第32卷 第20期 计 算 机 工 程 2006年10月
Vol.32 № 20 Computer Engineering October 2006
·安全技术· 文章编号：1000—3428(2006)20—0157—03 文献标识码：A 中图分类号：TP309

L2TP下可信的VPN方案设计与实现

黄 浩，谢冬青
(1. 湖南大学计算机与通信学院，长沙 410082；2. 中国科学院软件所计算机科学重点实验室，北京 100081)

摘 要：提出了一个用CA+对称L2TP路由器的模型，该模型身份认证和密钥由数字证书来完成，而加密和数据完整性认证则由L2TP路由器完成。和现有LAC+LNS的接入方案比较，该方案明确和简化了工作内容，并且解决了L2TP隧道内多路呼叫独立安全的问题。L2TP路由器在考虑了Linux内核的特点后，进行架构的设计来完成数据的处理。试验表明该方案兼顾了安全和性能，提供了一个高速可信的VPN解决办法。

关键词：L2TP；CA；数字证书；IPSec；UDP

Design and Implementation of Authentic VPN Scheme Using L2TP

HUANG Hao, XIE Dongqing
(1. College of Computer and Communication, Hunan Univ., Changsha 410082;
2. Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100081)

【Abstract】This paper proposes a model using CA plus symmetrical L2TP routers, the digital certificate fulfills identity-authentication and key distribution, the L2TP router fulfills encryption and data-intergrity. Compared with the present method using LAC plus LNS, the scheme distinguishes and simplifies the work, and it solves the problem that multiple calls in a L2TP tunnel are independently secure. After considering the feature of the Linux kenel, it designs the architecture of the L2TP router to deal with VPN data. The experiments show that the scheme gives attention to security and performance, it provides a speedy and authentic VPN solution.

【Key words】L2TP; CA; Digital certificate; IPsec; UDP

1 概述

VPN就是为了同一个团体内部数据通过公众网络进行安全保密传输而产生的。实现主要靠第2层的隧道技术：Cisco路由器支持的L2F协议、3COM等公司支持的PPTP协议以及由IETF提出的L2TP协议(Layer Two Tunneling Protocol)[1]。2000年，Zhao Aqun等人针对VPN的特点，具体化了VPN大致所要支持的功能，并比较了L2TP、GRE、IPsec、PP等协议的优缺点，提出了结合隧道实现技术的想法，用IPsec作为基本的加密机制[2]。2001年，用IPsec加密L2TP基本成熟。由Patel B和B. Aboda完成了RFC3193文档，弥补了L2TP安全性不足的问题[3]。但用IPsec加密L2TP是有缺陷的，当NAT在两端使用时，因为NAT会修改IPsec包的地址和端口域，终端的NAT对报文的认证显然是无法通过的。2004年5月，Atsushi Kara提出了一种用Meet-In-The- middle的网络模型，仍采用IPsec作为认证和加密机制，MIM网络负责路由功能，较好地解决了L2TP/IPsec无法进行NAT转换的问题[4]。2004年9月，Takahiro Suzuki等人提出了虽然L2TP/IPsec后的NAT可以解决，但是安全上有缺陷，提出了两种拒绝服务攻击的方法来断开L2TP断开连接，需要一种完全不依赖于IPsec的L2TP隧道保护机制[5]。

公钥基础设施PKI采用数字证书的办法解决了基于网络的身份认证，保证网上传输信息机密性、完整性和不可否认性，是一个权威且具有一般性的操作办法。L2TP引入数字证书来作为隧道保护机制对于一个有自己独立CA的企业来说是极为有效的。

现在Linux下开源的VPN解决方案吸引了更多人注意。如SnapGear's LITE+和SME550在μClinux下使用FreeS/WAN是一个很成熟的利用。

本文提出了CA+对称L2TP路由器的VPN模型，给出了具体的操作流程，依照X.509证书格式标准稍做修改，最后给出路由器的架构，将核心部分实现并同已有的一些产品进行安全性分析和性能比较。

2 VPN模型

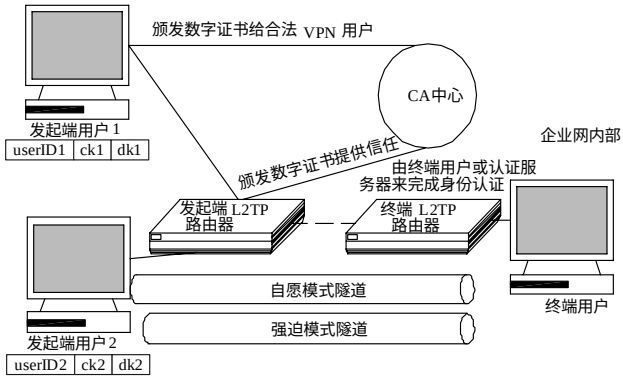

图1 CA+对称L2TP服务器的VPN

L2TP支持自愿和强迫两种隧道模式。自愿模式隧道起始于用户端，一般安全性没有问题，其灵活性对于一些移动用户来说尤其重要。强迫模式隧道是LAC(L2TP Network Server)

基金项目：国家科技成果重点推广计划基金资助项目(HD99-1)
作者简介：黄 浩(1978－)，男，硕士生，主研方向：信息安全理论和VPN技术；谢冬青，教授、博导
收稿日期：2005-11-18 **E-mail：**mengxihh@163.com

代表用户初始化的。建立隧道对于用户来说是透明的。前提是基于用户对于 LAC 的完全信任，LAC 大多由 ISP 服务商来提供，显然存在不安全因素。将身份认证和加密这两个分开是我们的基本想法。我们提出的 VPN 模型如图 1 所示。

身份认证由 VPN 的终端用户或认证服务器来完成，如果认证成功其将信息反馈给 CA，颁发给用户合法的 VPN 数字证书。

CA 中心：由 VPN 终端提供一个完整的 CA 中心。它负责对已认证的要进入企业私有网内部的公网用户颁发数字证书。同时对 VPN 发起端的 L2TP 路由器给出信任凭证。

终端 L2TP 路由器：其具有企业内部地址的完全信息，企业对其完全信任。是 L2TP 隧道的终点，完成进入私有网的控制与数据报文的解密、解压和数据完整性认证。

发起端 L2TP 路由器：由 CA 颁发的数字证书保证其可信性后，用户才放心地将数据包发送给该 L2TP 路由器，该路由器可以查询得到用户的密钥信息，包括两个字段：用第 1 个密钥进行控制报文的加密，用第 2 个进行数据报文的加密，实现了一条加密 L2TP 隧道内的多路呼叫。如果是自愿模式则用户端集成这项工作，没有信任的问题。整个流程如下：

(1)发起端用户将用户信息通过 L2TP 路由器发送到终端用户或认证服务器请求合法身份。

(2)身份认证合法之后，反馈给 CA，CA 颁发数字证书给该发起用户，将证书存储在目录服务器供查询。该证书要满足 L2TP 隧道内的多路呼叫问题，必须对 X.509 的证书格式稍作修改。ASN.1 语法中关于公钥的部分做如下修改：

```
SubjectPublicKeyInfo ::=SEQUENCE{
algorithm              AlgorithmIdentifier,
SubjectControlPublicKey      BITSTRING,
SubjectDatalPublicKey        BITSTRING
}
```

增加一个公钥字段来区分控制与数据的加密实现多路呼叫的功能。CA 同时颁发一份带有查询该种用户集合权限的证书给发起端 L2TP 路由器。X.509v3 证书的扩展项 Subject DirectoryAttribute 提供了该项功能。

(3)发起端用户收到证书之后可以得到自己需要的两个私钥(自愿隧道模式则自己分别加密控制和数据报文，传送出去，发起端 L2TP 只做转发的工作)。强制隧道模式用户必须得到发起端 L2TP 路由器合法的信息之后将 UserID 和口令提供给路由器，该路由器用自己的 ID 和证书提供的访问权限加上用户的 ID 和口令来查询得到用户的私钥。其他用户就算中途窃听了口令也没有访问权限，也无法得到该用户的私钥信息，就算得到了用户的相关报文也没法进入企业网内部，不会对企业网内部有任何干扰。

(4)用户将控制和数据报文提交发起端 L2TP 路由器，路由器用查询的两个私钥分别加密。如果用户提供的 Subject ControlKey 和目的地址已有相同的则认为该用户要求的隧道已建立只是另外一路呼叫。

(5)终端 L2TP 路由器解密报文发送隧道终点。

(6)有终止用户合法身份信息之后方可断开 L2TP 连接，VPN 结束时，注销相关证书。

本文方案将信任全部交到 VPN 终端来做，合理利用了数字证书的一般性，加密则由路由器来做，区分了权责。

下面将着重设计方案中的关键部件：L2TP 路由器。将把发起端和终端的路由器一致考虑，只不过完成的工作相反。

3 L2TP 路由器的系统架构

IPSec 对基于 L2TP 的 VPN 提供安全的服务。L2TP 与 PPTP 同样使用一条控制信道在隧道建立期间进行协商，与 PPTP 不一样的是，L2TP 不是使用一条分离的 TCP 连接作为控制信道，而是在 L2TP 报文外建立控制信道协议。PPTP 是使用 GRE 来封装报文头而建立的，但 L2TP 使用 UDP 协议(端口 1701)。后面的实验结果我们将看到使用 UDP 协议的 VPN 实现方案将在性能上明显超过使用 TCP 封装的方案。我们将现有的 Linux 下的 VPN 实现分成了两大类，如图 2 所示，可进行安全性以及性能的比较。

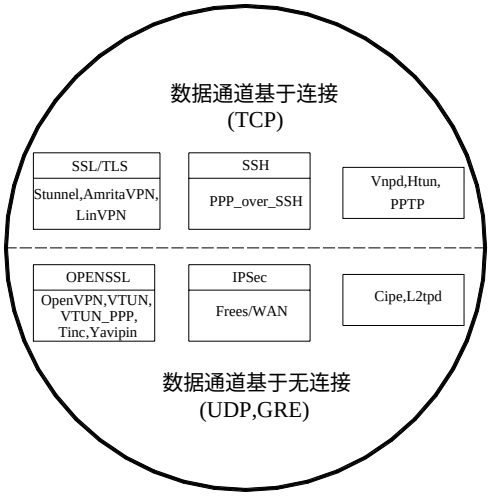

图 2　现有 VPN 按传输协议的分类

我们对 L2TP 路由器的系统架构，提出了自己的解决办法。它是对典型的 TCP/IP 栈模型稍做修改后的软件实现方法，增加了两个组件：VPN 后台和虚拟界面。

VPN 后台是一核心级的进程与 Linux 内核同步。控制阶段用来保持连接，包括每个路由器 IP 地址与私有网的映射。数据阶段用来处理数据加密、压缩和校验。两个阶段都采用 UDP 传输协议。所有 IPsec 加密和认证都要由其完成。

虚拟界面是一个特别的机制用来在 VPN 初始化时处理 IP 路由后台与 VPN 后台之间数据包无缝交换。

数据链路层协议的控制数据包都会传到虚拟界面。我们将采用一个伪终端的机制来创建该虚拟界面，系统模型如图 3 所示。

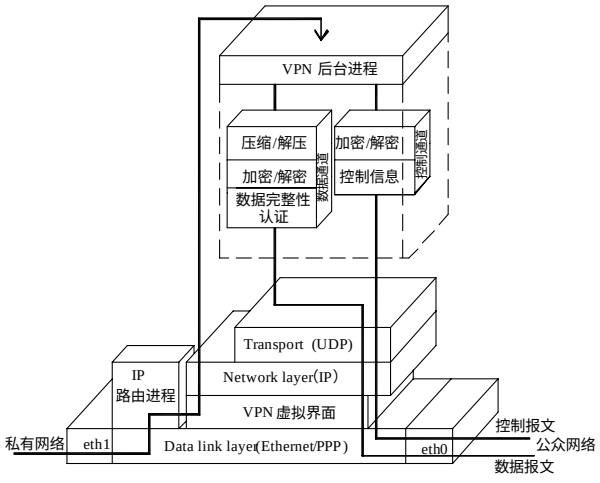

图 3 L2TP 路由器系统架构

一个私有网络的数据包到达路由器之后，去掉数据链路

层头部之后，IP 路由程序匹配该包的 IP 头部来决定该数据包的下一个路由或者目的地址，如果目的地址是私有地址，将其交给 VPN 虚拟界面，并且更新路由表。

VPN 虚拟界面则将包交给 VPN 后台进程，VPN 后台程序根据该包封装方式判断是控制报文还是数据报文，分别用两个不同的私钥加密。为保证路由器处理数据包的连续和高速，将 VPN 虚拟界面放在了数据链路层之后保证数据包的同步性和无序性。

4 实现与性能分析

我们用 0.69 版本 L2tpd 的源码（C 开发），在 Linux 下用我们的系统模型来实现。VPN 后台的核心模块加密采用 40 位的 3DES，完整性认证采用了 SHA-1。实现时设置为无压缩。实验环境为：两台不同私有网内的机器，均为 100Mb/s 的连接，PC1（P4, 3GHz 512MB 内存 Linux Redhat9.0）和 PC2（P3, 1GHz 256MB 内存 Linux Redhat9.0）。一个数据包捕捉工具 ethereal。

本文着重从 3 个方面比较 VPN 方案的性能：(1)VPN 安全性能；(2)VPN 路由的操作复杂性；(3)VPN 的带宽利用。

4.1 VPN 的安全性能

根据协议和各个产品方案得出安全性比较如表 1。由于加入 IPsec，因此 L2tp 提供了更好的安全性能。

表 1　VPN 安全性能比较

	数据保密性	数据完整性	身份认证	抗重放攻击
Vpnd	可	可	可	否
Htun	否	否	否	否
Cipe	可	可	否	否
PPTP	可	可	否	否
OpenVPN	可	可	可	可
VTUN	可	否	否	否
VTUN_PPP	可	否	否	否
Tinc	可	可	可	可
Yavipin	可	可	否	可
Frees/Wan	可	可	可	可
L2tpd	否	否	否	可
我们的方案	可	可	可	可

4.2 路由器操作的复杂性

表 2　路由器操作复杂性能比较

	更新配置文件	编辑路由信息	分配私钥	总操作*N
PPP_over_SSH	1	2（N-1）	N-1	N(3N-2)
Stunnel	2（N-1）	2（N-1）	1	N(4N-3)
AmritaVPN	0	2（N-1）	1	N(2N-1)
LinVPN	2（N-1）	2（N-1）	1	N(4N-3)
Vpnd	0	2（N-1）	N-1	N(3N-3)
Htun	2（N-1）	2（N-1）	0	N(4N-4)
Cipe	0	2（N-1）	0	N(2N-2)
Tinc	1	1	2	N(4)
Yavipin	2(N-1)	2(N-1)	1	N(4N-3)
FreeS/Wan	0	N	N	N(2N)
PPTP	N	2(N-1)	2(N-1)	N(5N-4)
OpenVPN	0	2(N-1)	1	N(2N-1)
VTUN_PPP	0	2(N-1)	0	N(2N-2)
L2tpd	1	2(N-1)	N-1	N(3N-2)
我们的方案	1	N	0	N(N+1)

假设一个网状的 VPN 有 N 个节点，由于缺乏一个中心管理部件，需要建立 N-1 条加密隧道，而且路由一般使用的私钥都要发送到每个节点，因此路由器的主要工作包括：更新配置文件，编辑路由信息和分配私钥。大致操作复杂性比较如表 2 所示。

我们的方案分配秘钥的工作完全由 CA 颁发的数字证书来完成，减轻了路由器工作。

4.3 VPN 的带宽利用

带宽利用是很多应用 QoS 必须关心的，我们也进行了比较。由图 4 可以看到，使用 TCP 的方案普遍差于使用 UDP 的方案。Tinc 方案安全性能和路由器性能都十分出众，但较低的带宽利用率限制了其的利用。由于使用了加密和认证，我们方案的带宽利用率相对 L2tpd 有了明显的下降，其中 IPsec 加密的速度成了瓶颈。

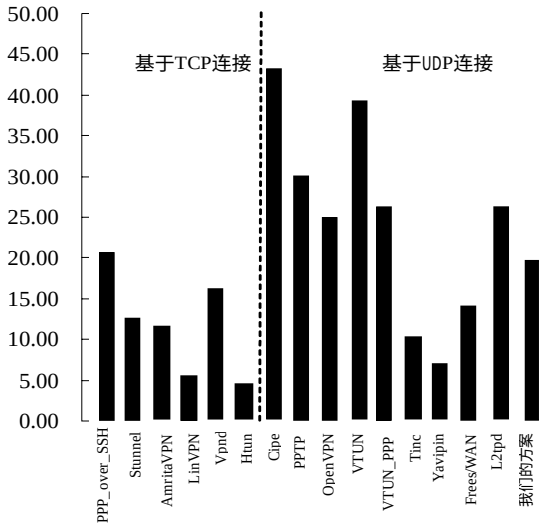

图 4 各 VPN 的带宽利用率（%）

5 结束语

本文提出了一种 L2TP 下可信的 VPN 模型，并对关键部件进行了设计，和现有的其它产品进行了比较。在高速的网络环境中给出一个灵活透明的 VPN 解决办法，可以根据不同用户要求创建一条隧道内的多路呼叫。如何适应网络速度提升的带宽利用率的不足，对于多域的 VPN，由于目的地址的不唯一性，路由器的 NAT 工作也要有相应的变化，这些问题都可以进一步研究。

参考文献

1 Townsley W, Valencia A. Layer Two Tunneling Protocol（L2TP）[S]. RFC2661, 1999-08.

2 Zhao Aqun, Yuan Yuan. Research on Tunneling Techniques in Virtual Private Networks[C]. Proc. of the International Conference on Communication Technology, 2000-08.

3 Patel B, Aboda B. Securing L2TP Using IPsec[S]. RFC3193, 2001-11.

4 Kara A. Private-to-Private Communications over the Internet[M]. IEEE Computer Society Published, 2004-05.

5 Kara A, Suzuki T, Takahashi K, et al. A DoS-vulnerability Analysis of L2TP-VPN[C]. Proc. of the Fourth International Conference on Computer and Information Technology, 2004-09.