Analysis and Comparison of major mechanisms implementing Virtual Private Networks

Anupriya Shrivastava[1], M A Rizvi[2]

[1] Department of computer engineering and application, NITTTR, Bhopal, India
[2] Department of computer engineering and application, NITTTR, Bhopal, India

Abstract—***Network Security issues are now becoming important as society is moving to digital information age. For securing the vital information in internet VPN is one of the safest techniques. Virtual Private Network (VPN) is fast growing technology which plays a great role by protecting data from hackers while transmitting through networks.VPN creates a tunnel for secure communication between two end systems.OSI models provides different VPN protocols in each layer for securing the communication through public network. In this paper, an attempt has been made to critically analyze different VPN protocols PPTP and L2TP in data link layer, IPSec in network layer and SSL in transport layer VPN there working methodology with their advantages and disadvantages.***

Index Terms — VPN, PPTP, L2TP, IPSec, SSL, Security.

I. INTRODUCTION

A virtual private network (VPN) incorporates a private network across a public network. With the help of VPN we can communicate between two systems in a public network as we are directly connected to that system in private network,

and have advantage from the functionality, management strategy and security of the private networks. Connection between two end points can be done by dedicated connections, or encryption techniques or combination of two Works for VPN. To access the private network VPN connections uses internet connection to connect two endpoints systems is same as WLAN between the different sites. For user it's same as they are using their private network resource directly.

A. Classification of VPN

1. Secure tunneling of private network traffic through public domain.

2. Location of end point e.g. customer acting as the terminating end or network-provider.

3. Division on the basis of connectivity like remote access, site-to-site etc.

4. The kind and strength of security needed.

5. The layer of OSI model at which the protocol works.

II.REQUISITE OF VIRTUAL PRIVATE NETWORK

Following are the main reasons for using Virtual Private Network technology in a public network: -

1. To protect your information from hackers and identity thieves-Technology like computers become more important into people's daily lives, people use it to save their important information's. Unfortunately online data have many security threats. So best way to protect your data form hackers is a technology named VPN it is the most effective way to keep your data saves from outside world as it makes secure network.

2. To hide your IP address for total anonymity-Many internet users does not have knowledge that IP address

ISSN: 2278 – 1323

provided to their technologies computers laptops, mobile devices keep all the internet tracks their traffic, by this IP address lot of information's on persons computer can be easily hacked or tampered. So VPN is the best solution for this kind of problems, VPN hides the original IP Address, and provide a virtual IP.

3. To bypass Internet censorship restrictions-In some of the countries there is some security like firewall for a reason that other countries resident cannot access there any networks or they cannot share, hear, with them. But in today's life is not possible to stick to one place, for personal for professional we have to move so for that we want to uses VPN services because in VPN we are tunneling our private network over public medium, accessing work related data only so countries security can also be maintained.

4. To be able to use Wi-Fi hotspots securely-Wi-Fi hotspots have become an adaptable part of our lives. This technology helps to connect to an internet even in most of the unlikely place. But every technology has some good and bad in it, in the case of Wi-Fi, privacy is the biggest problem in Wi-Fi connections. So VPN is the best solution for securing these connections and make internet. Access via Wi-Fi total secure and confidentiality of our personal information is also maintained .VPN just performs an encryption and firewalled links for Wi-Fi hotspots.

Fig. 1 show how a remote client can connect to his head office through internet using VPN for secure connectivity. By adding a VPN technology, an organization can extend all its intranet's resources to employees working from remote offices or their homes, by using tunneling mechanism between VPN client and VPN server.

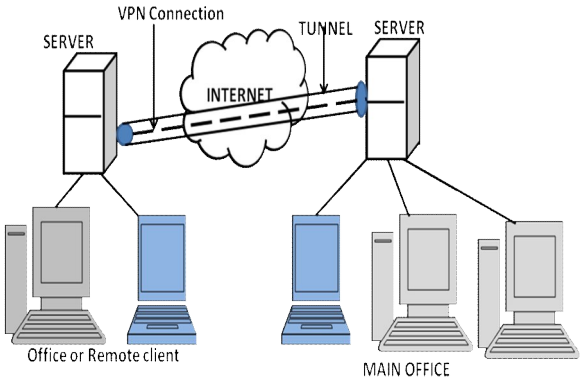


Fig.1. Remote access VPN

III. PROTOCOLS IN VPN

When we think about a secure connection we think about VPN. Virtual private networking helps us to access our records/files on our specific network through a remote location; that's why this technology is now a day's become necessary among various companies.

Once we have decided to use the VPN services then we have to decide which of the protocols in VPN we have to select. So List of protocols that are widely used Point to point tunneling protocol **(**PPTP), Layer2Tunneling protocol (L2TP), Internet protocol security (IPSec), Secure socket layer (SSL).

IV. POINT TO POINT TUNNELING PROTOCOL

PPTP is very simple lightweight VPN protocol based on PPP that provide online security with average speed. PPTP was created my Microsoft with it other technology companies are also associated .On Microsoft windows platform PPTP is the first VPN protocol that was supported and it was the mostly supported VPN technique for window users too. All the versions of Microsoft windows and most of the operating system such as (Mac, Linux) and OS for mobiles such as (IOS and ANDRIOD OS) have in built support for PPTP.

A. PPTP working

For data communication from sender to its destination IP packets are send, inside this IP Packets, PPP packets are present and inside that PPP packet PPTP stores data. PPTP can encrypt and compressed the data of those packets. PPTP

ISSN: 2278 – 1323

uses General Routing Encapsulation (GRE) to acquire send/receive data. Today's widely used VPN are PPTP VPN.

B. Steps for connections

1. The PPTP client/user connects to their VPN server using any of the networking devices that Support PPTP

2. Now TCP control connection is made from Client to server by PPTP to establish a virtual tunnel PPTP, for this entire process TCP port 1723 is used, as the tunneling is provided, PPTP will then work on this things:

For managing and mapping the VPN connection CONTROL is used and for frames which are sent and received from client and server for that DATA is used. For authenticating PPTP uses PAP CHAP and EAP protocols, and for authenticating users and for encrypting and maintaining the connections PPTP uses PPP. PPTP controls the VPN tunnel and data present in that tunnel also. PPTP also does more of the security for VPN data then PPP.

C. Advantage

1. PPTP provides inbuilt supports by default if we are operating computers with Microsoft's Windows.

2. With very basic knowledge of networking us can do it by our self, as it provide ease to user and for its setup too.

3. It provides data encryption without IPSec, which means need of installing computer certificates or a Public Key Infrastructure (PKI) is not at all needed by PPTP. So for PPTP we will not feel a lot of trouble for installing required software's and make it run with ease.

4. The forth hefty benefit of using PPTP is the fact it is very cheap compare to some of the other VPN protocols, because of two reasons first it is easy to install and second we don't have to spend lot of money to run the certificates.

D. Disadvantage

1. PPTP has Weak security compared to some other protocols.

2. It does not provide functionality data integrity and data origin verification. So we are not sure about the data sent over this protocol is correct or altered. So it is not so reliable, especially for the case of sensitive information.

3. It has low performance for unstable networks.

V. LAYER 2 TUNNELING PROTOCOL

L2TP is an advance VPN protocol. L2TP is an adjunct of PPTP used by ISP for VPN. L2TP have two main components

1. L2TP Access concentrator (LAC) this device is used to terminate call physically

2. The L2TP Network Server (LNS), this device is to terminates and to authenticate PPP streams

A. L2TP Working

The L2TP begins a tunnel between an LAC and LNS on the network to permit a Point-to-Point Protocol (PPP) link layer to be encapsulated and then carried across the internet. Here end users begin a PPP connection to as ISP, after this, the LAC accepts the connection and establishes a PPP link, during this time ISP performs partial authentication to get username, this user information helps to access the network now the connection request is send to LNS which can accept or reject the connection based on user information by using final authentication of the connection. Now if connection is accepted, a virtual PPP interfaces is a virtual PPP interface is generated and link layer frames can be passed over the tunnel. After these LNS accepts frames from the connection which is formed and then strips off the L2TP encapsulation and processes them as usual incoming frames.

B. Advantage

1. It provides high data security for censorious application.

2 It provides high level of encryption for sensitive information.

ISSN: 2278 – 1323

3 It provides efficient and best connectivity for both remote and direct access network.

4 It does not provide any overhead cost as it is implemented, it's really as cost effective protocol.

5 It is really a authentic, fast, flexible scalable and reliable

6 For VPN authentication it provides best authorization policy for users.

C. Disadvantage-

1. L2TP with some of the firewalls encapsulated the information twice so mostly it affects the speed of transmission of data.

2. For L2TP many configuration including computer certificates have to be done. For person with basic networking knowledge is may be a tough job.

3. Most of the time L2TP fail because of mismatch of security keys, because pre-shared key is used by L2TP,

4. So if key is changed ,it must be changed at both end of VPN tunnel.L2TP will not work with NAT without a NAT-T client and NAT-T VPN

5. IN encryption process by L2TP it have higher usage of CPU, it causes speed to slow down.

VI. INTERNET PROTOCOL SECURITY

IPSec is VPN protocol for implementing VPN for securing traffic over internet and for users at remote location to access to their private network through dial up connection. IPSec uses cryptography technique for security proposes over IP networks.

IN IPSec we have three options for security:

A. Authentication header-

1. It helps for authentication purpose for data origin system means to authenticate sender of data.

2. It is used to protect IP packets from unauthorized retransmission.

3. It is used for connectionless integrity

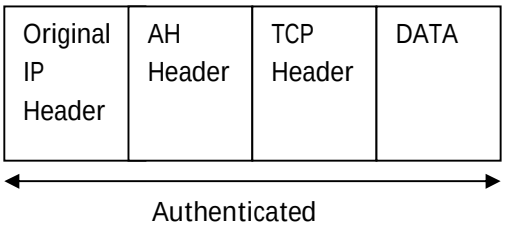
But there is one problem with AH does not encrypt the information, so here confidentiality of data cannot be maintained. As AH is used in two modes,

TRANSPORT MODE-It does not create every time a new IP address for each packet

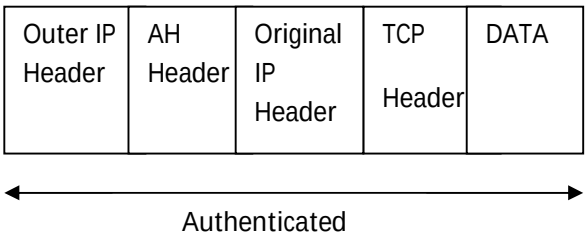
TUNNEL MODE-It provides each packet a new IP address.

So in a message format to main integrity and authentication of packets is done by placing AH between original IP and protocol header.

IPSec transport mode: After applying AH



IPSec tunnel mode: After applying AH



B. Encapsulating Security Payload (ESP)-

Encapsulating Security Payload (ESP), it is used as to authenticate the sender and for encryption of information and all encryption service and to maintain integrity,

ISSN: 2278 – 1323

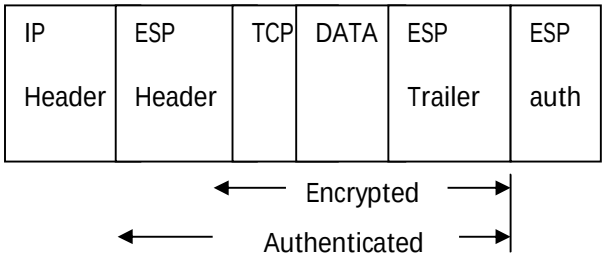
confidentiality. So with the help so encryption we can hide the original content of messages and forward in some encrypted format and at destination with the help o decryption technique we can decrypt the data, can obtain original message.ESP can also be used in two modes:

TRANPARENT MODE- this mode is only used for encrypting and protecting the data only because no IP header is created here.

TUNNEL MODE-In this new IP header each created for each packet. Function provided by this mode is to provide encryption and to protect the integrity of both IP header and data.

Original packet:

Packet with IPSec encapsulating security payload:



C. Internet Key Exchange (IKE)

It is a protocol used in an IP sec protocol suite to set up a security association and used between systems that transfer data, to exchange the keys. Firstly agreement for security is established between the two systems then data are exchanged in IKE.IETF for security association and key change between systems established a standard named Internet Key Exchange (IKE).so IKE for reducing the connection time uses Centralizes security association management .secrets keys that are used to secure the data are generated and manage.

D. IPSec Working

In IPSec VPN a virtual tunnel is made between two end systems. Then configure it. Once configured, IPSec sends data packets to its remote system using virtual tunnel, and data are encrypted to rescue from public networks. And as connection is done via VPN remote client can access company internal network.

E. Advantages

1. IPSec is easier to maintain and it is more secure, this makes it as international standard.
2. It have added layer of security.
3. IPSec uses a technology that is completely invisible and its operation never has to be learned by its users
4. Functionality of IPSec to monitors all the traffic that has been passed from the network, inbound as well as outbound, is because it is based on network layer.
5. In IPSec there is no compatibility issues as whole security is implemented at the network layer

F. Disadvantages

1. In IPSec there are hundreds of megabytes data flowing for encryption and decryption in machines it requires more processing power that's why it have CPU overhead.
2. Different software developers may have their different standards so sometimes there may some compatibility issues with IPSec.
3. There is a huge security risk as some of the security algorithm that are been used by IPSec are cracked.

VII. SECURE SOCKET LAYER

An SSL is a form of VPN that can be used with a standard Web browser. In SSL we don't need to install client software on client systems as in IPSec. Web application can be accessed by SSL .It give user at remote location client/server application and internal network. SSL protocols include handshaking Protocol, alert record protocols-

Handshaking Protocol is responsible for deciding the encryption parameters between client and server. This is done by sending CLIENT-HELLO message.

Alert Protocol When error is occurred it is used to terminate the conversation between hosts

Record Protocol is responsible for swapping the data which is applied.

ISSN: 2278 – 1323

A. SSL Working

There are one or more devices in SSL through which users connect through web browsers. With the help of SSL protocols the traffic between SSL VPN device and web browser is encrypted.

1: A connection is established to a website or domain such as abc.com, on a specific port, by the customer. In case of port 443, https is the connection type rather than http.

2: abc.com reverts back to the customer with a key known as public key. Once customer receives it, his/her browser decides if it is alright to proceed.

- The lifetime of public key obtained from abc.com must not be over.
- The public key provided by abc.com should only work for that domain.
- In order to establish the authenticity of public key, user must have such a tool installed in his/her browser that can verify the key.

3: In case a trust is established, customer will send his/her public key to the domain.

4: Next, the domain needs to encrypt a distinct hash created by it using a combination of its own private key and the public key provided by the customer. Once done, it has to be returned back to the client.

5: The hash received by the customer can now be decrypted by its browser. This should only be possible for the user with whom the trust has been established.

6: We can now have a secure transfer of data between the two entities.

B. Advantage

1. SSL is essential as we deal online to keep safe our information
2. In SSL it is not needed to configure purchase client software as we do for IPSec, so it is cost effective.
3. All modern browsers and other programs too like email clients support SSL.

C. Disadvantages

1. Tunneling in SSL is not supported in non window operating systems like LINUX.
2. To access the non web enable application JAVA or ActiveX is needed.
3. Through SSL we can access only those resources that are browsers accessible.

Table 1: Comparison table of different VPN protocols

VPN Protocols	**PPTP**	**L2TP**	**IPSec**	**SSL**
Approachability	Remote access	Remote access	Remote access	Site to site, Remote access
Application type	Remote user, Branch office	Remote user, Branch office	Remote user, Branch office	Mobile user, Partner Extranet
Complexity	Simplest	Simpler	More complex	Less complex
Confidentiality	Yes	Yes	Yes	Yes
Cost	Low	Low	High	Low
Encryption	Average	Average	Strong and consistent	Strong but Variable
Encryption strength	128 Bit MPPE	256 Bit AES	256 Bit AES	
Integrity	No	Yes	Yes	Yes

ISSN: 2278 – 1323

Ports	Open TCP 1723	Open UDP 1701	Open UDP 500 and 4500	Open TCP 443
Remote network	Managed and trusted	Managed and trusted	Managed and trusted	Managed or unmanaged
Supported layer	Data link layer	Data link layer	Network layer	Transport layer
Speed	Fast as there is lower encryption	Fastest speed	Greater processing speed is required	Low speed then IPSec because of higher overhead
Security	Average	Good	Good	Good
Terminal authentication	No	IPSec ESP Computer Certificates	Md-5,IKE with pre shared key or digital certificates	Digital certificates HTTP authentication
Guidance to user	Simple guidance	Simple guidance	Expert guidance	Not required
User authentication	PAP, CHAP, for mutual authentication digital certificates	PAP,CHAP for mutual authentication pre shared key	Digital certificates, for mutual authentication secret passwords	Digital certificates

After analyzing Table I, it can be summarized that technology characteristics of the four different VPN protocols including their authentication, security and each protocols working methodology with their pros and cons. PPTP is simpler protocol with low cost and faster speed but its security is average, while L2TP speed as well as security is good. IPSec and SSL are mostly preferred VPN protocols as SSL provide good security and high processing speed but in all IPSec protocol is best in terms of processing speed and security but its cost to high. So according to requirement of people can choose the VPN protocols as per their need and sensitivity of data and cost available, because no one protocols can be suggested as per the analysis done.

VIII.CONCLUSION

The VPN technology is being used almost two decades old now, and is still in development phase. Different protocols are used for establishing VPN connection. This paper brings forth the analysis and comparison of the prominent VPN technologies such as SSL, IPSec, PPTP and L2TP. Organization can choose the protocol according to their security requirement and business model. Because of the confidentiality provided by these protocols, they are also gaining significance in WLAN technologies. It can be seen that different VPN protocols have different strengths. So we need to make a trade-off among the features that are required. In some cases, the user may even go for a combination such as L2TP over IPSec.

REFERENCES

[1] Weili Huang and Fanzheng Kong, "The research of VPN over WLAN".
[2] A. Passito. ,"Evaluating Voice Speech Quality in 802.11b Networks with VPN/IPSe", Proceedings of the XIII IEEE international Conference on Networks, 2005.
[3] CarIton R.Davis,"The security implementation of IPSec VPN [M]".

ISSN: 2278 – 1323

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

[5][Online]Available:http://www.ciscopress.com/articles/article.asp?p=24833 &seqNum=6.

[6][Online]Available:http://www.josephsteinberg.com/Docs/SSL_VPN.pdf.

[7][Online]Available:http://netsecurity.about.com/cs/generalsecurity/a/aa111703.htm.

[8][Online]Available:http://www.cadincweb.com/wordpress/wpcontent/uploads/2010/11/Juniper- IPSec-vs-SSL-VPN.pdf.

[9] [Online]Available:http://www.giganews.com/vyprvpn/compare-vpn-protocols.html.

[10][Online]Available:http://www.steveneppler.com/blog/2005/12/07/pptp-and-l2tp-ports.

[11] Ritika kajal, Deepshikha Saini, Kus,m Grewal, "Virtual Private Network", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[12] Wafaa Bou Diab, Samir Tohme, Carole Bassil, "VPN Analysis and New Perspective for Securing Voice over VPN Networks", Fourth International Conference on Networking and Services, 0-7695-3094-X/08 $25.00 © 2008 IEEE.

[13] S. Huang, Z. Liu, and J. Chen," SIP-Based Mobile VPN for Real-Time Applications", Hsinchu, Taiwan 2005.

[14] M. Saarinen,"Legacy User Authentication with IPSEC", Helsinki, Finland, Feb 2004.

[15][Online]Available:http://www.csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf.

[16][Online]Available:http://www.documentation.netgear.com/reference/esp/vpn/ VPNBasics-3-05.html.

ISSN: 2278 – 1323