文章编号:1671-4598(2021)10-0133-06 DOI:10.16526/j.cnki.11—4762/tp.2021.10.024 中图分类号:TN915.08 文献标识码:A

基于大数据技术的智慧校园安全管控平台设计研究

廖海生
(广东科学技术职业学院 计算机工程技术学院,广东 珠海 519090)

摘要:针对传统校园网络安全防御手段已无法应对当前大数据背景下的智慧校园安全威胁问题,提出一种基于大数据技术的智慧校园安全管控平台设计方案;该方案将智慧校园体系分层、分类设计安全防护机制,实现对智慧校园安全的粒度防护管理;运用大数据技术构建智慧安全大脑,解决了智慧校园数据混乱、数据关联难问题,实现智慧校园数据融合存储;通过智能运营管理平台全面感知智慧校园安全态势,实现风险预测、安全预警、安全处置以及防护加固智能联动;通过模拟攻击测试与安全风险评估,部署智慧校园安全平台后智慧校园安全防御能力明显加强和安全风险等级明显降低,经过实际应用分析,智慧校园安全告警和自我处置能力也明显提高。

关键词:智慧校园;智慧安全大脑;数据融合;安全管控平台;安全态势

Research on the Design of Smart Campus Security Management and Control Platform Based on Big Data Technology

LIAO Haisheng
(School of Computer Engineering Technology, Guangdong Polytechnic of Science and Technology, Zhuhai 519090, China)

Abstract: Aiming at the problem that the traditional campus network security defense means can no longer deal with the security threat of smart campus under the current big data background, a design scheme of smart campus security management and control platform based on big data technology is proposed. In this scheme, the smart campus system is layered and classified to design the security protection mechanism, which realizes the granular protection management of the smart campus security; The big data technology is used to build a smart security brain, which solves the problems of data confusion and data association in smart campus, and realizes data fusion storage in smart campus; Fully perceive the security situation of smart campus through the intelligent operation management platform, and realize the intelligent linkage of risk prediction, security early warning, security disposal and protection and reinforcement. Through simulated attack test and security risk assessment, after deploying the smart campus security platform, the security defense capability of the smart campus is significantly strengthened and the security risk level is significantly reduced. Through practical application analysis, the security alarm and self-treatment capability of the smart campus are also significantly improved.

Keywords: smart campus; intelligent and safe brain; data fusion; safety management and control platform; security situation

0 引言

长期以来,校园网络安全体系的设计主要以防为主,受 PDR、P2DR、IATF 等指导模型的影响,以往校园网安全体系建设重点在检测与防御上建设,通过实时的在线检测御黑客于网络之外。但从近些年发生的大量网络攻击案例发现,现有的安全防御体系并未能彻底抵御所有的网络攻击,如美国国家安全部、NASA、伊朗核设施等组织的网络安全体系将检测、防御技术建设到极致,但仍然被攻击者成功渗透。

而随着云计算、大数据的兴起,高校信息化正从数字化进入智慧化,智慧校园建设成为高校发展建设、综合服务、竞争力的驱动力,智慧校园主要是利用云计算、大数据等技术构建全面感知校园物理环境,智能识别师生个体特征和学习、工作情景、行为轨迹,将科研、办公、管理、教学、生活等业务深度融合,将人与人、人与物、物与物的频繁互动行为进行互通融合,因此智慧校园数据种类繁多、数据量将成几何式的增长,校园大数据将对高校网络空间安全带来极大的冲击,特别是在日益猖獗的网络攻击面前,传统的网络安全防御手段已显得力不从心,无法应对当前大数据背景下的校园网络安全威胁。

1 大数据背景下校园网络存在的安全隐患

随着高校智慧校园建设的不断推进,各高校大力利用大数据、云技术与人工智能等新技术开发并拓展学校管理与服务应用,如 AI 摄像机构建的平安校园、物联网技术构

收稿日期:2021-08-04; **修回日期**:2021-09-01。
基金项目:广东省教育厅特色创新项目(2020KTSCX240);广东省高校党建研究课题(2020GZ048);校级教改资助项目(JG201901)。
作者简介:廖海生(1978-),男,江西樟树人,副教授,主要从事信息安全、网络舆情、教育信息化、大数据技术等方向的研究。
引用格式:廖海生.基于大数据技术的智慧校园安全管控平台设计研究[J].计算机测量与控制,2021,29(10):133-138,186.

建的绿色校园、人脸识别技术构建的行为管理系统、随时随地的网络教学平台、互联互通的新媒体等，高校业务对互联网越来越依赖，校园内人、物的关联性和复杂度不断提高，网络、设备、数据不断集中化。因此，高校网络空间安全将面临新的挑战，存在的安全隐患也将越来越多。

1.1 数据存储传输存在安全隐患

一是在大数据背景下，高校智慧校园大数据中心实现高校数据高度共享，数据共享给学校教学管理、数据应用等带来便利的同时，高校大数据中心也成为黑客攻击的重要对象；二是师生个人数据高度共享，个人数据完全暴露于网络，将存在个人隐私泄露问题；三是数据共享方便师生快速的查询到自己所需的信息资料，在不断普及信息共享意识和拓宽信息的获取途径的过程中也加大了信息被窃取的概率；四是随着互联网技术高速发展，高校万物互联，互联网高度互通，在方便用户快捷传输数据的同时也给网络黑客带来可乘之机，在传输中可能存在信息被暴露或被截获的安全隐患。

1.2 网络物理设备存在安全隐患

一是高校智慧校园的建设使得服务器、存储、交换机等网络设备种类、数量不断增加，网络设备集成共享度也越来越高，高校业务对网络设备的依赖性更加强，但由于经济问题很多高校没有建立容灾机制，网络设备存在单点故障风险；二是智慧校园部署了感知层，感知层节点数量多、感知设备多，部署比较分散，感知层设备的安全管控难度大。

1.3 网络安全管理机制存在隐患

一是高校智慧校园建设存在重建设、轻管理，重应用、轻安全的现象，高校网络安全管理工作受限于人员编制、运维成本等因素，缺乏顺畅的管理机制、精细的管控服务、规范的运维流程[1]，网络安全管理体系制度不健全以及组织机构设置不合理，存在管理风险；二是未对智慧校园网络安全进行全面评估，技术对策具有滞后性，依旧还是采用访问控制技术、入侵检测技术、防火墙等传统防御技术防御连接层，潜在于应用层的安全威胁难以及时预防和监控，网络管理对策也往往滞后于智慧校园安全管理，且都是被动防疫，难以满足大数据背景下的网络安全管理需求[2]。

2 智慧校园网络安全体系设计

2.1 安全风险分析

目前高校智慧校园建设体系主要分基础设施层、支撑平台层、智慧应用层和表现层，如图 1 所示。要有效防护整个智慧校园，就要针对智慧校园建设体系各层的应用特征分析各层可能存在的安全问题[3]。

1）智慧校园基础设施层安全问题：智慧校园基础设施层主要包括有线网络、无线网络、物联网、云存储与云计算架构，根据基础设施层的特征，主要存在服务器虚拟化安全、网络边界安全等安全问题。

2）智慧校园支撑平台层是整个智慧校园系统的核心部分，包括各种应用引擎、开发平台、数据中心、认证平台等，支撑智慧校园应用与服务，因此本层重点存在代码安全以及各类支撑平台的防御能力问题。

3）智慧应用层是智慧校园的各种应用系统，为各级用户提供智慧应用和服务，是用户体验感最强的部分，也是直接面对用户的部分，这些应用与服务大多采用微应用、微服务架构，每个微应用、微服务都可独立提供服务，因此本层主要需要考虑应用系统代码安全和系统应用安全问题，以及用户的身份认证安全、行为安全问题。

4）表现层是利用各类终端设备和 WEB 系统实现信息的进与出，即为信息采集和信息展示，所以本层安全主要存在终端设备的安全、WEB 系统安全、新媒体安全、移动终端的远程接入与工作安全问题。

2.2 安全体系设计思路

高校智慧校园网络安全体系设计总体思路是：基于智慧校园建设体系防护对象，遵循安全可靠、动态兼容、融合创新、管理便捷、先进与标准并存以及多重保护的原则，以数据安全为核心构建云＋端＋边界的互联网络安全生态体系，具有风险识别能力、安全防御能力、安全检测能力、安全响应能力与安全恢复能力，最终实现风险可见化，防御主动化，运行自动化的安全目标，保障学校业务的安全。

1）以数据为核心的设计思路。传统的网络安全防御体系设计思路是监测某一时刻的攻击行为，具有片面性，而以数据为核心的设计思路是监测某微小数据，它能将整个攻击过程都记录下来，并且能回溯分析全过程，还原攻击的全貌。

2）纵横协同防御思想。以智慧校园硬件基础架构层次为纵向，建立从虚拟化安全到网络层安全、应用及数据层安全的多层安全防护；以智慧校园业务应用为横向，建立账号及口令安全、文件权限、管理策略安全、运营安全等协同安全防护；针对外部攻击，建立边界安全防护、内网安全防护及终端安全防护的协同防护体系[4]。

3）内外兼顾的运营管理策略。应对内部应用快速变化带来的安全威胁，以漏洞为核心建立全生命周期的漏洞管理体系；应对外部攻击方式多样化带来的威胁，以威胁为核心结合威胁情报感知、应急响应和恢复过程流程，逐步摆脱被动应对方式，建立能够主动感知和预警的威胁防护体系[5]。

4）技术与管理相结合的思路。成立安全职责部门，设置专职安全运营岗位，完善信息安全管理制度、规定，组织安全培训并监督安全制度的执行情情况，实施奖惩制度，对安全策略的执行纳入员工考核[5]。

3 智慧校园安全管控平台设计

3.1 智慧校园安全管控平台总体框架

智慧校园安全平台是基于智慧校园体系而设计，针对智慧校园体系各层的应用特征进行安全防护设计，在智慧校园各层部署感知器以及在关键网络口部署流探针，通过数据采集器及时采集感知器和流探针的数据，经过预处理送智慧安全大脑，为智慧运营管理平台全面感知智慧校园安全态势提供数据支撑，及时分析处置安全威胁，预测智慧校园安全风险[6]。其总体架构图 2 所示。

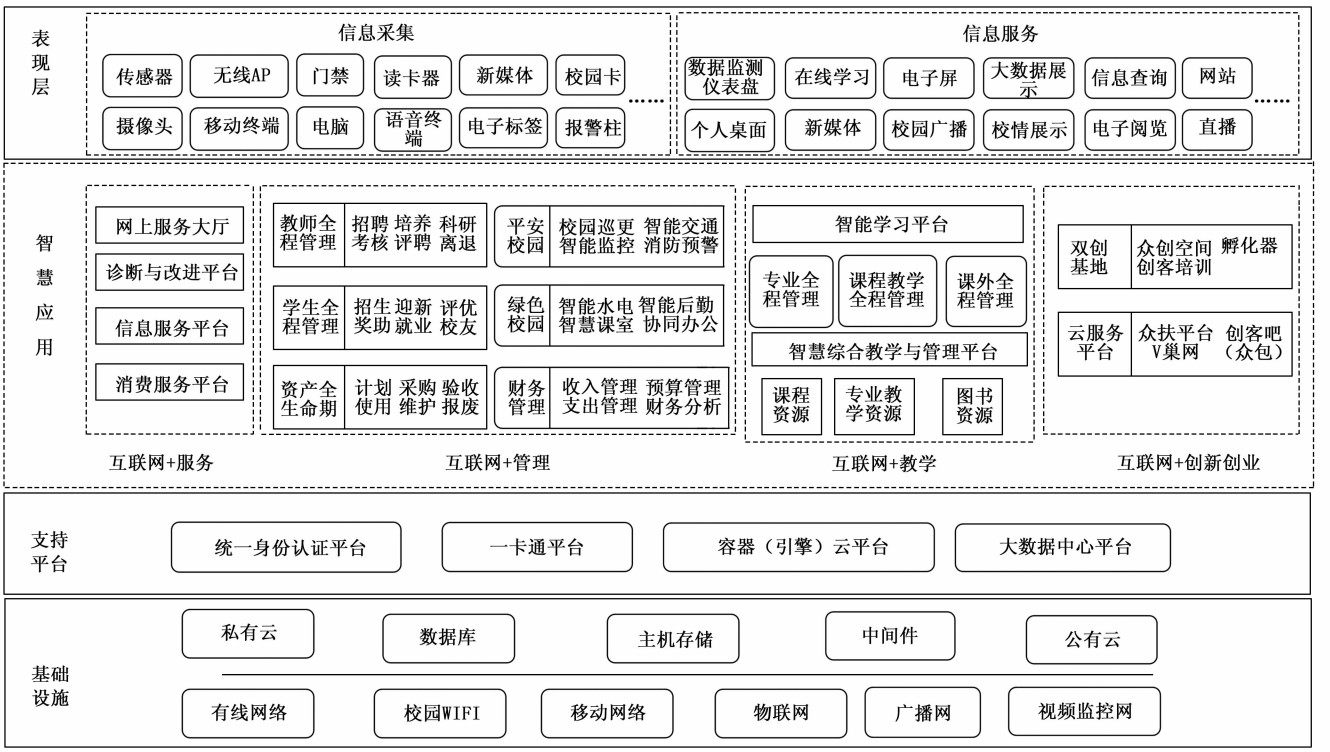

图 1　智慧校园建设体系架构

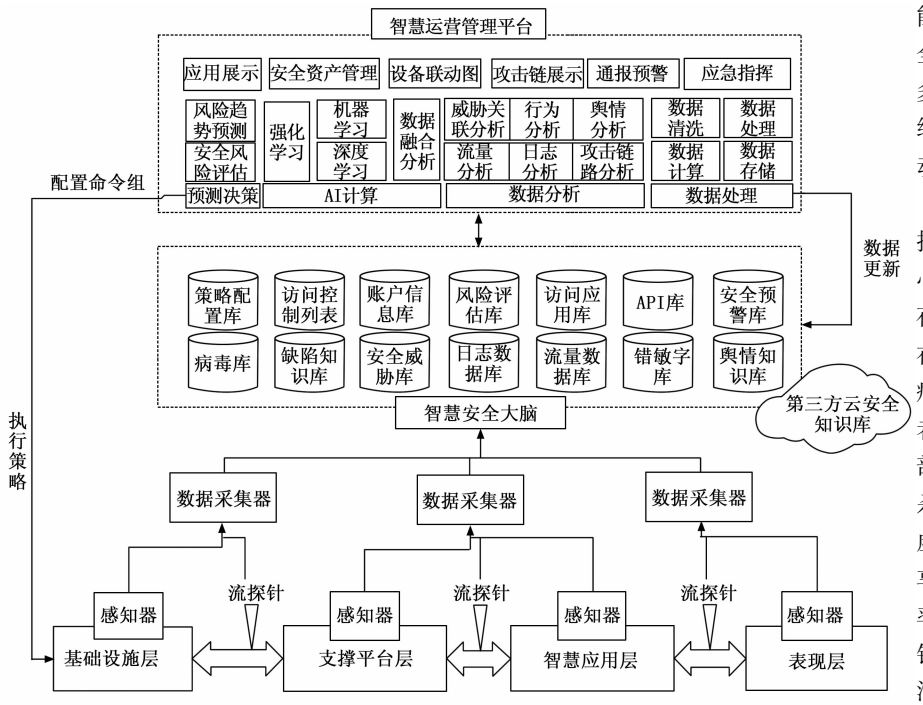

图 2　智慧校园安全管控平台总体框架

3.2　智慧校园基础设施层安全设计

智慧校园基础设施层主要包括有线网络、无线网络、物联网、云存储与云计算架构，它既是智慧校园第一道防线又是最底防线，主要存在服务器虚拟化安全、网络边界安全等安全问题。面对大数据时代安全风险，只依靠本地的高性能、多功能的安全产品来防护基础层安全远远不够，要从传统的被动防护转为多层安全防线的主动防御，采集大量网络数据，通过智慧安全大脑智能分析，动态感知安全威胁[7]，主动防御攻击。

1）服务器安全设计。智慧校园是把物理服务器资源虚拟化构建云数据中心，不受物理的界限隔离，构建计算、存储动态资源池，实现集中管理应用。在设计服务器安全时，一是要设计智能病毒查杀功能。服务器虚拟化后，攻击者一般是直接通过应用侵入到虚拟机内部，根植木马病毒，因此需要设计云查杀＋本地查杀相结合病毒防御模式，对虚拟机及服务器进行扫描结果缓存共享，采用增量扫描模式提高扫描效率[8]；二是物理主机的安全防护重点是针对 Windows 或 Linux 等操作系统的漏洞设计，通过智慧安全大脑智能感知系统漏洞，并进行统一管理和更新；三是智能安全策略更新机制。服务器虚拟化后各虚拟机数据将动态互迁移，这就可能造成将不同安全策略的数据迁移到不同安全策略的虚拟机上，导致虚拟安全域混乱，因此需要在各虚拟机中安装智能感知模块，将感知信息传回智慧安全大脑，智慧安全大脑匹对涉及的各虚拟机安全策略，并以增量模式更新各虚拟机安全策略，

有效解决虚拟机漂移造成的虚拟机之间的互相攻击问题。

2）边界安全设计。边界安全是智慧校园网络第一道防护，主要是保护校园网络由外至内，保障校园资源不受外部攻击，以及由内向外，防止外部网络攻击。传统的边界安全部署有防火墙、行为审计、VPN 系统、入侵检测系统等安全产品，重点是在高校网络出入口的位置对攻击进行封堵，但网络的物理出入口并不是攻击者进入到网络的唯一途径[9]，入侵到网络内部有很多可选择的途径与突破口，如 PC、智能终端、师生用户、应用软件、网络服务等都将成为攻击者攻击的入口与突破口，因此网络的安全边界是逻辑边界，不是传统的物理边界。其安全设计思路：一是设置多层级防护，延长攻击路线和攻击时间，让攻击者尽可能多的暴露出异常行为，获取攻击行为数据，依靠大数据分析提前发现分析威胁，主动出击；二是设计精细化的用户访问控制策略和数据进出策略。即时在各逻辑边界安装威胁感知模块，并与智慧安全大脑、云端威胁检测中心联动，形成立体化分析检测，对进出数据和用户访问请求进行检测分析，及时响应，作出处置、防护[10]。

3.3 智慧校园平台层安全设计

智慧校园支撑平台层是整个智慧校园系统的核心部分，犹如应用引擎主板，连接各种应用，包括各种应用引擎、开发平台、数据中心、认证平台等。支撑平台是智慧校园系统的核心代码，平台软件的代码安全漏洞和未声明功能（后门）是智慧校园支撑平台的重要安全隐患，因此支撑平台本身的代码安全问题和平台防御能力是重点问题。

智慧校园支撑平台层的安全只依靠基础设施层的安全防护远远不够，无法解决自身代码安全问题，因此需要设计一款智能代码安全管理平台对平台软件的代码安全进行安全管理。一是代码安全自动检测机制，智能代码安全管理平台实时监测平台软件及各类接口应用代码，一旦源代码变化即预警，自动分析代码与漏洞库进行匹配，一旦代码存在漏洞也及时预警[11]；二是源代码安全自动加固机制。智能代码安全管理平台联动两个以上成熟的第三方代码安全加固软件，检测发现代码变化或漏洞，将调用第三方代码安全加固软件修复代码，同时对代码进行代码混淆及代码加固处理。

3.4 智慧应用层安全设计

智慧应用层主要包括门户网站和其它业务系统，信息系统等级保护第三级要求业务系统自身应具备“身份鉴别、访问控制、安全审计、通信完整性、通信保密性、软件容错和资源控制”等安全功能[12]。因此本层主要需要考虑应用系统代码安全和系统应用安全问题。应用系统代码安全采用智能代码安全管理平台进行防护，系统应用安全问题则重点考虑用户身份认证安全、行为安全问题。

1）智能访问控制平台设计。随着高校智慧校园建设的推进，学校应用系统不断丰富，为解决用户账户繁多，方便用户使用，智慧校园采用了统一身份认证系统，但也使得各类应用安全管理、用户权限管理存在巨大难度。智能访问控制平台就是解决应用安全管理、用户权限管理、账户安全管理等问题，包括智能身份认证、智能感知等功能。

智能身份认证提供统一用户身份管理服务和权限管理服务。（1）将各应用系统的账户统一收回，集中管理，实现应用统一入口认证；（2）将各应用系统访问权限收回，实现应用权限统一管理，建立包括账户与应用权限对应的访问控制列表，实现细粒度的访问权限控制；（3）执行过程。智能身份认证模块收到访问请求（包括账户信息、访问应用），将验证访问者的用户身份信息，验证通过后由智能权限管理模块验证应用身份，从访问控制列表中匹对其访问权限，然后由智能权限管理模块充当代理与应用系统建立应用/API 访问服务，提供授权访问，虽然该账户可能具有多个应用访问权限，但是本次未申请访问的内容不具有访问权限，实现一申请一访问[13]。

智能感知是感知用户访问过程中的各种行为，通过行为日志如对用户请求、身份认证、访问授权、应用访问等行为变化进行风险分析与评估，并及时预警，根据访问风险行为和异常信息，进行智能分析，及时更新用户的身份及权限信息，实现自我学习能力，不断提升风险防范能力。

2）智能行为安全管理设计。智能行为安全管理平台包括数据采集、智能分析、智能预警等功能。通过采集用户上网行为、网络设备以及应用系统日志等数据，利用大数据技术进行分析，为智慧校园安全起到事前预警、事中控制，事后溯源的作用[14]。（1）校园舆情预警作用。通过师生上网行为数据分析，可及时发现师生异常动态，如晚归、高消费、网贷趋向、沉溺网络、思想动态等，及时采取措施避免校内舆情事件；（2）业务预警作用。通过学生学习、图书资源等数据分析，可实现学生成绩、资源利用效率等预警；（3）设备故障预警。通过设备日志数据分析，可提前分析出设备异常，提前做好维护，保障设备不间断运行。

3.5 表现层安全设计

表现层是用户使用各种终端体验智慧校园各类应用的入口，高校内网终端设备数量多、种类丰富以及用户种类多等原因给智慧校园网络造成巨大安全隐患，其主要做好终端设备和 WEB 页面的安全防护。

1）智能终端设备安全防护机制。为解决在终端设备安装杀毒软件只是被动防范，而不能主动发现未知安全威胁的问题，本设计采用蜜罐原理设计多层次的终端威胁防护机制。第一层为引诱层，将空闲 I P 分配给蜜罐服务，将攻击者流量重定向到隔离网络内的蜜罐环境中，在保护真实 IP 免受入侵的同时收集攻击者信息；第二层为动态虚拟层，当攻击者识破不是他们真正的目标 IP，发现攻击者试图改变攻击路线，根据捕获攻击者日志，将真实 IP 切换到热备 IP，而将原来真实 IP 动态构建为虚拟环境，为了拉长攻击者攻击路径，捕获攻击者更多攻击行为数据，动态虚拟层将根据实际自动构建多层次，直到通过分析攻击行为数据能有效捕杀攻击者为止[15]。

2）智能 WEB 安全防护平台。目前高校应用系统都采

用 B/S 架构，通过 WEB 页面直接与用户打交道，因此 WEB 页面也成为攻击者首先对象，数据泄露、页面篡改、挂黑链、错敏内容等时有发生。结合当前 WEB 攻击内容，利用大数据分析技术构建基于公有云的智能 WEB 防护平台。该平台包括智能监测、智能分析、智能处理等功能模块。智能监测是 7 * 24 小时服务模式，实时监测网站内容变化情况，如是否被篡改、网站是否有外链、是否存在敏感图片、潜在问题等，与原内容模板进行匹配，生成网站内容安全监测报告；依靠第三方云端安全大数据资源库，智能分析模块利用大数据技术分析网站内容安全监测报告，并提出可行的处理方案给管理者，管理者通过向导式方法进行人工处理。

3.6　智能安全运营管理平台

智慧校园各层都部署了各类安全设备，并收集了大量安全日志和行为数据，为了能实现各层安全防护的联动性，安全日志和行为数据的统一管理分析，依托智慧安全大脑构建一个安全运营管理平台，使管理者能够全面感知智慧校园安全问题，及时处置安全隐患。包括感知模块、数据处理分析模块、决策处置模块[16]。

1）数据采集模块。数据采集模块主要的功能是采集各类安全数据。（1）通过在校园网出口、数据中心出口、各汇聚层等网络出口安装流探针监听流量，实时感知网络流量变化，生产流量日志；（2）通过在智慧校园各层部署数据采集器，捕获各层安全设备和软件的日志数据和行为数据。感知模块对采集器和流探针采集来的数据进行预处理，按照统一的归一化数据格式进行转换，转存到智慧安全大脑大数据平台，为后期安全事件分析、威胁呈现、追踪溯源等提供数据支撑。

2）数据处理分析模块。智慧安全大脑大数据平台对感知层采集的数据进行分布式存储、索引，利用数据关系规则引擎、资源管理引擎、数据搜索引擎、统计分析引擎等进行进行数据融合关联分析，基于数据融合分析的基础上，采用深度学习、机器学习、强化学习等技术分析识别并理解攻击行为和攻击意图，生成分析报告，及时告警响应。

3）决策处置模块。决策处置模块的主要任务是依据分析报告评估安全风险等级，预测威胁趋势。（1）根据安全风险的级别，生成联动策略下发给防火墙、IPS、WAF 等网络安全设备，采取相应的执行策略[17]；（2）根据安全威胁趋势分析，生成一组命令集合，触发各有关网络安全设备或软件进行更新安全防护策略，加固安全防御；（3）通过关联规则分析、同源分析、机器学习等技术对流量和日志数据进行挖掘，分析不同攻击阶段的关联流量元数据、行为、日志数据，重塑攻击者攻击全链，从而还原攻击原貌，准确反映出被攻击的网络资源、攻击者信息、受害人信息等。

4　实验结果与分析

4.1　测试场景

为了验证本设计各安全层的有效性，选取作者所在学校的智慧校园实际场景进行测试，测试场景主要选取智慧校园的边界区 W、隔离区 DMZ、数据服务区 D、终端设备区 H、应用服务区 B 等部分关键设备和应用作为测试对象[18]，部署后的测试网络拓扑图如 3 所示，部署前 W1、F1、F2、F3、F4 都为普通级防火墙。

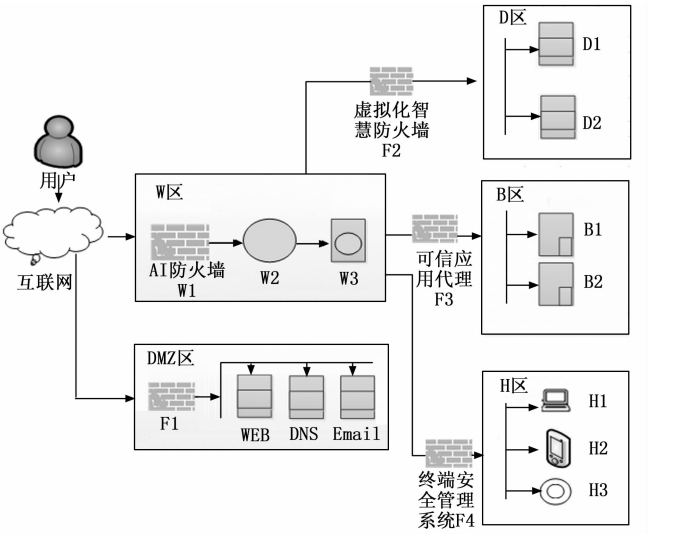

图 3　智慧校园安全平台部署后测试网络拓扑图

DMZ 是位于内部网络与外部网络之间[19]，该区域部署了 WEB、Email、DNS 等服务器，实验选取 WEB 服务器进行测试；W 区为网络边界区，部署了防火墙 W1、边界路由器 W2、核心交换机 W3 等，选取防火墙 W1 进行测试；D 区为云数据中心，选取 1 台虚拟数据服务器 D1 和一台虚拟应用服务器 D2 进行测试；H 区为终端设备区，选取终端主机 H1 和移动终端 H2，无线 AP 设备 H3；B 区放置应用服务器，选取教务系统 B1、OA 办公系统 B2 作为测试对象。智慧校园安全平台部署前与部署后各测试对象网络安全环境情况如表 1 所示。

表 1　智慧校园安全平台部署前后网络安全环境情况

区域	部署前方案		部署后方案
W 区	传统防火墙＋入侵防御系统＋入侵检测系统		边界 AI 防火墙＋威胁情报中心
D 区	数据库防火墙＋数据库审计系统		虚拟化智慧防火墙＋数据库审计系统＋安全代码卫士
H 区	H1	防病毒系统＋安全卫士	防病毒系统＋可信浏览器＋终端环境感知系统
	H2	防病毒系统＋安全卫士	移动环境感知系统＋移动应用自防护系统
	H3	传统防火墙＋无线 AP 安全策略	无线入侵防御系统＋无线 AP 安全策略
B 区	传统防火墙＋统一身份认证系统		可信应用代理平台＋用户行为分析系统＋隐私卫士
DMZ 区	防火墙＋WAF＋邮件威胁检测系统＋网页防篡改系统		Web 防火墙＋网站安全云防护系统＋邮件威胁感知系统

4.2　测试数据

为了进行智慧校园安全性能测试，设计了 4 条测试攻击路线，并使用不同攻击方式进行模拟测试[19]，如表 2 所示。

表 2 智慧校园安全性能测试数据

序号	攻击目标	攻击路线	节点数	模拟攻击方式
1	WEB 服务器	攻击者→互联网→F1→WEB	4	Web 渗透
2	B1 应用系统	攻击者→互联网→W1→W2→W3→F3→B1	7	DDOS 攻击
3	D1 数据库	攻击者→互联网→W1→W2→W3→F2→D1	7	漏洞扫描
4	H1 主机	攻击者→互联网→W1→W2→W3→F4→H1	7	病毒攻击

4.3 模拟攻击测试结果与分析

采取不同次数的循环攻击，通过安全设备管理系统捕获攻击数据到达攻击路线上各节点情况（以攻击者为第一个节点）[20]，各路线测试情况如图 4～图 7 所示。

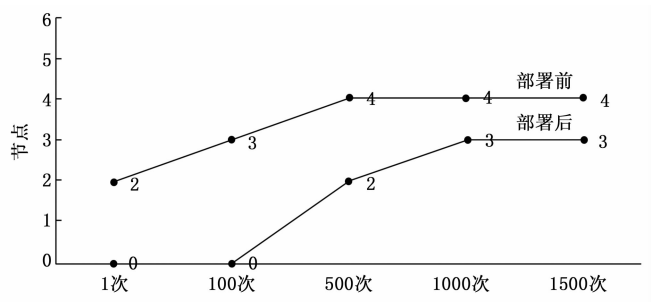

图 4 路线 1 测试结果

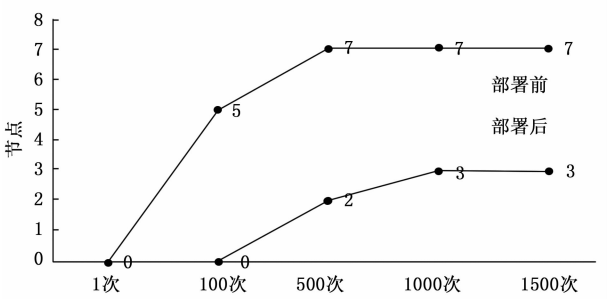

图 5 路线 2 测试结果

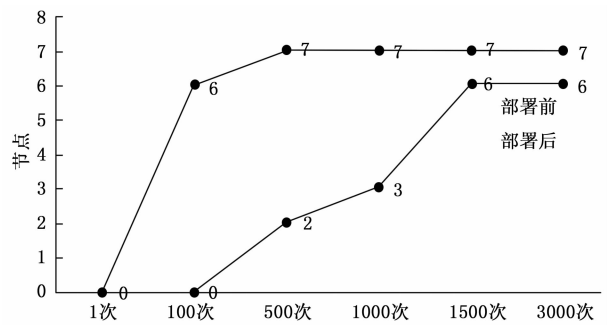

图 6 路线 3 测试结果

由图 4 可知，安全平台部署前在发起 500 次渗透时，在 Web 服务器端就收到攻击信息，而部署后在进行 1 500 次循环渗透，攻击者还未通过边界 AI 防火墙。

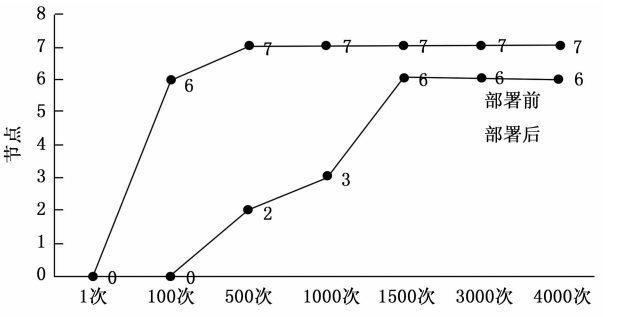

图 7 路线 4 测试结果

由图 5 可知，安全平台部署前在发起 100 次 DDOS 攻击时，核心交换机 W3 就收到攻击信息，在发起 500 次 DDOS 攻击已经攻破目标系统 B1，100 次时目标应用系统瘫痪；而部署后在发起 1 500 次 DDOS 攻击还未攻破边界 AI 防火墙。

由图 6 可知，安全平台部署前在发起 100 次漏洞扫描时，D 区防火墙已收到攻击信息，并在 500 次时攻破 D 区防火墙，D1 服务器收到攻击信息，在 1 000 次时 D1 服务器宕机；而部署后在发起 1 500 次漏洞扫描时，F3 才收到攻击信息，并一直有效防御未被攻破。

由图 7 可知，安全平台部署前在发起 100 次病毒攻击时，H 区防火墙已收到攻击信息，并在 500 次时攻破 H 区防火墙，H1 主机收到攻击信息，在 1 000 次时 H1 被病毒感染；而部署后在发起 1 000 次病毒攻击时，W1 才收到攻击信息，1 500 次攻击时 F4 才收到攻击信息，并一直有效防御，H1 未被病毒感染。

由此可见，部署智慧校园安全平台后，智慧校园各关键区域和关键设备安全防御能力明显增强，遭受多次循环攻击后安全防护能力都趋于稳定。

4.4 安全风险测试结果与分析

对智慧校园安全平台部署前后进行智慧校园安全风险评估，使用开放式漏洞评估系统 OpenVAS 对智慧校园安全平台部署前后各路线的各服务器和主机进行漏洞扫描，获取各关键漏洞脆弱性信息[21]，如图 8 所示。从评估结果可看出部署了智慧校园安全平台后整体漏洞数明显减少，智慧校园安全水平明显提升。

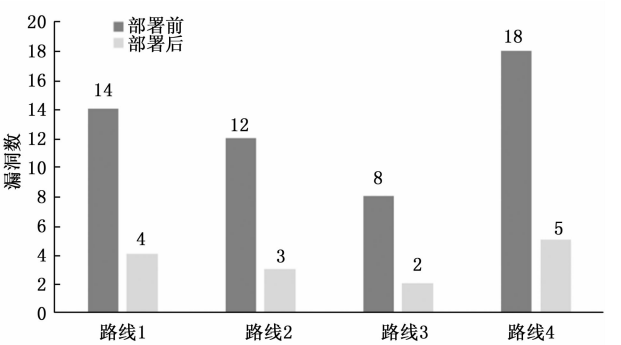

图 8 测试结果与分析图

（下转第 186 页）