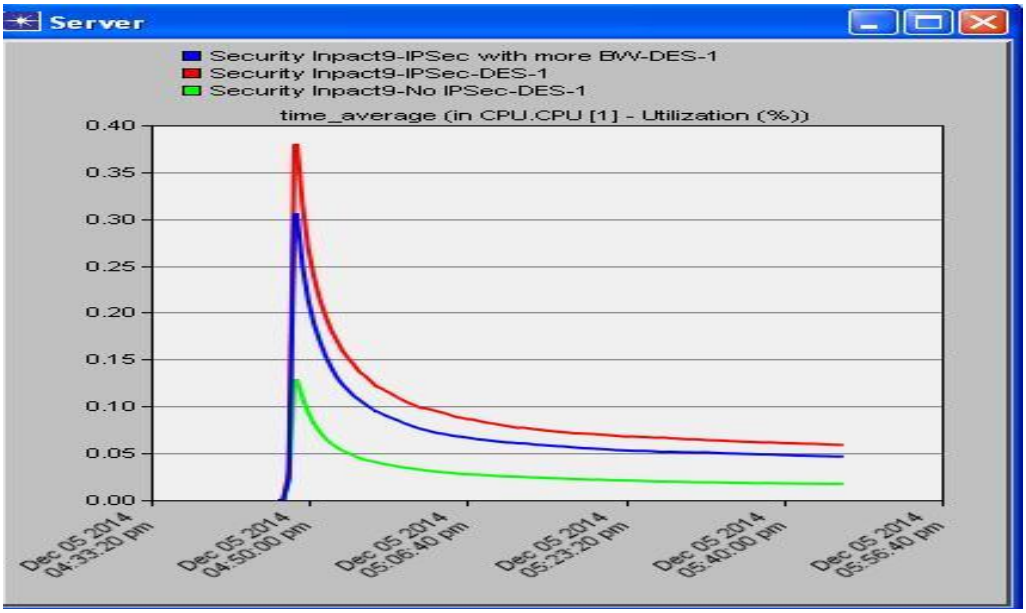

Figure 8: Time average in CPU Utilization

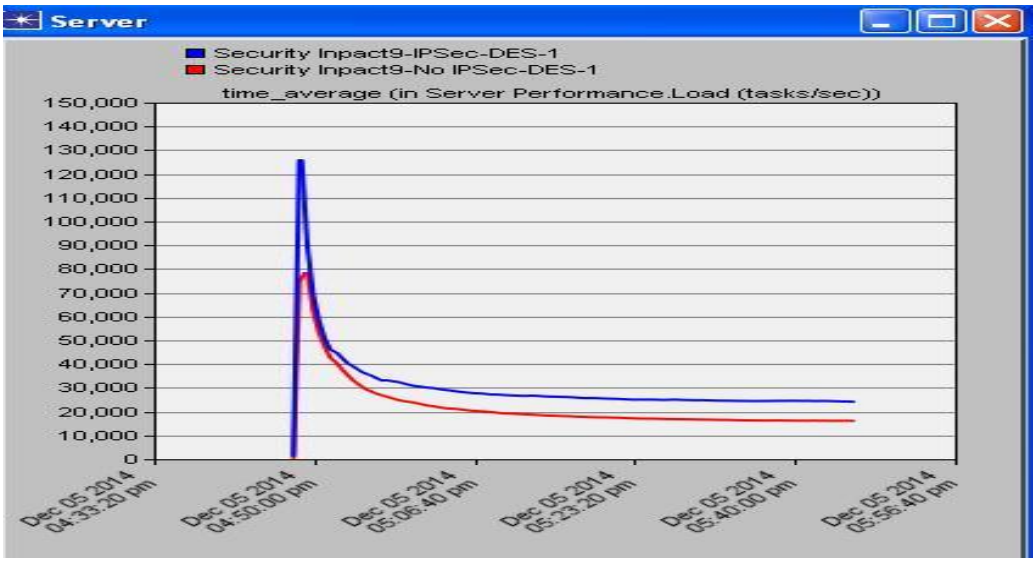

Figure 9: Time Average in server performance (Load/second)

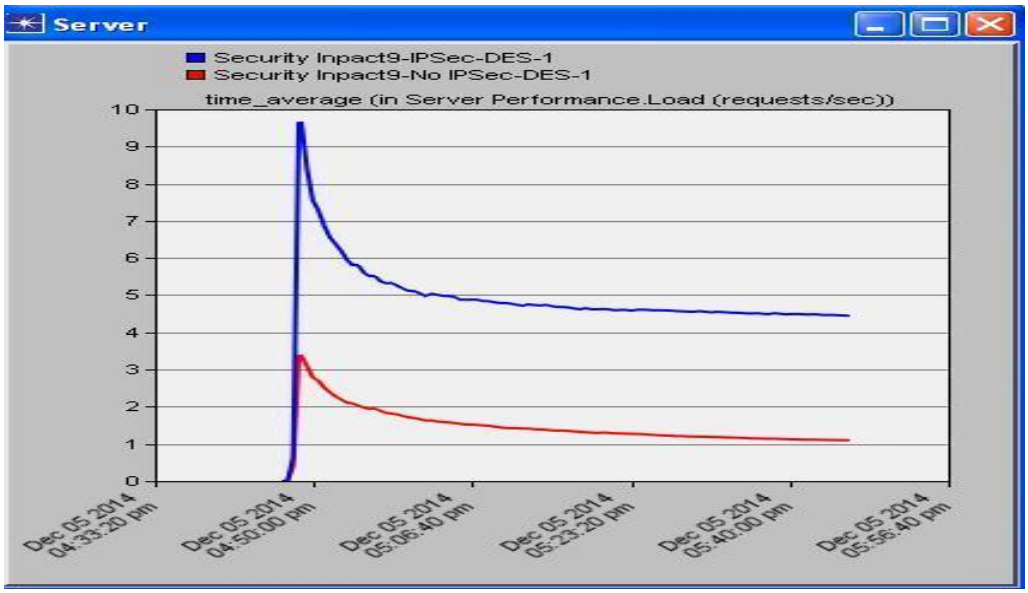

Figure 10: Time Average in server performance (Request/second)

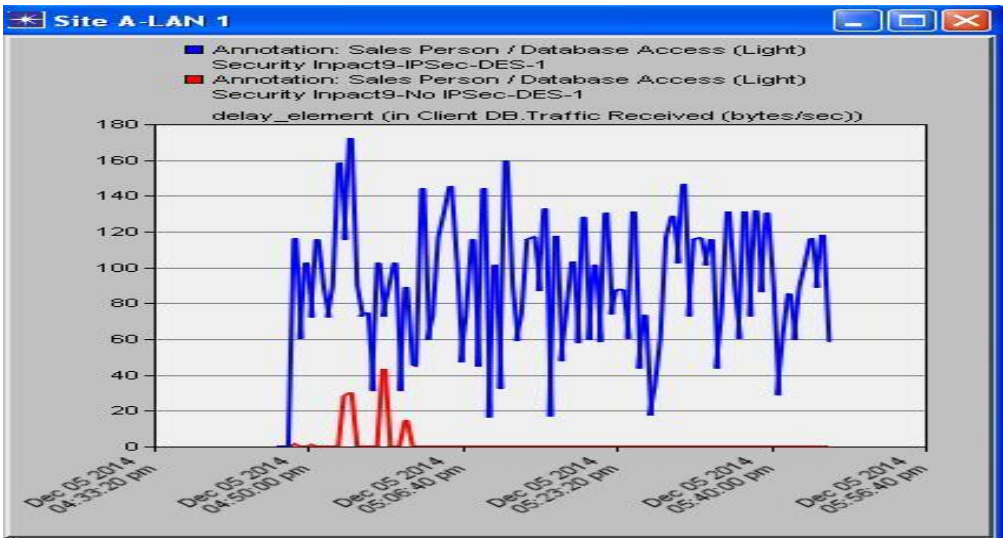

Figure 11: delay element (in client DB. traffic (bytes/second))

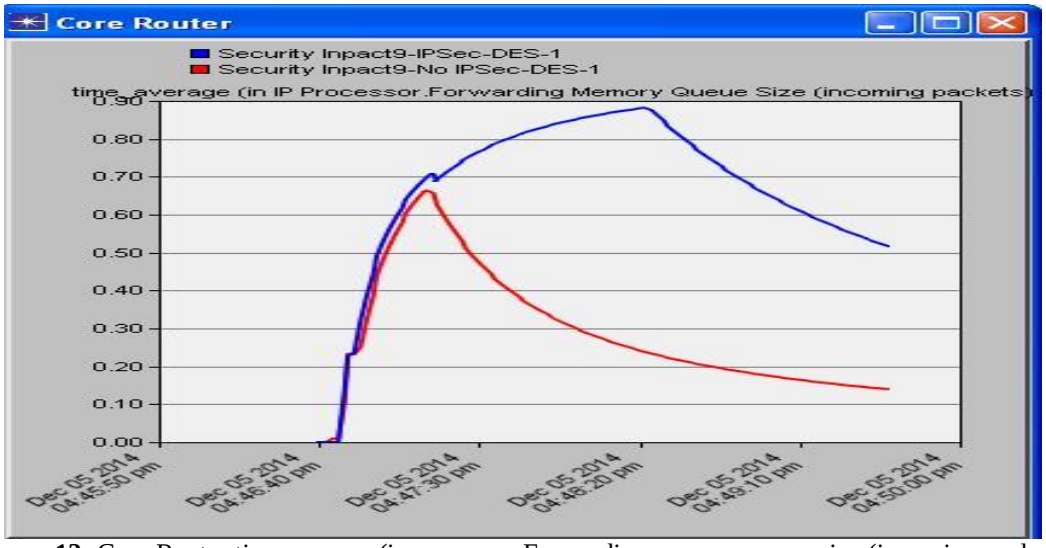

Figure 12: Core Router time average (in processor Forwarding memory queue size (incoming packets)

V. Conclusion

Referring to the graphs we get that there is a vast overloaded traffic after applying the IPsec tunnels which injects additional traffic within network. The server's CPU utilization is increased according to the huge amount of traffic and decreased when increasing the bandwidth. The number of tasks/second handled by the server becomes very high after applying IPSec Tunnels, also The delay in the traffic received by DB clients increased .

Security mechanisms inject additional traffic within network that leads to increase the utilization of the network's resources and the task's response time which will affect the network performance and stability. VPN tunnels are the most effective secure communication across long distances. To reduce the effect of additional traffic, network's active components and servers with high specifications (CPU, RAM, and Storage) required. Increasing the bandwidth is a main factor in solving the IPSec protocol delay issues .

References

[1]. Henric Johnson , Network Security , Blekinge Institute of Technology, Sweden.
[2]. W.~Diffie and E.~Hellman, {New directions in cryptography}, IEEE Transactions on Information Theory {22} (1976).
[3]. Douglas E.Comer,Computer Networks and Internets
[4]. McDysan. D.(2000),VPN applications Guide
[5]. Behrouz A. Forouzan (2007), Data Communications and Networking
[6]. J. Walrand and P. Varaiya, High-Performance Communication Networks.
[7]. Dina Katabi, Mark Handley, and Charlie Rohrs, "Congestion Control for High Bandwidth-Delay Product Networks,"
[8]. David D. Clark, Van Jacobson, John Romkey, and Howard Salwen, "An Analysis of TCP Processing Overhead," IEEE Communications Magazine, June 1989
[9]. Kent, IP Authentication Header, November 1998.
[10]. IPsec VPN WAN Design Overview,http://www.cisco.com
[11]. IPsec Direct Encapsulation Design Guide— http://www.cisco.com/en/US/docs/solutions.
[12]. Kosiur, D,"Building and Managing Virtual Private Networks," New York, NY(1998).
[13]. Erwin, M., Scott, C,Wolfe ," Virtual Private Networks" Sebastopol CA: O'Rielly , Associates Inc(1999).