医院云计算安全防护中基于 SDN 架构的网络安全平台建设应用

王 弢 金 蕾

（上海交通大学医学院附属瑞金医院信息中心 上海 200025）

〔摘要〕 **目的/意义** 建设基于软件定义网络（software defined networking，SDN）架构的网络安全平台，以增强医院云计算安全防护。**方法/过程** 基于 SDN 架构构建网络安全平台，并与入侵检测系统联动形成主动防御系统。对比分析平台应用前后租户横向攻击数量、攻击成功率、策略无阻断业务数、勒索软件加密数据量和安全团队操作工时等指标，验证平台的有效性。**结果/结论** 基于 SDN 架构的网络安全平台可有效识别并阻断恶意流量，增强对医院云计算的安全防护。

〔关键词〕 软件定义网络；网络安全平台；医院；云计算；安全防护

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2026.01.013

Construction and Application of a Network Security Platform Based on SDN Architecture in Hospital Cloud Computing Security Protection

WANG Tao, JIN Lei

Information Center, Ruijin Hospital Affiliated to Shanghai Jiao Tong University School of Medicine, Shanghai 200025, China

〔**Abstract**〕 **Purpose/Significance** To build a network security platform based on the software defined networking (SDN) architecture, and to enhance the security protection of hospital cloud computing. **Method/Process** A network security platform is built based on the SDN architecture and is linked with the intrusion detection system to form an active defense system. By comparing and analyzing the number of tenant horizontal attacks, the success rate of attacks, the number of unobstructed businesses by strategies, the volume of data encrypted by ransomware, and the operating hours of the security team before and after the application of the platform, the effectiveness of the platform is verified. **Result/Conclusion** The network security platform based on SDN architecture can effectively identify and block malicious traffic, and enhance the security protection for hospital cloud computing.

〔**Keywords**〕 software defined networking (SDN); network security platform; hospital; cloud computing; security protection

1 引言

医疗云计算平台存储海量敏感信息，其数据一旦泄露，不仅直接侵害患者权益、造成机构损失，还可能危及社会公共卫生体系的稳定。然而，当前多数医院依赖传统安全架构，如部署独立防火墙、入侵检测系统（intrusion detection system，IDS）/入

〔修回日期〕 2026－01－08

〔作者简介〕 王弢，工程师，发表论文 8 篇；通信作者：金蕾，工程师。

〔基金项目〕 上海市黄浦区卫生健康委员会科研课题（项目编号：2023－KY－25）。

侵防御系统（intrusion prevention systems，IPS）等设备，策略分散、响应滞后，难以动态适应虚拟化环境中东西向流量激增的情况，也无法满足微隔离需求，导致安全策略配置复杂、威胁感知能力弱、应急响应效率低。有研究[1]指出，医院云计算安全防护问题已成为影响医疗机构“上云”的关键性因素。因此亟须探讨新的医院云计算安全防护模式，以解决上述问题。软件定义网络（software defined networking，SDN）是一种新型网络创新架构[2]，其设计理念为逻辑上分离、集中控制与数据转发，通过控制器可编程化控制底层硬件，可实现网络虚拟化和网络资源灵活调配。根据既往研究，基于 SDN 架构的云计算安全防护系统中，每个安全代理只保留极少部分经常访问的网页地址缓存，以提高检测速度[3]；与传统防御方案相比，SDN 高效协同防御分布式拒绝服务攻击方案的防御有效性和及时性分别提高了 33.33%、28.57%[4]。郭雅等[5]结合云计算中心网络安全防护需求设计基于 SDN 架构的防护体系，成效理想；Mehmood K T 等[6]通过在 SDN 控制器上实施动态主动感知服务器负载管理算法，可根据网络服务质量控制参数共享服务器负载，总体延迟降低，网络服务质量随之提升。另有研究[7]在医院数据中心网络完全闭环体系中引入 SDN，提高了安全访问控制效率。SDN 架构在医疗云安全管理中优势突出，但其在医院云计算安全防护中的应用效果尚缺乏研究探讨。本研究设计基于 SDN 架构的网络安全平台，并应用于医院云计算安全防护，以提升医疗云的整体安全性。

2 研究设计

2.1 研究框架

SDN 架构包括应用层、控制层和转发层[8]，见图 1。SDN 在云计算中的具体工作流程，见图 2。

2.2 医院云计算安全防护中基于 SDN 架构的网络安全平台建设

2.2.1 设计目标及思路 解决医院云计算安全防护中东西向流量失控、响应延迟、医疗物联网暴露面多等问题[9]。设计基于 SDN 架构的网络安全平台，包括基础设施层、控制层和应用层，同时将 SDN 与 IDS 联动，以实现对数据信息安全的精细控制。

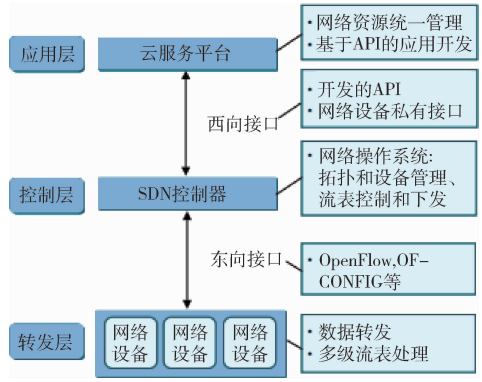

图 1 SDN 架构

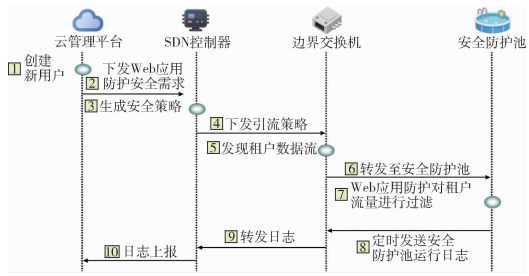

图 2 SDN 在云计算中的具体工作流程

2.2.2 基础设施层 （1）物理/虚拟交换机。作为 SDN 的转发层，接收来自控制器的流表，根据流表规则对数据包进行转发、丢弃、修改或重定向引流。（2）安全防护资源池。其中 Web 应用防火墙对重定向过来的 Web 流量进行深度检测，识别并阻断 SQL 注入、XSS、CC 攻击等，负责数据包实际转发和安全的承载。处理后的“干净”流量被放行回主路径，防火墙提供传统的网络层/传输层访问控制，基于物理地址和端口进行过滤，入侵检测/防御系统对流量进行深度包检测，识别已知攻击特征和异常行为。负载均衡器主要在安全池内或面向应用，实现流量分发和高可用。根据需要加入防病毒网关，以及防数据泄露等安全设施。（3）云资源池。为上述设备提供运行环境。（4）日志采集探针。部署在交换机、安全设备、服务器上，负责收集原始日志（如 NetFlow、sFlow、设备日志、系统日志），并按需发送给控制层或应用层。

2.2.3 控制层 （1）SDN 控制器。核心作用是作为东向接口与基础设施层的交换机通信，下发流表规则。核心流程包括接收来自上层的策略指令、生成/更新流表、通过东向接口下发给指定交换机。该模块包括 SDN 审计控制器、SDN 网络控制器和 SDN 安全控制器。其中 SDN 网络控制器可根据数据信息特点主动选择路由器完成数据转发；SDN 安全控制器可标识数据流量，并对恶意流量自动增加安全管理监控和网络攻击抵御[10-11]。（2）SDN 防火墙决策模块。包括多个控制器组构成的 SDN 防火墙控制器集群模块，由转发器、调度器、决策器和监测器进行调度，并向 SDN 防火墙控制器集群模块输出决策信息，见图 3。

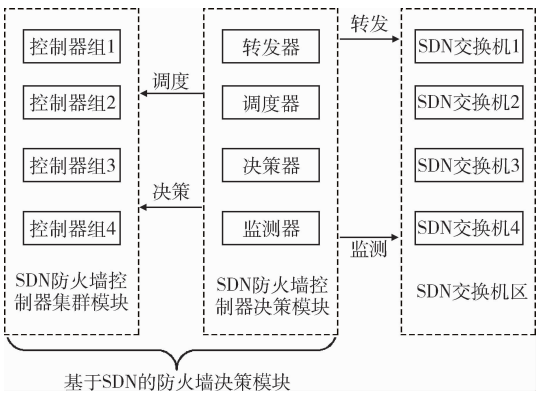

图 3 SDN 与 IDS 联动模块

其中转发器可动态收集数据信息后转发至控制器；调度器可依照预定周期将调度指令传输至决策器；决策器可接收监测器与调度器传输的信息，并进行审计，如果结果不一致则主动开展安全风险分析、加强流表审计，调度或切换控制器组件。（3）SDN 防火墙检测器。可对跟踪控制器系统实施跟踪和监控，动态评价控制器是否有异常。（4）SDN 与 IDS 联动模块。主要作用是实时接收来自 IDS/IPS 的告警信息、分析告警的严重性和可信度、自动触发控制器生成阻断流表、动态隔离攻击源或阻断攻击流量，是实现“检测－响应”闭环的关键。主要流程包括接收 IDS 告警、风险评估、触发阻断指令、传递给 SDN 控制器、控制器生成阻断流表并下发，最终能实现秒级响应。（5）服务编排器。管理安全资源池中的虚拟实例。主要流程包括接收“需要为新租户部署 Web 应用防火墙”的指令、调用云平台 API 创建 Web 应用防火墙虚拟机、配置网络、通知 SDN 控制器建立引流路径。（6）策略管理器。存储和管理所有安全策略，为决策模块提供策略依据。（7）接口。东向接口用于与基础设施层通信、西向接口用于与云管理平台和应用层通信。

2.2.4 应用层 （1）云管理平台集成接口。作用是与 OpenStack、VMware vCloud 等云平台对接，负责策略的输入、监控、分析和报告。工作流程包括云平台创建新租户、通过西向 API 通知本平台、平台自动为该租户网络下发默认安全策略。（2）安全管理控制台。采用图形化界面，供安全管理员进行策略配置、设备监控、告警查看、日志分析等。（3）可视化与分析系统。接收来自基础设施层的日志和控制层的策略执行数据，并进行关联分析，生成安全态势图、实现攻击路径还原、输出合规性报告。主要流程包括日志收集、数据清洗与关联、威胁检测与分析、生成可视化图表和报告。（3）自动化工作流引擎。定义和执行复杂的自动化任务。（4）API 网关。统一对外提供西向 API，供其他系统集成调用。

3 数据收集与分析

收集平台应用前后租户横向攻击数、攻击成功率等指标数据。采用 SPSS22.0 软件进行统计学分析，计数资料用“%”描述、χ^2 检验；计量资料用平均值 ± 标准差描述、独立样本 t 检验。$P<0.05$ 为差异有统计学意义。结果显示，基于 SDN 架构的网络安全平台应用后租户横向攻击数、攻击成功率、策略无阻断业务数、勒索软件加密数据量均较应用前减少（$P<0.05$），且安全团队操作工时较应用前大幅缩短（$P<0.05$），见表 1。

表 1 基于 SDN 架构的网络安全平台应用前后对租户的防护性能指标比较

阶段	安全事件数（起）	租户横向攻击数［起（%）］	攻击成功率［起（%）］	策略无阻断业务数（次/月）	勒索软件加密数据量（TB/年）	安全团队操作工时（h/月）
应用前	247	193（78.14）	62（32.12）	15 ± 3	4.2 ± 0.6	1 340 ± 215
应用后	212	85（40.09）*	1（1.18）*	0 *	0 *	220 ± 18 *

注：* 表示 $P<0.05$。

4 讨论与启示

4.1 讨论

4.1.1 医院云计算安全现状分析 目前仍普遍使用传统边界防火墙对医院云计算进行安全防护，技术防护能力滞后，存在网络能见度缺失，策略部署僵化、不合规等问题。有报道[12]称混合云环境中超过 70% 的医院无法监控跨虚拟私有云数据流，安全策略变更手动配置物理设备的耗时达 48h。而该时长无法满足急诊业务需求。

4.1.2 基于 SDN 架构的网络安全平台作用分析 本研究构建基于 SDN 架构的网络安全平台，在医院云计算安全防护中取得显著成效，具体表现如下。（1）提升医院核心业务系统的稳定性和可用性。既往频繁的安全事件（247 起/年）和租户间的横向攻击（193 起）常导致关键服务器过载、网络拥塞甚至服务中断。平台上线后，通过精准引流和实时防护，横向攻击降至 85 起。这意味着核心业务系统遭受外部攻击和内部威胁干扰的事件大幅减少。（2）增强患者隐私数据和医院敏感信息的安全防护能力。平台应用后攻击成功率从 32.12% 降至 1.18%，勒索软件加密数据量从每年 4.2TB 降至零。该平台通过 SDN 控制器与 IDS 的深度联动，实现了“分钟级”甚至“秒级”的自动响应。一旦检测到可疑行为或已知攻击特征，控制器能立即下发流表，动态隔离受感染主机或阻断恶意流量。同时，策略无阻断业务数从 15 次降至 0 次，表明平台的策略配置更加精准，避免了传统防火墙规则粗放导致的误拦截。（3）降低安全管理成本和人力投入。实践数据显示，安全团队操作工时从每月 1 340 小时减少至 220 小时，降幅超过 80%。本研究使用 SDN 与 IDS 联动模块实现对数据信息安全的精细控制，且将 SDN 架构应用于医院云计算安全防护，弥补了传统防护模式的不足。

4.2 启示

为了不断优化医院云计算安全防护技术，提出以下建议。一是医院云计算安全防护技术的优化不应仅依赖于模块叠加，还应融入网络底层设计。SDN 可将控制平面与数据平面分离，实现网络策略的集中化、程序化和实时响应，为安全防护提供有力支持。二是医院云计算安全防护技术的优化应遵循从“边界防御”向“零信任 + 动态授权”的总方向，确保在医院云环境中，电子病历、影像系统、科研数据等敏感资源仅能被授权主体访问，基于 SDN 架构的网络安全平台可实现按用户、设备、应用、流量类型甚至时间的精细化访问控制。三是与事后溯源相比，应更注重快速响应，以满足医疗业务连续性的高要求。另外为实现自动化威胁识别 – 决策 – 处置闭环管理，应探索结合使用人工智能或机器学习模块。

5 结语

本研究针对当前医院云计算安全防护中业务敏捷性不足、东西向流量不可视、安全拖慢业务、审计粒度不足等问题，构建基于 SDN 架构的网络安全平台，在实际应用中可主动发现恶意流量、判断入侵事件，提交 SDN 控制器模块，生成并自动下发安全策略，形成动态阻断系统，最终实现主动防御，极大提升了对医院云计算安全防护能力。本研究仍有不足：医疗协议深度感知不足、异构设备纳管能力较弱、策略智能化临床适配困难和安全资源池性能瓶颈，后续将探索引入医疗语义感知引擎、医疗设备数字孪生、临床情境自适应策略和异构安全资源池化架构等技术进行优化。

作者贡献：王弢负责研究设计、数据收集与分析、论文撰写与修订；金蕾负责提供指导、论文审核与修订。

利益声明：所有作者均声明不存在利益冲突。

参考文献

1 杨凝，周璇．国内智慧医疗领域研究热点及前沿文献可视化分析［J］．中国数字医学，2023，18（4）：104 – 111.

（下转第 101 页）

2025, 31 (5): 119 - 128.
17 燕建欣, 张晓琳, 刘晓宇, 等. 数智时代医学检验技术专业建设的转型路径探究 [J]. 卫生职业教育, 2025, 43 (15): 7 - 10.
18 王金, 王秋杰, 赵文龙, 等. 教育数字化转型背景下智慧医学人才培养探索 [J]. 医学信息学杂志, 2024, 45 (10): 1 - 6.
19 肖瑞, 蔡晓鸿, 胡芳, 等. 智能医学背景下医工融合型一流专业人才培养模式探索 [J]. 医学信息学杂志, 2024, 45 (8): 96 - 99.
20 University of California, Irvine. Health informatics, minor [EB/OL]. [2025 - 09 - 09]. https://catalogue.uci.edu/donaldbrenschoolofinformationandcomputersciences/departmentofinformatics/healthinformatics_minor/.
21 李斌, 陈晶, 韩玉玺, 等. MES 训练结合检验流程对医学检验技术教学的优化效果 [J]. 中国卫生产业, 2021, 18 (6): 3.
22 ERTL H. The concept of modularisation in vocational education and training: the debate in Germany and its implications [J]. Oxford review of education, 2002, 28 (1): 53 - 73.
23 邹蕾, 鄢荣曾, 陈丽, 等. 新医科视域下“口腔医学 +”医工复合型创新创业人才培养模式探索研究——以 F 高校为例 [J]. 现代职业教育, 2025 (18): 37 - 40.
24 杨涛, 任海燕, 周作建, 等. 人工智能赋能中医学高质量发展面临的问题与挑战 [J]. 南京中医药大学学报, 2024, 40 (12): 1285 - 1290.
25 赵静, 陆宁云, 谢非, 等. 面向新工科的“AI + X”课程体系建设 [J]. 控制工程, 2024, 31 (12): 2230 - 2234.
26 IKUO S, HAJIME K, KIYOSHI S, et al. Developing medical education curriculum reform strategies to address the impact of generative AI: qualitative study [J]. JMIR medical education, 2023, 9 (11): e53466.
27 College of Public Health and Health Professions, University of Florida. AI in public health and healthcare [EB/OL]. [2025 - 09 - 09]. https://phhp.ufl.edu/academics/certificates/ai - in - public - health - and - healthcare/.
28 Department of Biomedical Informatics, National University of Singapore. Minor in biomedical informatics [EB/OL]. [2025 - 09 - 09]. https://medicine.nus.edu.sg/dbmi/education - 3/minor - in - biomedical - informatics/.
29 吕文晶, 李国杰. 计算工程教育范式转变 [J]. 高等工程教育研究, 2025 (6): 8 - 12, 46.
30 张斌, 祝小静, 闫雪, 等. 面向未来学习的学术资源保障平台建设研究 [J]. 大学图书馆学报, 2025, 43 (2): 5 - 15.

(上接第 93 页)

2 QAFZEZI E, BYLYKBASHI K, AMPRIRIT P, et al. An intelligent approach for cloud - fog - edge computing SDN - VANETs based on fuzzy logic: effect of different parameters on coordination and management of resources [J]. Sensors, 2022, 22 (3): 878.
3 王刚. 一种基于 SDN 技术的多区域安全云计算架构研究 [J]. 信息网络安全, 2015, 15 (9): 20 - 24.
4 葛晨洋, 刘勤让, 裴雪, 等. 软件定义网络中高效协同防御分布式拒绝服务攻击的方案 [J]. 计算机应用, 2023, 43 (8): 2477 - 2485.
5 郭雅, 李泗兰, 林国安. 基于 SDN 架构的云计算中心网络安全防护体系设计 [J]. 信息与电脑, 2024, 36 (22): 86 - 88.
6 MEHMOOD K T, ATIQ S, HUSSAIN M M. Enhancing QoS of telecom networks through server load management in software - defined networking (SDN) [J]. Sensors, 2023, 23 (23): 9324.
7 裴炜旻, 王继伟, 彭宏, 等. 基于 SDN 技术的数据中心网络改造设计与实践 [J]. 微型电脑应用, 2023, 39 (2): 27 - 29.
8 ASAITHAMBI S, RAVI L, KOTB H, et al. An energy - efficient and blockchain - integrated software defined network for the industrial internet of things [J]. Sensors, 2022, 22 (20): 7917.
9 陈宇, 韩久江, 刘建, 等. 云环境下面向“虚实融合”网络的 SDN 构建方法 [J]. 计算机工程与应用, 2023, 59 (3): 234 - 243.
10 HUSSAIN M, SHAH N, AMIN R, et al. Software - defined networking: categories, analysis, and future directions [J]. Sensors, 2022, 22 (15): 5551.
11 AHOUANMENOU S, VAN LOOY A, POELS G. Information security and privacy in hospitals: a literature mapping and review of research gaps [J]. Informatics for health and social care, 2023, 48 (1): 30 - 46.
12 GU J, SONG C, DAI H, et al. ACM: accuracy - aware collaborative monitoring for software - defined network - wide measurement [J]. Sensors, 2022, 22 (20): 7932.