中国科技资源导刊 ISSN 1674-1544
2008年9月 第40卷第5期 44-48
CHINA SCIENCE & TECHNOLOGY RESOURCES REVIEW
ISSN1674-1544 Vol.40 No.5 44-48,Sep. 2008

VPN技术在高校图书馆数字资源共享中的应用

薛 鹏
(山东大学威海分校图书馆,山东威海 264209)

摘 要:本文在简要介绍VPN技术和其工作原理的基础上,详细阐述了利用VPN技术组建高校图书馆资源共享虚拟专用网的可行性,实现方案及其存在的问题,并提出在高校图书馆应用VPN技术,能有效实现数字资源安全传递和有效利用,提升高校图书馆的服务能力。

关键词:VPN;数字资源;远程访问
中图分类号: G250.7 **文献标识码**: A DOI: 10.3772/j.issn.1674-1544.2008.03.008

The Application of VPN Technology in University Library Digital Resource Sharing

Xue Peng
(The Library of Shandong University at Weihai, Weihai 264209)

Abstract: This research paper introduces the Virtual Private Network (VPN for short) technology and its operational principles, and expounds how to use VPN technology to build the Virtual Private Network of Resource Sharing for University Libraries, so as to ensure the security and efficiency of digital resource transmission, and to enhance the service capacity of university libraries.

Keywords: VPN, digital resources, remote access

随着数字图书馆及其技术的发展,各高校图书馆的数字资源在文献中占有的比率不断提高。同时,读者也趋于网络化,数字资源成为其获取信息的重要来源。然而,数字资源本身具有的开放性和专用性特点限制了数字资源的利用。一方面,资源可以为广大师生员工共享;另一方面,资源只能在学校的局域网中使用,无法满足局域网以外的读者需求。如何使高校图书馆的数字资源综合化、开放化和社会化,达到优势互补、资源共享的目的,适应网络环境下读者需求的变化,充分发挥高校图书馆在地区发展中的作用,是我们亟待解决的问题。而通过VPN技术,我们可以实现处于不同地域、不同网络环境下的读者对数字资源安全有效的访问。

1 VPN技术

1.1 VPN的含义

VPN(Virtual Private Network)即虚拟专用

第一作者简介:薛鹏(1979-),男,助理馆员,研究方向是文献组织与采访。

收稿日期:2008年4月12日。

网。顾名思义，虚拟专用网不是真的专用网络，但能够实现专用网络的功能。虚拟专用网指的是依靠 ISP(Internet 服务提供商)和其他 NSP(网络服务提供商)，在公用网络中建立专用的数据通信网络的技术。在虚拟专用网中，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是利用某种公众网的资源动态组成。IETF(互联网工程任务组)草案对基于 IP 的 VPN 定义为，“使用 IP 机制仿真出一个私有的广域网”，通过私有的隧道技术，在公共数据网络上仿真一条点到点的专线技术。所谓虚拟，是指用户不再需要拥有实际的长途数据线路，而是使用 Internet 公众数据网络的长途数据线路。所谓专用网络，是指用户可以为自己制定一个最符合自己需求的网络，如图 1 所示[1]。

1.2 工作原理

通过 VPN 的定义可知，VPN 就是通过共享，即公用网络在两台机器或两个网络之间建立的点对点专用连接。实际上，VPN 技术使各馆或部门可以安全地通过 Internet 将网络服务延伸至远程用户、分支机构和合作单位，并保证数据的安全传输。点对点隧道协议(PPTP)数据包流通过专用线路传输。在 VPN 上，IP 数据包流是由一个 LAN 上的路由器发出，通过共享 IP 网络上的隧道到达另一个 LAN 上的路由器。这两者的不同点是隧道代替了实在的专用线路。隧道好比是在 WAN 中拉出一根串行通信电缆。用户只要接入 Internet，就可以用 Internet 来访问内部网络资源，如图 2 所示[3]。

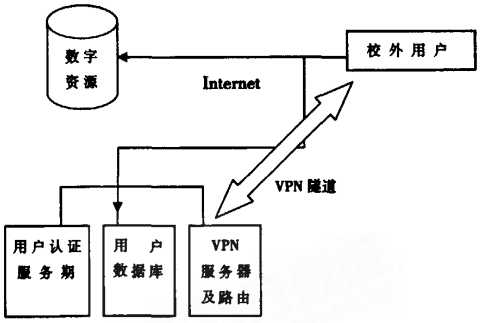

图 2 VPN 工作原理示意[3]

校外用户通过 ISDN、ADSL、CDMA 等网络接入方式向 VPN 服务器发出连接请求时，用户验证服务器对拨入的用户进行分析认证。如果用户的身份合法，则由 VPN 服务器与用户建立 VPN 隧道，服务器接受此连接，允许用户访问数字资源，通过隧道技术对传输的数据进行封装、加密，并传输给用户。

1.3 VPN 的应用领域及其发展情况

其实，VPN 技术并不是什么新鲜事物。早在 1993 年，欧洲虚拟专用网联盟 (EVUA) 成立，力图在全欧洲范围内推广 VPN。目前，VPN 可以通过多种方式如路由器、防火墙、操作系统和独立的加密设备等实现。国内外许多研究机构和国际标准化组织都致力于 VPN 标准的制定和推广，如 IETF 研制推出 IPSec, Cisco 推出 L2F, Microsoft 推出 PPTP 等。如今，VPN 的国际标准还未成熟，但基于 IPSec 的 IP VPN 逐渐被广泛看好。用于保障 QoS 的基于多协议标记交换 MPLS 的 VPN 方案也在不断完善中。由此可见，现在对 VPN 的研

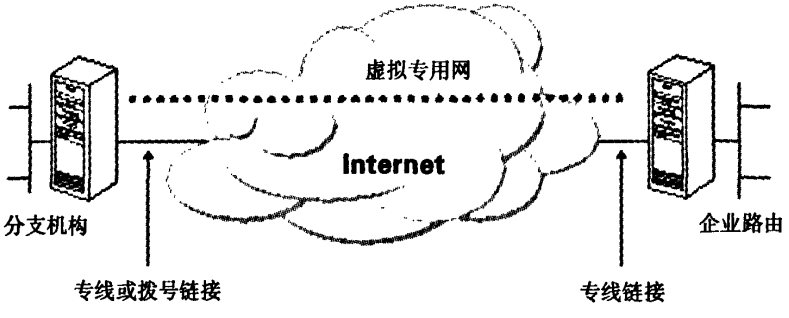

图 1 VPN 结构图[2]

究，正处在一个高速成长的阶段。在未来的几年里，网络应用的Web化趋势将得到延续，因此VPN的发展势头也将得到延续。基于IPSec的VPN是VPN发展的主流方向，安全VPN已成为计算机网络信息系统的重大发展方向之一[4]。

2 VPN的应用分类

在具体的应用中，VPN技术主要有基于纯软件平台、专用硬件平台和辅助硬件平台3种方法。

(1)纯软件平台VPN。当系统对数据传输速率、安全等性能要求不高时，可以利用一些知名公司（Citrix Avential Corp、Check Point Software等）基于纯软件的VPN产品来实现简洁的VPN功能。其中包括了VPN的应用软件、应用服务器和用户产品软件等，可以用于Linux、Windows NT/2003 Server等网络操作系统平台。

(2)专用硬件平台VPN。专用硬件平台具有较好的通信性能，可以提供便捷的服务，满足各类型用户对数据安全和通信性能的需求。常见的厂商有Cisco、Bay、Networks等。它们可以提供先进、完整的解决方案，功能齐全，且具有良好的可扩展性、灵活性、可靠性和可管理性。不过，价格比较昂贵。

(3)辅助硬件平台VPN。该类VPN平台性能介于前两者之间，基于现有网络设施，再添加适当的VPN软件或硬件，是性能最好、应用最多的一种。

3 高校图书馆组建VPN网络的可行性

3.1 用户需求

图书馆的数字资源在使用上不受时空限制，便于检索使用。然而，在具体的使用过程中，不论是图书馆的自建数字资源，还是购买的数字资源，考虑到安全使用及版权、授权等因素的制约，图书馆普遍都会对这些数字资源的使用加以限制，大多数的做法是限制IP的访问。即处于这个IP地址范围内的用户才能检索使用这些数字资源，IP地址范围以外的用户，服务器拒绝访问。随着学校的发展和高校图书馆社区化职能的不断扩展，越来越多的学校师生和社区读者迫切希望能够在学校以外的地方使用这些数字资源[5]。

3.2 VPN的技术优势

(1)可用性。虚拟网组成后，远程用户只需拥有本地ISP的上网权限，就可以访问图书馆内部资源，这对于多校区、多分馆以及实行馆际互借的图书馆来说很有意义，特别是当图书馆将VPN服务延伸到合作馆方时，便能极大地降低网络的复杂性和维护费用。

(2)安全保障。虽然实现VPN的技术和方式很多，但所有的VPN均保证通过公用网络平台传输数据的专用性和安全性。在非面向连接的公用IP网络上建立一个逻辑的、点对点的连接，称之为建立一个隧道，可以利用加密技术对经过隧道传输的数据进行加密，以保证数据仅被指定的发送者和接收者了解，从而保证了数据的私有性和安全性。

(3)可扩展性和灵活性。VPN能够支持通过Intranet和Extranet的任何类型的数据流，方便增加新的节点，支持多种类型的传输媒介，可以满足同时传输语音、图像和数据等新的应用对高质量传输以及带宽增加的需求。根据需要，可以随时增加或减少用户。

(4)费用低廉。VPN可以充分利用现有的网络资源，提供经济、灵活的联网方式，大大减少了网络维护和设备的费用。

(5)易于管理。从用户角度和图书馆的角度可方便地进行管理、维护。在VPN管理方面，要求管理者做好网络认证和授权工作。其他网络管理任务可以交给服务提供商去完成[6]。

4 图书馆基于辅助硬件平台VPN网络的实现方案

4.1 平台

考虑到数据安全、传输速率、方便管理、可扩充性以及费用等因素，采用辅助硬件平台VPN这种方式比较合理，可以大大减少维护和管理的成本。

4.2 基本要求

一般来说，图书馆在选用一种远程网络连接方案时，都希望能够对访问资源和信息的要求加以控制，所选用的方案应当既能实现授权用户与局域网资源的自由连接及不同分馆之间的资源共享，又能确保图书馆数据在公共互联网络或局域网络上传输时的安全性。因此，一个成功的 VPN 方案应当至少能够满足以下 5 方面的要求。

(1) 用户验证。VPN 方案必须能够验证用户身份并严格控制，只有授权用户才能访问 VPN。另外，方案还必须能够提供审计和计费功能，显示何人在何时访问了何种信息。

(2) 地址管理。VPN 方案必须能够为用户分配专用网络上的地址，并确保地址的安全性。

(3) 数据加密。通过公共互联网络传递的数据必须经过加密，确保网络其他未授权的用户无法读取该信息。

(4) 密钥管理。VPN 方案必须能够生成并更新客户端和服务器的加密密钥。

(5) 多协议支持。VPN 方案必须支持公共互联网络上普遍使用的基本协议，包括 IP、IPX 等。以点对点隧道协议 (PPTP) 或第 2 层隧道协议 (L2TP) 为基础的 VPN 方案既能够满足以上所有的基本要求，又能够充分利用遍及世界各地的 Internet 互联网络的优势[7]。

4.3 实现过程

(1) 创建 PPP 链路。PPP 使用链路控制协议 (LCP) 创建、维护或终止一次物理连接。在 LCP 阶段的初期，将对基本的通讯方式进行选择。应当注意在链路创建阶段，只是对验证协议进行选择。同样，在 LCP 阶段还将确定链路对等双方是否要对使用数据压缩或加密进行协商。

(2) 用户验证。客户端 PC 将用户的身份证明发给远端的接入服务器。该阶段使用一种安全验证方式避免第三方窃取数据或冒充远程客户接管与客户端的连接。大多数的 PPP 方案只提供了有限的验证方式，包括口令验证协议、挑战握手验证协议和微软挑战握手验证协议。

(3) PPP 回叫控制。微软设计的 PPP 包括一个可选的回叫控制阶段。该阶段在完成验证之后使用回叫控制协议 (CBCP)，如果配置使用回叫，那么在验证之后远程客户和 NAS 之间的连接将会被断开。然后由 NAS 使用特定的电话号码回叫远程客户。这样可以进一步保证拨号网络的安全性。NAS 只支持对位于特定电话号码处的远程客户进行回叫。

(4) 数据传输阶段。一旦完成上述 4 阶段的协商，PPP 就开始在连接对等双方之间转发数据。每个被传送的数据包都被封装在 PPP 包头内，该包头将会在到达接收方后被去除。如果在阶段 1 选择使用数据压缩并且在阶段 4 完成了协商，数据将会在传送之前进行压缩。类似地，如果已经选择使用数据加密并完成了协商，数据 (或被压缩数据) 将会在传送之前进行加密[8]。

4.4 实际应用

VPN 结构主要由两部分组成：身份认证服务器和 VPN 服务器。身份认证服务器运行在一台独立的服务器上，主要提供用户身份验证及权限管理、流量控制和日志记录等功能。VPN 服务器主要是由一些路由器、软件等组成，为服务器与远程客户之间建立隧道，完成加密、解密，并实施访问控制策略。用户首先通过 Web 页面登入身份认证服务器进行身份验证，认证成功提交证书申请请求，获得数字证书。验证成功后就可以与 VPN 服务器建立起 VPN 隧道连接，此时远程用户就可以使用 VPN 服务器分配的 IP 地址访问图书馆资源。在实际使用中，本地用户是不需要登陆身份认证服务器的，而是直接由 VPN 服务器来判定其身份的合法性。这样做可以减轻服务器的负荷，同时也便于分类管理。另外，我们也可以把数字证书和用户名进行绑定，即同一数字证书只能使用特定的用户名进行登陆，从而进一步增强了该系统的安全性。VPN 网络的结构见图 3[9]。

5 高校图书馆在 VPN 建设中存在的问题

5.1 版权问题

数字图书馆的版权问题不容忽视，不管什么

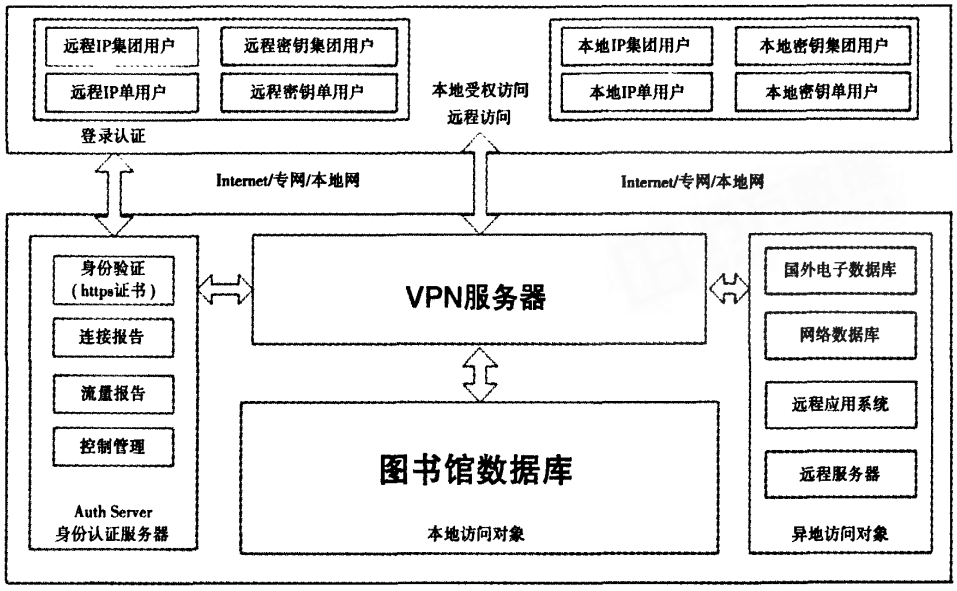

图3 VPN网络结构图[9]

类型的数字资源，都要遵循数字版权保护的规定，通过安全和加密技术控制数字内容及其分发途径，防止对数字产品非授权使用。

5.2 跨运营商网络互联问题

对于高校图书馆来说，大量校外用户采用电信、网通提供的ADSL等上网线路，其直接访问教育网资源的速度并不理想，如果使用有多线路智能选路这个功能的网关，图书馆仅需向其运营商申请一条普通线路（如ADSL），即可实现校外用户的高速访问。

5.3 安全问题

信息访问的安全性对系统来说非常重要。图书馆在数字资源共享时，必须有效控制用户的下载流量，防止恶意下载。有效利用VPN网关和认证服务器的功能，随时监控异常登陆的用户，防止黑客的攻击。

参考文献

[1] 高海英，薛元星，等. VPN技术[M]. 北京：机械工业出版社，2004：2－11.

[2] 51cto.com. 虚拟专用网VPN[EB/OL]. [2008－04－12]. http://network.51cto.com/art/200702/39583.htm.

[3] 刘宇翔. 基于VPN的图书馆系统研究[J]. 科技资讯，2006(21)：106－107.

[4] 刘卫国，楼佳. VPN技术在高校图书馆的应用[J]. 图书馆工作与研究，2007(6)：39－41.

[5] 陈秋萍. VPN技术在图书馆的应用实现[J]. 图书情报，2007(10)：65－66.

[6] 51cto.com. VPN纵横概念[EB/OL]. [2008－04－12]. http://network.51cto.com/art/200702/39501.htm.

[7] 曾巧红，徐文贤，林绮屏. 基于SSLVPN的图书馆远程访问系统的构建[J]. 情报科学，2007(10)：1520－1524.

[8] 张文丰. VPN技术在档案信息化中的应用[J]. 科技资讯，2007(25)：100.

[9] 北京英富森信息技术有限公司. 远程访问与移动办公解决方案[EB/OL]. [2008－04－08]. http://www.infcn.com.cn/company.asp?bigid=37&id=43.