A Novel Approach for the Analysis & Issues of IPsec VPN

Pankaj Kumar Singh[1], Pawan Prakash Singh[2]

[1]Suresh Gyan Vihar University, Jagatpura , Jaipur-302025,India

[2]Head of Department, Cluster A, Suresh Gyan Vihar Univesity, Jagatpura, Jaipur-302025, India

Abstract: ***Virtual Private Network is the technology to setup a private network in the public network. It is broadly accepted technology for corporate world for strengthen their business. A VPN connection can be represent as a pipe carrying enclosed private data via a public network. Internet Protocol Security (abbreviated IPSec) is a protocol suite for securing the Internet Protocol (IP) communications by the authentication and encryption of each IP packet transmission of a data stream. The IPSEC private network layer security and it is more suitable for VPN technology .This research paper exclusively explain the quality issues in IPsec base VPN for data transmission over a secure network.***

Keywords: Authentication Header (AH), Encapsulating Security Payload (ESP), IP Security (IPSec), Tunnel, Transport, Virtual Private Networks (VPN), Quality of Service (QoS)

1. Introduction

1.1 Virtual Private Network

Virtual Private Network (abbreviated VPN) it shows the technology to establish a private network in the public network or virtual private network (VPN) is an extension of a organization private intranet across a public network such as the Internet. It creates a secure private connection through a private tunnel [4].

VPNs securely connect remote users and offices in a corporate network. The objective of a Virtual Private Network is to add a level of security to the exchange of data. Even when a company is using a leased line, they can deploy a VPN network to protect their data. It is a virtual network, because of the connection be tween any two nodes of the whole VPN is not a physical link which basically private network uses. Instead, it builds up a logic network on top of the platform which an Internet Service Provider provides, for example, Internet, Asynchronous Transmission Mode (ATM), Frame Relay (FR) and so on. And the client data is transmitted in the logical link.VPN uses the tunneling technology, encryption and decryption process, and key management, user and device identity authentication technologies. It covers the package across the shared or public networks, the encryption and authentication validation link, extension of the private network.

1.2 IP Security (IPsec)

IP Security (IPsec) protocol is a security standard which is published by IETF in November of 1998. (RFC 2401) Its main motto is to provide password-based security, strong interoperability and high quality communication with security for the IPv4 and IPv6. IPsec protocol is used to establish high intensity security process to the packet at the IP layer. It aid the origin authentication, data confidentiality connectionless data integrity, and the various other security services. IPsec protocol includes three things that is Internet Key Exchange (IKE) protocol, Encapsulation Security Payload (ESP) protocol and Authentication Head (AH) protocol. IKE protocol is mainly used for the Internet Key Exchange and builds up the security policy. When using Internet Key Exchange protocol, it can establish Security Associate (SA) dynamically and guarantee about the security during the establishment process. ESP is main motto is responsible for keeping the transmission packet's confidentiality, integrity and authentication security. AH is used for authentication and keeping the data integrity. Using the IPsec protocol can make all kinds of applications sharing the IP layer's security services and also the key management process, without having to design and implement their own security methodology. It meant that IPsec will minimize the cost of key exchange negotiation and the potential of security vulnerabilities [4].

2. IPSEC PROTOCOLS

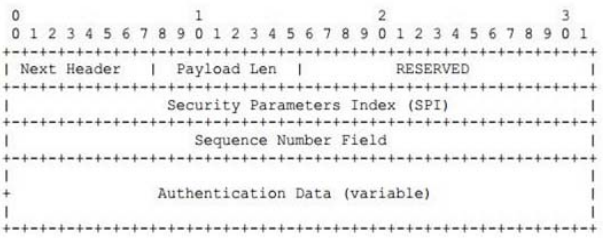
This area will focus on the three primary components which are used for the security purpose of data .The Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE) protocols. Explaining each security protocols with their purpose and function and describing the working process to create IPsec connections. IPsec is a collection of protocols that assist in securing communications over IP networks [2].

2.1 Authentication Header (AH)

Authentication Header (AH) [3] provides the data integrity check, authentication and optional anti-replay protection, but it does not have the data confidentiality protection. AH provides the authentication protection as much as possible, the packets which are not able to authenticate themselves will be discarded from the destination point. Because AH will not encrypt the data, AH will not guarantee about the data confidentiality, so it does not require encryption algorithm.

AH will work with the algorithm of choice, depending on the level of security required. Currently the algorithm options are HMAC (Hashed Message Authentication Code) MD5

(Message Digest 5), HMAC-SHA1, HMAC-SHA256. AH have two modes of operation: transport mode and tunnel mode. In tunnel mode, AH creates a new IP header for each packet where as in transport mode, AH does not create a new IP header.

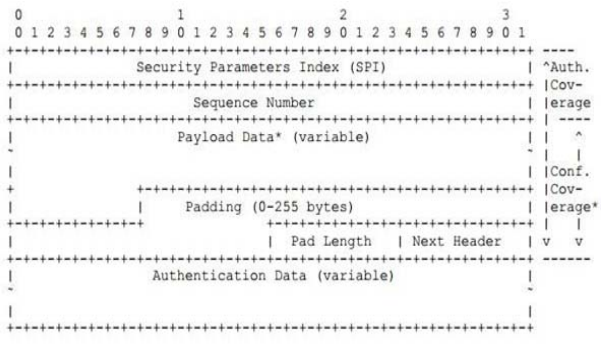


AH format (RFC 2402)

2.2 Encapsulating Security Payload (ESP)

ESP main motto is to provide confidentiality service by encrypting the data, but the ESP can also provide authentication for packet payload. In the up gradation of second version the ESP became more flexible. ESP uses the algorithm independent and the options are: Digital Encryption Standard (DES) (64 bit, commonly called 56bit), 3DES, RC5, Blowfish, Idea, Cast, AES-128 bit, AES-192 bit, and AES-256.

ESP has two modes of operations: transport and tunnel. In transport mode, ESP can provide encryption and integrity protection for the payload of an IP packet, as well as integrity protection for the ESP header. Transport mode is not compatible with NAT. In tunnel mode, ESP can provide encryption and integrity protection for an encapsulated IP packet, as well as authentication of the ESP header. [5]



ESP format (RFC 2406)

2.3 Key Management

From the Security Association's parameters, AH and ESP can provide security services for the IP packets. Security Association can be created manually or automatically. When number of users is in small amount, and the key updating frequency is not high, we can choose to establish Security Association manually. But when number of users is in large amount, the network size is large; we should choose to use the automatic mode. Internet Key Exchange (IKE) is a protocol that IPsec defines to manage the Security Association automatically. Its motto is to establishes, negotiates, modifies and delete Security Association. [6]

Internet Key Exchange is a part of Internet Security Association and Key Management Protocol (ISAKMP), it is an Oakley and SKEME key exchange protocol mixed agreement. ISAKMP defines a framework of the authentication and key exchange policy, but does not define any key exchange protocol. ISAKMP is independent from the key exchange. It straight forward means that ISAKMP is designed to support a variety of different key exchanges alternatives. The Oakley and SKEME both define authenticated key exchange method respectively, including the structure of payload, processing order, payload information and how to use them in key management [10].

3. Quality of Service (QoS)

Quality of service (QoS) accredits to resource reservation control mechanisms rather than the accomplish service quality. Quality of service (QoS) is the capability to provide different priority to different applications, users, or data flows, or to guarantee an assured level of performance to a data flow [9].

A. Packet Loss

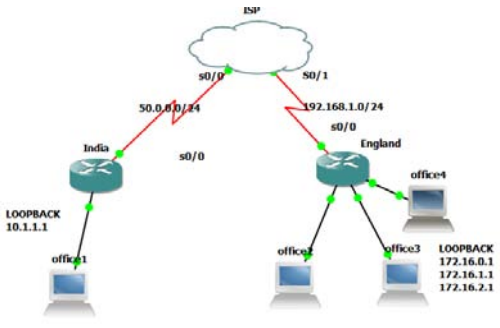
This term refers to the loss or de-sequencing of data packets in a real-time audio/video data stream. A packet loss rate of 1% produces roughly a loss of one fast video update per second for a video stream producing jerky video. Lost audio packets produce choppy, broken audio. *D.*

B. Jitter

This refers to the variability of latencies for packets within a given data stream and should not exceed 20 - 50 milliseconds. If a single packet encountered a jitter of 145 milliseconds or more (relative to a prior packet), an under run condition may occur at the receiving endpoint, potentially causing either blocky, jerky video or undesirable audio

4. Network Model and Methodology

The network is designed with TWO ROUTERS, ISP and 4 HOSTS. The simulation tool is used GNS3 and the analyzing tool is WIRESHARK. By which we can find out the value of average packet loss and the jitter value of the data by implementing the UDP in real time traffic by creating an IPsec VPN. The IPSec cipher description was AES-128 as the encryption algorithm, HMACSHA-1 as the integrity mechanism, ESP and AH security protocols for encapsulation and authentication, IKE as the key interchange protocol and the IPSec authentication was made with pre-shared keys.



5. Test Scenario

Testing consisted on capturing the UDP packets that traveled from India office to England Offices with the use of GNS3. The offices have installed the wireshark so that both can capture the incoming and outgoing traffic. The results only considered the UDP packets. The remaining traffic (FTP, HTTP and ICMP) was discarded since it was just injected for increasing the traffic In order to perform the QoS evaluation; we established 20 minute real-time packets with 5 minute each session collect 4 samples. In test scenario, five minute for every sample was implemented firstly without the IPSec VPN, all others using the IPSec VPN with different security protocols like providing firstly only authentication (AH), then providing the confidentiality (ESP) and providing both authentication plus confidentiality (AH + ESP).

6. Result Analysis

Packet Loss-The important parameter considered in quality of service was the packet loss. As shown in Table.
Packet loss=Number of lost packets / Number of lost packets+No. of packets received

Packet Jitter-This refers to the variability of latencies for packets within a given data stream.
D (i,j)=(Rj - Ri) - (Si - Sj)
D (i,j)=(Rj - Sj) - (Ri - Si)
J(i)=J(i -1)+ (|D (i-1,i)|-J(i-1)) /16

DATA20minute(4 sample)	*Average Packet Loss*	*Average Packet Jitter*
Without IPsec	*0.56%*	*32.9ms*
With IPsec AH	*1.08%*	*43.8ms*
With IPsec ESP	*1.9%*	*56.7ms*
WithIPsec AH+ESP	*2.26%*	*61.4ms*

7. Conclusion

VPN is an absolute new network technology. IPsec allow VPN network a standard security for the corporate network. IPSec is the most trusted and secure VPN solution available in the current market. The dispute of VPN is agreeably solved by IPSec enable VPN by compromise certain level of overhead, performance (QoS) parameter in order to enable both QoS and security with IPSec.

References

[1] Mr. Hitesh dhall, Ms. Dolly Dhall, Ms. Sonia Batra, Ms. Pooja Rani IMPLEMENTATION OF IPSEC PROTOCOL 2012 Second International Conference on Advanced Computing & Communication Technologies*978-0-7695-4640-7/12*

[2] RFC 2401, Security Architecture for the Internet Protocol, provides an overview of IPsec. The RFC is available for download at *http://www.ietf.org/rfc/rfc2401.txt.*

[3] AH is IP protocol number 51. The AH version 2 standard is defined in RFC 2402, IP Authentication Header, available at *http://www.ietf.org/rfc/rfc2402.txt*

[4] Olalekan Adeyinka Analysis of problems associated with IPSec VPN Technology 2008

[5] *978-1-4244-1643-1/08*

[6] ESP is IP protocol number 50. The ESP version 2 standard is defined in RFC 2406, IP Encapsulating Security Payload (ESP), available at *http://www.ietf.org/rfc/rfc2406.txt.*

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

[8] Ankur Lal, Dr.Sipi Dubey,Mr.Bharat Pesswani "Reliability of MANET through the Performance Evaluation of AODV, DSDV, DSR "International Journal of Advanced Research in Computer Science and Software Engineering Vol. 2, No. 5,May 2012,pp. 213-216.

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

[10] Muhammad Awais Azam, Zaka-Ul-Mustafa, Usman Tahir, S. M. Ahsan, Muhammad Adnan Naseem, Imran Rashid, Muhammad Adeel" Overhead Analysis of Security Implementation Using IPSec "

[11] S. P. Meenakshi S. V. Raghavan "Impact of IPSec Overhead on Web Application Servers"

Author Profile

Pankaj Kumar Singh is pursuing M. Tech (Dual) course from Suresh Gyan Vihar University, Jaipur in the field of Information & Communication Technology.