ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.18, No.28, October 2022
E-mail: jslt@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

VPN技术在校园网络安全体系中的应用研究

高淑光

(烟台职业学院,山东 烟台 264670)

摘要:随着信息科技水平的持续提高,校园网络系统成了学校现代化信息技术建设的基础平台。一方面,校园网络系统为学校的教学、科研、管理等工作提供了相应的服务;另一方面,很多学校在不同地区开设了分校区,为了能够更完全地将各校区之间的网络连接起来,在校园网络安全体系中,必须开展VPN技术的应用。本文将全面阐述VPN技术的基本概念、主要工作原理,以及当今校园网络发展中普遍存在的安全问题,探析VPN技术在校园网络安全体系中的应用原则、需求分析以及应用设计。

关键词:VPN技术; 校园网; 安全体系; 连接; 应用

中图分类号:TP393 **文献标识码:**A

文章编号:1009-3044(2022)28-0063-03

DOI:10.14004/j.cnki.ckt.2022.1812

开放科学(资源服务)标识码(OSID):

21世纪以来,信息技术的发展以前所未有的速度从各个方面影响着人们生活,校园网络系统的建设也成了学校信息化技术发展的关键点。校园网络的有效应用,可以让教师和学生更好地开展教学工作,更方便地查阅电子数据资料。同时,学校规模正在不断地扩大,很多学校在不同省份或是同省不同市之间开设起了分校,为了确保能够有效对各个校区的网络安全进行统一规范的管理与远程控制,VPN技术应该被应用到整个校园网络安全体系的开发与建设中。VPN技术的应用不仅可以随时随地为学校教职工提供教学服务,解决各校区之间的网络访问限制问题,还可以完善校园网络的开发体系。

1 VPN的概念及工作原理

1.1 VPN的概念

VPN全称虚拟专用网络(Virtual Private Network)。一般来说VPN是由客户机、服务器、传播媒介组成的,是利用专门的隧道将专用网络与公共网络进行连接,来最终实现服务器与客户机的连接[1]。利用VPN进行网络连接,用户不必拥有实际的数据线路,只是通过公共网络就可以构建一个有针对性的虚拟的专用网络。VPN技术存在多种分类方法,一种是协议分类法,可以分为PPTP、L2TP与IPSec,也可以按应用将VPN技术分为Intranet VPN、Access VPN、Extranet VPN[2]。在校园网络中对于VPN技术的应用,是将校园网和公网连接,构建专用网络,从而为校职工以及学生提供如教职工在家办公、在校外访问学校图书馆查询资料等一系列的远程服务。

1.2 VPN的工作原理

VPN技术主要是通过三道防护屏障,来确保网络连接的安全性,它们分别是身份验证、数据加密以及隧道协议。工作原理:首先是数据请求方将需求发到VPN服务器上;然后,VPN服务器收到来自请求方的需求,就会通过特殊的方式来验证请求方的身份,如果数据请求方拥有远程访问的权限,那么VPN服务器将会响应请求。此外,在数据传输过程中,数据发送方还需要加密数据需求方的身份认证,让传送数据的加密状态得到保障。拆除、保持以及建立数据传输的渠道是隧道协议的3项主要工作[3]。

现阶段主要有两种方式的VPN连接,拨号VPN和专线VPN。拨号VPN主要是为VPN用户提供同一个网络内部的远程访问,主要运用的协议有PPTP协议和L2F协议。专线VPN指的是VPN的终端服务器通过专门的隧道与公共网络产生连接,这种连接方式一般需要提供静态的IP地址[4]。

2 校园网络存在的安全问题

随着信息化技术的不断进步,各大高校为学校教师和学生提供了越来越多的信息化服务,信息化门户的服务也日趋成熟,学校的日常工作已离不开校园网络。但即便如此,校园网络也面临着一些安全问题。

2.1 外网入侵与攻击

校园网络为了方便教学工作的顺利展开,开放性

收稿日期:2022-03-10

作者简介:高淑光(1969—),男,山东烟台人,实验师,主要研究方向为计算机与网络。

很强，可以直接和互联网相连，这就意味着校园网络有可能会受到网络攻击。企业网通常会限制与企业无关或是病毒网站的网页浏览，拒绝外部网页的访问请求。校园网络做不到企业网络的这一点，所以就让有些不法分子有机可乘。这些人通过在网络上攻击校园网络，非法入侵校园网来获取校园资源、破坏学校系统、窃取机密文件、删改数据信息等，破坏校园网的安全运行。

2.2 存在病毒与网络漏洞

大多数校园网计算机运用的是Windows系统，且很多学校没有及时进行版本更新，还在使用Windows系统低版本。这种网络环境下，存在很多安全隐患。防火墙、服务器、tcp/ip协议等都有可能引发校园网络的安全问题，计算机病毒往往会通过这些安全漏洞来攻击校园网络。同时，校园网络中的影音视频、软件等被反复下载，不仅占用网络资源，还常常携带木马病毒。这些病毒具有很强的传染性以及破坏性。一旦入侵校园网络，容易造成系统崩溃、文件丢失，还容易引来非法入侵。

2.3 校园网络技术更新速度慢

很多学校可能会因为经费的问题，忽视校园网技术的迭代更新。比如说当我们访问学校系统时，如果使用最新的Windows版本，将出现访问失败，要求将Windows系统调到低版本才可以登录学校的系统。使用老版本，往往限制了校园网络访问的速度，也容易让病毒入侵。另外，现在很多学校推出了校园微信公众号，信息化门户系统不仅可以在电脑上操作，也可以在手机上操作，但是由于校园网络的维护不是很及时，经常会发生访问不成功、速度卡顿或者出现闪退等现象。

3 VPN技术在校园网络安全体系中的应用

3.1 VPN技术的应用原则

如果想要在校园内通畅地使用VPN技术，了解校园网络的需求以及应用原则是必需的工作事项。VPN技术的主要应用功能模块有4个，如图1所示。1) 后台管理模块：建立VPN后台主要是对VPN技术服务器的访问记录进行收集，然后根据收集的记录内容，整理和总结用户的访问情况、行为习惯等。2) 浏览控制模块：这个模块主要是整合VPN浏览与控制的方案，保障系统设定的正确性，给客户提供精准性服务。3) 身份验证：网络两端用户（数据发送端、数据请求端）的身份认证方式是不一样的，数据发送端的验证，在校园内网中运用数字认证技术进行验证；而对数据请求端的验证，是在外网中利用用户名以及用户密码，来达到验证效果。4) 数据传输模块：是VPN技术应用的核心模块，主要是提供加密数据以及转发数据的服务。

图1 VPN技术的主要应用功能模块

3.2 VPN技术的需求分析

据调查，VPN技术不断地在我国各大高校引起关注，尤其是2020年初爆发肺炎疫情以来，更是加剧了校园网络对VPN技术的需求。学校对于VPN技术的应用需求几乎都是相同的，大致可以归纳为下面几类：1) 电子数据资源的需求。学校图书馆或是个别院系为了教学科研需求，都会购买文献数据库资源，如中国知网、国外期刊数据库等，这些数字资源的服务器并不在校内，为了保护数据的安全性，大多网站会严格限制访问的IP地址，也就是说只有在校园网的条件下才能够访问网站并下载数据。疫情管控期间，学校师生不能随意进出校园，不能下载这些资源做教学科研工作，为了使广大师生在校园外也能访问这些网站，很多高校推出了远程访问的VPN技术。2) 满足师生在校外对校内网站的远程访问。根据业务需求，学校各部门会开发各自的业务系统，如教务系统、选课系统、就业系统、教学管理系统等。部分系统对外开放，无论校外或是校内，只需要教师或学生输入统一身份认证即可登录，但也有部分系统安全等级要求较高，只能够在校园网环境下才可以操作，在校外操作时，就需要接入VPN技术，同时输入统一身份认证后才可以访问。当各学校开设网上课程学习时，师生只能在家访问学校网站，通过VPN网络，可以使广大师生顺利地访问学校的系统，开展教学工作。3) 满足各校区之间的互相访问。由于学生人数变多以及经济发展等多方面的原因，很多学校建立了好几个校区，这些校区分布在各个地区。但各个校区不仅使用同一个校园局域网，还需要对各校区的邮件站点以及网页站点进行统一的管理。为了满足各校区之间的便捷且快速的互相访问，同时也为了对分校区实施更好的安全管控，VPN技术的开发与应用必不可少。

3.3 VPN技术的应用设计

3.3.1 各校区构建校园内部虚拟专用网

学校的各个校区因为拥有其特有的共享网络设施，各校区之间可以运用Intranet VPN技术（即网关到网关）将相互间的网络连接在一起。对于Intranet VPN技术的应用，首先，在学校的每个校区使用相同

供应商的公共网络连接(比如中国电信、中国移动等),设置其中一个校区为主校区,网络出口的设置要在主校区内;其次,学校为了要保证网络的安全性,采用IPSec VPN技术可以确保数据信息是在加密的状态下被传输,这样就充分保障了数据信息是在安全的环境下进行传播。

对于那些要求安全性比较高的系统访问,比如教务部门、财务部门、学校一网通等,二层协议网络隔离的技术被较多地使用,其步骤是校园网络接收到用户请求后,利用二层OSPF协议在校园网络的核心交换机中完成数据的传输,并实现各个校区间数据的安全传输。而对于普通型用户的访问,对安全的要求等级比较低,因此在设计安全方式的时候,可以提升VPN的服务性能,允许用户自由访问各校区间的网络。如果对普通用户设置较高的安全级别,不仅会影响访问速度,降低用户访问的体验感,还会花费一些不必要的成本,浪费网络系统资源。此外,对于主校区与分校区之间的网络连接,还需要安装路由器设备,在访问网络资源以及数据信息传输的时候,都需要经过这个路由器设备。面对校园网络资源大且范围广的特点,学校在选择路由器的时候,确保成本合理的情况下,最重要的是应该考虑设备的安全性以及稳定性。构建各校区安全的VPN技术通道,学校网络中心人员应该定期检查并维护路由器设备、终端服务器等,才可以将学校的数据、资源等安全地传输给用户。

3.3.2 在校园内部网络设置VPN服务器

当学校老师和学生,需要在校园网覆盖范围以外的地方远程访问学校资源,或者移动使用校园网络时,就可以选择Access VPN技术来链接校园网络,Access VPN的工作原理就是,在校园网内部构建学校的VPN服务器,通过网络运营商(如ISP)提供的互联网服务,将远程用户与校园网络连接在一起,对数据进行加密和封装处理,构建虚拟的专用网络通道。用户发送请求给校园网络,在这过程中VPN服务器完成连接功能。以这种形式来链接校园网络很方便,而且不需要支付多余的费用,只需要支付ISP网络宽带使用的费用即可。

Access VPN形式下,首先,可以使用Linux系统来架构校园网络平台的基础环境,这是因为该系统稳定性好,扩展性强,而且可以免费使用。通过对比数据可以发现,Linux系统的性能比Windows系统良好。其次,在选择学校的VPN系统软件的时候,可以首要选择Open VPN软件,因为可以通过Open软件来创建SSL VPN应用系统。SSL VPN的简单应用设计如图2所示[5],其工作原理是SSL协议作为传输数据的基础,把客户端的请求转发到校园内网的VPN服务器,然后通过专用的隧道实现远程访问。SSL VPN可以灵活接入,且操作简单,支持较多的认证方式[6]。同时,考虑到数据的安全性,防火墙与NAT设备是一定要配备的。SSL VPN是工作在传输层上的,它的应用可以让数据穿过所有的防火墙与NAT设备,SSL VPN保证了用户可以随时随地通过VPN连接到校园网络[7]。但是应用SSL VPN的话,每个需要远程访问校园网络的用户都需要有一个内网IP地址,因此DHCP服务器的配备也是必需的,而这个服务器是用来自动分配IP地址的。此外,学校还可以架构一台LDAP服务器,通过学校的SSL VPN系统进行访问请求的时候,要先搜索该用户的用户名以及密码,确认用户信息是否存在于学校的数据信息服务器中,确认了用户身份后,才能建立远程访问的虚拟专用网络通道。SSL VPN系统可以根据用户的需求分配不同的访问权限,可以有效地防止用户的非法访问,保障了校园网络的安全。

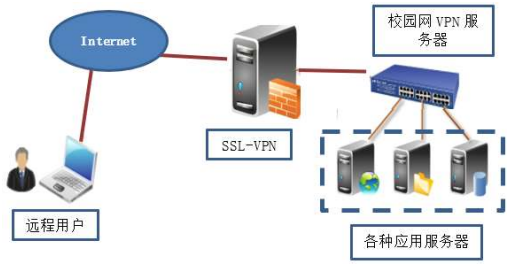

图2　SSL VPN的应用设计图

4 结束语

综上所述,随着现代化信息技术的进一步发展,在校园网络安全体系的建设与应用中,VPN技术的使用已经很普遍了。VPN技术的应用过程中,学校应该结合自身的需求,构建最适合本学校的VPN服务系统。本文从VPN技术的应用原则、需求分析,以及应用设计这三方面,简单系统地探析了现阶段VPN技术在校园网络安全体系中的应用,期望能对VPN技术在校园网络安全体系的应用研究有一定的参考意义。

参考文献:

[1] 蒋佳霖.基于P-WPDRRC模型的校园网络安全体系构建及实现[D].湘潭:湘潭大学,2020.
[2] 尚红艳.VPN技术在医院网络建设的应用[J].电子技术与软件工程,2018(17):20.
[3] 王真.VPN技术在校园网络安全体系的应用[J].网络安全技术与应用,2021(9):101-103.
[4] 金志敏.基于VPN技术实现高校图书馆数字资源的远程访问[J].办公自动化,2020,25(15):27-29,53.
[5] 童长卫.VPN技术在院校资源共享中的设计与实现[J].长江技术经济,2020,4(S1):185-187.
[6] 杨朋,殷旻昊.SSL VPN技术在统一身份认证平台的实现与研究[J].网络空间安全,2020,11(7):67-70.
[7] 黎伟.VPN技术在校园网络安全体系中的应用[J].科技创新与应用,2013(9):40.

【通联编辑:张薇】