VIRTUAL PRIVATE NETWORK TECHNOLOGY BASED ON MULTI-PROTOCOL LABEL SWITCHING

J.Revathi
Assistant Professor Department of Computer Science & Applications,
Vivekanandha College of Arts and Sciences for Women (Autonomous), Namakkal, Tamil Nadu, India

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 the pair of hosts; once the 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. The VPN technology based on MPLS is the current mainstream VPN technology that uses isolations of routing and address or other information technologies to resist attacking and marking spoofing, in which the security of data transmission is guaranteed to a certain extent. Inthis paper, Securities of MPLS VPN are analyzed in three levels, in which the overall securities of MPLS VPN network are enhanced by deploying the appropriate security measures.

Keywords: *VPN, MPLS, Network Security, IPsec, SSL.*

Introduction

A **Virtual Private Network** (**VPN**) extends a private network across a public network, such as the Internet. It enables a computer or Wi-Fi-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions.

A VPN connection across the Internet is similar to a wide area network (WAN) link between websites. From a user perspective, the extended network resources are accessed in the same way as resources available within the private network.

VPNs allow employees to securely access their company's intranet while traveling outside the office. Similarly, VPNs securely connected geographically separated offices of an organization, creating one cohesive network. VPN technology is also used by individual Internet users to secure their wireless transactions, to circumvent geo-restrictions and censorship, and to connect to proxy servers for the purpose of protecting personal identity and location.

A Virtual Private Network (VPN) is a private network that uses a public infrastructure (usually the Internet) to connect remote sites or users. The VPN as the name suggests 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.

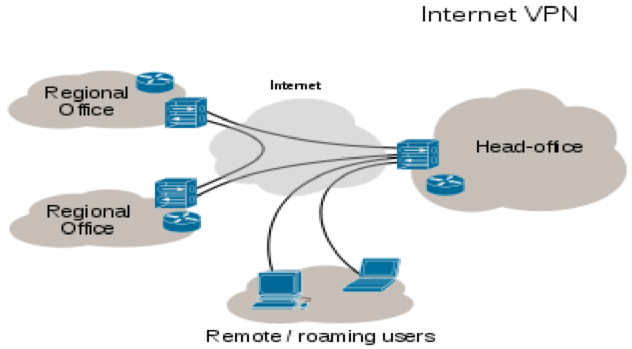


Fig. 1: VPN Connectivity Overview

With the development of computer network technology and internet, it is increasing that requirements of the flexibility and efficiency and security in network, virtual private network (VPN) technology was widespread concerned. The VPN technology Based on MPLS is the current mainstream VPN technology that uses isolations of routing and address or other information technologies to resist attacking and marking spoofing, in which the security of data transmission is guaranteed to a certain extent. But as an IP-based network technology, it is not solving illegal access of a protected the network element and the error configuration as well as internal attacks and other security issues which widespread in the management of the shared network.

A VPN maintains privacy of data through security procedures and tunneling protocols. In effect, data is encrypted insender's side and forwarded via "tunnel" which is then decrypted at receivers 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 into 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.

MPLS VPN Technology

Multi-Protocol Label Switching(MPLS) is a new network technology for booting high-speed data transmission and exchange by utilizing fixed-length label in open communication network[1]. It is powerful to overcome packet forwarding technology limitations of the traditional IP for the performance characteristics of a perfect combination of flexible routing functionality in the network layer (Layer 3) and the high-speed switching data in link layer (Layer 2).The key to MPLS technology is Label concept which is short and easy-to-handle and only has a local significance of information content. The Label is short for easy-to-handle which is directly referenced by index. A Local significance is designed for easy distribution. The value of MPLS is that connected modes are introduced into connectionless network.

MPLS VPN is a kind of VPN technology Based on MPLS of IP-VPN which is IP virtual private network for using the application of the MPLS technology and simplifying core router's routing on equipment's of network routing and switching, the label swapping combining traditional routing technology [2]. Multilevel mesh network structure is generally used in MPLS VPN. It is consist of several different sites collection in VPN which a site can belong to different VPN and sites can be controlled for visits and isolation. Network framework of MPLS VPN is shown in figure 1.

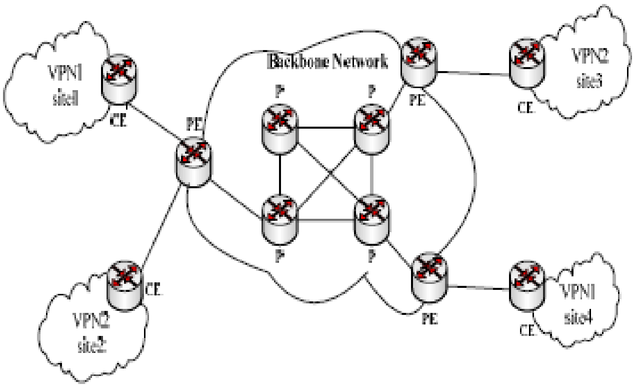


Fig. 2: Network Framework of MPLS VPN

The architecture of MPLS VPN consists of three components: CE, PE and P[4].

- ***Customer Edge (CE):*** the user interface. There are edge devices directly with the service provider network. CE can be either a router or a switch or a host. Typically, CE "perception" does not exist VPN, also not need to support MPLS.
- ***Provide Edge (PE):*** the service provider of edge router, which is directly connected with the user's CE. All managements of the VPN occur on PE, which the VPN routing information are maintained that is directly connected to, while all other VPN routing do not need to.

- *Provide (P):* the backbone routers of service provider in the network not directly connected with CE, which have MPLS forwarding capabilities.

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.

This section will focus on three primary components

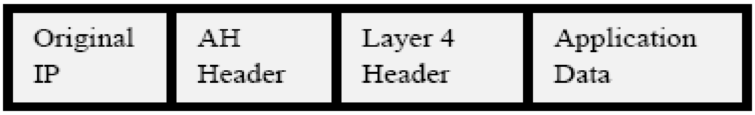
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Key Exchange (IKE) protocols.

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:

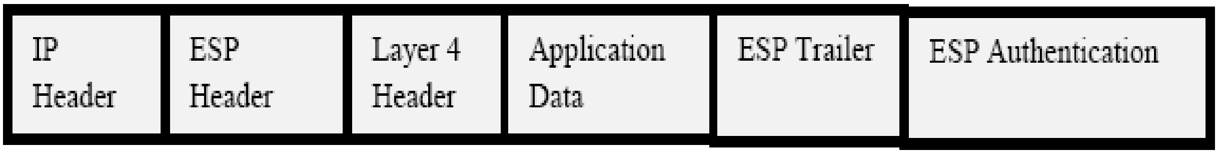


Original IP	AH Header	Layer 4 Header	Application Data

Fig. 3: AH Header

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.



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

Fig. 4: ESP Header

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. 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.

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.

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.

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 lead 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.

The Security of MPLS VPN

The transfer and processing of information are divided into control, data, and manage three levels in MPLS VPN network. In the control plane, the exchange and processing of routing information are completed and VPN routing tables are established and maintained. In the data plane, implementation of VPN data is fast forwarded. Configuration of the equipment is completed and appropriate management information is delivery in the management plane. The security threats of MPLS VPN network also come from these three levels.

The security threats of the control plane

- The attacking to VPN routing protocol

This kind of attack is typically found in members and routing information publication stage. For example, the attacker pretends as a PE equipment to establish a session with other equipment for the routing information. The internal routing information of VPN is disclosed. The attacker can also be forged or altered routing information so that the user data are passed to the wrong direction and user internal information are theft.

- The attacking to P/PE router

Usually, P/PE router is attacked for means of squeezing the resources. For example, Denial of Service Attacks affect and destroy the routing information to be sent properly, it interferes with the routing information for establishing and maintaining that impact VPN packets transmitted, the user businesses are affected ultimately.

The security threats of the data plane

- The security threats of internet

In the case of VPN users are connected with internet, attacks are launched with IP source address spoofing, TCP session hijacking and planting Trojans, in which the user data streams are viewed, modified and deleted on-authorized.

- The security threats of the shared device

In the MPLS VPN network, it is shared of network resources by normal VPN users, such as CE and PE equipment. In this case, although the VPN tunnel system can guarantee the security of information delivery to a certain extent, all security measures only will increase security threshold, the possibility of an attacker illegal capture, forgery and replay the possibility of MPLS label package cannot rule out.

The security threats of the management plane

- The attacking to network devices through the administrative interface

An attacker accesses network management system remotely through the network access control management interface illegal gained using guessing. Configuration management information of the device is viewed, extracted and changed.

- Impact or damage management information delivery through clogging resource

If deliveries of resources are not through a specialized transport channel or the use of a "band" way of delivery, the management information does not normally pass for network resources are excessive extending by an attacker.

- The disclosure of internal information

The proper configuration can guarantee VPN routing information not leak for VPN is strictly isolated between address space and routing space.

The Improvements of MPLS VPN Security

The design of MPLS VPN should be sure of routing information of the control plane are accurate, reliable and guaranteed, data delivery of the data plane are privacy, accuracy and integrity, configuration information of the management is secure.

A. Control plane safety

The safe measures of control plane are mainly guaranteeing the deliverable security of the routing information and isolation of routing. The condition of PE equipment are Overburdened should be prevented for the abuse of routing information through strictly to limit the total number of routing information on the side of PE to CE. The interface address On the CE site on PE VRF should be strictly prohibited while it is not needed. These addresses are absolutely forbidden for CE site access in case of it is not required, such as the Loopback address of VPN Routing and Forwarding table (VRF).

B. Data plane safety

CE-PE data encryption

The transmission path between CE and PE is relatively safe for multiple CE devices are connected into the PE via Ethernet switches with Virtual Local Area Network (VLAN) which the transmission path is determined by the network administrator, the date are allowed to access with non-encrypted way at the case of the consideration of the business costs and simplification of the configuration. If the way of access is wireless or remote, one of the encrypted access methods is necessary.

- PE-PE data encryption

In order to guarantee the security of data transmission, Internet Protocol Security (IPsec) is deployment to authenticate or encrypt the data flow between ingress to export[5]. The transmission of information between the PE is not encryption in general. The reasons are that it has a degree of security for the technology of MPLS VPN tunnels are used to transmit information.

- CE-CE data encryption

IPsec tunnel is deployed to provide user data security in mutual communication between sites. This technology is deployed in the CE or between hosts requiring data protection in sites.

C. Management plane safety

- The access control of Network management system

The attack of hacker to network management system is primarily implemented through network management interfaces. In order to prevent the information of management thieving and malicious tampering, access authentication should be deployed at the administrative interface.

- The delivery channel of network management information

In order to prevent information of resource network management abnormal delivering for resource squeezed, management terminal should be used with out-of-band access management interface. The use of the link is isolated physically or logically with other infrastructure in VPN. If manage terminal is in-band access management interface, a filter or firewall must use to limit access to non-authorized users.

- The correctness of device configuration

Network administrators should guarantee the correctness of the VPN device configuration to prevent leakages of user data, which require improving the skillful level of administrator and increasing the moral quality of education at the same time.

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.

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.

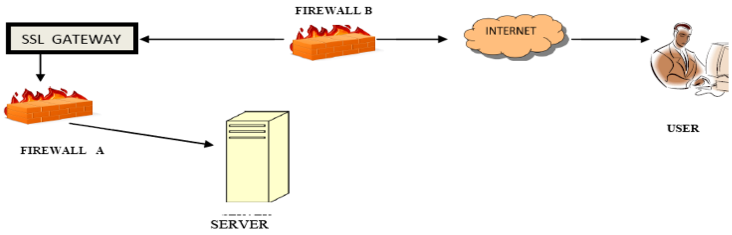


Fig. 5: SSL Architecture

Firewall-A protects the internal application servers and it allows connections only from SSL VPN gateway. Firewall-B is the outside firewall and it allows any internet machine to Connect to SSL VPN Gateway. SSL VPN gateway encapsulates the response received from the 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 An Application Server.

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.

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.

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 technologies given more effective and secure communication. As the sign of the network communication, MPLS VPN will gradually replace the traditional circuit communication and become future trends of network for the performance of its flexible, high-speed switching and routing and the high security

References

1. Ayan B, "Generalized Multi-protocol label switching: An overview of signaling enhancements and recovery techniques," IEEE Communications Magazine, vol. 39, pp.144-151, 2001.
2. Eric W. Gray, *MPLS – Implementing the Technology*, Addison Wesley,2001.
3. J. Arturo Perez, Victor Zarate, Angel Montes, Carlos Garcia, "Quality of Service Analysis of IPsec VPNs for Voice and Video Traffic,", Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT-ICIW'06), pp. 43,2006.
4. Jian C, Chin L, "A restorable MPLS-based hose-model VPN network, " Computer Networks, vol. 5l, pp. 4836-4848, 2007.
5. Jim Guichard and Ivan Pepelnjak, *MPLS and VPN Architectures*, Cisco Press, 2000.
6. K.G.Ramakrishnan, D.Mitra, and J.A.Morrison, "VPN DESIGNER:A tool for design of multiservice virtual private networks," in *Proc.8th International Telecom. Network Planning Symposium, NETWORKS*,1998, Sorrento, Italy.
7. Myoungju Y, Jongmin L, Tai-Won U, "A new mechanism for seamless mobility based on MPLS LSP in BCN,"IEICE Transactions on Communications, vol. 91, pp. 593-596, 2008.
8. Rosen E, Rekhter Y, RFC 4364 BGP/MPLS IP Virtual Private Networks(VPNs)[S], IETF, 2006.
9. Wafaa B.D., Samir T. & Carole B.,'VPN Analysis and New Perspective for Securing Voice over VPN Networks Full text' Proceedings of the Fourth International Conference on Networking and Services, pp. 73-78, 2008.
10. Yang Yanyan, Martel Charles U, Fu Zhi, Wu Shyhtsun Felix, "IPsec/VPN security policy correctness and assurance," Journal of High Speed Networks, vol. 15, pp.275-289, 2006.