A Review on IPsec and SSL VPN

Article *in* International Journal of Scientific and Engineering Research · November 2014

O P Gupta
Punjab Agricultural University

A Review on IPsec and SSL VPN

Baljot Kaur Chawla, O.P. Gupta, B. K. Sawhney

Abstract - In today's secenario of security, deciding Virtual Private Network (VPN) is a complex task. VPN connects remote sites or users using a public infrastructure (usually the Internet), thereby providing anytime and anywhere remote access to travellers. The objective of VPN is to add a level of security to the exchange of data from the organisations to remote sites. VPN creates a private tunnel for transferring the data securely. Internet Protocol Security (IPSec) and Secure Socket Layer (SSL) are the two dominant VPN technologies being used today. Both have their strengths and weaknesses. A comprehensive study of both the technologies has been presented in this paper. It exclusively explains the architecture and protocols of both the technologies including their advantages and disadvantages for real kind of applications.

Index Terms— Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Protocol Security (IPSec), Secure Socket Layer (SSL), Tunnel, Transport, Virtual Private Network (VPN).

1 Introduction

Virtual Private Network (VPN) extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of the private network with all the functionality, security and management policies of the private network. The decision of selecting the type of VPN depends on the applications to be used [13]. The objective of VPN is to add a level of security to the exchange of data.Privacy of data in VPN is maintained through tunneling protocols and security procedures.In effect, encryption of data is done at sender's side and forwarded via tunnel which is then decrypted at receiver's side. By encrypting the originating and receiving network addresses an additional layer of security can be added.

VPNs have two common uses: remote access for users and site-to-site connectivity. Individual users can establish secure connections with a remote network using remote – access VPN.Whereas a site-to-site VPN allows mulitiple offices in fixed locations to establish secure connection with each other. IPSec (Internet Protocol Security) and SSL (Secure Socket Layer) VPN are the two dominant VPN technologies being used today. Both have their strengths and weaknesses.

2 IPSec VPN

IPsec is a set of security protocols which was developed by IETF (Internet Engineering Task Force) in November of 1998. It is an official standard for network security and was designed for interoperability. It works both with IPv4 and IPv6. IPsec provides data integrity, basic authentication and encryption services to protect modification of data and unauthorized viewing. Three primary components of IPSec include: Authentication Header (AH), Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) protocols.

2.1 Authentication Header (AH)

It provides authentication, data integrity check and replay protection, but it does not include any support for confidentiality, Authentication protection is provided by AH. Packets are discarded from the destination point if they are not able to authenticate themselves. Because AH does not guarantee about the data confidentiality, it will not encrypt data, so it does not require encryption algorithm.

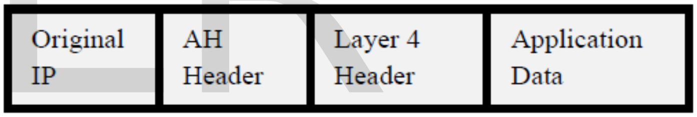

Fig 1: AH Header [1]

Only the IP header and data are authenticated by the AH Header. AH tries to protect all fields of an IP datagram excluding the ones which change during transfer (for example the TTL field in the IP header). Depending on the required level of security, AH uses hashing mechanism like HMAC-MD5 or HMAC-SHA1.AH can be used in tunnel mode and transport mode. A new IP header for each packet is created by AH in tunnel mode whereas no new header is created in transport mode.

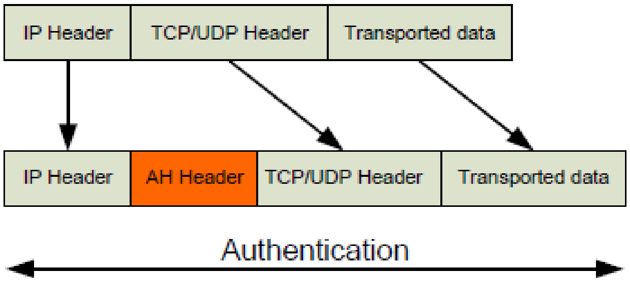

Fig 2: AH in transport mode [8]

- *Baljot Kaur Chawla is currently pursuing masters degree program in computer science engineering in Punjab Agricultural University, Punjab, India, E-mail: baljotchawla@gmail.com*
- *Dr. O.P. Gupta is Deputy Director and Associate Professor of Computer Science in Punjab Agricultural University, Punjab, India*
- *Dr. B.K. Sawhney is Associate Professor in Punjab Agricultural University, Punjab, India*

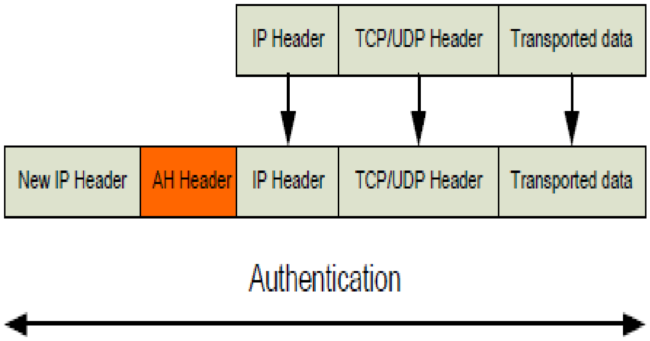

Fig 3: AH in tunnel mode [8]

2.2 Encapsulating Security Payload (ESP)

It provides data confidentiality, in addition to integrity and source authentication. Encryption services are also provided by ESP.Encryption translates a readable message into an unreadable format to hide the message content. Decryption, the opposite process translates the message content from an unreadable format to a readable message. ESP uses symmetric encryption algorithms to provide data privacy. Packet payload authentication can also be provided be ESP.It can also support authentication-only or encryption- only configurations.

mc
tur
boi
car
nev

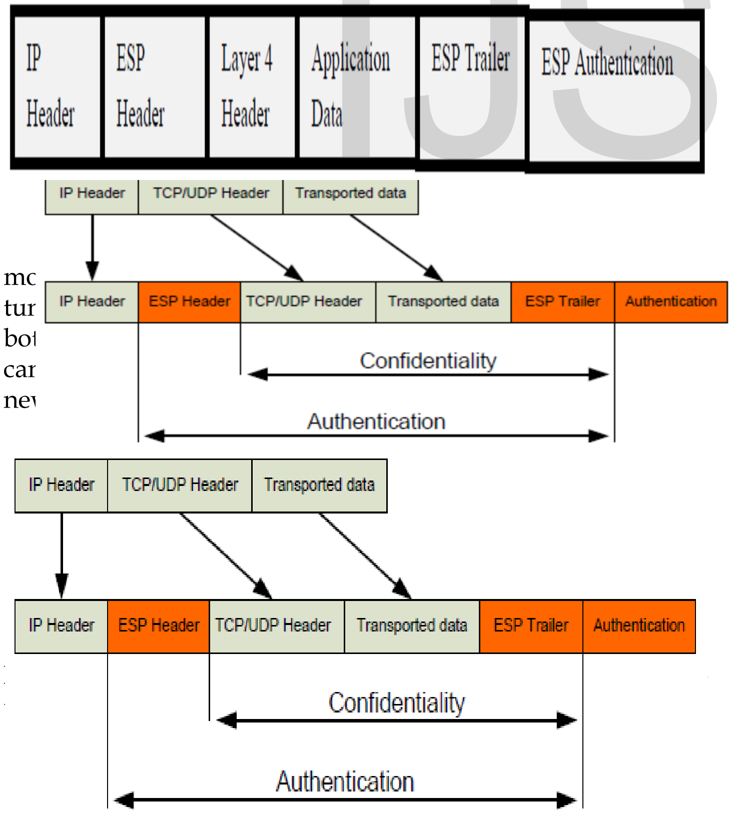

Fig 5: ESP in transport mode [8]

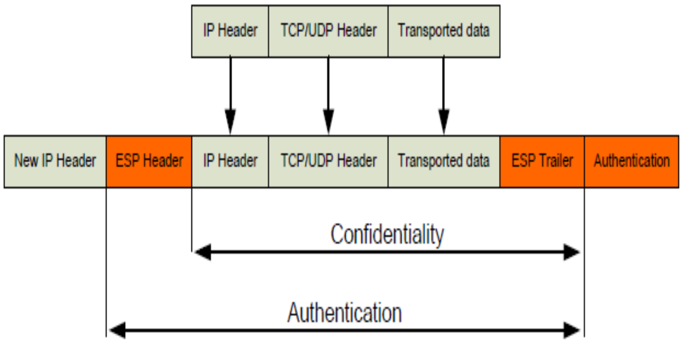

Fig6: ESP in tunnel mode [8]

2.3 Internet Key Exchange (IKE)

IPSec uses Internet Key Exchange (IKE) as the default protocol to determine and negotiate algorithms, keys and protolcols, and to authenticate the two parties. It is used to setup security associations (SA). A security agreement must be established between the two computers before exchanging the secured data. This agreement is known as security association in which both the parties agree on how to protect and exchange information. Protocols like ISAKMP (The Internet Security Association and Key Management Protocol) and Oakley are used by IKE to define procedures for creation, generation and management of SA and authentication. It also reduces the connection timeby centralizing the security association management.

2.4 How IPSec Works

Between two endpoints a virtual "tunnel" is created when IPSec VPN is used. At first sensitive packets are configured. Then via tunnel an IPsec peer sends the packet to the remote peer. All the traffic within the VPN tunnel is encrypted. The client computer can see and potentially access the entire network when connected on an IPSec VPN.

3 SSL VPN

An SSL (Secure Socket Layer) VPN can be used with a standard web browser. It is based on the SSL protocol which provides encryption for http traffic and data authentication. Real Time Protocol (RTP) traffic can also be secured using the SSL. SSL VPN gives remote users access to internal network connections, client/server applications and web applications. Client-server communication is used by SSL.It includes 3 protocols: Handshake protocol, record protocol and alert protocol.

3.1 SSL Protocols

During the handshake protocol, negotiation of encryption algorithm takes place and server authenticates itself to the client.For data encryption, symmetric cryptography is used by SSL whereas to negotiate the shared key asymmetric cryptography is used. In the record protocol, client and server use the shared key to encrypt the data. A format for these messages is specified by the record protocol.In general a message digest is included to ensure that message has not been altered and using a symmetric cipher whole message is encrypted. In alert protocol, an alert containing the error is sent, if an error is detected by either the server or the client. Types of alert messages include warning, critical and fatal. The session can be terminated or restricted based on the received alert message.

3.2 How SSL VPN Works

Working of SSL VPN is explained through following example:

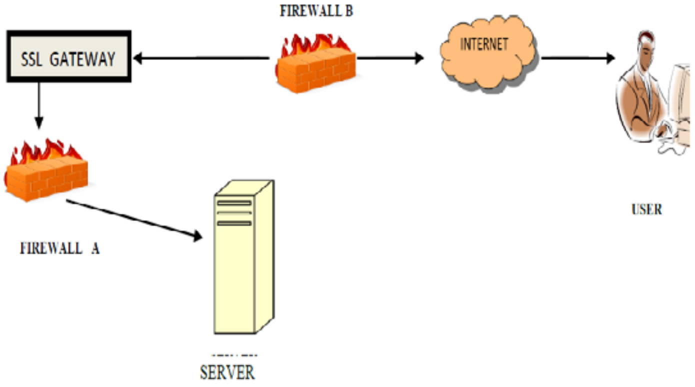

Fig 6: SSL Architecture [1]

All the VPN connections of the company are accepted through SSL VPN gateway. All the connections to the internal application servers are also initiated by SSL VPN gateway. Internal application servers are protected by Firewall A whereas outside Firewall B allows any Internet machine to connect to SSL VPN gateway. Firstly, a user connects to the company's gateway, after successful authentication a list of applications is provided by the gateway which the user of company need to access. At the same time, connection to internal application server is initiated by the gateway through Firewall A.Response received is encapsulated by the SSL VPN gateway and is sent to the user. In this way, SSL VPN tunnel is established between SSL VPN gateway and user's machine. [1]

4 Strengths and Weaknesses

A permanent connection is provided by IPsec between locations. It works at the network layer which makes it application agnostic i.e. any IP based protocol can be tunneled through it. Therefore instead of a dedicated circuit or expensive leased line, IPsec makes a better alternative. However, application agnostic nature of IPsec is also its weakness. At a granular level, IPsec does not havs the ability to restrict access to resources. Remote users can access any corporate resource once a tunnel is setup as if they were directly plugged into the corporate network. IPsec is a complex protocol and is more involved to maintain. Additioanl configuration and maintenance is required to support the remote user population.

On the other hand, SSL VPNs have been designed to support remote access. No special software is required to be installed. Browser-based session using SSL provides remote access. It also has the ability to control access at granular level. Specific authentication and authorization schemes for access to an application can be limited to a particular user population. However, this does not mean SSL VPNs are the panacea to all the IPsec weaknesses [7] .If an always on-link is required to be maintained for remote site, SSL VPN would not be the solution. Because of application agnostic nature of IPsec VPN, it can support client/server application and number of legacy protocols with minimal effort. However SSL VPNs have been built around web based applications. By installing a Java or ActiveX based agent on the remote asset, SSL VPNs cover this weakness.

Table I
Comparison of IPsec and SSL VPN [1], [12]

Component	IPsec VPN	SSL VPN
Connectivity	Site-to-site Remote access	Remote access
Installation	Requires installation of client VPN	No installation of client VPN
Gateway Location	Gateway usually implemented on the firewall	Gateway typically deployed behind the firewall
Complexity	More complex	Less complex
Cost	More cost	Less cost
Security/Control	Broad access creates security concerns	More granular controls require more mangement
Endpoints	Requires host-based clients	Browser based with optional thin clients
Application	Can support all IP based applications	Best for e-mail, file sharing and browser based applications
Layer it Works on	Operates at layer 3	Operates at layers 4-7
Training	Requires specialized training	No specialized training required

5 Conclusion

In any enterprise, accessing the private data over the internet is complex and time consuming. Ideally, SSL and IPsec VPNs should both be implemented as they serve different purposes and complement each other. It is of utmost importance to consider what each deployment is designed to accomplish rather than focusing on what each protocol provides. The deployment choices become clearer once the cost/benefit of each type of deployment is considered keeping in mind the problems each technology was designed to address. On studying the architecture of the protocols, SSL VPN is more suitable to site to site connections. In this, there is no need to install the client software and provide the access to specific application rather than complete network. If the application is IP specific then IPSec VPNs can be ultimate solution and have an IPSec gateway located at your organization.

REFERENCES

[1] R. Kajal, D. Saini and K. Grewal, "Virutal Private Network" International Journal of Advanced Research in Computer Science & Sofware Engineering, 2012, Vol. 2 (10), pp. 428-432.

[2] P.K. Singh and P.P. Singh, "A Novel approach for the Analysis & Issues of IPsec VPN" International Journal of Sciences and Research, 2013,Vol 2 (7), pp. 187-89.

[3] Wikipedia (www.en.w.ikipedia.org/wiki/IPsec)

[4] Root, Don and R. Rissler,"IPsec and SSL VPN Decision Criteria A Technology White Paper by Juniper Networks"(2006), May, 1-13.

[5] Pathan, A. Hassan and M. Irshad,"IP Based Virtual Private Network Implementation on Financial Institution and Banking System", (2014) pp. 30-34.

[6] J. Scarpati, IPsec vs SSL VPNs Understanding the Basics (http://searchnetworking.techtarget.com/feature/ IPsec-vs-SSL-VPNs-Understanding-th-basics), 2014

[7] A. Sastry, IPsec VPN vs. SSL VPN: comparing respective VPN security risks (http://searchsecurity.tech target.com/tip/IPsec-VPN-vs-SSL-VPN-Comparing-respective-VPN-security-risks), 2011

[8] K.V.Besien "Implementation of a VPN Network" Master Thesis, University of La Rochelle. (2006)

[9] I. Akbar and K. Shahzad "Security in Private Branch IP-Telephony Network with QoS Demands" Master Thesis, Halmstad University. (2009)

[10] The Government of the Hongkong Special Administrative Region, "VPN Security". (2008)

[11] White Paper "Virtual Private Networks: Improving Network Security for a diverse user community". (http://www.pdfio.net/k-7234709.html).

[12] L. Phifer, Tunnel Vission : Choosing a VPN-SSL VPN vs IPsec VPN. (http://searchsecurity.techtarget.com/feature/Tunnel-Vision-Choosing-a-VPN-SSL-VPN-vs-IP sec-VPN). 2003

[13] Gupta, OP, Rani Sita, "Accelerating Molecular Sequence Analysis using Distributed Computing Environment" International Journal of Scientific & Engineering Research – IJSER, Oct 2013. ISSN 2229-5518