# 基于 IPSec 和 L2TP 隧道实现技术的研究

李 琦 蒙 杨 卿斯汉

（中国科学院信息安全工程中心 100080） （北京中科安胜信息技术有限公司 100080）

**摘 要** 对于构建 VPN 系统来说，网络隧道(Tunnelling)协议是关键技术。当前隧道协议主要有两种：链路层隧道协议和网络层隧道协议。从安全的角度分析，链路层隧道提供的主要安全功能是基于用户和连接的认证，而网络层隧道还提供了数据加密的功能。要提供一个完整的 VPN，即一方面该 VPN 支持点对点接入，提供多协议封装；另一方面需要提供包括认证和加密的功能。所以，L2TP 协议和 IPSec 协议的结合使用成为研究和实现的热点，本文研究和探讨了基于 IPSec 协议和 L2TP 协议隧道的原理，并且提出了基于 L2TP 和 IPSec 结合使用的实现。

**关键词** L2TP，IPSec，PPP，隧道

## Research on Implemention Techniques of L2TP Tunneling with IPSec

LI Qi MENG Yang Qin Si-Han

(Information Security Engineering Center, CAS, Beijing 100080)

**Abstract** It is well known that tunnelling is a crucial technique for constructing Virtual Private Network(VPN). At present, tunnelling protocol primarily has two categories: data layer tunneling protocol and network layer tunnelling protocol. From the view of security, data layer tunnelling protocol provides authentication based on user and connection; and network layer tunnelling protocol provides data encryption. Since IPSec and L2TP are respectively representative security protocols in data layer and network layer, research and implemention of L2TP tunnelling with IPSec are focused. In this paper, the principles of L2TP tunnelling with IPSec are researched at first, then a scheme of L2TP tunnel and IPSec tunnel is designed; at last, the future of VPN with L2TP and IPSec is proposed.

**Keywords** L2TP, IPSec, PPP, Tunnel

## 1 引言

随着 Internet 和 Intranet 的迅速发展，VPN 技术被越来越多的企业和团体所采用，VPN 所使用的技术便是网络隧道技术。该技术利用一种网络协议来传输另一种网络协议，目前研究集中于网络隧道技术以及三种网络协议（网络隧道协议、隧道协议下面的承载协议和隧道协议的承载的被承载的协议）。到现在为止，比较成熟的协议有：(1)链路层隧道协议，主要分为点对点隧道协议 PPTP、第二种转发协议 L2F 以及第二层隧道协议(L2TP)；(2)网络层隧道协议，主要有通用路由封装协议(GRE)和 IP 安全协议(IPSec)。

PPTP 的缺点主要是缺乏基于权标的身份认证和加密功能薄弱，PPTP 依赖于 PAP（密码认证协议）、CHAP(Challenge Handshake 认证协议)、类似微软 Windows NT 中 NT 域级身份认证和 MS-CHAP(微软 Challenge Handshake)认证协议。L2F 是链路层隧道协议，和 PPTP 一样，该协议只提供了用户和连接的认证[1]。L2TP 是链路层隧道协议，尽管许多人相信 L2TP 是安全的协议，但是它不能提供安全的隧道。它和 L2F 一样，方便了用户和连接的认证[2]。

IPSec 则不然，它工作在网络层（第三层）。其最大的优点是提供了非常强的安全功能。IPSec 的使用方法有两种，是把认证和加密程序分成两个包造成的。分别是隧道模式和传输模式。在传输模式下，传输层是唯一认证和加密的层。隧道模式认证或加密整个包，这个包提供对未授权访问、数据截取、攻击等更多保护[3]。

但是我们知道，尽管许多人相信 L2TP 是安全的协议，但是它不能提供安全的隧道。因此，L2TP 并不能满足用户对安全性的需求。如果需要安全的 VPN，则依然需要 IPSec 和 L2TP 结合使用。所以本文对 L2TP 和 IPSec 分别进行讨论，然后对利用 L2TP 和 IPSec 提供一个完整的 VPN 进行讨论，最后详细阐述实现细节。本文一共分为以下几个部分：L2TP 和 IPSEC 分析、协议机制比较、我们的实现机制，最后对该实现的不足和优点进行了总结。

## 2 L2TP 和 IPSEC 协议分析

### 2.1 第二层隧道协议(L2TP)

2.1.1 *协议过程* L2TP 协议是将 PPP 分组进行隧道封装并在不同的传输媒体上传输，所以 L2TP 可看作虚拟 PPP 连续，并且它利用 PPP NCP 来协商 IP 的分配。主要由 LAC(L2TP Access Concentrator)和 LNS(L2TP Network Server)构成。LAC 又称为 L2TP 访问集中器，它是一台邻近 PPP 用户端的网络访问服务器(NAS)成为主机。它能进行 PPP 处理以及 L2TP 处理，是 PPP 链接 LCP 的逻辑终端。它将已成帧的 PPP 分组进行适当的处理，并封装 L2TP 之中，发送给 LNS。它是入站呼叫的发送者，出站呼叫者，是 L2TP 协议的客户端/服务器模式客户端[1]。LNS 是 L2TP 的服务端，是 PPP 协议中 NCP 协议的逻辑终端，在 LNS 处能进行 L2TP 封装或解封，并能进行 PPP 处理。

2.1.2 *协议特点描述* L2TP 解决了多个 PPP 链路的捆绑问题，PPP 链路捆绑要求其成员均指向同一个 NAS，L2TP 可以使物理上连接到不同 NAS 的 PPP 链路，在逻辑上的终结点为同一个物理设备。L2TP 扩展了 PPP 连接，在传统方式中用户通过模拟电话线或 ISDN/ADSL 与网络访问服务器(NAS)建立一个第 2 层的连接，并在其上运行 PPP。其第 2

李 琦 高级工程师。蒙 杨 博士，助理研究员。卿斯汉 研究员，博士生导师。

层连接的终结点和 PPP 会话的终结点在同一个设备上(如 NAS)。L2TP 作为 PPP 的扩展提供更强的功能,第 2 层连接的终结点和 PPP 会话的终结点可以是不同的设备。

L2TP 可认为是 PPTP 和 L2F 的继承,PPTP 是一种典型的自愿通道模式,L2F 是一种强制通道模式,而 L2TP 实现了以上两种的通道模式。在本文将详细讨论这两种模式。

### 2.2 IP 安全协议(IPSec)

IPSec 结构的第一个主要的部分是安全结构。Internet 草案文件《IP 协议的安全结构》描述了用于 IPv4 和 IPv6 的安全机制和服务。它提供了对 IPSec 包的介绍并且描述了结构的每一个组件。IPSec 的安全结构由三个主要的协议组成:

封装安全负载(Encapsulating Security Payload, ESP)提供了加密服务。认证头(Authentication Header, AH)提供数据报认证服务。ESP 和 AH 协议都有一个确定特定的算法和可选功能的支持文献集。

Internet 安全协会和密钥管理协议(ISAKMP)是 IPSec 的另一个主要组件。ISADMP 提供了用于应用层服务的通用格式,它支持 IPSec 协议和密钥管理需求。IETF 设计了 Oakley 密钥确定协议(Key Determination Protocol)来实施 ISAKMP 功能。这个协议在通信系统之间建立一个安全联系,它是一个产生和交换 IPSec 密钥材料并且协调 IPSec 参数的框架。

最后,解释域 DOI(Domain of Interpretation)将所有的 IPSec 小组的文献捆绑在一起。它可以被认为是所有的 ISPec 安全参数的主数据库,这些参数可以被相关 ISPec 服务的系统参考调用。

因为 ISAKMP 协议是设计在协议栈的所有层而不只是 IP 层上,所以每个安全协议必须有自己的 DOI 或存放相关参考数的数据库。目前,只有 IPSec 的 DOI 进行了定义。

## 3 我们的方案

### 3.1 基于 L2TP 的两种隧道模式[4]

将 L2TP 的 LAC 安装在不同位置,就产生了 L2TP 的两种不同的模式。第一种模式是将 L2TP 集成到远程用户主机。此时用户主机充当了 LAC,这种配置方式就是自愿模式(Voluntary Mode)。在这种模式中,用户自主对 L2TP 进行配置和管理,如图 1。另一种模式是将 L2TP 安装于 NAS,一般是 ISP,这种模式称为强制模式(Mandatory Mode)。这种模式下,对 L2TP 实现的配置和管理要被委托于 NAS,用户能透明地得到 L2TP 服务。

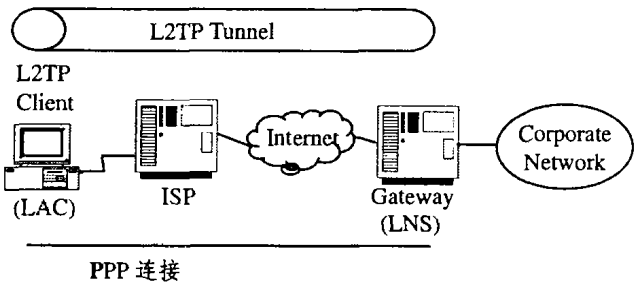


图 1 L2TP 自愿隧道

### 3.2 基于 L2TP 和 IPSec 的隧道模式

3.2.1 基于 IPSec 和 L2TP 的自愿隧道的模式 根据图 1 的自愿隧道的模式,提出分别在两种情况下两种自愿隧道。LAC 将 L2TP 包发送到 ISP,再经过 Internet 到 LNS。通过一个拨号连接将 L2TP 依次封装在 PPP 和 IP 包中,这样 LAC 可以取得它与 LNS 端的 SA 属性。如果 LNS 取得 SA,它能获得 LAC 和 LNS 的安全服务[5]。由于 LNS 可以得知它和 LAC 之间是否保密、是否得到认证、是否进行完整性检查、或者重放保护。它可以利用这些属性去修改它的 PPP ECP 和 CCP 的协商[2]。由于 LAC 和 LNS 之间有安全服务,它可以利用 IPSec 而取消 PPP 的加密和压缩。然而在图 4 有 IPSec 保护的终端的情况下,会导致重复的加密,这样可以通过协商 LAC 和 LNS 的两个 SA,这样使一个 ESP 为空,而另外一个来保护和压缩。

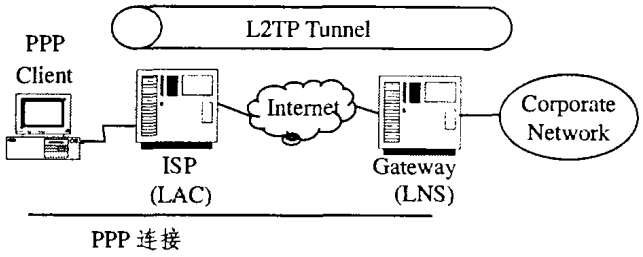


图 2 L2TP 强制隧道

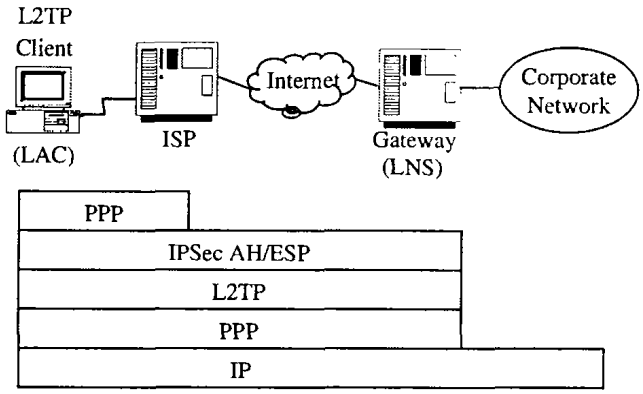


图 3 没有 IPSec 保护内图终端的自愿隧道

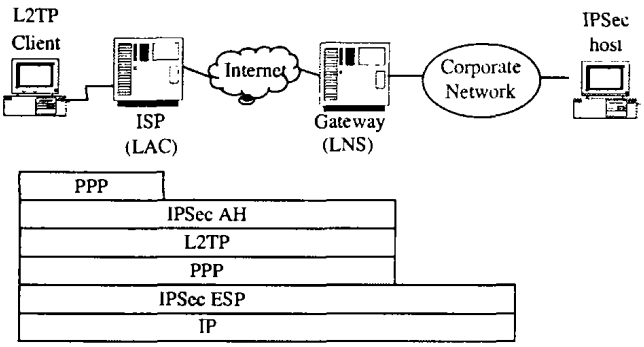


图 4 有 IPSec 保护内网终端的自愿隧道

3.2.2 基于 IPSec 和 L2TP 的强制隧道的模式 图 5、图 6 描述的是一种典型的不用加密封装的情况,即 PPP Client 发送 PPP 帧给 LAC。在 LNS 端收到的数据包,IP 包是封装了 PPP 的 L2TP 包。在这种模式下,Client 和 LNS 拥有安全服务的不同的信息,PPP 加密和压缩是否执行,要依靠 Client 的策略[2]。由于 Client 没有任何 LAC 和 LNS 之间的服务,而 Client 不信任 LAC 以及它和 LAC 之间的线路,Client 一般要求它到 LNS 的端到端的 IPSec 加密或者 PPP 的加密/压缩[5]。Client 协商它和终端的端到端的安全,以确定 LNS 到终端的保密。如图 6,如果 Client 知道它们之间通讯的终端有 IPSec 保护,它可以不协商 PPP 加密/压缩,而是协商终端 IPSec ESP。

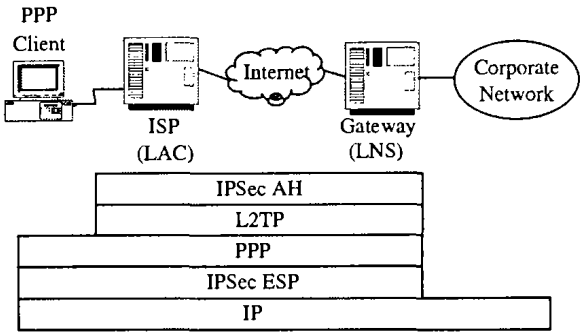


图 5　没有 IPSec 保护内网终端的强制隧道

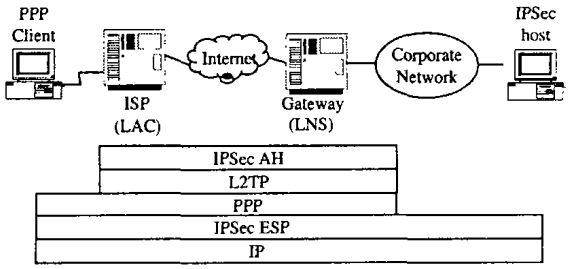


图 6　有 IPSec 保护内网终端的强制隧道

### 3.3　加入 RADIUS 认证/计费

基于以上的以 L2TP 和 IPSec 的隧道，PPP 的拨入端可以设有 RADIUS 认证和记费。同样，LNS 属于某个公司，也可以设有 RADIUS 认证和记费。

**结束语**　通过 L2TP 和 IPSec 的结合使用，L2TP 利用 IPSec 强的安全功能，以弥补自身安全方面的不足，而 IPSec 也可以在 L2TP LNS 端利用 RADIUS 的集中统一的鉴别和授权机制。该实现提供了具有多协议封装和完备的完全功能的 VPN，提供了基于链路层的加密和认证。在我们的实现过程中，这种结合使用也产生如下的不足：(1)重复封装带来的系统开销；(2)由于重复封装大大增加了分组的长度。尽管有这些不足，但在协议实现中加以处理，这些缺点是可以避免的，比如使用 PPP LCP 协商更小的 MTU，形成较短的分组的长度，可以减少分段的频率。在研究 L2TP 和 IPSEC 结合的同时，我们注意到 IETF 的其他一些工作组也在为 VPN 制定相关协议，其中的很多建议已形成草案。这些草案中涉及的协议有：MPLS、RADIUS、LDAP、VPMT 等。因此，L2TP、IPSEC 和 MPLS 等 VPN 协议集成的有效使用会成为新的 VPN 研究热点。

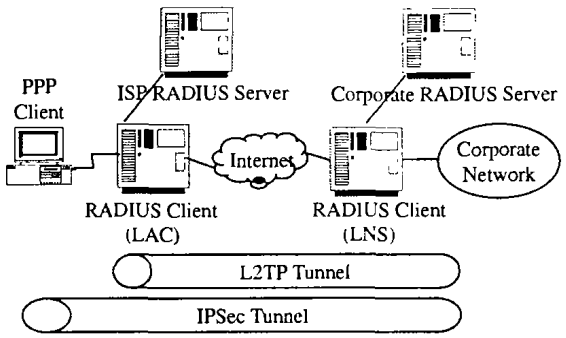


图 7　L2TP 强制通道

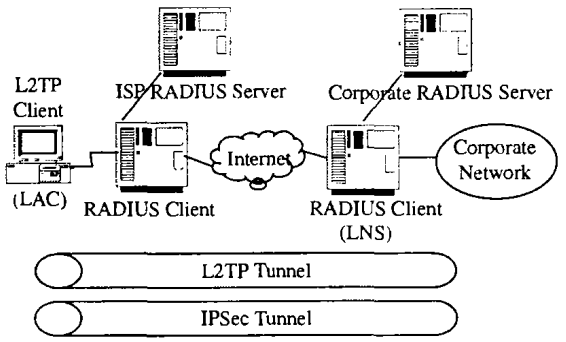


图 8　L2TP 自愿通道

## 参 考 文 献


1　何宝宏. IP 虚拟专用网技术. 北京：人民邮电出版社，2002
2　Black U. PPP and L2TP Remote Access Communications. Prentice Hall PTR，2000
3　[美]Davis C R. IPSec VPN 的安全实施. 周永彬，冯登国，徐震，李德全. 等译. 北京：清华大学出版社，2002
4　Townsley W，et al. RFC 2661：Layer Two Tunneling Protocol (L2TP) Aug. 1999
5　Patel B，et al. RFC 3193：Securing L2TP using IPsec. Nov. 2001


(上接第 34 页)

组播服务和群组特性，灵活地采用不同的方法来支持。随着一些相关领域研究工作的进展(例如安全组播路由协议等)，群组用户机制的具体研究和实现也要随之做相应的调整。

## 参 考 文 献


1　Deering S. Host Extensions for IP Multicast. RFC1112，1989
2　Bhattacharyya S，Diot C. An Overview of Source-Specific Multicast(SSM). draft-ietf-ssm-overview-05. txt，01 May 2003
3　Zhang B，Jamin S，Zhang L. Host Multicast：A Framework for Delivering Multicast to End Users. IEEE，2002
4　Hardjono T，Weis B. The Multicast Security Architecture. draft-ietf-msec-arch-01. txt，May 2003
5　Arkko J. MIKEY：Multimedia Internet Keying. draft-ietf-msec-mikey-06. txt，February，2003
6　Harney H，Schuett A，Meth U，Colegrove A. GSAKMP. draft-ietf-msec-gsakmp-sec-01. txt，Feb. 2003
7　Baugher M，Hardjono T，Harney H，Weis B. The Group Domain of Interpretation. draft-ietf-msec-gdoi-07. txt Dec. 2002
8　Waller D，Harder E. Key Management for Multicast：Issues and Architectures. RFC2627，June 1999
9　Mittra S. Iolus：A Framework for Scalable Secure Multicasting. ACM SIGCOMM '97，Canes，France，1997
10　Hardjono T，Cain B. Key Establishment for IGMP Authentication in IP Multicast. IEEE ECUMN，CREF，Colmar，France，2000
11　Ballardie A，Crowcroft J. Multicast-Specific Security Threads and Countermeasures. In：Proc. ISOC Symp. Net. and Distirb. Sys. Sec. San Diego，CA，Feb. 1995. 2～16
12　Judge P Q，Ammar M H. Gothic：Group Access Control Architecture for Secure Multicast and Anycast. IEEE INFOCOM，July 2002
13　Gennaro R，Rohatgi P. How to Sign Digital Streams. LNCS，1997，1294
14　Wong C，Lam S. Digtal Signatures for Flows and Multicasts. IEEE/ACM Trans，Net，1999，7
15　Golle P，Modadugu N. Authenticating Streamed Data in the Presence of Random Packet Loss. Net and Distrib，Sys. Sec，Symp，2001
16　Rohatgi P. A Compact and Fast Hybrid Signature Scheme for Multicast Packet Authentication. ACM Conf. Comp. and Commun，Sec，Nov. 1999
17　Canetti R. Multicast Security：A Taxonomy and Efficient Constructions. IEEE INFOCOM，New York，NY，Mar. 1999
18　Perrig，Canetti，Whillock. TESLA：Multicast Source Authentication Transform Specification. draft-ietf-msec-tesla-spec-00. txt，April，2002
19　Chu H，Qiao L，Nahrstedk. A Secure Multicast Protocol with Copyright Protection. In：Proc. of IS&T/SPIE Symposium on Electronic Imaging：Science and Technology. Jan. 1999
20　Brown I，Perkins C，Crowcroft. Watercasting：Distributed Watermarking of Multicast Media. In：First Intl. Workshop on Networked Group Communication(NGC '99)，Pisa Nov. 1999
21　Judge P，Ammar. WHIM：Watermarking Multicast Video with a Hierarchy of Intermediaries. In：The 10th Intl. Workshop on Network and Operation System Support for Digital Audio and Video. Chapel Hill. NC June，2000