Volume 2, Issue 10, October 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Virtual Private Network

Ritika kajal
Software Engineering
I T M University
Sector 23-A, Gurgaon

Deepshikha Saini
Computer Science Engineering
I T M University
Sector 23-A, Gurgaon

Kusum Grewal
Astt. Prof. Dept. of ECE
I T M University
Sector 23-A, Gurgaon

Abstract - Virtual Private Network (VPN) is rapidly growing technology which plays a great role in Wireless LAN (WLAN) by providing secure data transmission. The purpose of VPN is to provide safe and secure communication by creating virtual tunnels between pair of hosts, once tunnel is created data transfer can take place. This paper presents a comprehensive study of VPN- IPSec and SSL VPN, architecture and protocols used . The salient of this paper to present comparison analysis of both technologies IPSec and SSL VPN together with their advantages and disadvantages.

Keywords – Virtual Private Network, Authentication Header, Encapsulating Payload, Secure Socket Layer

I. INTRODUCTION

A VPN is a private network that uses a public infrastructure (usually the Internet) to connect remote sites or users. The VPN as the name suggest uses “virtual “connections routed through the Internet from the business's private network to the remote site or remote employee. It is a new technology which can be applied to LAN as well as to WLAN.

A VPN maintains privacy of data through security procedures and tunneling protocols. In effect, data is encrypted at sender’s side and forwarded via "tunnel” which is then decrypted at receiver‘s side. An additional layer of security can be added by encrypting not only the data, but also the originating and receiving network addresses.

Two VPN technologies that are being used are:

Site-to-site VPN - A site-to-site VPN allows multiple offices in fixed locations to establish secure connections with each other over a public network such as the Internet. It also provides extensibility to resources by making them available to employees at other locations.

Remote Access VPN - A remote-access VPN allows individual users to establish secure connections with a remote computer network. These users can access the secure resources on that network as if they were directly plugged in to the network's servers.

Features in VPN

- Provide extended connections across multiple geographic locations without using a leased line.
- Improved security mechanism for data by using encryption techniques.
- Provides flexibility for remote offices and employees to use the business intranet over an existing Internet connection as if they're directly connected to the network
- Saves time and expense for employees who commute from virtual workplaces
- VPN is preferred over leased line since leases are expensive, and as the distance between offices increases, the cost of leased line increase.
- IPSec VPN and SSL VPN are two solutions of VPN which are widely used in WLAN. We will discuss both of them together with their advantages and disadvantages.

II. IPSec VPN

IPSec is a protocol used for securing traffic on IP networks, including the Internet. IPSec is used to encrypt data between two devices that include router to router, firewall to router etc. It operates at Internet Layer of the Internet Protocol Suite.

A. This section will focus on three primary components

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Key Exchange (IKE) protocols.

A.1 Authentication Header (AH)

The IP Authentication Header (AH) is used to provide

- Connectionless integrity
- Data origin authentication for IP data grams.
- Anti-replay protection, which protects against unauthorized retransmission of packets.

But one problem with AH is that it does not provide confidentiality, which means it does not encrypt the data. So the data is readable and protected from modification.
AH can be used in two modes**:** transport and tunnel mode. In tunnel mode, AH creates new IP header for each packet while in transport mode no new header is created.

Integrity and authentication are provided by the placement of the AH header between the IP header and the transport (layer 4) protocol header, which is shown as:

Original IP	AH Header	Layer 4 Header	Application Data

Fig 1. AH HEADER

AH may be applied alone or in combination with the IP Encapsulating Security Payload (ESP). ESP when used with AH provides same anti-replay and integrity services with add on service of data confidentiality.

A.2 Encapsulating Security Payload (ESP)

ESP is the second core security protocol which provides authentication, integrity, and confidentiality which protects against data tampering and most importantly, provides message content protection. ESP also provides all encryption services. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption/decryption allows only the sender and the authorized receiver to read the data.
Like AH, ESP can also be used in two modes: transport and tunnel. In tunnel mode, ESP creates a new IP header for each packet. This mode encrypts and protects the integrity of both IP header and data. While in transport mode no new IP header is created so ESP can only encrypt and protect the integrity of the data.
ESP header is placed prior to the transport layer header (TCP or UDP) or the IP payload data for other IP protocol types.

IP Header	ESP Header	Layer 4 Header	Application Data	ESP Trailer	ESP Authentication

Fig.2 ESP HEADER

A.3 Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is the protocol used to set up a security association (SA) in the IPSec protocol suite and to exchange keys between parties transferring data. Before secured data can be exchanged, a security agreement between the two computers must be established. In this security agreement, called as security association (SA), both agree on how to exchange and protect information. To build this agreement between the two computers, the IETF has established a standard method of security association and key exchange resolution named Internet Key Exchange (IKE) which

- Centralizes security association management, reducing connection time.
- Generates and manages shared, secret keys that are used to secure the information.
- Using keys ensures that only the sender and receiver of a message can access it.

B. How IPSec VPN Works

When IPSec VPN is used, a virtual "tunnel" connecting the two endpoints is created. Configure which packets are sensitive. Once configured, an IPSec peer sends the packet through the tunnel to the remote peer. The traffic within the VPN tunnel is encrypted so that other users of the public Internet can not readily view intercepted communications. When connected on an IPSec VPN the client computer is "virtually" a full member of the corporate network that is, it is able to see and potentially access the entire network.

C. Advantages of IPSec VPN

- IPSec provides data confidentiality services to ensure that it is not illegal eavesdropping by users in the transmission

- It provides data authentication and integrity services. The authentication data of AH and ESP is derived from HMAC. Authentication ensures that data is being sent from only authorized users.
- IPSec VPN provides data encryption from 'end-to-end' in a virtual network.
- The greatest advantage of IPSec is its transparency to applications. Since IPSec operates at Layer 3, it has essentially no impact on the higher network layer.

D. Disadvantages of IPSec VPN

- To establish a secure connection using IPSec VPN, a VPN Client is needed to be configured and installed on every terminal for data transmission.
- Installation and management of VPN client on every machine leads to expenditure which consequently increases with growing number of mobile users.
- IPSec VPN operation requires specialized training because of the software and hardware client installed.

III. SSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPSec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's Computer. It is used to give remote users with access to Web Applications, client/server applications and internal network connections.
SSL protocols include handshaking Protocol, record and alert Protocol where

Handshaking Protocol: Is responsible for determining the conversation encryption parameters between client and server.
Record Protocol: Is responsible for exchanging the applied data.
Alert Protocol: Is responsible for terminating the conversation between hosts when an error occurred.

A. How SSL VPN Works

An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor. To understand the working of SSL VPN let us look at the figure.

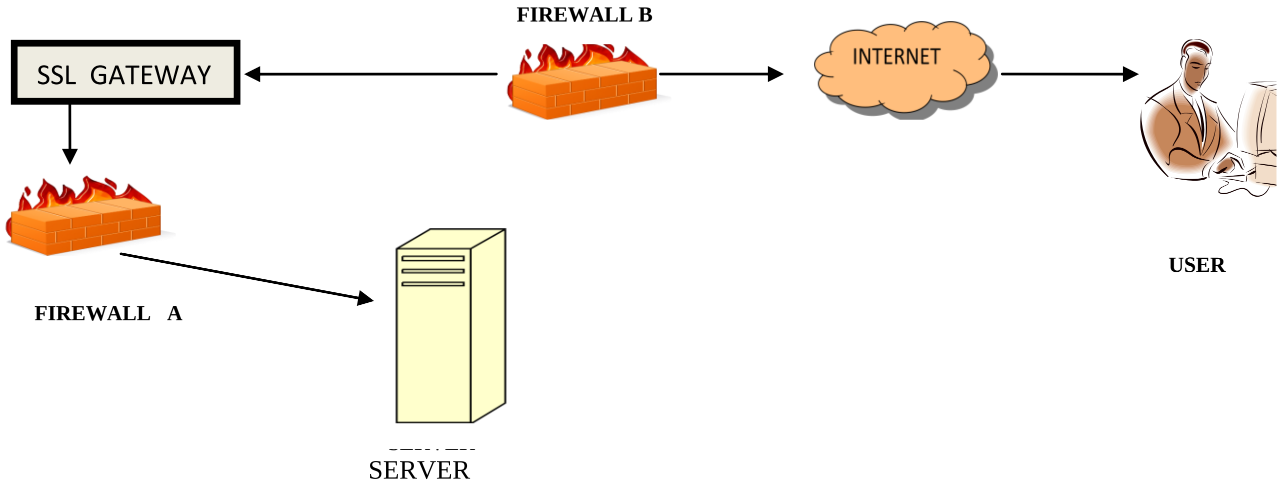

Fig 3 SSL ARCHITECTURE

Figure 3. Shows an SSL VPN gateway of Company through which all the VPN connections will be accepted and which in turn initiate connections to the internal application servers. Firewall-A protects the internal application servers and it allows connections only from SSL VPN gateway. Firewall-B is the outside firewall and it allow any internet machine to Connect to SSL VPN Gateway. So whenever any user wants to connect to its company he will first connect to its gateway. Upon successful authentication, the gateway provides the list of applications, which the user of the company need to access. At the same time, gateway initiates connection to internal application server through firewall-A. SSL VPN gateway encapsulates the response received from application server and sends it to the user. Thus, the SSL VPN

tunnel gets established between SSL VPN gateway and user's machine. The key point here is that the SSL tunnel exists only up to the SSL VPN gateway and not up to Application Server.

B. Advantages of SSL VPN

- SSL is supported by all modern Web browsers and many other programs, such as Email clients.
- There is no need to buy or configure separate client software as used in IPSec VPN thus saving cost.
- Given the universality of web browsers, SSL remote access is extremely mobile in nature. Users can access the corporate network from any web browser whether at customer site, in an airport or at a conference.

C. Disadvantages of SSL VPN

- SSL's primary disadvantage is that it operates at application layer, limiting access to only those resources that are browser- accessible.
- Requires Java or ActiveX downloads to facilitate access to non-Web-enabled applications.
- SSL tunneling is not supported on Linux or non Windows operating systems.

IV. COMPARISON OF BOTH TECHNOLOGIES

COMPONENT	SSL VPN	IPSEC VPN
CONNECTIVITY	Remote access	Site-to-site, remote access
ACCESSIBILITY	Can be accessed from any where at any time	Applies only to have well defined secure access
INSTALLATION	No installation of client VPN	Requires installation of client VPN
COMPLEXITY	Less complex	More complex
TRAINING OF USERS	No specialized training required	Require specialized training
COST	Less cost	High cost
ENCRYPTION	Strong but variable	Strong and consistent
APPLICATION TYPE	Mobile user, Partner Extranet	Remote user, Branch office
LAYER IT WORKS ON	Application Layer	Network Layer
Remote Network	Managed or Unmanaged	Managed and Trusted

TABLE I. TECHNOLOGY COMPARISON

V. CONCLUSION

This paper explains IPSec and SSL VPN together with their protocols. Both technologies are emerging out as a popular trend in WLAN as they provide better data confidentiality services. Based on the requirement and need an enterprise can choose any of them. Combination of advantages of both technologies giver more effective and secure communication.

ACKNOWLEDGMENT

We would like to give our sincere gratitude to our guide Ms. Kusum Grewal who guided us to pursue this topic and helped us to complete this topic. We would also like to thank her for providing us remarkable suggestions and constant encouragement. I deem it my privilege to have carried out my research work under her guidance.

REFERENCES

[1] Weili Huang and Fanzheng Kong. The research of VPN over WLAN.

[2] CarIton R．Davis．The security implementation of IPSec VPN [M]．

[3] Baohong He, Tianhui. Technology of IPSec VPN [M]. Beijing: Posts & Telecom press, 2008, 7.

[4] NetGear VPN Basics (www.documentation.netgear.com/reference/esp/vpn/ VPNBasics-3-05.html)

[5]National Institute of Standards and Technology: Guide to IPSec VPNs (www.http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf)

[6] SSL IPSec over SSL (www.vpntechnology.com/ipsec_or_ssl.htm)

[7] CISCO VPN and VPN technologies (www.ciscopress.com/articles/article.asp?p=24833&seqNum=6)

[8] Wikipedia (www.en.wikipedia.org/wiki/IPsec)

[9] SSL VPN Security (www.josephsteinberg.com/Docs/SSL_VPN.pdf)

[10] CISCO SSL VPN (http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html)

[11]VPN's: IPSec vs. SSL (http://netsecurity.about.com/cs/generalsecurity/a/aa111703.htm)

[12] IPSec and SSL decision Criteria (http://www.cadincweb.com/wordpress/wpcontent/uploads/2010/11/Juniper-IPSec-vs-SSL-VPN.pdf)