第32卷 第22期 计 算 机 工 程 2006年11月
Vol.32 No.22 Computer Engineering November 2006
·网络与通信· 文章编号：1000—3428(2006)22—0133—03 文献标识码：A 中图分类号：TP393.02

虚拟专用网分类和比较研究

李 频，唐家益，陈丹伟，王海平
(南京邮电大学计算机学院，南京 210003)

摘 要：给出了一个比较好的VPN分类标准，提出了一个较为完整和系统的VPN系统分类图。在介绍每种VPN的基础上，阐述了对各种VPN特点的评价，并比较了MPLS VPN与IPSec VPN、IPSec VPN与SSL VPN的优缺点。
关键词：虚拟专用网；分类研究；比较研究

Study on Classification and Comparison of Virtual Private Network

LI Pin, TANG Jiayi, CHEN Danwei, WANG Haiping
(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003)

【Abstract】 This article puts a better classification criterion and a more integrated and systematic classification chart of VPN, emphatically evaluates the different VPNs after briefly discussing every VPN. Then the merits and drawbacks of several VPNs are compared in greater detail, including MPLS VPN and IPSec VPN, IPSec VPN and SSL VPN.
【Key words】 Virtual private network(VPN); Classification study; Comparison study

虚拟专用网(Virtual Private Network，VPN)是在2台计算机之间建立一条专用连接，通过附加的安全隧道、加密和密钥管理、用户认证和访问控制等技术实现与专用网类似的安全性能，达到在公共网络上建立虚拟的逻辑网络，从而安全传输私有的重要数据的目的。

从广义的角度来说，最早出现的VPN是通过拨号和专用的租赁线路互连用户网络设备而构成，其次出现的VPN是基于第2层数据链路的，如通过X.25广域网进行包交换构成VPN。帧中继(FR)和ATM交换的出现形成了FR/ATM VPN，它们更简单和费用低，但是存在设备昂贵、维护困难、难以推广等缺点。随着Internet可靠性和可用性的增强，它可以提供最廉价和普遍的广域网通信。然而与上述专用网相比，Internet不能提供相同的安全性、带宽及服务质量(QoS)保证，于是，一种具有二者优点、且运行在Internet之上的VPN技术——IP VPN成为近年来兴起和占主流的VPN技术。

1 VPN分类标准和分类

到目前为止，国际标准化组织、相关厂商和研究人员已提出多种IP VPN的概念和技术，但分类标准混乱。本文结合VPN技术的各个分支当前发展情况，提出了一个相对完整和系统的分类标准[1,2]，根据上述标准划分VPN得到的VPN系统分类如图1所示[1]。

(1)根据所利用的公共主干网是否是IP网，VPN分为Non-IP VPN和IP VPN。

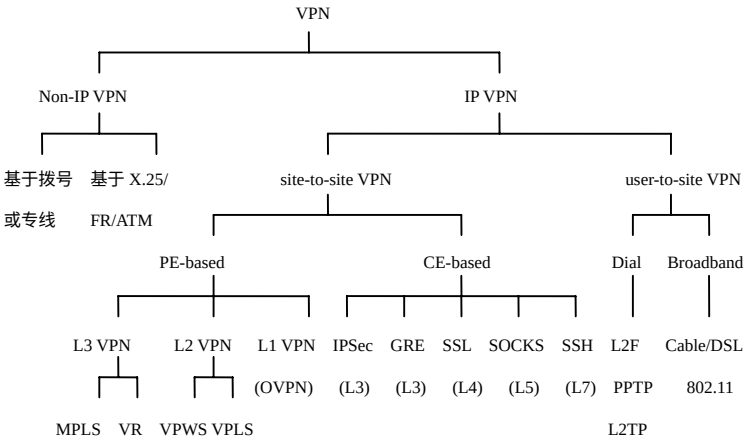
(2)根据所连接的VPN站点的类型，IP VPN分为site-to-site VPN和user-to-site VPN。

(3)根据提供商和用户维护VPN运作的责任，site-to-site VPN分为PE-based VPN和CE-based VPN。

(4)根据VPN所提供的服务在OSI模型中的层次，PE-based分为L3 VPN、L2 VPN和L1 VPN。

(5)根据VPN所使用的具体不同技术，CE-based分为基于IPSec、GRE、SSL、SOCKS、SSH的VPN。

图1 VPN系统分类



2 PE-based VPN

PE-based分为L3 VPN、L2 VPN和L1 VPN。其中L3 VPN和L2 VPN的主要差异为[3]：(1)L3 VPN的PE根据数据包的第3层路由信息(IP地址)来转发包；而L2 VPN的PE执行桥接功能而非路由功能，根据数据包的第2层信息来转发包；(2)L2 VPN基于第2层信息，故其扩展性不好；L3 VPN基于第3层信息，扩展性好，且易于和其它IP安全机制(防火墙等)配合使用；(3)L3 VPN只能用于IP网络；而L2 VPN对于多协议网络以及非IP网络也是合适的。

基金项目：国家“十五”科技攻关项目(2002BA811B04)
作者简介：李 频(1974－)，女，讲师，主研方向：网络信息安全；唐家益，教授；陈丹伟，副教授；王海平，讲师
收稿日期：2005-11-17 **E-mail：**lipin7421@163.com

2.1 L3 VPN

(1)MPLS 技术

由于 IP 技术和 ATM 技术在各自发展领域都遇到实际困难，彼此都要借助对方来进一步发展，因此这 2 种技术结合有必然性。多协议标签交换(MPLS)技术就是为了综合利用网络核心的交换技术和网络边缘的 IP 路由技术各自优点而产生的。MPLS 将灵活的三层 IP 选路和高速的二层交换技术完美地结合起来，从而弥补了传统 IP 网络的许多缺陷，为 QoS 提供了更可靠保证。MPLS 能够兼容各种主流网络技术，曾经被认为是数据通信领域内最有前途的网络解决方案之一。但由于 ATM 在技术界还处于一种争论状态，因此也会在一定程度上影响 MPLS 的发展。与 IPSec 不同，MPLS VPN 的安全性不是通过加密等手段，而是通过对不同用户间、用户与公网间的路由信息隔离实现，其安全性可以达到专线的水平，它能够替代使用 FR/ATM 建立 PVC 的方案，大大节约了成本。

(2)VR 技术

虚拟路由器(Virtual Router，VR)能提供物理路由器的所有功能，但实际上只是对物理路由器的软件仿真，一般作为 PE设备出现，但多个VR物理上可以在一个PE设备上共　存[3]。VR对路由和数据的转发采用了和物理路由器相同的机制，但是同一个PE上的不同VR必须维护独立的路由表，它们在逻辑上是隔离的，所以一个VR的操作不会影响同一个PE的其他VR。正因为VR是相互独立的，所以由不同VR所构建的不同VPN的地址空间可以相互重叠(即可以使用用户私有的IP地址)。与MPLS相比较，VR的优点是：概念清晰；结构灵活，便于业务扩充；可以使用标准的路由协议和策略机制支持一些附加业务(防火墙、NAT等)。其缺点是：支持大量VR时实现较为困难；不同运营商VR之间的互通比较繁琐；要求高性能边界路由器[4]。

2.2 L2 VPN

L2 VPN通过共享的IP或MPLS(主要是MPLS)包交换网络来传输第 2 层帧，使用几种不同隧道封装方案中的一种来穿越包交换网络。与L3 VPN相比，L2 VPN最重要的是保留了传统基于第 2 层专用网解决方案的优势，有利于它们向L2 VPN的平滑过渡，最大限度地为运营商节省网络升级的投资。L2 VPN技术可以实现多种链路仿真服务和 2 层链路技术的互通，实现真正意义上的多网合一[3,6]。L2 VPN可以分为如下 2 类：

(1)VPWS 技术

VPWS(virtual private wire service)被IETF定义为在IP和支持MPLS的IP网络上提供点到点面向连接的二层服务[3]。对于以太网而言，这种机制也被称为Ethernet over MPLS。如果提供商想在包交换网络上实现优于传统的FR/ATM PVC服务时，使用VPWS是合适的。

(2)VPLS 技术

VPLS(virtual private LAN service)被IETF定义为在IP和支持MPLS的IP网络上提供点到多点和多点到多点面向无连接的二层服务[3,5]。VPLS利用Internet来模拟局域网段，与VPWS相同，它仍然基于仿真虚电路的建立，增加了MAC地址学习、基于MAC的转发和包复制功能，使得从终端用户的角度看，像一个LAN交换机在提供服务。即使是多个企业通过同一个PE接入同一个骨干网络，它们的数据流在逻辑上也是相互独立的，充分保证了用户数据的机密性。对大多数运营商来说，目前其数据业务的主要来源还是传统的　第 2 层VPN。MPLS VPN作为一项新业务，在没有经验时贸然实施有很大风险。而基于MPLS的VPLS的出现是MPLS VPN技术的一个新亮点。VPLS当前面临的最大问题就是协议没有标准化，各厂商解决方案无法实现互通，造成VPLS需要大量手工配置，不适合组建大规模的网络。

2.3 L1 VPN

L1 VPN/OVPN(Optical VPN，光虚拟专用网)是目前最被看好的VPN业务之一。L1 VPN使运营商能将其光网络分成多个虚拟网络提供给多个用户，可提供区别于传统带宽型的业务[6]。L1 VPN具有资源共享的经济性、灵活性、可靠性和可扩展性等优势，VPN用户可以自己管理租赁的光网络资源，当然也可以委托给第三方管理。L1 VPN在网络第 1 层为CE提供TDM(时分多路复用)或OTN(光传送网络)连接。L1 VPN与L2/L3 VPN的不同之处如下：(1)L2/L3 VPN的连接可以是点到点或点到多点方式，而L1 VPN一般只提供点到点连接；(2)L1 VPN提供的业务都是面向连接的，而L2/L3 VPN提供的业务有面向连接和无连接 2 种类型；(3)L1 VPN可以提供严格的QoS和安全保障，而L2/L3 VPN只能提供相对的QoS和安全保障。L1 VPN适用于对网络传送资源需求量较大并对QoS和安全有严格要求的用户。

3 CE-based VPN

3.1 IPSec 技术

IPSec(IP Security)是一个由IETF IPSec工作组设计的端到端的确保IP层通信安全的协议集，包括安全协议部分和密钥协商部分[8]。IPSec通过在IP层提供安全保护，实现了对应用层的透明性，允许任何一个应用程序无需修改就可以充分利用其安全特性。IPSec是目前唯一能为任何形式的Internet通信提供安全保护的协议，已经成为Internet安全标准。但是IPSec不支持TCP/IP以外的其它网络协议，而且提供的访问控制方法也仅限于包过滤技术，并且只能进行地址认证。IPSec和MPLS不是互斥的，可以结合使用。服务提供商可以为需要较高认证和机密性的数据流实现IPSec，而为对带宽、流量工程和QoS有较高要求的数据流提供MPLS。MPLS VPN与IPSec VPN的比较如表 1 所示[7]。

表 1　MPLS VPN 与 IPSec VPN 的比较

选项	MPLS VPN	IPSec VPN
可扩展性	很强(便于维护大型网络)	一般(一个站点的改变可影响多个站点)
速度	快(高速二层交换)	较慢(三层 IP 路由)
配置	简单(不需配置 CE)，减轻用户管理负担	模式较多，比较难以掌握
与 NAT 兼容性	不需要进行 NAT(可以使用原来的私有地址)	往往存在问题，难以兼容
QoS	好(实现 DiffServ、流量工程等)融合多种业务	难以保证
普遍性	QoS 只能在一个 ISP 网段内保证、不能为远程拨号用户提供接入	支持全球范围内多种方式的接入
故障解决	对路由协议依赖性强、结合使用路由和交换，使故障更难以排除	对路由协议依赖性较弱
安全性	很好(可达到专线水平)	比较好(比 PPTP/L2TP 好)
安全机制	路由信息隔离，但明文传输数据，仍可能有漏洞	机密性、完整性、身份认证、抗重放攻击

3.2 GRE 技术

GRE 是通用路由封装协议，用于在 IP 包中封装任何协

议数据包(IP/IPX/NetBEUI 等),使得非 IP 数据包能在 IP 互联网上传送。虽然 GRE 隧道技术有很多优点,但由于它提出较早,存在着如下的一些缺点:(1)GRE 只提供了数据包的封装,而没有加密功能,因此经常与 IPSec 一起使用;(2)由于 GRE 与 IPSec 采用的是同样的基于隧道的实现方式,因此 IPSec VPN 在管理、组网上的缺陷,GRE VPN 也同样具有;(3)因为 GRE 是手工配置的,所以配置和维护费用与隧道数量直接相关,费用较高。GRE VPN 适用于一些小型点对点的网络互联、实时性要求不高、要求提供地址空间重叠的网络。

3.3 SSL 技术

随着Web的出现和具有安全套接层(SSL)加密功能的浏览器盛行,用户只要使用支持HTTPS(以SSL为基础的HTTP)的Web浏览器,可以方便地建立标准安全通道访问远程应用,这种基于SSL协议、可通过浏览器访问的VPN就是SSL VPN[10]。SSL VPN与IPSec VPN的最大不同是无客户端,因此大幅度减轻VPN系统管理员负担,成本也比IPSec VPN低很多。然而无客户端这一特性也使SSL VPN允许用户利用不安全的计算机访问企业网络。SSL VPN最适合下述情况:企业需要通过Web远程接入互联网;客户端与目标服务器之间有防火墙,允许HTTPS数据包通过,但不允许IKE或IPSec数据包通过;需要精细访问控制能力的场合。SSL VPN与IPSec VPN的比较如表 2 所示[10]。我们建议最佳的方案是:以IPSec VPN作为一般远程接入方案和点对点连接方案,辅以SSL VPN作为访问Web服务的远程接入方案。当前的一个研究方向是如何使IPSec VPN兼容于SSL VPN。

表 2 SSL VPN 与 IPSec VPN 的比较

选项	SSL VPN	IPSec VPN
身份验证	单向身份验证、双向身份验证、数字证书	双向身份验证、数字证书
加密	强加密、基于 Web 浏览器	强加密、依靠执行
全程安全性	端到端安全、从客户到服务器全程加密	网络边缘到客户端、仅对从客户到 VPN 网关之间的通道加密
可访问性	适用于任何时间、任何地点访问	适用于受控用户的访问
费用	低(无需任何附加客户端软件)	高(需要管理客户端软件)
安装	即插即用安装、无需任何附加客户端软硬件安装	通常需要长时间的配置、需要客户端软件或硬件
用户的易使用性	使用熟悉的 Web 界面,无需终端用户的培训	没有相应技术的用户比较困难,需要培训
支持的应用	基于 Web 的应用、文件共享、E-mail	所有基于 IP 协议的服务
用户	客户、合作伙伴用户、远程用户、供应商等	更适用于企业内部使用
可伸缩性	容易配置和扩展	在服务器端容易实现自由伸缩,在客户端比较困难

3.4 SOCKS 技术

虽然SOCKS在PPTP和IPSec以前出现,但早先SOCKS版本存在使用复杂、不安全等缺点,所以未受特别重视。SOCKS v5 纠正了以前版本的错误,不仅提供认证和数据完整性,还提供加密[11],并对这些技术提供插件式支持,使得SOCKS数据包能够安全透明地通过防火墙的防御。SOCKS v5 支持低层IPSec/PPTP/L2TP/PPP,由它们提供隧道封装功能。SOCKS v5 同时支持TCP和UDP,使得基于UDP的对实时性要求较高的流业务得以广泛使用。由于组成Extranet的各子网之间通常存在很大差异,因此Extranet VPN需要工作在足够高的层次以便充分屏蔽底层技术差别并实现互操作,而且VPN技术需要实现对应用层防火墙技术的兼容性,所以Extranet VPN最适合利用会话层以上技术实现,典型的就是采用SOCKS v5 技术实现(同SSL协议配合使用)。虽然SOCKS v5 提供强认证和访问控制方法,但整体性能较差,管理复杂,且推广使用较晚。但随着整体应用水平的提高,其使用前景还是看好。

3.5 SSH 技术

SSH,即 Secure Shell,是一种介于传输层和应用层之间的加密隧道协议,具有客户机/服务器的体系结构。SSH 可以在本地主机和远程服务器之间设置“加密隧道”,它可以跟常见的 FTP、SMTP、POP、X11 应用程序相结合,在非安全的网络上提供安全的远程登录和相应的网络安全服务,这就形成了一种应用层的特定的 VPN——SSH VPN。SSH 协议既可以提供主机认证,又提供用户认证,同时还提供数据压缩、数据机密性和完整性保护。从 SSH2.0 协议开始允许同时使用 PKI 证书和密钥,这样可以降低密钥管理的负担并提供更强大的安全保障。虽然 SSH 还有不足之处,但相对于其他 VPN 和专业防火墙的复杂性和费用来说,也不失为一种可行的网络安全解决方案,尤其适合中小企业部署 VPN 应用。

4 结束语

纵观各种 VPN 技术,我们认为具有良好发展前景的几种 VPN 技术是:MPLS(IP 和 ATM 的结合),VPLS(FR/ATM 等专用网向 L2 VPN 的平滑过渡),OVPN(利用光传送网提供严格的 QoS 和安全保障),IPSec(适用面最广的 IP 隧道协议),SSL(具有高层安全协议的优势)以及正在开发中的宽带和无线 VPN 安全协议。各种现有 VPN 技术的相互结合、取长补短更是未来 VPN 研究的发展方向。

参考文献

1 Metz C. The Latest in Virtual Private Networks: Part Ⅰ[J]. IEEE Internet Computing, 2003, 7(1): 87-91.

2 Carugi M, Jeremy De C. Virtual Private Network Services: Scenarios, Requirements and Architectural Constructs from a Standardization Perspective[J]. IEEE Communications Magazine, 2004, 42(6): 116-122.

3 Knight P, Lewis C. Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standardization Efforts[J]. IEEE Communications Magazine, 2004, 42(6): 124-131.

4 李秀忠. 基于 IP 骨干网的虚拟专用网理论与实现[J]. 中国工程科学, 2002, 4(3): 84-91.

5 蔡 鸣. 城域以太网体系标准、业务模型和新技术剖析[J]. 电信科学, 2004, 20(3): 12-17.

6 荆瑞泉. L1 VPN 业务和网络结构[J]. 电信科学, 2004, 20(7): 16-19.

7 李 博. 两种基于 IP 的 VPN 体系及比较[J]. 计算和工程与应用, 2002, 38(9): 154-156.

8 黎 静, 曾 华. 虚拟专用网(VPN)[J]. 计算机应用, 1999, 19(10): 26-29.

9 张羽佳, 黄本雄. 基于安全套接层协议的虚拟专用网[J]. 电信快报, 2005, (1): 36-39.

10 冯运波, 蔺新华, 杨义先. 虚拟专用网技术[J]. 电子科技导报, 1998, (8): 2-6.