文章编号:1008-0570(2010)07-3-0107-02

SSL VPN 技术在高校图书馆数字资源中的应用

Application of SSL VPN in Digital Resources of University Library

(牡丹江师范学院图书馆) 付凯东
FU Kai-dong

摘要: 针对我国高校目前提供的远程访问图书馆数字资源服务远远不能满足用户需求日益增加的现状，为解决多校区高校的校区间及校外用用户图书馆数字资源共享问题，本文提出了采用基于 Web 方式的 SSLVPN 技术来实现校区间的信息资源共享。旨在应用 SSL VPN 技术更好的提高我国高校远程访问图书馆数字资源的服务能力,从而满足更多用户远程访问图书馆数字资源的需求,提升高校图书馆的服务质量和工作效率。

关键词: SSL VPN 技术; 远程访问; 数字资源
中图分类号: TP393 **文献标识码:** A

Abstract: For the service that remote access to digital resources of library provided by universities in our country is far from the increasing demands,,research on SSL VPN and its application which is a remote access technology growing maturity use SSL VPN to improve the capabilities of remote access to digital resources of library in universities,to meet the demands to remote access to digital library resources of many users.

Key words: SSL VPN; Remote access; Digital Resources

技术创新

引言

为了更好满足教学、科研和学科建设对信息资源的需求,高校图书馆斥巨资购买的数字资源也越来越多。但数据库商为保护自己的知识产权,一般都要求高校图书馆只向校园网 IP 范围之内开放，这就造成了大量不在校园网范围内的合法用户无法利用图书馆的数字资源。图书馆虽然可以通过电话拨号或专线来建立局域网,但专用线路的实施也加大了投资负担,而通过校内专用拔号网络上网速度又太慢,严重影响用户信息检索效率。近十年来,远程访问图书馆数字资源服务在美国、英国、澳大利亚等国家已开展了相当多的研究，相关技术及解决方案应用也已经非常广泛，我国高校图书馆也越来越重视提供数字资源的校外访问服务。目前比较典型的远程访问图书馆数字资源技术有 VPN、传统代理服务器和地址重写代理服务器。新兴的 SSL VPN 技术非常适合移动用户的远程接入访问,因此探讨如何应用 SSL VPN 技术,提高我国高校远程访问图书馆数字资源能力具有实际意义。

1 SSL VPN 技术的内容与特点

1.1 什么是 SSL VPN?

VPN(Virtual Private Network 虚拟专用网络)是一种网络新技术,它利用公共网络基础设施,通过加密、认证、封装以及密钥交换技术在公网上开辟一条隧道等手段达到类似私有专网的数据安全传输。它提供了一种通过公共网络安全地对单位内部专用网络进行远程访问的连接方式,是一种逻辑上的、虚拟的专用网路。这种虚拟的专用网络技术可以在一条公用线路中为两台计算机建立一个逻辑上的专用“通道”,它具有良好的保密和不受干扰性,使双方能进行自由而安全的点对点连接。

SSL VPN 是 VPN 的一种。SSL(Secure Sockets Layer,安全套接层协议层)是一种基于 Web 应用的安全协议,它指定了在应用程序协议(如 HTTP、Tel-net、FTP 等)和 TCP/IP 协议之间进行数据交换的安全机制,为 TCP/IP 连接提供数据加密、服务器认证以及可选的客户机认证。SSL 也是一种网络上最普遍使用的安全通讯协议,保障服务器与客户端之间的数据传输的安全性。通过使用这个协议,网络上的数据传输会按照认证的种类(40 位、128 位)进行不同程度的加密,更会检查资料的完整性。这种安全措施犹如自己的钥匙般,可以锁住资料,也就是密码加密的过程,而且必须经过授权之后方可认证。使用 SSL 可保证信息的真实性、完整性和保密性。一个最基本的 SSL VPN 由两部分组成—客户端浏览器和 SSLVPN 网关。客户端浏览器利用 SSL 技术加密访问请求,发送到 SSLVPN 网关,网关将接收到的加密信息解密后再转发到内网中的 Web 服务器，从而在 Internet 上形成客户端到 SSL VPN 网关之间的加密隧道。在实际应用中，利用 SSL VPN 技术,校外用户在直接使用浏览器接入校园网络,当校外用户通过鉴权后,SSL VPN 网关会给远程用户分配一个校园网虚拟 IP 地址,从而实现远程用户以校园网用户身份访问数字图书馆资源。

1.2 SSL VPN 的特点

SSL VPN 具有虚拟的特点,VPN 并不是某个单位专有的封闭线路或者是租用某个网络服务商提供的封闭线路，但具有专线的数据传输功能,这是因为 VPN 能够像专线一样在公共网络上处理自己单位的信息。首先,SSL 是一个安全协议,数据是全程加密传输的,由于 SSL 网关隔离了内网服务器和客户端,只留下一个 Web 浏览接口,从而客户端受外界木马、病毒感染、黑客攻击的可能性大大减小;其次,在大多数执行基于 SSL 协议的远程访问是不需要在远程客户端设备上安装软件，只需通过标准的

付凯东: 副研究馆员

Web 浏览器连接因特网,即可以通过网页访问到图书馆的网络资源;另外,由于基于 SSL 的远程访问使用 NAT(网络地址转换)服务,所以远程用户或者因特网代理服务的用户可以绕过防火墙和代理服务器进行访问图书馆资源,这是采用基于 IPSec 安全协议的远程访问很难或者根本做不到的。

2 SSL VPN 的应用

2.1 SSL VPN 的部署

SSL VPN 一般部署在内网中防火墙之后,要依据安全控制策略为分散、移动的用户提供从外网访问图书馆内网资源的安全访问通道。一般的方式是图书馆内部的资源服务器向外网用户提供一个虚拟的 URL 地址,当用户从外网访问图书馆内网资源时,发起的连接被 SSL VPN 网关取得,而 SSL VPN 网关则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,通过认证后映射到不同的应用服务器。

根据高校的具体情况(绝大多数校外用户为公网用户),我们可以选择带有 SSL VPN 功能的 CiscoASA5510 设备架设在策略分流交换机和公网之间。具体实施方案是:利用 CiscoASA 5510 建立 Web VPN 服务器,由一台 Radius Server 服务器验证用户身份,校外用户只需要通过当地的 ISP 接入 Internet 再连接到 Web VPN 服务器并进行身份验证,验证合法后就可以访问校园网的图书资源。CiscoASA5510 部署后的网络拓扑结构如下图所示。ASA5510 一端(外网口)与 ChinaNet 相连,配置公网 IP 地址,使校外用户可以访问它,另一端(内网口)与策略分流交换机相连,配置校园网 IP 地址,保证它能与 Radius Server 服务器通讯来验证用户身份,通过验证的用户将被分配一个校园网的 IP 地址,就可以访问资源服务器群了。

ASA5510 部署后的网络拓扑结构

2.2 SSL VPN 关键配置介绍

利用 CissoASA5510 提供的 SSL VPN 功能建立一个基于 Web 的 VPN 服务器,对 SSL VPN 的接口地址、网关和 DNS 等基本配置进行初始化的设置。接下来就是配置 SSL VPN 设备以达到共享图书资源的目的,这里只介绍几个关键的配置。

2.2.1 添加用户认证服务器 由于只能允许属于高校的教师和学生作为合法的校外用户,因此我们要求提供用户名和密码来进行身份的确认,权限包括用户的并发数和 SSL VPN 的使用期限。Cisco ASA5510 支持多种身份认证协议,管理员可以选择使用 SSL VPN 内部的自建帐号认证用户,也可以结合单位内部的认证服务器进行认证,在此采用 Radius 认证协议,它的配置如下所示:

```
# 启用 radius 协议认证
aaa-server aaa-radius protocol radius reactivation-mode depletion deadtime 3
# 配置 radius 服务器的 IP 地址和使用的 key (这里假设为 123456)
aaa-server aaa-radius hostXXX.XXX.XXX.XXX
key 123456
authentication-port 1812
accounting-port 1813
radius-common-pw 123456
# 配置 VPN 组使用 radius 协议并应用于内网口
tunnel -group Default Wt EBVPN Group general -attributes
authentication-server-group aaa-radius
authentication-server-group ( inside) aaa-radius
```

2.2.2 添加访问资源和内网资源 在资源管理里面添加相应的 APP 资源或 Web 资源。在"Name"栏填入自己想要的名字,例如"学术期刊网";在"Description"栏填入相关的描述;在"URL"中填入访问网站的 IP 地址或是主机域名,例如我校学术期刊网的内网地址"http://10.1.136.24"。接着"Auto-allow Bookmark"和"Everything under this Url",然后保存后学术期刊网的远程访问条目就添加完成。

2.2.3 设置用户角色管理 对用户或用户组建立不同权限的角色,然后和图书资源关联起来。使不同角色的帐号登陆 SSL 之后,即可访问相应角色所具有权限的内网资源。由于采用 Radius 协议进行身份认证,所以用户的建立和管理是由 radius 服务器来完成的,而 ASA5510 本身不需要建立本地用户,这样降低了用户管理的工作量。

2.2.4 远程用户访问方式 由于学校 CiscoASA5510 的外网口与公网相连,所以外网口的 IP 地址就是对外提供 Web VPN 的地址。校外用户在能访问 Internet 的前提下,在 IE 浏览器的地址栏中输入内网地址后,就会出现 SSL VPN 服务的界面,输入用户和密码,认证通过后就可以获得校园网的 IP 地址,并访问图书馆资源。

3 对 SSL VPN 的分析总结

3.1 用户使用简单、方便 SSL VPN 无需安装任何特殊客户端软件,仅需要一个 Web 浏览器,比如常见的 Internet Explorer,只要打开浏览器链接 VPN 服务器网址,就可以自动建立 SSL VPN 通道。

3.2 用户管理简便、快捷 图书馆远程访问系统用户数据量大、变化频繁,因此要求能快速地添加和修改用户信息。SSL VPN 的优势就在于它与网络层无关,在添加用户或改变用户信息时相对快速和容易,VPN 管理员只要许可新用户的用户名和密码(或者其它认证机制),并提供 VPN 网关的 Web 地址就可以了。

3.3 适应性、兼容性好 图书馆的远程访问用户分布在不同的地域中,网络环境呈多样化,而图书馆很难去更改用户网络防火墙的设置,这就要求图书馆的远程访问系统必须具有很好的穿透防火墙、代理服务器的能力,能提供无障碍的远程访问连接。适用大多数设备及不同的操作系统,图书馆的远程访问系统必须适用于任何的终端及操作系统,这样才能最大限度地满足不同的用户需求。SSL VPN 一般部署在内网中防火墙之后,可以随时根据需要,添加需要 VPN 保护的服务器,因此如果增添新的设备无需影响原有网络结构。

3.4 完善的资源访问控制 SSL VPN 提供的基于 Web 的代理访问方式,允许为远程访问用户进行详尽的资源访问控制,即根据用户的不同身份,给予不同的访问权限,这为图书馆不同用户类型,使用的不同的网络资源,实现用户分组与资源绑定功能提供可能。依据安全策略确保只有授权的用户才能够访问特定的内部网络资源。

(下转第 117 页)

技术创新

都在升高,但从图 3 中可以看出,由于改进的 QEM 算法综合考虑用户请求的时效性,其成功率要高于 QEM 算法。

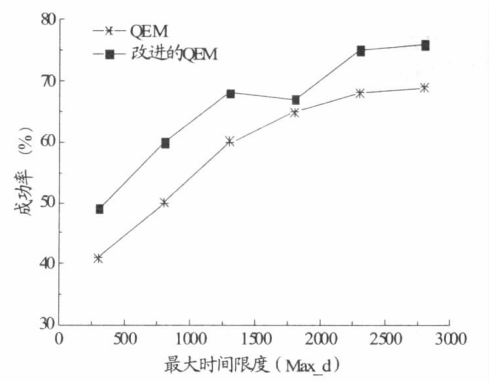

图 4 时间限度对成功率的影响

图 4 通过用户请求的不同最大时间限度,对 QEM 算法以及本文改进的 QEM 算法在成功率方面进行了比较。随着时间限度的增加,成功率都在升高。同样由于改进的 QEM 算法考虑到了用户请求的时效性,其成功率要高于 QEM 算法。

根据图 3 与图 4 可知,改进后的 QEM 算法在成功率方面要越于 QEM 算法,提高了多数据项请求的时效性。

6 结束语

本文综合考虑了用户请求的时间限制、访问概率以及未调度的数据项个数对成功率的影响,对多数据项请求的 QEM 算法在广播内容选择上进行了改进,提高了多数据项请求广播的时效性。

在下一步的研究工作中,将对用户请求超过截止日期失败时,服务器对该用户请求如何处理做进一步的研究。

本文作者创新点:对广播内容的选择进行了研究,提出了新的广播内容选择方式,并对多数据项请求广播调度算法 QEM (Query Extend Method) 进行了改进。试验结果表明改进后的算法进一步提高了多数据项请求广播的时效性。

参考文献

[1]Imielinski T., Badrinath B.R. Wireless mobile computing: challenge in data management. Communications of the ACM, 1994,37(10): 19–28

[2] 邵雄凯,郭卫华,李莉. 移动数据库中数据更新与广播的并发控制[J].微计算机信息,2003,23(12):177–179.

[3]Lee G L., Lo S.C. Broadcast data allocation for efficient access of multiple data items in mobile environments. Mobile Networks and Applications, 2003,8(4):365–375.

[4]Yuen J.C.H., Edward C., Lam K. Adaptive data broadcast strategy for transactions with multiple data requests in mobile computing environments. Proceedings of the 6th International Conference on Real–Time Computing Systems and Applications, Washington, USA: IEEE press, 1999:376–448.

[5]Chung Y.D., Kim M.H. QEM: a scheduling method for wireless broadcast data. Proceedings of the 6th Int Conf on Database Systems for Advanced Applications, Washington, USA: IEEE press, 1999:135–142.

[6]Chang Y.I., Hsieh W.H. An efficient scheduling method for query–set–based broadcasting in mobile environments. Proceedings of the 24th International Conference on Distributed Computing Systems Workshops.2004:478–483.

作者简介:李庆文(1966–),男(汉族),湖南郴州人,郴州职业技术学院,讲师,研究方向为移动数据库技术。

Biography:LI Qing–wen (1966–), male (Han nationality), Hunan, Chen Zhou Polytechnic, instructor, Research area is mobile database.

(423000 湖南郴州 郴州职业技术学院) 李庆文

(Chen Zhou Polytechnic, Hunan Chenzhou 423000, China) LI Qing–wen

通讯地址:(423000 湖南省郴州市曹家坪 45 号郴州职业技术学院学生处) 袁 菲 转 李庆文

(收稿日期:2009.08.20)(修稿日期:2009.11.20)

(上接第 108 页)

3.5 良好的安全性 有效防止病毒、黑客入侵。SSL VPN 只开放 443 端口传输数据,所以黑客不易侦测出系统内部的网络结构,内部网络受攻击的机会将大大减少,同时病毒从远程客户端入侵的可能性也会大大降低。其安全性包含 3 层含义:一是客户端接入的安全性;二是数据传输的安全性;三是内部资源访问的安全性。

4 结语

据估算,如果放弃租用专线而采用 SSL VPN 整个网络的成本可节约 21% ~45%,相对于以电话拨号方式联网存取数据,采用 SSLVPN,则可以节约通讯成本 50% ~80%。总之,由于费用低廉、安全、可靠、灵活性大等特点,使 SSL VPN 技术成为目前高校图书馆为所有非校园网的师生提供资源共享的最理想的方案,SSL VPN 在真正意义上达到随时、随地、随需访问查询,使图书馆所购数字资源得到更充分利用,提高文献资源检索效率。SSL VPN 技术本身所具备的优势,使得它在高校的数字文献资源建设乃至高校信息化建设中都会发挥十分重要的作用。

本文作者创新点:将 SSL 与 VPN 技术相结合应用于高校校外用户远程访问图书馆数字资源,为用户提供更方便、快捷、安全的访问图书馆的途径与方式。

参考文献

[1]张杨,乐红兵.开放分布式资源系统中 Web Services 的研究与应用[J]微计算机信息,2009,09–3:56–58

[2]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.

[3]高国奇. SSL 安全传输技术的探索应用实践[J].中国金融电脑,2007,03 :19–25.

[4]陈麟,林宝刚,李焕洲.基于电子钥匙的远程访问 VPN 身份鉴定方案[J] 微计算机信息,2009,02–3:123–124.

作者简介:付凯东(1969),女,黑龙江牡丹江人,牡丹江师范学院图书馆副研究馆员 ,研究方向为图书馆信息资源建设。

Biography:FU Kai–dong (1969),female,Mudanjiang Heilongjiang, a assistant researcher of Mudanjiang Normal University Library. Research area:Library information resources.

(157012 黑龙江牡丹江 牡丹江师范学院图书馆) 付凯东

(Mudanjiang Normal University Library .Mudanjiang 157012, China) FU Kai–dong

通讯地址:(157012 黑龙江省牡丹江市兴中路文化街 19 号牡丹江师范学院图书馆) 付凯东

(收稿日期:2010.05.31)(修稿日期:2010.07.15)