Research Paper

Volume : 2 | Issue : 8 | August 2013 • ISSN No 2277 - 8179

L2TP/IPsec Interworking

Computer Science

KEYWORDS :

Sridevi Assistant Professor,Department of computer Science,Karnatak University Dharwad

ABSTRACT

L2TP does not provide strong authentication by itself, instead it often uses IPsec to secure packets by providing confidentiality, authentication and integrity. This Paper introduces why L2TP/IPSec is necessary, how L2TP and IPsec work together, and then will discuss the details of the L2TP/IPsec tunnel establishment and authentication. Finally, discuss the implementation of the L2TP/IPsec tunnel under FreeBSD (UNIX).

1. Introduction

Layer 2 Tunneling Protocol (L2TP) is one of VPN protocols. It receives packets on the OSI Layer 2 (Data Link Layer) and secures the packets inside the OSI Layer 5 (Session Layer). It does not provide strong authentication method by itself and often the L2TP packets are sent inside IPsec for a better security. Compared with current VPN technologies, a VPN that transfers Layer 2 packets has a better range of applications as it can transfer almost all kinds of Internet packets: IP packets, non-IP packets (such as IPX packets) and Layer 2 packets (such as PPP packets).

Internet Protocol Security (IPsec) is one of the VPN technologies and is a suite of protocols. It receives packets on the OSI Layer 3 (IP Layer) and secures the packets inside the IP layer. IPsec uses Internet Key Exchange (IKE) protocol to generate security keys and to handle security key exchange between the VPN server and the VPN concentrator, and uses Authentication Header (AH) or Encapsulating Security Payload (ESP) to encrypt and to protect IP packets. IPsec has strong security and it has already been integrated into the next generation network (IPv6).

2. L2TP/IPSEC TUNNEL

Although IPsec can be used as an independent secure tunnel, it cannot tunnel layer 2 packets. Tunneling layer 2 packets is necessary when several persons inside a moving vehicle are connected to a network at layer 2 and they want to connect to the company network through VPN.

L2TP is used to tunnel Layer 2 packets (usually PPP packets) over public networks. However, it does not provide strong authentication by itself. Both the control and data packets of L2TP protocol are vulnerable to attack: snooping data packets, modifying both control and data packets and launching Denial of Service (DoS) attacks by terminating PPP connections or L2TP tunnels. To address these threats, L2TP security protocols must provide authentication, integrity and reply protection for control and data packets, and confidentiality protection is desirable [4]. IPsec meets this category. IPsec provides per-packet authentication, confidentiality protection, and integrity and reply protection for network or upper layer packets. Both control and data packets of L2TP are UDP packets which can be protected by IPsec. Moreover, IPsec has demonstrated strong security features in the last years and it has already been integrated into the next generation network (IPv6). That is why IPsec is often used to secure L2TP packets. In order to protect L2TP packets (both control and data packets), they should be put inside the IPsec packets. Two protocols can be used to protect data in the IPsec protocol suite: ESP [2] and AH. Compared with ESP, AH does not provide confidentiality. In other words, attackers can easily see the content of the packets transferring over the public Internet even with AH protection. That is why ESP is usually used to protect L2TP packets.

Two modes under IPsec can be used to protect L2TP packets: transport mode and tunnel mode. The IPsec Transport mode only protect the payload of the IP packet (network layer or upper layer protocols of the packet), while tunnel mode protects the entire IP packet (both payload and IP header). In L2TP standard (RFC 3193) defined by Internet Engineering Task Force, the IPsec transport mode must be supported while the IPsec tunnel mode may be supported [4]. To simplify implementation, the IPsec tunnel mode is used in this thesis. Similar algorithms will be used in the IPsec transport mode.

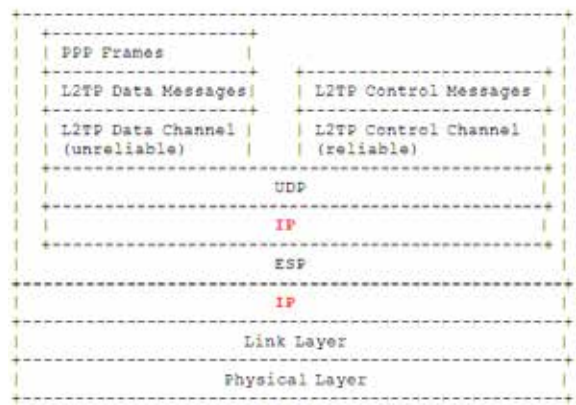

Figure 1: The packet structure of L2TP/IPsec tunnel in IPsec tunnel mode.

3. L2TP/IPSEC TUNNEL ESTABLISHMENT

As IPsec protects L2TP in an L2TP/IPsec tunnel, IPsec should be negotiated first and then L2TP. The process of setting up an L2TP/IPsec VPN is as follows:

(1) Negotiate IPsec Security Association (SA, shared security information between two network entities) [1], typically through Internet Key Exchange (IKE). Digital certificates should be issued (via Certificate Authority) before this step.
(2) Negotiate and establish L2TP tunnel with the protection of ESP.
(3) Layer 2 packets can be sent via L2TP/IPsec tunnel.

3.1 L2TP/IPSEC TUNNEL AUTHENTICATION

In general, PPP provides initial authentication, but not per-packet authentication. The authentication in L2TP is optional and is usually not used, as IPsec provides per-packet authentication. During the setup phase of an L2TP/IPsec tunnel, the authentications will be used in the sequence below:

(1) Negotiate IPsec Security Association (SA), typically through Internet Key Exchange (IKE).
(2) Do PPP initial authentication using PPP Challenge Handshake Authentication Protocol (CHAP) [5].

The setup phase is a relatively short period. The possibility of changing IP addresses in setup phase is very limited. Furthermore, there are several states during setup phase, which add complexity to mobility solutions. Also, it is hard to decide whether authentication failure is caused by changing IP addresses or some other issues. Due to the reasons above, we decided to add mobility support only in data transfer phase.

In data transfer phase (when a packet arrives at a tunnel), the following authentication will be used:

(1) Check Security Association (SA) information in IPsec according to the ESP header and the IP header.

The IPsec component fetches and checks the SA from the Security Association Database (SADB) using the destination address (end point of IPsec tunnel), protocol (ESP), and Security Parameter Index (SPI). The payload is then decrypted according to SA [3].

(2) Check the security policy of the packet by querying the Security Policy Database (SPD). The source and destination addresses in SPD will be checked and they are the addresses of end users (Point A and Point F in Figure 5). Other information will also be checked in SPD such as valid time, relevant SA information and upper layer protocols [3].

(3) Verify that the IP addresses and port values in the L2TP packet match the socket information which was used to setup the L2TP tunnel [4].

3.2 L2TP/IPSEC TUNNEL IMPLEMENTATION

An L2TP/IPsec tunnel can be easily configured under Windows. However, there is no native support for creating an L2TP/IPsec tunnel under FreeBSD. The L2TP and IPsec tunnel can be configured separately under FreeBSD, but not as a whole. This thesis will analyse the implementation of the L2TP and IPsec tunnel under FreeBSD, and will propose and compare some solutions to create an L2TP/IPsec tunnel. The topology of an L2TP, or IPsec, or L2TP/IPsec tunnel is shown in Figure 2. Point B and Point E, which usually use private IP addresses, are called internal interfaces. Point C and Point D, which usually use public IP addresses, are called external interfaces.

IPsec tunnel concentrator listens to IP packets at Point B, encapsulates and encrypts the IP packets into ESP packets and sends them through Point C. L2TP tunnel concentrator (LAC) listens to layer 2 packets at Point B, encapsulates packets into UDP packets and sends them through Point C. L2TP and IPsec concentrator listen on the same network interface. If they handle packets at the same time, only one of the concentrators (L2TP or IPsec) will eventually receive and handle the packets. Under FreeBSD, the L2TP concentrator will receive and handle packets from Point B first, as callback functions (the functions which are defined under user space but are used under the FreeBSD kernel) from L2TP will be called before IPsec functions in the ip_input( ) functions .

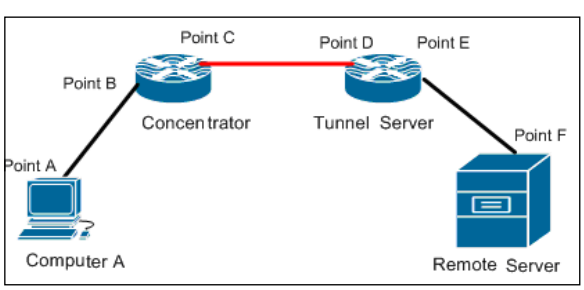

Figure 2 IPsec, or L2TP, or IPsec/L2TP Tunnel Topology

Similar things happen when tunnel servers receive tunnel packets from Point D. There is also a confliction between the L2TP tunnel server (LNS) and the IPsec tunnel server. The L2TP tunnel server will receive and handle tunnel packets first under FreeBSD. Therefore, if you simply configure L2TP and IPsec using the topology above, the whole system will work like an L2TP tunnel.

4. Upper and Lower Protocol Solution (ULP solution)

One solution [6] is to regard L2TP as an upper layer protocol and to regard IPsec as a lower layer protocol. For example, the input and output functions of TCP (upper layer protocol) are the tcp_input( ) function and the tcp_output( ) function; the input and output functions of IP (lower layer protocol) are the ip_input( ) function and the ip_output( ) function. The relationship of these functions is shown in Figure 5-8. However, this solution is not easy to implement, as each packet has to call both input and output functions of upper and lower layers. Security policy checking in IPsec is also a significant problem in this solution, as source and destination addresses are changed to the addresses of Point C and D after L2TP receives and handles a packet from Point B, and these packets will not pass the security policy checking and will not be encrypted. It would be extremely difficult to implement this solution under FreeBSD and so we rejected this solution path. However, under other platforms (such as Linux which uses Openswan [7] for IPsec and OpenL2TP [6] for L2TP), this solution is possible; as L2TP directly calls IPsec functions. IPsec and L2TP listen to the same port number in an L2TP/IPsec tunnel under that platform [6].

5. Loopback Interface Solution

The solution we have developed is to add a loopback interface to both concentrator and tunnel server. A loopback interface is a virtual network interface implemented only in software. Any traffic that sends to the loopback interface is immediately received on the same interface. Adding a new interface to concentrator and tunnel server solves the confliction, as L2TP and IPsec can listen on different network interfaces. The topology is shown in Figure3.

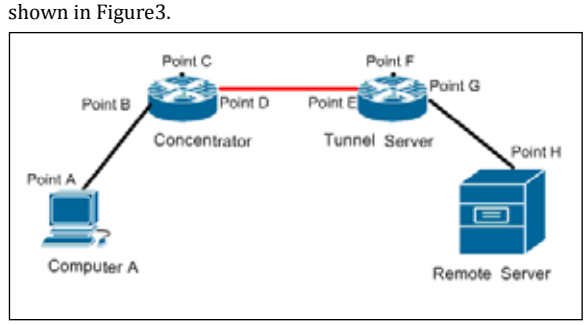

Figure 3 Loopback Interface Solution for IPsec/L2TP Tunnel

The L2TP concentrator receives a packet (source: Point A, destination: Point H) from Point B, encapsulates the packet and sends the new packet (source: Point C, destination: Point F) through Point C. The packet will go back to Point C immediately. The IPsec concentrator receives the packet from Point C, encapsulates and encrypts the packet and sends the new packet (source: Point D, destination: Point E) through Point D. The IPsec tunnel server receives the packet from Point E, decrypts and decapsulates the packet into the original packet (source: Point C, destination: Point F) and forwards the packet through Point F. The packet will go back to Point F immediately. The L2TP tunnel server receives the packet from Point F, decapsulates the packet into the original packet (source: Point A, destination: Point H) and forwards the packet to Point H. Similar algorithm is used for the returning traffic. Table 6-1 shows some configuration of the loopback interface solution.

	Concentrator		Tunnel Server	
	Internal Interface	External Interface	Internal Interface	External Interface
IPSEC	Point C	Point D	Point F	Point E
L2TP	Point B	Point C	Point G	Point F

Table 1 Configuration of Loopback Interface Solution

This solution is simple and stable, because a loopback interface provides a stable address to minimize impact of a physical interface going down. The approach taken in this solution could be used on any POSIX (a software interface to different operating systems) [8] operating system.

A routing loop [9] is a common problem with computer networks. It will cause the traffic to be forwarded into an endless

loop. It is formed when an error occurs in the operation of the routing algorithm. Loopback interfaces are similar to physical network interfaces. This loopback interface solution does not add any new routing loops to public networks. Routing loops can be avoided by correctly configuring routing protocols such as OSPF [10].

6. Conclusion

Although IPsec is a VPN protocol with strong security, it cannot tunnel layer 2 packets. L2TP tunnels layer 2 packets, but does not provide strong authentication by itself. It is often used with IPsec to provide a secure layer 2 tunnel. ESP (a part of IPsec) is usually used to protect L2TP packets. During L2TP/IPsec tunnel establishment, IPsec is negotiated first, and then PPP and L2TP. During data transfer phase, SA, SP and L2TP information will be checked. There is no native support for creating an L2TP/IPsec tunnel under FreeBSD. The L2TP and IPsec tunnel can be configured separately under FreeBSD, but not as a whole.

REFERENCE

[1] Ed. C. Kaufman, "Internet Key Exchange (IKEv2) Protocol", IETF RFC 4306, December 2005. | | [2] Errata and S. Kent, "IP Encapsulating Security Payload", IETF RFC 4303, December 2005. | | [3] N. Doraswamy and D. Harkins, "IPSec: The New Security Standard for the Internet, Intranets, and Virtual | Private Networks", Prentice Hall PTR, 2003. | | [4] B. Patel, B. Aboba, W. Dixon, G. Zorn and S. Booth, "Securing L2TP using IPsec", IETF RFC 3193, | November 2001. | | [5] W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", IETF RFC 1994, August 1996. | | [6] "openl2tp.org a linux l2tp solution for enterprise vpn and isps", openl2tp project website, | http://www.openl2tp.org/ | | [7] P. Wouters and K. Bantoft, "Openswan: Building and Integrating Virtual Private Networks", Packet | Publishing, 2006. | | [8] "IEEE POSIX Certification Authority", IEEE website,http://standards.ieee.org/regauth/posix/ | | [9] J. Moy, "OSPF Version 2", IETF RFC 2328, April 1998. | | [10] "Triangular routing", Wikipedia website, http://en.wikipedia.org/wiki/Triangular_routing |