基于 MPLS 骨干网络的 VPN 解决方案

赵 鹏,罗 平,刘蓓洁
(清华大学计算机科学与技术系,北京 100084)

摘 要: 现有的虚拟专用网(VPN)方案大多基于 IP 协议,这种结构的 VPN 在数据包转发速度、扩展性、服务质量等方面都存在欠缺,所以本文提出了基于多协议标记交换(MPLS)骨干网络的 VPN 解决方案.由于 MPLS 和 IPSec 在身份认证方面都没有定义,所以我们在方案中把认证中心(CA)的证书管理引入进来.该方案的核心思想是:利用 MPLS 在传输效率上的优势,通过 CA 进行身份认证、IKE 协议[1]进行密钥协商以及 IPSec 协议[2]进行数据包加密,从而在 MPLS 骨干网络上建立一个安全高效的 VPN.本文对实现 MPLS VPN 的每个关键部件都做了进一步的描述.

关键词: 多协议标记交换;虚拟专用网;认证中心;密钥交换;IPSec 协议;边界网关协议
中图分类号: TP393.2 **文献标识码:** A **文章编号:** 0372-2112 (2002) 12A-2024-03

Solution of VPN on MPLS Backbone Networks

ZHAO Peng, LUO Ping, LIU Bei-jie
(*Department of Computer Science & Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: Currently, most VPNs are based on Internet Protocol which has disadvantages in speed, expansibility and quality of service etc. Accordingly, we bring forward a solution of VPN on Multiprotocol Label Switching (MPLS) backbone network. We introduce Certificate Authority (CA) in this solution because both MPLS and IPSec haven't made a clear definition of authorizing identity. Taking advantages of MPLS in transporting efficiency, authorizing identity by CA, exchanging keys by Internet Key Exchange Protocol (IKE) and encrypting data by IPSec protocol, we construct a secure and efficient VPN on MPLS backbone network. Furthermore, we describe the realization of every component of MPLS VPN in detail.

Key words: MPLS; VPN; CA; IKE; IPSec; BGP

1 引言

如今,以 Internet 为骨干网络的 VPN 业务取得了巨大的发展,但是由于 Internet 网络带宽不足、路由处理能力不够、IP 地址资源短缺并且难以保证服务质量(QoS),所以这种结构的 VPN 在传输效率上往往不能满足要求.于是,MPLS 技术应运而生,它结合了 IP 技术与 ATM 技术二者的优势,在保证灵活性的同时,大大提高了传输效率,成为下一代 IP 骨干网络的有力竞争者.如何利用 MPLS 的技术特点,实现一个高效、安全的 VPN 系统是一个值得研究的问题.本文就是针对这一问题提出了基于 MPLS 骨干网络的 VPN 解决方案,既提高了数据传输效率,又保证了数据的安全性.

本文首先描述了 MPLS VPN 的整体结构和工作流程,然后给出了每一工作步骤所涉及部件的具体实现方法,最后对本方案的安全性进行了分析.

2 MPLS VPN 的整体结构和工作流程

实现 VPN 的关键技术主要有四项:隧道技术、使用者或设备身份认证技术、加解密技术和密钥管理技术[3].本文就是综合了这四项技术,从而设计出 MPLS VPN 的整体结构.

MPLS 实际上是一种分类转发技术,它把具有相同转发处理方式(目的地相同、转发路径相同、服务等级相同等)的分组归为一个转发等价类(FEC).属于相同 FEC 的分组在 MPLS 网络中将获得完全相同的处理.通过标记分发协议(LDP),各种 FEC 将对应于不同的标记,在 MPLS 网络中,各个节点将通过分组的标记来识别分组所属的 FEC.

2.1 MPLS VPN 的整体结构

MPLS VPN 的组件包括客户边缘设备(CE)、标记边缘路由器(LER)、标记交换路由器(LSR)、认证中心 CA 和在 IPSec 保护下的各个 VPN 节点,如图 1 所示,其中 CE 与用户这一端仍然使用 IP 网络的各种协议进行数据包转发,而在骨干网络中则使用 MPLS 技术进行数据包转发.IP 协议与 MPLS 协议之间的适配由 CE 与 LER 共同完成.

2.2 MPLS VPN 的工作流程

(1)申请证书.证书是 VPN 用户的身份凭证,是接入 VPN 的必要条件.对于尚未接入 VPN 的用户,首先要向 CA 提交必要的信息来申请证书.在证书的有效期内,这个步骤只需要进行一次.

(2)协商密钥.只有持有通过验证的证书的用户,才有可能被 VPN 接纳,而且用户还可以选择是否对数据包进行加密传输.如果选择是,则用户首先需要与通信的对等体协商密钥;否则可以跳过这一步骤.密钥协商在通信双方开始具体的通信之前进行,而在通信过程中,用户可以根据需要来决定是否更新密钥,进而重新执行这一步骤.密钥协商过程采用 IKE

收稿日期:2002-06-15;修回日期:2002-09-08
基金项目:国家科技部 973 项目(No.G1998030420)

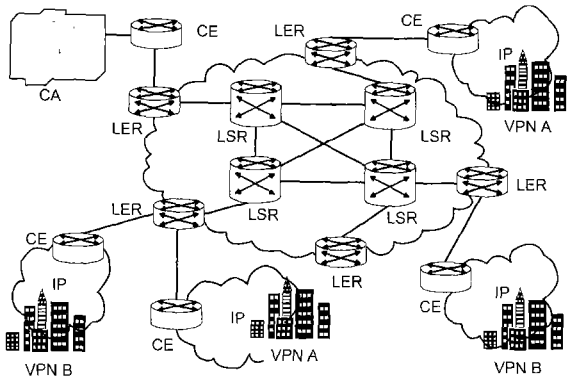

图 1　MPLS VPN 整体结构

协议来实现.虽然 IKE 协议建立在由 Internet 安全联盟和密钥管理协议(ISAKMP)定义的一个框架之上,但它并非专用于 Internet,IKE 协议所定义的各阶段的信息交换同样可以在 MPLS 骨干网络上进行.

(3)加密数据包.在 IKE 协商确定的 IPSec 安全联盟(SA)的保护下,进入 MPLS 网络的数据包将被加密.如果用户不需要对数据包加密,则可以跳过这一步骤.

(4)在 MPLS 骨干网络上转发数据包.MPLS 技术在无连接的 IP 网络中引入了面向连接的机制,通过一个短的、固定长度的"标记",利用标记交换来转发分组.其核心思想就是:边缘的路由、核心的交换.标记交换的具体过程,简单地可以分成以下四个步骤[4]:

(a) LDP 与传统路由协议(如开放最短路经优先算法 OSPF)一起,在各个 LSR 中为有业务需求的 FEC 建立路由表和标记转发表.

(b)入口 LER 接收分组,完成第三层功能,判定分组所属的 FEC,并给分组加上标记形成 MPLS 标记分组.

(c)MPLS 骨干网络中的 LSR 依据分组标记以及标记转发表,通过交换单元转发分组.

(d)出口 LER 去掉分组中的标记后继续转发.

可以看出,MPLS 实际上是一种隧道技术,网络内部的节点不关心分组的高层内容,这一特点在一定程度上保证了信息传输的安全性.因此,使用 MPLS 来支持 VPN 是十分简单而高效的.

(5)解密数据包.此步骤在目的端的 CE 处进行.如果用户选择不对数据包加密,则可以跳过这一步骤.

3　MPLS VPN 的实现

本节将按照 MPLS VPN 的工作流程中所涉及的部件的顺序,分别给出各个部件的实现方法.

3.1　认证中心(CA)

CA 是负责发放和管理数字证书的权威机构,在整个网络安全方案中处于重要地位.本文提出的 VPN 解决方案是基于 MPLS 骨干网络的,规模非常大,所以在具体实施的时候,最好采用公认的权威的认证系统,如人民银行总行的 CA 等.但是在实验阶段,出于调试方便和经济上的考虑,采用了作者所在项目组开发的证书发放系统 AFIN.

CA 的主要功能包括证书的颁发、更新、查询、作废以及归档等.证书中包含用户信息,如名字、端口号、所属部门、IP 地址以及公共密钥的拷贝等.通过 CA,VPN 接纳新用户或设备(以下简称设备)非常方便.当一个新设备加入到网络中时,只需要简单地利用 CA 来接纳它,其它任何设备都不需要改动.当两个设备希望通信时,它们就可以互相交换认证信息和每一方的数字签名来认证对方的身份.

3.2　客户边缘设备(CE)

CE 的第一个重要功能是运行 IKE 协议来协商密钥,协商的最终结果是生成一个通过验证的密钥和 IPSec SA.IKE 要求交换的所有信息都要经过认证和加密,以保证别人不能窃听到密钥信息,并且密钥信息只能在认证实体之间传递.在本方案中,我们采用 RSA 的数字签名认证方法,数字签名中用到了证书.IKE 定义了两个阶段的信息交换,在第一阶段定义的 IKE SA 的保护下,可以并发地执行多个第二阶段的信息交换.

第一阶段:建立 IKE SA 和验证过的会话密钥.IKE SA 中包含了通信双方协商制订的各种参数,如加密算法、散列算法、验证方法、Diffie-Hellman 组以及有效期限等.IKE SA 的作用就是为双方的 IKE 通信提供机密性、信息完整性和信息源验证服务.

第二阶段:利用 IKE SA 定义 IPSec SA.IPSec SA 决定了用来保护数据包的加密协议、转码方式、密钥以及密钥的有效期限等.在 CE 中有一个 SA 数据库(SADB),其中的每一条记录代表着一个逻辑连接,通常用三元组唯一地表示:〈安全参数索引,目的 IP 地址,安全协议〉.其中,安全参数索引(SPI)是一个 32 比特数,用于标识具有相同 IP 地址和相同安全协议的不同的 SA.SPI 位于安全协议的头部.安全协议可以是 AH 或 ESP.

CE 的第二个重要功能是加解密,即在 IPSec SA 的保护下,实现数据的密文传输.目前已经有很多具体的 IPSec 实现产品,本方案采用开放源码、基于 Linux 操作系统的 FreeS/WAN 1.91[5].FreeS/WAN 支持手动和自动密钥协商,配置方法灵活,可构建多种结构的 VPN,如主机-主机、主机-子网、子网-子网、远程 VPN 接入等.而且,FreeS/WAN 与防火墙及安全代理等配合使用,安全效果更好.加解密是一项可选的功能,它的好处是使得在 MPLS 骨干网络中传输的数据包也是密文的,缺点是降低了传输效率.

3.3　标记边缘路由器(LER)

LER 主要完成连接 MPLS 域和非 MPLS 域的功能,并实现业务分类、分发标记及剥去标记等等;它还可以实现策略管理、流量控制等功能.每个 LER 中都有一个非 VPN 转发表和多个 VPN 转发表,每个 VPN 转发表对应着一个与此 LER 直接相连接的 CE(或 VPN 节点).LER 从 CE 接收到数据包,查找相应的 VPN 转发表,如果符合转发条件(如目的地址、端口、身份等),则将数据包转发到 MPLS 骨干网络上;如果数据包目的地址是 CA 或者数据包为 IKE 信息包,则根据非 VPN 转发表将数据包转发到相应的 LSR;否则,数据包将被丢弃.LER 的实现方案如图 2 所示(以入口 LER 为例,出口 LER 的实现结构与此相反).

我们以转发信息库(FIB)为例简要说明 LER 的部分工作原理.如图 3 所示,VPN1 中的用户与 VPN2 的用户之间是隔离的.LER 中只包含与之直接相连的 VPN 用户的地址入口,这样,LER 就可以拒绝非法用户进入 MPLS 骨干网络.通过为每一个 VPN 分配一个逻辑上分离的转发表,用户就可以在公共网络上建立私有的、无连接的专用网络.

3.4 标记交换路由器(LSR)

LSR 的实现方案如图 4 所示.LSR 要完成路由器的控制功能和标记管理功能.LSR 要象通用的路由器一样完成路由控制,不断更新和维护路由表.LSR 所采用的路由技术通过标准的第三层路由协议(如边界网关协议 BGP[6] 和 OSPF)来实现.同时它的路由表在 MPLS 控制信号的作用下,建立并维护标记信息库 LIB.通常 LSR 在 LDP 的控制下,对标记的主要操作有:标记划分、标记分发、标记维护等.MPLS 网络中的每个节点都必须建立 LIB,其中含有标记绑定信息.这样就可以利用 LIB 中的信息,根据输入分组所携带的标记进行交换,例如标记入栈、标记出栈、标记替换等,然后利用第二层的交换机制转发分组.

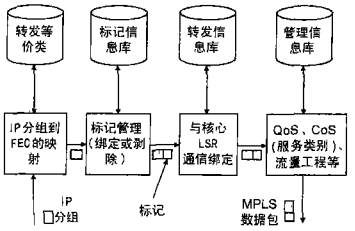

图 2 入口 LER 实现方案

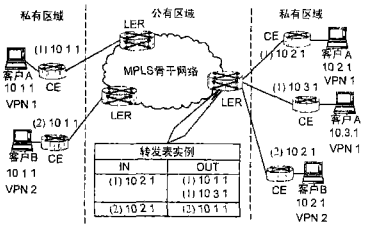

图 3 LER 中的 FIB

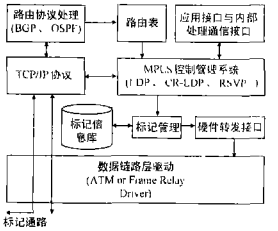

图 4 LSR 实现方案

4 MPLS VPN 的安全性分析

通过结合 CA、MPLS 中的 BGP 协议及 IP 地址解析协议、IKE 协议和 IPSec 协议,基于 MPLS 骨干网络的 VPN 解决方案提供了多重的安全保障,分析如下:

(1)利用 CA.只有持有可信任 CA 颁发的证书的用户才能证明自己的身份,从而被 VPN 接纳.由于伪造证书非常困难,所以 CA 有效地防范了非法用户进入 VPN.

(2)利用 BGP.BGP 是 MPLS 骨干网络上的路由信息分发协议,它用多协议的扩展和共同的属性来判断谁和谁可以通信.VPN 成员根据逻辑端口和 VPN-ID 进入 VPN,VPN-ID 是在配置 VPN 时唯一分配给每一个 VPN 的,VPN 的终端用户并不知道这个 VPN-ID.只有预先分配的端口才可以加入 VPN.BGP 把 VPN 的 FIB 表的更新信息只向特殊的 LER 分发,即必须有此 VPN 的节点与之相连.这就避免了在所有 LER 中都维护所有 VPN 的 FIB.

(3)利用 IP 地址解析.每个 VPN 都有一个唯一的标识符 VPN-ID,该 VPN-ID 与终端用户的 IP 地址合在一起,就得到一个 VPN-IP 地址.网络中每个终端用户的 VPN-IP 地址都是唯一的.VPN-IP 地址存放在该 VPN 的每个节点的 FIB 中.由于用标记代替了 IP 地址而不需要网络地址转换(NAT),所以当用户的数据包通过服务提供商的公共网络时,就可以保证自己 IP 地址的机密性.由于使用 BGP 分发 VPN-IP 地址并建立 FIB,所以各 VPN 之间是互不可见的.

(4)利用 IKE 与 IPSec.对于大多数业务,BGP、VPN-IP 地址的结合就可以提供足够的安全性.然而,由于所有的数据包都以明文传输,因此就不能保证完全的机密性.通过使用 IKE 密钥协商技术和 IPSec 加密技术,可以提供各种水平的保护措施.当然,由于密钥协商和加解密都需要额外的硬件和软件处理能力,增加了系统开销,所以密钥协商和加解密可以根据用户的需要来决定是否进行.

5 总结

本文提出的基于 MPLS 骨干网络的 VPN 解决方案,集成了身份认证、信息完整性与信息源验证以及密文传输的功能,同时具有高速、易于管理、良好的 QoS 等特征,为当前关键业务网络系统的建设提供了一个实用的安全解决方案.本方案所采用的 MPLS、CA、IKE、IPSec 符合国际标准,充分利用了下一代骨干网络 MPLS 带来的优点,透明地解决用户的网络安全问题,具有良好的实用前景.另外,本文为每个部件给出的具体实现方法也具有很好的参考价值.

参考文献:

[1] RFC2409.The Internet Key Exchange (IKE) [S].

[2] RFC2411.IP Security [S].

[3] 石晶林,丁炜,等.MPLS 宽带网络互联技术 [M].北京:人民邮电出版社,2001.638 - 648.

[4] D Hosein, F Badran. Service Provider Networking Infrastructures with MPLS [A]. IEEE Computers and Communications [C]. Proceedings. Sixth IEEE Symposium on, 2001:312 - 318.

[5] FreeS/WAN Project: Documentation [EB/OL]. http://www.freeswan.org/doc.html, 2002 - 06 - 01.

[6] RFC2547.BGP/MPLS VPNs [S].

作者简介:

赵 鹏 男,1975 年 12 月生于吉林,清华大学硕士研究生,主要研究方向为网络安全和文件保密,如虚拟专用网、防火墙、安全电子邮件、文件虚拟存储等.Email:penggy 717 @ sina.com.

罗 平 男,1959 年生于湖南,清华大学副教授,主要研究领域为密码学、通信保密、网络安全等.Email:luop@mail.tsinghua.edu.cn.