基于 IPSec 的 MPLS IP VPN 的设计与实现*

任德玲，韦 卫
(中国科学院 研究生院，北京 100085)

摘 要：从 VPN 的需求出发，分析了 IPSec VPN 和 MPLS VPN 各自的优势和局限性，提出了基于 IPSec 的 MPLS VPN 设计方案和实现模型。该方案既具有 IPSec VPN 的高安全性和可靠性又具有 MPLS VPN 的高速交换、QoS 保证、流量工程以及可扩展性的优点。

关键词：IP 安全协议；多协议标签交换；虚拟专用网
中图法分类号：TP393.08 文献标识码：A 文章编号：1001-3695(2006)03-0116-03

Design and Implementation of IPSec-based MPLS IP VPN

REN De-ling, WEI Wei
(School of Graduate, Chinese Academy of Sciences, Beijing 100085, China)

Abstract: This paper analyses the advantages and disadvantages of IPSec VPN and MPLS VPN according to VPN requirements, and puts forward a design scheme of IPSec-based MPLS VPN and its implementation model. The design scheme can share the advantages of IPSec's high security and reliability and MPLS's high speed switching, QoS guarantee and flow engineering as well as expandability.

Key words: IPSec; MPLS; VPN

1 引言

虚拟专用网(VPN)就是企业内部网在因特网等公共网络上的延伸，通过一个私用的通道来建立一个安全的私有连接，虚拟专用网通过安全的数据通道将远程用户、公司分支机构、公司的业务伙伴等与公司的内部网连接起来，构成一个扩展的公司企业网，由因特网服务提供商提供高性能、低价格的因特网接入，这样通过虚拟专用网络既实现了传统专用网络所需的性能，同时相对于传统的专用网络又大大降低了网络的运营成本。

目前 VPN 技术主要分为两类：①以安全隧道技术为核心的 IPSec VPN；②基于多协议标签交换的 MPLS VPN。网络层隧道协议 IPSec 提供了一种标准的、可靠的、可扩充的安全机制，用于在网络层提供数据源验证、面向无连接的数据完整性、内容机密性、抗重发攻击等安全服务。MPLS 技术采用集成模型，将 IP 技术与下层技术结合在一起，兼具了高速交换、QoS 性能、流量控制以及可扩展等特性。本文提出了基于 IPSec 的 MPLS VPN 设计方案，把 IPSec VPN 和 MPLS VPN 的优势集成起来，提供设计优良、运行正常和综合性的 VPN 服务。

本文讨论的 VPN 都是指 IP-based VPN，即主干网是以 IP 为主要通信协议的公共网络，包括 Internet 和服务提供商的 MPLS 核心网络(BGP/MPLS VPN)。BGP/MPLS VPN 是 RFC 2547bis 中定义的一种机制，允许服务提供商用他们的 IP 主干网来给客户提供 VPN 服务。

收稿日期：2005-03-19；修返日期：2005-05-14
基金项目：国家“863”计划资助项目(2002AA142030)

2 IPSec VPN

IPSec 协议是网络层协议，它是为保障 IP 通信安全而提供的一系列协议簇。它针对数据在通过公共网络时的数据完整性、安全性和合法性等问题，设计了一整套隧道、加密和认证方案。RFC 2401[1] 规定了 IPSec 的基本结构，它利用认证头(AH)和封装安全载荷(ESP)实现数据的认证和加密。前者用来实现数据的完整性，后者用来实现数据的机密性。

IPSec VPN 是通过 IPSec 技术建立安全数据隧道的 VPN 解决模型，安全数据隧道本质上是提供独立封闭的数据包安全传输。IPSec VPN 如果按功能划分由四大块组成：IPSec 进程、因特网密钥交换(IKE)进程、安全联盟数据库(SAD)和安全策略数据(SPD)。IPSec 进程本身就是用来实现整个 IPSec 的守护进程，用户可以通过和这个进程打交道来管理自己的安全策略，对要输出的 IP 数据包添加 AH 头或 ESP 头，实现适合自己需要的网络安全。IKE 是 IPSec 最为重要的部分，在用 IPSec 保护一个 IP 包之前，必须先建立一个 SA，IKE 用于动态建立 SA。IKE 代表 IPSec 对 SA 进行协商，并对 SAD 数据库进行填充。RFC 2409 所述 IKE 是一个混合型的协议，它建立在由 Internet 安全联盟和密钥管理协议(ISAKMP)定义的一个框架上。IKE 使用了两个阶段的 ISAKMP：第一阶段建立 IKE 安全联盟；第二阶段利用这个既定的安全联盟为 IPSec 协商具体的安全联盟。安全联盟数据库(SAD)和安全策略数据库(SPD)是构成 IPSec 的基础，用来管理安全联盟数据和安全策略信息。IPSec 有两种不同的 IP 包封装模式：①传输模式，用于隧道终点是主机的场合；②隧道模式，用于隧道终点是网关的环境。

IPSec VPN 的主要优势在于：

(1) 强大的安全性。IPSec 协议固有的强大的安全特性能够使用户进行认证, 保证数据的机密性和完整性。用户可以用数字证书或者预共享密钥进行认证, 与安全策略不一致的包被丢弃。

(2) 支持远程办公和移动办公。IPSec VPN 数据转发设备能够为数万地址上分散的用户提供服务。

(3) 易于配置。搭建 VPN 并不需要服务提供商的介入, 尽管许多企业为了降低花费、加快服务入门和减轻风险, 选择利用服务提供商对区域性或者全局性多个站点配置的管理服务经验。

(4) 减轻在集线器站点的拥挤。当对分散隧道配置时, 远端 VPN 客户端能直接转发预定的 Internet 流量, 替代通过IPSec 隧道, 并仅对相关的正在被转发到集线器的流量建立隧道。这降低了在集线器点的拥挤。

IPSec VPN 的局限性在于:

(1) 不支持 QoS(服务质量) 。由于 IPSec VPN 是基于传统 IP 网络的, 因此无法保证核心网络上的 QoS。

(2) 可伸缩性差。在大部分典型的星型网络拓扑上, VPN 站点之间都通过一个中心节点实现相互访问, 这样每次增加一个新站点, 只要在中心节点和新节点上配置即可, 但是这样会带来双倍的延时效应, 降低网络性能。如果在大的或者网关的 IP VPN 拓扑配置下, 可伸缩性受到了很大的挑战, 需要充足的计划和协同来解决密钥分发、密钥管理和对等配置。

3　MPLS VPN

MPLS(Multi-Protocol Label Switching) 即多协议标签交换, 属于第三层交换技术, 它引入基于标签的机制, 把选路和转发分开, 由标签来规定一个分组通过网络的路径。标签作为 IP 包在网络中的替代品而存在, 在网络内部 MPLS 在数据包所经过的路径沿途通过交换标签来实现转发, 当数据包要退出 MPLS 网络时, 数据包被解开封装, 继续按照 IP 包的路由方式到达目的地。

MPLS VPN 是指利用服务提供商的 MPLS 核心网络构架的 VPN 解决方案。在 MPLS VPN 网络构架中存在三种路由设备: 客户边缘路由器(CE) 在客户站点提供对外路由, CE 被连接到提供商 MPLS 网络上的边缘路由器(PE) , PE 存有 VPN 的路由表(VRF) , 提供商核心路由器(P) 作为 MPLS 核心网络的传输主干。

MPLS VPN 的主要优势在于:

(1) 网络安全性比较高。MPLS 通过使用路由识别器加强了在同一个核心网络不同 VPN 之间的流量分离, 当把 VPN 放置在包头时, 独特的路由识别器将自动分配。MPLS VPN 和传统广域网架构下的帧中继和 ATM 安全性一样。服务提供商能够设计这样的网络, 即客户路由器不了解核心网络, 核心路由器也不了解客户的边界。

(2) 高度的可伸缩性。基于 MPLS VPN 可以非常容易地配置来适应公司的增长和变更, 不必像其他 VPN 结构需要全网状或者端到端。例如, 当一个新的站点被增加到 VPN 时, 公司或者服务提供商仅仅需要建立在新站点和提供者边界之间的本地对等, 并不需要在其他的现成站点重新配置 CE, 赢得了重要的优化成本节约。

(3) 对 SLAs(Service-Level Agreements, 服务品质协议) 的支持。SLAs 对网络性能和弹性有迫切需要的用户是非常重要的, 基于 MPLS VPN 通过提供可升级的、健壮的 QoS 机制、带宽保证和流量管理性能来支持 SLAs。通过在核心网络配置流量管理、服务提供商网络管理能帮助确保实现优化流量分发和全面改进网络使用的策略。

(4) 流量工程。能够提供以往 IP 网中无法保证的流量工程业务, 可最佳利用链路和节点, 平衡负荷。

MPLS VPN 的局限性在于:

(1) 无法完全保证数据的机密性和完整性。由于 MPLS VPN 的数据安全性并不是通过加密和验证算法来保证的, 所有的数据包都以明文的方式传输, MPLS VPN 是通过转发分离和路由表项分离来实现安全性的。

(2) 访问的灵活性不强。MPLS VPN 主要是基于网络到网络(LAN-to-LAN) 的, 不易实现移动用户的 VPN 接入。

综合以上分析, MPLS VPN 可以方便地实施流量控制, 保证 QoS, 同时具有很强的伸缩性和可管理性; 另一方面, 虽然 MPLS VPN 为业务流提供了一定的隐蔽性, 但是其明文传输的特点导致了抗攻击的能力非常差, 在安全性上有很大的缺陷, 同时不能解决移动用户接入的问题。IPSec VPN 的安全性比较高, 比较容易解决移动用户接入的问题; 另一方面, IPSec VPN 的伸缩性差, 保证 QoS 和实施流量工程比较困难, 同时也增加了用户使用这种 VPN 的复杂性和成本。

4　基于 IPSec 的 MPLS VPN 的设计

4.1　几种设计方案分析

方案 1　在客户端路由器 CE 上进行 IPSec 的处理, 在服务提供商的边缘路由器 PE 上进行 MPLS 封装。

方案 2　在服务提供商的边缘路由器 PE 上进行 IPSec 处理, 并进行 MPLS 封装。

方案 3　在服务提供商的边缘路由器 PE 上先进行 MPLS 封装, 再进行 IPSec 处理。

方案 4　在服务提供商的边缘路由器上先进行 MPLS 封装, 再进行 IPSec 处理, 最后进行 MPLS 封装。

方案 1 需要用户端进行策略配置, 增加了用户网络的复杂性。方案 2 中如果 PE 连接多个 VPN, 这种方案不能解决 VPN 的私有地址的空间重叠问题。方案 3 具有 IPSec VPN 的功能, 外层 IPSec 负责在骨干网中搭建 IPSec 隧道, MPLS 标签是 VPN 标签, 可以在骨干网络边缘路由 PE 上, 由 MPLS 标签映射连接到具体的 VPN 的逻辑端口, 解决了 VPN 的私有地址空间重叠问题, 同时保证了数据包在骨干网上传输的安全性问题, 这实际上也是 IETF LSVPN 工作组在 draft-ietf-l3vpn-ipsec-2547-02[2] 草案中的主要思想。但是, 由于这种封装的形式导致了数据包在骨干网传输过程中, 实际上是以 IP 报文的形式传输的, 这样就丧失了 MPLS 本身在流量工程、QoS 等方面的优势。方案 4 外层 MPLS 标签用来在骨干网中进行标签交换, IPSec 保证数据传输中的安全性, 内层 MPLS 为 VPN 标签, PE 可以根据它将报文映射到合适的逻辑端口上, 解决了私有地址的空间重叠问题。

4.2 设计方案的实现

基于对以上几种方案的分析,我们采用方案 4,即 MPLS + IPSec + MPLS VPN 方案。在这种 VPN 中,对于客户端路由器和骨干网中的 P 路由器设计没有改变,网络结构与 MPLS VPN 的结构一致;如图 1 所示,主要改动的是 PE 路由器,PE 路由器需要在支持原传统路由协议和 MPLS 协议的基础上,增加对 IPSec 的相关处理。由于在 PE 端 MPLS 使用标签建立 LSP 隧道,并通过 VPN ID 及用户 IP 对身份进行了严格控制。为了提高效率,该设计在 PE 路由器上只使用 IPSec 的 ESP 进行加密。

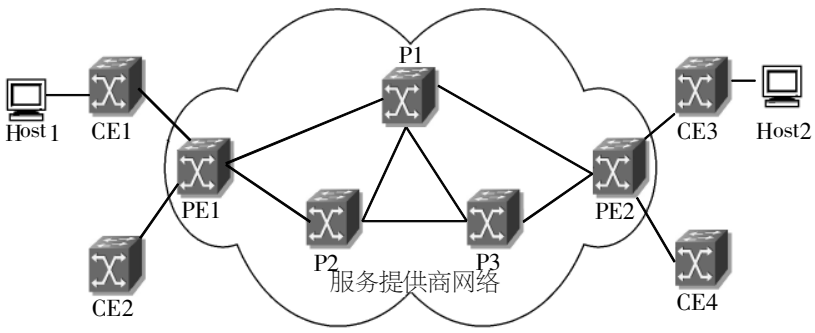

图 1 基于 IPSec 的 MPLS VPN 的网络结构

4.2.1 基于 IPSec 的 MPLS VPN 设计方案在 PE 上的实现模型

在 PE 上和 VPN 相关的部分主要可以分成如图 2 所示的几个模块。

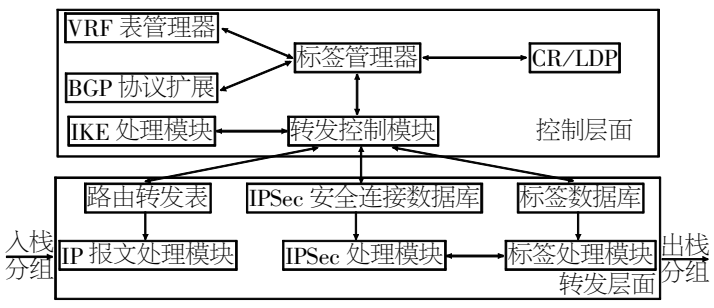

图 2 基于 IPSec 的 MPLS VPN 模块示意图

4.2.2 服务提供商边缘路由器 PE 的数据包处理流程

对于 PE 中的数据包处理流程,分为发送端 PE 和接收端 PE 两种情况。由于通信是双向的,同一个 PE 既可能是发送端 PE,也可能是接收端 PE,所以下面分析的两个流程同时存在于任一个 PE 内。

下面假设是 Host1 发起的通信,接收方为 Host2:

(1) 发送端 PE

发送端 PE 从它直接相连的一个 CE 上接收传统的 IP 报文。在经过一系列的处理后形成 MPLS 分组,向骨干网中的下一跳转发,如图 3 所示。

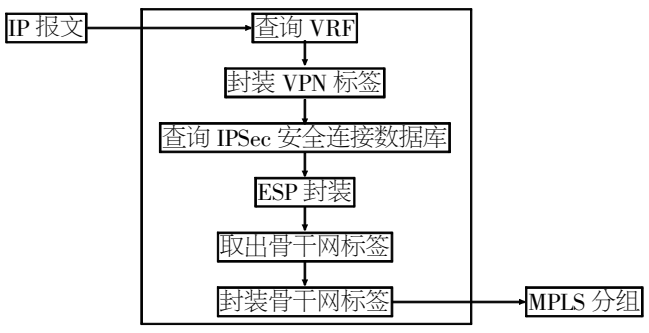

图 3 发送端 PE 处理流程图

当 IP 报文到达 PE1 的时候,PE1 根据 IP 报文传输过来的逻辑端口得知 IP 报文所属的 VPN。由于 IP 报文中的 IP 地址为私有 IP 地址,也就是说不同 VPN 的地址可能是重叠的。为了解决这个问题,每个 VPN 的路由器中都有自己的路由表和转发表,因此 MPLS VPN 的所有 PE 路由器都包含大量单-VPN 路由表以及一个全局路由表。后者用于到达提供商网络中的其他路由器以及外部的全局性可达的目的地。这样,只要到达的 IP 报文的地址在该 VPN 中是唯一的,那么 PE1 就可以根据其所属 VPN 查询对应的 VPN 路由表(VRF),获得目标网络和其接收端 PE2 的信息。根据目标网络对报文进行第一次封装——加上内层 MPLS 标签,也就是 PE1 和 PE2 协商好的 VPN 标签。PE1 查询 IPSec 安全连接数据库,获得对应的 SA,IPSec 进程对报文进行 ESP 封装,增加序列号字段(如果没有 SA 的安全策略,则触发 IKE 进程,建立新的 SA,存入通信双方网关的 SAD 中)。IPSec 封装完毕,将获得的报文再次交给标签处理模块,查找标签库,为报文封装上外层 MPLS 标签,也就是骨干网标签。PE 将已封装好的数据发送至 MPLS 网中。

(2) 接收端 PE

再分组经过骨干网的传输,最终将到达接收端 PE2。在图 1 中,PE2 收到的将是一条 IP 报文,准确地说,是一条经过 IPSec 封装的报文。其骨干网标签由于 MPLS 中的“倒数第二跳弹出机制”,已经在 PE2 之前的一跳弹出了。因此,接收端 PE 的处理流程如图 4 所示。

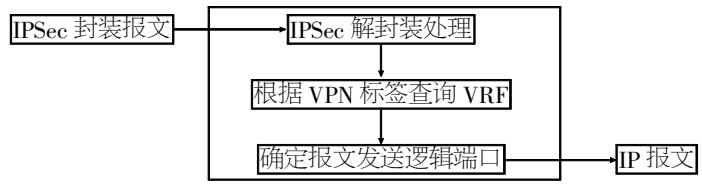

图 4 接收端 PE 处理流程图

接收端 PE2 的处理相对简单一些,首先进行 IPSec 处理,将加密的报文还原。根据 IPSec 头中的上层协议判断出 IPSec 封装的是一个 MPLS 分组,将之交给标签处理模块。标签处理模块根据分组中的 VPN 标签查询 VRF 表,得到对应的逻辑端口,弹出 VPN 标签,将 IP 报文通过得到的逻辑端口上转发到 CE3。

5 结束语

通过现有的骨干网建立企业网络的互连,最终建立起一个虚拟的私有网络,这不仅会节省网络的建设和运行维护费用,而且增强了网络的可靠性和安全性。MPLS 与 IPSec 结合有利于把 MPLS 的高速交换、QoS 保证、流量控制以及灵活性、可扩展性与 IPSec 的高度安全、可靠的优势发挥出来,提供设计优良、运行正常和综合性的 VPN 服务。

参考文献:

[1] Kent, R Atkinson. RFC 2401[EB/OL]. http://rfc.net/rfc2401.html, 1998-11.

[2] Eric C Rosen, Jeremy De Clercq, Yves T'Joens, *et al*. Use of PE-PE IPSec in RFC 2547 VPNs[EB/OL]. http://ietf.mirror.netmonic.com/draft-ietf-l3vpn-ipsec-2547-02.txt, 2004.

[3] E S N Murthy, Bill Herbst. Implementing Effective Provider-provisioned VPNs[EB/OL]. http://www.eetasia.com, 2003-09.

[4] E Rosen, Y Rekhter. RFC 2547, BGP/MPLS VPNs[EB/OL]. http://www.ietf.org/rfc/rfc2547.txt, 1999-03.

作者简介:

任德玲(1976-),硕士研究生,研究方向为网络与信息安全;韦卫,联想研究院首席研究员,硕士生导师,研究方向为网络与信息安全、密码学。