校园网络安全体系中 VPN 技术的应用研究

康秀兰

（朝阳师范高等专科学校，辽宁 朝阳 122000）

摘 要：结合某学院校园网升级改造的需求，提出了以虚拟专用网络（Virtual Private Network，VPN）技术为基础的安全体系建设方案，实现了移动用户和远程用户接入校园网访问资源的目的。利用 Linux 系统和 Open VPN 建立了安全套接字协议（Security Socket Layer，SSL）VPN，使用户可以通过外网访问校园资源，再对 VPN 安全体系性能进行实验测试，验证了本文提出方案的可行性和有效性。

关键词：虚拟专用网络（VPN）；网络安全体系；校园网

中图分类号：TP309 **文献标识码：**A **文章编号：**1003-9767（2023）01-065-03

Research on the Application of VPN Technology in Campus Network Security System

KANG Xiulan

(Chaoyang Teachers College, Chaoyang Liaoning 122000, China)

Abstract: In combination with the upgrading and reconstruction requirements of a college campus network, a security system construction scheme based on Virtual Private Network(VPN) technology is proposed. According to this scheme, mobile users and remote users can access the campus network to access resources. Finally, Security Socket Layer(SSL) VPN is established by using Linux system and Open VPN, so that users can access campus resources through the external network. Finally, the performance of VPN security system is tested, which verifies the feasibility and effectiveness of the scheme proposed in this paper.

Keywords: Virtual Private Network(VPN); network security system; campus network

0 引言

高校校园资源具有开放性，师生可以随意访问，但是也存在独有性，校园网络覆盖区域外的师生无法通过外网直接访问校园资源。另外，校园网中的部分重要服务，如一卡通、财务以及图书馆等网络传输既要保证传输优先性，也要保证数据传输的可靠性和安全性。针对以上问题，需要在校园网中建立一种方便易行、节省成本的网络安全体系，而虚拟专用网络（Virtual Private Network，VPN）技术可以满足以上需求。

1 校园网现状

某学院校园网建立于 2002 年，经过 20 多年的发展与建设，已经具备了一定规模，网络覆盖学院的办公楼、学生宿舍楼、图书馆、教职工住宅楼和实验室机房等[1]。

学院校园网建成初期，学院公共网际互连协议（Internet Protocol，IP）地址共 16 个 C。随着网络用户数量的快速增长，IP 地址无法满足用户使用需求。为解决该问题，学院基于网络地址转换（Network Address Translation，NAT）技术，建立了内部 IP 地址，实现了内网与外网地址的自由转换。该设计方案虽然减少了 IP 地址使用量，但是在不连接校园网络的情况下，用户无法访问学校网络资源，教师只能通过学院内网进行办公、收发邮件以及浏览校园新闻等。

2 校园网 VPN 应用方案

2.1 需求分析

校园网应用 VPN 的需求包括以下两点。一方面，远程访问学院资源的需求。当节假日或休息日时，大部

收稿日期：2022-11-06

作者简介：康秀兰（1971—），女，辽宁朝阳人，硕士研究生，副教授。研究方向：网络安全、云计算、云存储。

分学生和教师不在学校内，为查询分数、接收和发送邮件等都需要异地远程访问服务。另一方面，远程访问学院图书馆教学资源。学院开放远程访问功能后，如何正确认证远程用户身份、保证信息完整性和保密性，是建立一套安全、可靠、可认证网络安全体系的基础 [2]。

2.2 VPN 系统功能模块

根据学院校园网 VPN 应用需求，可以将 VPN 系统功能分为身份认证功能、数据转发功能、访问控制功能和后台管理功能。

（1）身份认证功能。当用户远程访问时，采用用户名和密码的方式认证用户身份。在使用学院内网的情况下，采用数字证书认证用户身份。

（2）访问控制功能。根据规则库设定的网络访问控制策略判断用户是否为访问控制对象 [3]。

（3）数据转发功能。该功能主要将数据进行加密，并发送至用户或者接收隐私文件。

（4）后台管理功能。该功能负责 VPN 服务器工作信息管理，便于审计调阅。同时，它可以按照时间、会话持续时间以及日期等使用情况，向用户提供汇总报告。

2.3 VPN 应用方案设计

根据以上分析结果并结合学院校园网实际情况，VPN 应用方案如下。

在学院校园网中搭建 VPN 服务器，移动用户或远程用户可以通过 VPN 封装加密功能，远程接入校园网。想要实现远程用户或移动用户接入校园网 VPN 的目的，必须搭建 VPN 服务器。该服务器主要负责远程用户或移动用户接入管理。Linux 系统具有扩展性强、稳定、免费的优点，在性能方面优于 Windows 系统，因此采用 Linux 系统作为服务器搭建平台 [4]。

一方面，利用 Linux 系统搭建 VPN 服务器平台，将校园网服务作为建立 VPN 服务器的主要载体。另一方面，选择 Open VPN 作为搭建 VPN 服务的软件。该软件采用安全套接字协议（Secure Sockets Layer，SSL），可以建立以 SSL 为基础的 VPN 服务器系统。

由于校园网络拥有防火墙设备和 NAT 设备，SSL VPN 可以便利所有防火墙设备和 NAT 设备，进而消除用户访问地点和时间的限制。另外，远程用户访问校园网时，需要利用动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）服务器为用户分配校园 IP 地址，因此需要搭建 DHCP 服务器。为确保远程用户顺利接入校园网，需要建立 VPN 的域名，保证用户可以在任何地方均可以通过外网解析该域名 [5]。

2.4 Access VPN 构建

根据 Access VPN 规划，采用 Open VPN 接入服务器；操作系统采用 Linux 系统；服务器硬件采用 IBM x346。Open VPN 是一款以 SSL 协议为基础的 VPN，支持多种身份认证方法，如用户名和密码数字证书认证、智能卡等 [6]。

Open VPN 可以为用户提供多种数据加密算法，如国际数据加密算法（International Data Encryption Algorithm，IDEA）标准、数据加密标准（Data Encryption Standard，DES）、3DES 以及 RC2 等。在身份认证方面，Open VPN 支持哈希消息认证码（Hash-based Message Authentication Code，HMAC）数据认证、安全传输层协议（Transport Layer Security，TLS）密钥交换以及插件接口认证等。

（1）采用 Linux 系统自带的 MySQL 配置用于存放用户登录信息的数据库。

（2）配置身份认证系统，如服务器端证书和密钥、认证中心证书和密钥等。为保证身份认证证书的完整性和可靠性，由第三方担任认证中心。认证中心私钥负责证书签名，公钥负责签名认证。为保证网络安全性，认证中心私钥不可以泄露，公钥可以公开。认证中心建立完成后，调用 Open SSL 生成 Root CA 证书 ca.crt 和认证中心私钥 ca.key，即认证中心的私钥文件和公钥文件。生成 server.crt 和 server.key 文件后，在客户端本地生成证书和密钥，然后交由认证中心进行签名后交还于客户端。通常情况下，客户端密钥需要由客户端自己保存，且不能泄露。在密钥生成过程中，客户端私钥均在本地生成，不存在私钥传递过程中，因此避免了密钥泄露的问题。为减少客户端配合操作流程，本文客户端密钥文件和证书文件均在服务端生成，不仅省去了文件拷贝转移的过程，而且保证了私钥的安全性。

（3）生成 Diffie Hellman 文件。该文件主要用于密钥交换过程。

（4）添加静态路由。Open VPN 搭建完成后，为保证移动用户顺利接入校园网，需要在移动端安装 VPN 客户端，至此 Access VPN 建立工作完成。移动用户或远程用户通过 VPN 客户端访问校园网图书馆资源、查询成绩、收发邮件等。

（5）为便于外网用户接入校园网，需要为服务器配置域名，将 VPN 服务器域名设置为 vpn.xxxxy.cn。由于校园网已经建立了 DNS 服务器，因此只需要修改 DNS 中的 BIND9 文件即可。DNS 服务器配置过程中，可以在 /var/named 文件中添加主机文件，即可将 VPN IP 地

址与域名相对应。

3 校园网 VPN 体系性能测试

校园网 VPN 体系建立完成后，对网络性能进行实验测试，明确 VPN 体系建立后对校园网络的影响和远程拨号接入对校园网网速的影响。

3.1 测试方法

一方面，通过移动客户端接入 VPN，计算平均延迟，再关闭 VPN 服务，再次计算平均延迟时间，以计算 VPN 网络体系对现有网络产生的影响。另外，在网络高峰时间段测试路由器内存和中央处理器（Central Processing Unit，CPU）占用率，分析 VPN 是否会对网络设备的性能产生影响。另一方面，通过外网接入 VPN，测试用户是否可以正常校园资源，如查询成绩、收发邮件等。

3.2 性能测试

按照以上测试方法，分别选取 1000 个和 10 000 个数据包展开测试实验，测试结果如表 1 所示。

从表 1 测试结果来看，用户接入校园网并访问资源时并未出现丢包情况。在 1000 个数据包的情况下，网络访问延迟平均时间分别为 1.7 ms 和 1.2 ms，在 10 000 个数据包的情况下，网络访问延迟平均时间分别为 3.5 ms 和 3.1 ms。可见，VPN 网络体系对现有校园网性能影响较小，大多用户在使用网络时无法清晰察觉 VPN 服务的存在。

在网络使用高峰时间段对路由器内存和 CPU 使用率进行实验测试，实验结果如表 2 所示。

由表 2 可知，网络使用高峰时间段，在开启 VPN 服务的情况下，路由器内存和 CPU 利用率均有一定程度提升，但是利用率提升幅度较低，对路由硬件性能影响较小。可见，在开启 VPN 服务的情况下，路由性能可以满足网络高峰时间段的使用需求。

表 1 ping 值测试结果 单位：ms

数据包	VPN 服务启动				VPN 服务停止			
	第 1 次	第 2 次	第 3 次	平均值	第 1 次	第 2 次	第 3 次	平均值
1000 个数据包	1.8	1.7	1.7	1.7	1.2	1.2	1.3	1.2
10 000 个数据包	3.5	3.4	3.6	3.5	3.1	3.1	3.0	3.1

表 2 路由器性能测试结果 单位：%

数据包	VPN 服务启动				VPN 服务停止			
	第 1 次	第 2 次	第 3 次	平均值	第 1 次	第 2 次	第 3 次	平均值
CPU	33	34	36	34	20	25	26	23
内存	70	71	78	66	60	66	66	64

3.3 远程访问校园网测试

利用外网对 VPN 远程连接进行实验测试，在个人计算机（Personal Computer，PC）端输入域名 https://vpn.xxxxy.cn，检查是否可以正常弹出登录窗口。然后，通过用户名和密码登录系统，并访问图书资源，如果可以正常访问，则表明 SSL VPN 成功生效。

利用 Wireshark 软件进行抓包分析。经过抓包实验测试发现，客户端可以正常发送 hello 报文，且服务器响应后系统可以向客户端发送 VPN 安装证书。需要注意，该信息传输过程中的信息均为加密状态，加密方式为 SSLv3 协议。

4 结语

首先，从校园网实际情况出发，分析了校园网应用 VPN 的需求，并根据该需求阐述了 VPN 应用方案。其次，以移动用户和远程用户为例，描述了 VPN 在校园网络中的架设步骤。最后，通过实验测试，分析了本文构建的校园网 VPN 体系访问延迟和路由器硬件占用率。结果表明：在开启 VPN 服务的情况下，网络延时有一定程度提升，但是对用户使用体验影响较小；路由器内存和 CPU 占用率有所提升，但是路由器性能仍能满足网络高峰时间段的使用需求。

参考文献

[1] 孙临花 . 手机网络安全视域下大学生“校园网贷”治理体系建构 [J]. 许昌学院学报 ,2022,41(3):148–152.
[2] 郭倩 , 张桦 , 何岚岚 . 高校数字校园网络信息安全保障体系建设 [J]. 数字技术与应用 ,2022,40(3):224–227.
[3] 侯加兵 , 吕家云 . 高校全方位网络安全防护体系构建研究 [J]. 信息与电脑 (理论版),2021,33(8):214–217.
[4] 王克栋 . 高职院校数字化校园网络安全防控体系探讨 [J]. 信息与电脑 (理论版),2020,32(16):186–187.
[5] 白亚秀 . 基于 BAS–RVM 的校园网络安全量化评估体系设计与研究 [J]. 微型电脑应用 ,2020,36(6):100–103.
[6] 张宁 , 唐佳 , 刘识 , 等 . 基于 MPLS VPN 大型网络安全防护体系研究 [J]. 软件 ,2020,41(4):130–133.