 DOI: https://doi.org/10.12345/bdai.v6i4.30546

Research on Campus Network Security Based on Multi-System Collaboration

Yuanyang Li Feng Pang

Nanjing Forestry Univeristy（XinZhuang）, Nanjing, Jiangsu, 210000, China

Abstract

Cybersecurity has emerged as a critical and highly relevant research focus in recent years. In particular, cybersecurity within higher education institutions plays a pivotal role in ensuring the security and stable operation of campus networks. Traditional single-system defense mechanisms are increasingly inadequate in the face of sophisticated and multifaceted cyber threats and intrusion techniques. Moreover, isolated security systems often fail to collaborate effectively for joint defense. This paper introduces a network security defense architecture based on multi-system collaboration. By integrating this architecture, the overall security posture of campus networks can be significantly enhanced. The proposed approach coordinates previously independent defense systems, leveraging a combination of security mechanisms to establish a more efficient and robust security framework.

Keywords

Cybersecurity, Defense Systems, Multi-System Collaboration

基于多系统协作下的校园网络安全研究

李远洋 庞峰

南京林业大学（新庄），中国·江苏 南京 210000

摘 要

网络安全作为当前热点和重要研究课题，尤其是高校网络安全，负责整个校园网络的安全与稳定运行，传统单个系统的防护措施难以满足当前多手段的渗透与网络攻击，且多个单系统防护无法有效联合进行共同防御，本文介绍了一种基于多系统协作的网络安全防护体系，并通过该基础架构对校园网络安全的整体防护进行增强，将独立的个体防御系统协同工作，联合多种安全防御手段建成高效且更安全的防护体系。

关键词

网络安全，防御系统，多系统协作

1 引言

随着当前高校信息化建设的不断推进，和高校管理和科研工作对信息化和数字化程度的要求不断提高，信息化建设和数据上网在高校已逐步深化和细化，校园网络作为数据传输的基础设施，在教学科研和行政管理方便有着不可或缺的重要作用。当下校园网络中安全形式十分严峻，尤其是信息系统漏洞频发 [1]，且终端设备安全更新的缺乏，导致校园网络中安全情况难以管理和控制。当前高校网络安全防护体系通常是由校园网主防火墙进行统一防护，其数据中心再进行一道正常 WAF 和 IPS 进行安全控制，但多个安全系统缺乏联动，为实现全链路的责任和数据审计，多系统协作的网络安全防护刻不容缓。

【基金项目】江苏省现代教育研究 2023 年度智慧校园专项立项课题《人工智能在校园网络安全中的应用》（项目编号：2023-R-107323）；《智慧校园背景下密码技术应用实践研究》（项目编号：2023-R-107333）。

【作者简介】李远洋（1997-），男，助理工程师，从事网络安全，人工智能研究。

2 当前高校网络安全环境的隐患

终端接入混杂：高校网络中接入的终端类型繁多，包括教职工和学生的 PC、移动终端、物联网设备等。这些终端往往由用户自带或自行安装管理，缺乏统一认证和管控机制。若无集中化的准入控制，各类设备可随意访问校园网资源，容易成为攻击入口。实践表明，将身份认证、终端评估与准入控制相结合，可在终端接入时进行实时安全检查，拒绝未安装安全补丁或异常的设备进入网络。否则，网络中任意未授权终端都有可能带来恶意程序，形成安全隐患。此外，由于师生的网络安全意识参差不齐，不规范使用终端设备现象普遍存在，如随意下载不明应用、连接未知 Wi-Fi、USB 设备交叉使用等，这些行为都可能引入病毒或木马程序。一

旦感染，将在网络内迅速扩散，对数据安全与网络稳定运行构成威胁。

业务系统漏洞频发：高校各类信息系统（如教务系统、OA、科研平台等）规模庞大，多数由第三方软件构建。由于维护不足或人员意识淡薄，系统补丁和安全更新往往滞后，漏洞频发。一旦存在系统漏洞，勒索病毒、挖矿木马等恶意软件可迅速在网络内横向传播。实践表明，因系统漏洞或木马导致主机 / 终端被感染、外联的事件，已经超过 APT 攻击、网页篡改等，成为高校最常见的安全事故，常造成严重数据泄露。在安全演练中，遭到攻击的内部终端往往被当作跳板，进而突破内网防线，说明漏洞和终端失陷极易诱发更大范围的入侵。

内部人员威胁：高校内部人员数量众多，管理相对开放，且权限分散。一些用户可能在未受管控的情况下浏览不安全网站或安装软件，甚至有恶意人员故意篡改数据、外传信息。如果缺乏严格的权限管控和审计机制，内部人员的误操作或有意行为很难被及时发现和阻止。上述终端混杂和内部威胁表明，单靠传统单点防御（如仅依靠边界防火墙）已经难以应对现实中的多源攻击和内部风险，单一防护机制无法满足高校多层次网络安全需求。此外，部分管理人员由于岗位轮换或权限配置不合理，出现“越权操作”现象。一旦账号被盗，攻击者便能以合法身份在系统中进行敏感操作，造成更大破坏。上述终端混杂和内部威胁表明，单靠传统单点防御（如仅依靠边界防火墙）已经难以应对现实中的多源攻击和内部风险，单一防护机制无法满足高校多层次网络安全需求。

3 高校安全体系的建设

面对日益复杂的网络安全形势，高校必须构建纵深防御 [2] 的安全体系，从组织、制度、技术等多个维度协同发力。

图 1 高校网络安全组织架构

组织管理层面：加强顶层设计，成立由校领导挂帅的网络安全领导小组，明确分工、压实责任，形成全校联防联控格局。高校应制定完善的网络安全管理制度、岗位职责和应急预案，将安全工作纳入日常管理。正如已有研究指出，高校需要“从顶层设计开始”，组建专门领导小组组织统筹网络安全和信息化工作。通过制度化的责任落实和定期考核，提升整体安全管控水平。通过制度化的责任落实和定期考核，提升整体安全管控水平。此外，建立网络安全考核机制，纳入单位绩效评价体系，可有效激励各学院、各部门主动履责，营造网络安全共建共治的良好氛围。

制度规范层面：建立健全安全管理流程和规范。制定严格的终端接入策略、账号权限管理、敏感数据保护等制度，实现网络资源的全生命周期安全管控。完善校内网络使用、终端安全和漏洞管理等制度，明确违规责任和处置流程。据报道，系统化的制度文件和安全流程构建能够规范管理流程，提升管理队伍水平，支撑校园网络安全体系的长效运行。同时，应注重制度的实效性与可操作性，避免文件流于形式。可通过设立定期的网络安全检查机制、用户行为审计制度，确保制度落地执行。在突发事件应对方面，应形成闭环的应急响应流程，明确各方职责、处置步骤与信息上报机制。

技术手段层面：实施多层次的技术防护体系。在网络边界、业务系统和终端等环节分别部署安全设备，形成纵深的防护架构。可采用“外防渗透、内防横向移动”的指导思想，在校园网边界、云平台边界和终端安全三个层面建立安全防线。在边界端部署流量防火墙、IPS、防病毒网关等设备，对内严格划分网络区域、实施白名单访问控制；在关键应用前部署 WAF，对 Web 攻击进行专项防护；对内部云主机和终端，则部署终端安全管理平台（EDR）和安全监测系统，动态检测并响应威胁。

4 校园网络安全防护技术建设

尽管高校部署了大量传统安全设备，但单一体系存在明显局限性，导致防护效果不尽如人意。

传统安全设备的不足：常用的边界防火墙、WAF、入侵检测 / 防御系统（IPS/IDS）主要针对已知的攻击模式发挥作用。随着攻击手段的多样化和加密流量的增多，传统防火墙无法深入分析和阻断隐蔽攻击。例如，对于现代远程办公模式下的数据外泄风险，传统防火墙几乎不起作用。WAF 和 IPS 等系统多依赖特征匹配，对高级持续性威胁（APT）或零日攻击防御力弱；一旦对手采用加密隧道或未知漏洞，传统防护体系往往难以察觉。

系统间信息孤岛：校园网环境中存在众多安全设备和管理系统，它们往往独立工作，缺乏有效的数据共享与协同。一些研究指出，网络安全运营团队在日常防护中经常面临“工具孤岛”问题，即各种安全工具彼此之间难以交互，预警信息分散，整体安全态势难以统一掌握。例如，部署大量点产品后并未提高威胁发现效率，反而带来了运维负担增加的问题。信息孤岛导致安全事件处置难、误报率高，也阻碍了对攻击链的综合追踪。

协同防护不足：在传统模式下，网络设备和终端安全产品往往独立响应事件，缺乏自动化联动。例如，当某个终端被检测出恶意行为时，相关告警无法快速传递给边界防火墙或身份认证系统进行联动拦截。实践中发现，网络侧探测到的威胁往往无法准确同步到终端安全平台进行处置，使得联动功能形同鸡肋。这种缺乏协同的局限性使得校园网络安

全难以从根本上形成完整的防御闭环。

随着信息化水平的不断提高，高校网络承载了越来越多的业务系统和数据服务，其网络安全问题也愈发突出。传统的安全防护措施主要依靠防火墙、入侵防御系统（IPS）和网页应用防火墙（WAF）等安全设备进行边界防护。然而，在应对复杂多样的新型网络威胁时，这些设备往往存在一定局限性。

首先，防火墙主要用于控制网络流量的进出，通过设定访问控制策略过滤不合法的访问请求。虽然其可以有效抵御外部的非授权访问，但难以应对针对应用层的攻击和内部网络的异常行为。其次，IPS 虽然能够检测并阻断一些已知的攻击行为，但对于加密流量的识别能力有限，且面对零日攻击和未知漏洞时防御效果不足。再者，WAF 主要针对 Web 应用攻击，如 SQL 注入、跨站脚本等，能够为高校门户网站和在线教学平台提供一定防护能力，但对非 Web 类业务系统保护能力较弱。此外，传统安全设备之间缺乏联动机制，各自为政，不具备数据共享与行为联动能力。

5 多系统协作的安全体系建设

为破解上述局限，必须构建多系统协作 [3-4] 的全链路防护体系，实现信息共享和联动响应。具体而言，高校应将校园网出口的流量控制系统、身份认证系统、边界防火墙、WAF、IPS 以及终端安全管理平台等多个子系统有机整合。

统一安全感知平台：建设统一的安全运营中心（SOC），实现各类日志、告警、流量、资产信息的集中采集、分析和展示。通过 SIEM 系统汇聚来自防火墙、IDS、EDR、WAF 等系统的告警信息，结合 AI 分析实现威胁研判与告警分级，提升发现威胁的效率。

信息共享与协同决策：通过安全态势感知平台汇聚各设备的日志和告警，实现跨系统信息共享。一旦某个组件发现可疑活动，能够立即向其他组件通知。例如，当流量监测发现异常行为时，可联动终端管理平台和 WAF 共同分析；身份认证系统可根据终端状态下发访问控制策略。通过共享威胁情报和设备日志，不同系统可以协同识别攻击意图、定位攻击阶段，提高整体防御效率。

跨系统策略联动：将终端检测平台与身份管理系统（如 LDAP、统一身份认证）和网络准入控制系统（NAC）联动，实现对违规行为用户的自动隔离。例如，当 EDR 平台发现某终端疑似中毒，即可通过 NAC 下发隔离指令，阻止其访问核心资源，实现快速闭环。

自动化联动响应：借助 SOAR（安全编排）等自动化平台，实现预案化的快速响应流程。当网络侧发现安全事件时，系统能够自动下发命令，协调防火墙、IPS 等同步封堵攻击源，并同时触发终端安全产品进行查杀。理论上，网端联动可以实现提前预警和实时处置，但实践中往往效果不佳，需要优化联动策略。通过改进联动机制，如引入大数据分析平台将网络和终端日志聚合为安全事件，可实现对入侵行为的快速定位和清除。例如，当某一主机尝试外联连接时，流量监测与终端防护平台能快速响应，一方面阻断可疑通信，一方面追溯恶意进程，从而有效遏制威胁扩散。

动态访问控制：根据用户的行为、风险等级、终端状态等动态调整其访问权限。例如学生在校内登录正常可访问全部教学资源，若检测到异常登录或终端高风险行为，可自动限制其权限，仅保留基础服务。

智能分析与预测预警：利用 AI 与大数据技术，对海量安全日志进行分析，建立行为画像，实现威胁预测、异常检测和溯源分析。通过构建知识图谱等方式，挖掘潜在攻击路径和隐匿行为。

构建闭环防护流程：在实践中，可以设计“检测—分析—阻断—追溯—反制”的协同处置流程。具体来说，先借助流量管控设备和态势感知技术检测异常流量和入侵行为；再结合入侵检测、日志审计等手段进行分析；发现攻击时，阻断相应流量并调动防火墙 /WAF 封堵攻击；同时启动溯源机制查找攻击路径；最后根据溯源结果反制攻击源并修复漏洞。这样的闭环流程确保当面临复杂攻击时，多系统能够联动执行，从而将攻击者拦截在校网边界之外。

综上，多系统协作不仅提高了校园网络安全事件响应的速度，也增强了整体的预测、阻断和防御能力，是应对未来复杂威胁态势的核心手段。

6 结语

本文围绕高校校园网安全建设，从隐患分析、体系构建到协同防护技术，进行了系统论述。高校网络面临的威胁日益复杂多变，迫切需要从管理机制到技术平台进行全面升级。正如研究所指出的那样，新型有组织的网络威胁要求“采取更加主动、多方协同的防御策略”，升级已有安全架构，实现全天候、全链条的防护能力。多系统协作模式能够打破安全孤岛，实现信息共享和联动处置，对提升高校网络安全防御水平具有重要现实意义。展望未来，随着教育信息化和智慧校园建设的深入，基于流量管控、身份认证、边界安全、终端管理等多种系统协同联动的安全体系，将成为高校网络安全防护的主流方向，为维护校园网络环境安全提供可靠保障。

参考文献

[1] 王宇,王卫东,温占考.网络攻防视角下的高校网络安全防护[J].中国教育网络,2020,(12):64-65.

[2] 司艳波,柳丹彤.基于IATF思想构建网络安全治理体系[J].中国教育网络,2023,(10):60-62.

[3] 张钰梅.多层纵深校园网络安全工作框架构建[J].网络安全技术与应用,2025,(05):77-80.

[4] 严蕾.基于动态模型的校园信息网络安全研究[J].网络安全和信息化,2025,(05):25-27.