The Building Method of Campus Local Area Network

Ning Jia

Staff Training Office, Jiangsu Petroleum Exploration Bureau Co., Ltd., Yangzhou, Jiangsu, 225002, China

Abstract

Campus LAN (local area network) is a platform that provides campus education, campus management, campus education resources and social education resources integration. The construction of campus LAN mainly uses existing network technology for construction and management. The design will be based primarily on technologies that can be used to build and implement campus LAN and provide insights into the construction of campus networks.

Keywords

Campus local area network; network technology; planning

校园局域网的组建方法

贾宁

江苏石油勘探局有限公司职工培训处，中国·江苏 扬州 225002

摘　要

校园局域网是一个提供校园教育，校园管理，校园教育资源与社会教育资源整合的平台。校园局域网的建设主要采用现有的网络技术进行建设和管理。该设计将主要基于可用于校园局域网的构建和实施的各种技术，并为校园网络的构建提供自己的见解。

关键词

校园局域网；网络技术；规划

1 引言

校园局域网的建设极大地丰富和完善了教育教学资源，拓宽了学生获取知识的渠道，提高了教学效果，提高了企业的现代管理水平。如何进一步完善校园网建设，如何构建高性能、低成本的大学校园网络系统是每个大学都需要思考和探索的问题。

2 背景

经过几年的信息化建设，中国的信息化水平不断提高，信息技术的应用取得了一定的成效。为顺应全球教育信息化发展趋势，推动信息技术与职业教育与教学的深度融合，落实中国职业教育工作会议精神和第二届中国教育信息化工作会议精神，落实教育部“教育信息化十年发展规划”（2011–2020），“教育信息化”“十三五”规划，本文以我企业服务的中国江苏省某校校园局域网为例，进行分析和讲解。

3 网络现状

（1）我企业服务的中国江苏省某校校园局域网现网核心设备为华三 S7506E，因购买时间较长，设备无法支持未来 IPv6 网络运行，并且随着大数据、云计算等新兴业务的发展对网络适应能力及网络性能的要求越来越高，现网核心设备不足以支撑业务需求的发展需求。

（2）该校互联网出口部署 1 台防火墙及 1 台上网行为管理，起到出口 NAT 及审计内网我校上网行为功能，不具备抵御恶意入侵攻击防护、防病毒及大流量 DDOS 攻击的能力，互联网出口一旦遭遇以上安全攻击，将波及整网。

（3）该校业务系统大部分为基于 B/S 架构，使用 Web 页面进行业务系统的访问，对于基于 web 的业务系统没有针对性的防护手段，Web 漏洞及其被黑客利用造成业务系统瘫痪。

（4）安全设备随时都在产生大量日志，日志种类复杂且格式不统一，并且分散在不同的安全设备上，从海量的日志

教学方法创新与实践·第 02 卷·第 03 期·2019 年 07 月
DOI: https://doi.org/10.26549/jxffcxysj.v2i3.1897

中获取有用信息非常困难，没有办法从宏观的角度分析现网安全问题。

4 项目必要性

4.1 响应国家政策必要性

为了促进学校信息安全的发展，响应国家和上级的要求，进一步落实水平保护，巩固水平保护作为国家信息安全的国家政策。我校计划参考“信息安全技术信息系统安全等级保护等级指南”（GB/T22240-2008）的要求，建议将该校系统设置为二级，按照“信息安全技术信息系统安全等级保护基本要求”（GB/T22239-2008）完成系统建设等保险。[1] 同时，为了提高整个网络的安全防护能力，该院校计划参照其他标准建立整个网络。

4.2 实际使用必要性

（1）该校具备一定的基础安全防护能力，但对于应用层威胁防御基本为 0，在互联网出口、用户认证、数据中心、运维管理方面均存在被恶意入侵、病毒侵害的风险，需要根据各区域实际进行针对性防护。

（2）该校即将拉通 Cernet2IPv6 链路，校园网及校园网站对 IPv6 的支持是该校当前非常紧迫需要解决的问题。

5 设计目的及要求

5.1 安全性与可靠性

（1）应该具备在现有条件下和规定时间内完成规定功能的能力；

（2）应该具备长期可靠和稳定工作的能力；

（3）具备合理的冗余能力、灾难备份能力（包括：链路冗余、关键设备冗余和重要业务模块冗余）；

（4）设计中没有单点故障存在，对可能存在单点故障环节，在设计中，要尽可能减少其对整个系统的影响；

（5）整个网络系统的服务器供电系统的可靠性，应该不低于百分之九十九。

5.2 灵活性与扩展性

网络系统中的数据中心应具有良好的灵活性和可扩展性。整个系统应该能够根据未来的业务继续发展（扩大系统中网络设备的容量，增加该校网络设备的数量和质量）。系统必须能够支持多个网络传输和多个物理接口。此外，系统还可以随时灵活地升级和更新网络设备。

5.3 先进性与实用性

在满足系统数据中心的安全性和可靠性大前提下，要采用国际上最先进最成熟最实用的尖端技术，要建设合理并且超前的技术框架结构。整个系统中的软件和硬件配置要采用开放式的框架结构，各分系统和子系统的设计，都要根据今后业务的发展需要与设备的使用需求的实际状况来设计。

6 网络方案设计

6.1 总体框架（图 1）

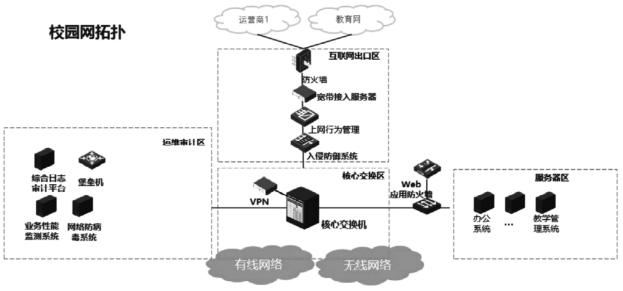

图 1 方案总体框架

本次建设在四个区域部署：

（1）核心交换区：核心交换区中部署 1 台核心交换区负责整网的数据交换，同时也是连接各个区域的枢纽。增加 VPN 系统解决移动办公安全问题。

（2）互联网接入区：互联网接入区中增加，宽带接入服务器（认证系统）、入侵防御系统。

（3）服务器区：在服务器区前端部署 Web 应用防火墙；综合管理平台、集中存储系统等。

（4）运维审计区：在运维审计区中部署堡垒机、及综合日志审计平台、认证系统、业务性能监测系统、网络防病毒系统。

6.2 技术方案

6.2.1 网络及综合布线

本次替换原有核心交换机，为正交 CLOS 架构，配置双主控、四电源保障核心设备的可靠性，并且具有 10 个业务槽位，保障后期的扩展性要求，同时可扩展多种类型的安全插卡，可满足未来更大流量、更精细化的安全需求。本次核心交换机配置 52 个万兆光口，24 个千兆电口，20 个千兆光口，用于实现万兆连接校内汇聚交换机，及其他各区域连接的要求。[2]

6.2.2 安全

（1）Web 应用防护系统。Web 服务的安全性面临两种差异化程度非常严重的情况：一方面，Web 服务的易操作性使 Web 服务覆盖范围更广，大多数人没有基本的网络安全意识，网络上的陷阱稀疏。为了防止这种情况，很容易在不知情的情况下成为攻击的目标，但另一方面，由于信息技术的快速发展，网络上的各种材料和工具可以轻松访问和下载，不同的攻击工具可以很容易地在网络上传播。攻击者需要的技术知识逐渐减少。即使没有网络和 Web 基础设施，您也可以根据攻击软件的指令攻击 Web 服务器。

（2）综合日志审计。集成日志审计平台从企业和组织信息系统资源中的各种设备和应用程序收集安全日志，并可以结合云的威胁信息对大量安全日志进行统计分析和相关分析，帮助中国江苏省的这所学校更准确，快速地识别安全事故，从而及时响应。架构可分为四个层次（图 2），数据采集层，数据处理层，数据分析层和业务表示层。

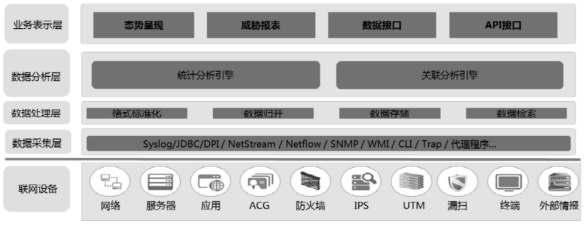

图 2 架构的四个层次

（3）VPN。“统一服务安全访问平台”为组织的服务访问需求和组织的安全需求提供了完整而简单的解决方案，使员工可以随时随地轻松访问公司的 Intranet 并使用 Intranet。应用并确保公司信息安全性并避免敏感数据泄漏。集成服务访问平台为教师提供端到端的移动安全管理和灵活的应用程序发布功能。从用户端，网络传输和服务器端充分考虑用户安全要求，加强安全性，以及设备安全管理和防止远程应用程序泄漏，提供全面保护我们的移动办公系统，使网络系统成为可能在效率与组织和信息安全之间找到适当的平衡点。

（4）堡垒机。本次部署 1 个运营维护堡垒主机，堡垒机可以为我校提供全面的运维管理系统和运维能力，支持资产管理，该校管理，双因素认证，指挥拦截，门禁，自动更改，审核等功能，可以有效保证操作和维护过程的安全。在协议方面，Fortress 机器完全支持 SSH / TELNET / RDP（远程桌面）/ FTP / SFTP / VNC，虚拟机管理，如 VMware / XEN，Oracle，数据库管理，如 HTTP / HTTPS，并通过应用中心技术支持小规模机器管理等。

（5）网络防病毒系统。与单病毒保护相比，病毒在网络环境中传播得更快。使用独立版本的防病毒产品很难删除网络病毒。因此，需要适用于域网络的各种防病毒产品。服务器版防病毒软件可以部署在应用服务器和网络上，以防止和控制计算机病毒。防病毒软件可以安装在终端网络服务器上，通过集中管理防病毒终端，实现集中管理和控制。

（6）认证系统。实现校园网认证系统全网业务数据自动同步，实现全网校际漫游多层级业务数据保留本地认证数据，保留全网漫游数据。我企业有线无线统一认证，实现校际漫游，提升用户体验。满足普教多样化场景，提升多功能访客系统体验度，支持内部授权访客管理。支持学校教工多样化外部认证源，融合现有校园信息系统、如 LDAP、POP3、OA 等，实现便利的统一认证。支持短信 Portal、微信连 Wi−Fi、二维码认证、1x 等多种认证方式。支持 DHCP、MAC、SNMP 等多样化无感知认证解决方案。

（7）IPS 入侵防御系统。IPS 入侵防御系统是网络安全防护系统中最重要的环节。它可以及时识别网络系统中的入侵行为，实时报警，有效拦截和保护。

7 结语

企业校园网建设是一项系统工程，需要运用各种技术，即网络技术和工程建设技术，以及项目管理系统的知识。随着通信技术和信息技术的快速发展，随着网络性能需求的不断增加，各种新技术和网络新思路将不断得到改进和发展。更多更好的组网技术将应用到新的校园网络建设之中，校园网络的功能也将得到大大的提高。

参考文献

[1] 苗凤君 . 局域网技术与组网工程 [M]. 清华大学出版社 .2014.

[2] 邱冬，闫韶松 . 网络操作系统 −Windows2003server 管理与配置 [M]. 清华大学出版社，2014.