网络信息安全防护体系构建与技术研究

李 莉

南京交通职业技术学院 江苏 南京 211188

【摘 要】：云端业务与移动办公的普及，让网络边界呈现泛在化特征，智能化、定向化的新型网络攻击日益增多。当前多数政企沿用设备堆叠式被动防护模式，防护体系零散，风险识别和处置存在明显滞后性，难以适配复杂的网络攻防场景。本文结合基层网络运维实际痛点，搭建多层级立体化闭环防护体系，优化态势感知、动态访问控制、数据防护、攻击溯源四项核心技术，配套完善落地性运维与管理制度。该方案可有效弥补传统防护模式的技术与管理短板，提升网络安全防控效能，可为政企网络安全规范化、实战化建设提供一定的实践参考。

【关键词】：网络信息安全；防护体系；智能防御；安全技术；风险防控

DOI:10.12417/2811-0528.26.19.069

引言

网络信息安全是数字政务与企业数字化转型的重要基石，直接关系业务系统稳定运行与核心数据资产安全，是现阶段网络治理工作的核心内容。云计算、泛在互联技术的广泛应用打破了传统固定网络边界，多元终端混合接入使得网络运行环境愈发复杂，变异木马、数据勒索、定向渗透等新型威胁频发，网络安全防控压力持续增大。现有学界研究多聚焦单一安全技术迭代或宏观制度框架设计，整体偏向理论推演，与基层常态化运维场景适配度有限。多数成果缺乏体系化层级设计，未能打通技术应用与日常管理的衔接渠道，难以解决防护割裂、复盘不足、管控松散等实操问题，相关落地性研究仍存在明显缺口。基于上述研究现状，本文围绕架构搭建、技术优化、机制完善三个维度开展系统性研究，构建分层联动的立体化防护体系，优化适配新型攻防场景的核心技术，配套闭环运维保障策略。研究兼顾合规要求与实战需求，可有效补齐传统防护短板，为基层网络安全常态化、实战化治理提供新的实践思路与参考方案。

1 网络信息安全防护体系整体架构构建

1.1 体系构建的基本原则与设计思路

为有效解决传统网络防护体系空泛化、形式化的建设弊端，本次体系构建全程贴合政企网络运维实战场景，摒弃脱离实际的顶层设计思路，将解决落地难题、补齐运维短板作为核心建设目标。体系建设首先遵循全覆盖防护原则，防护范围全面覆盖机房硬件、网络链路、业务系统、数据文件、办公终端等所有网络组成部分，以此杜绝局部防护遗漏、风险管控空白等问题。与此同时，建设过程严格坚持动态适配原则，彻底摆脱传统固定边界防护策略的局限性，可根据终端实时接入状态、数据动态流转范围、系统漏洞更新情况灵活调整防护规则，能够有效适配移动办公与云端部署的新型网络运行环境[1]。

在实操落地层面，体系运行严格落实技管结合的核心原则，在部署技术防护设备的同时配套完善对应的管理制度与运维流程，从根源上规避硬件设备盲目堆砌但安全管理缺位的常见问题。整体架构采用闭环迭代的运行思路，将风险排查、实时监测、事件处置、复盘优化各个环节有效衔接，形成可持续优化、动态升级的循环防护模式。除此之外，架构设计兼顾通用性与扩展性，既能满足现阶段网络安全等级保护的基础合规要求，又可适配后续业务扩容、设备更新与新型安全设备接入的发展需求，能够保障整套防护体系长期稳定、高效可用。

1.2 立体化多层级防护总体架构设计

为适配政企单位真实网络拓扑结构与常态化运维流程，本文结合实际防护需求，设计五层防护层级搭配全域管理保障的实战化安全架构。其中五层防护体系分别对应物理设备、网络边界、业务系统、数据资源、终端设备五个网络运行核心环节，各层级均设置专属防护对象与标准化处置流程，实现风险的分层管控、逐级防御。在此基础上，全域管理运维体系贯穿所有防护层级，可统一汇总各类安全日志数据、统筹调度全网运维工作、规范各岗位责任分工，有效解决传统防护模块独立运行、数据不通、联动不足的落地难题。

作者简介：李莉（1978.03-），女，汉族，江苏省溧阳市，副教授，大学本科，计算机网络技术，信息安全。

整套架构的各层级功能定位清晰明确、互不重叠，完全贴合基层实际运维工作，不存在防护内容重复交叉的问题。具体来看，物理层主要负责硬件设备的稳定运行保障，网络边界层承担内外网数据交互的安全过滤工作，系统应用层聚焦业务程序与系统漏洞的常态化管控，数据层专门针对核心业务数据开展专项防护，终端层重点管控办公设备与用户操作行为。而管理保障体系主要负责制度落地、运维考核与应急处置工作，能够为每一项技术防护措施匹配对应的标准化管理流程，真正实现技术部署与日常运维的深度融合、协同发力[2]。

1.3 各防护层级功能定位与防护逻辑

物理安全层构成整套防护体系的底层根基，主要承担机房硬件设施防护职能，应对断电、设备故障、线路老化、外力损毁等实体风险。运维依托 7×24 小时机房监控、定期巡检、核心设备双备份保障硬件稳定，从源头规避硬件故障引发的全网瘫痪问题。在此基础之上，网络边界层作为内外网交互首道关口，通过管控高危端口、过滤异常流量、拦截恶意 IP，有效抵御外网批量扫描与渗透攻击。

若威胁突破边界防线，系统应用层面向服务器、业务平台常态化更新补丁、分级管控权限、扫描程序漏洞，及时封堵开源组件与程序后门。数据安全层是整体防护核心，覆盖数据传输、存储、使用、销毁全生命周期，针对性化解窃密、篡改、违规拷贝等高频风险，保障核心业务数据完整可控。

终端用户层为体系末端防线，借助安全软件、接入身份核验、全量操作日志约束终端病毒、违规入网、越权操作等人为隐患。全域安全管理运维体系统筹全部防护层级，统一规范运维流程、明晰岗位权责、制定巡检与应急标准，整合碎片化防护工作，为整套多层防护体系长效落地提供一体化支撑。

2 网络信息安全核心防护关键技术研究

2.1 主动式安全监测与态势感知技术

现有传统网络监测多依靠固定规则库识别攻击，这种被动检测模式存在显著局限性，面对持续演化的变异攻击与隐蔽渗透行为，极易出现大量漏报、误报，直接削弱风险识别精度。为弥补该技术缺陷，本文引入机器学习驱动的主动监测方案，重构传统被动匹配的检测逻辑。系统持续采集全网流量、账号登录、端口访问、系统操作等多维运维数据，通过算法挖掘网络常态运行特征，构建适配单位业务环境的专属安全基线[3]。在此基础上，系统实时比对实时行为与基线标准的偏差，精准识别异常登录、批量扫描、异常外联等隐性风险。与此同时，态势感知模块打通防火墙、终端、服务器的数据孤岛，统一归集安全信息并以可视化形式展示全网风险分布。借助集中化风险展示能力，运维人员无需人工逐条核对多设备日志，有效简化排查流程、提升处置效率，最终实现风险早发现、早预警、早处置的前置防护目标。

2.2 零信任架构下动态访问防护技术

传统内外网静态隔离模式适配场景有限，难以支撑远程办公、云端登录、外勤异地接入等新型业务；加之内网默认可信的静态授权机制，易滋生闲置账号、权限冗余、离职账号未注销等隐患，大幅提升非法越权访问风险。针对上述边界管控短板，本文引入零信任动态访问防护技术，彻底破除内网固有信任特权，建立持续核验、动态管控的访问体系。针对每一次登录行为，系统均从账号凭证、设备安全状态、接入网络、登录位置多维度完成综合校验。完成身份核验后，系统严格遵循最小权限原则分级授权，普通账号仅开放基础查询权限，核心数据操作、系统配置等高权限功能需单独审批、按需发放，从权限层面杜绝越权操作。一旦识别异地登录、陌生设备接入等异常行为，系统将自动触发二次核验或临时拦截，及时阻断账号盗用行为。该技术从根源化解泛互联场景下边界失控难题，使所有访问行为全程可控、可追溯，显著提升访问管控精细化程度。

2.3 数据全生命周期安全防护技术

从基层运维实际来看，数据安全风险集中体现在传输窃密、存储篡改、违规拷贝、过期残留四大场景，零散的单点防护手段难以形成完整防控能力。为此，本文构建覆盖数据全流转流程的防护技术体系，针对性化解各类实操风险。传输阶段采用高强度加密算法保护报文与文件，规避公网传输中的窃取、篡改风险；存储环节搭配密文存储与异地多备份，抵御硬件故障、恶意删改引发的数据损毁。在数据共享使用阶段，系统自动脱敏屏蔽身份证、手机号等敏感字段，同时为文件拷贝、外网发送附加溯源水印与操作记录，泄露后可快速定位责任源头；针对过期数据则采用专业粉碎销毁技术，消除普通删除带来的数据残留隐患。整套技术完整覆盖数据全生命周期，能够直接落地支撑单位数据合规管理工作。

2.4 网络安全事件溯源与研判技术

传统安全处置普遍停留在漏洞修复、病毒查杀等浅层操作，缺少对攻击链路的完整复盘，进而造成同类攻击反复爆发。为提升事件处置深度，本文采用实战化溯源研判技术，依托全量日志留存机制搭建完整行为溯源数据库。安全事件发生后，系统依托海量日志快速还原入侵端口、攻击时序、完整操作路径与影响范围，精准定位攻击源头。在此基础上，系统结合攻击特征库自动判定风险等级，区分端口探测、普通病毒、定向高危攻击等事件类型，为分级处置提供数据支撑。运维人员依据溯源结果定向封堵恶意 IP、修复漏洞、优化防护策略，同时将历次攻击样本纳入本地模型持续迭代，降低同类攻击复发概

率，长效巩固整体防护体系防御能力。

3 网络安全防护体系优化与落地保障策略

3.1 防护体系运行流程优化

纵观当前政企运维现状，传统网络运维流程呈现碎片化特征，风险处置环节存在明显滞后性，整体建设思路难以适配主动防御的发展方向。基于这一现实痛点，本文结合一线运维场景重构标准化闭环运维流程。在常态化运维阶段，单位先行搭建分层周期性排查机制，分阶段落地周度漏洞扫描，月度全域风险排查与季度合规自查。通过前置化隐患排查工作，各类弱口令、高危端口、系统漏洞等风险能够提前处置，从源头降低安全事件爆发概率。在此基础上，系统依托智能监测功能持续捕捉全网风险动态，结合风险危害范围划分对应处置等级。针对不同等级隐患，运维人员采取差异化处置手段，低危隐患做到当场整改，高危风险执行快速隔离，重大紧急隐患第一时间阻断，待安全事件处置工作全部收尾后，运维人员依托完整溯源日志开展深度复盘分析[4]。

3.2 常态化安全管理机制建设

从防护体系整体架构来看，技术防护设备是安全建设的硬件基础，完善的管理制度则是保障防护效果落地的关键支撑。二者相互配合，才能充分发挥防护体系实战价值。各单位结合等保规范与自身业务特征，细化设备管理、账号权限、数据外发审批、应急处置等实操制度，清晰界定各类网络操作标准。配套制度落地的同时，单位同步推行常态化合规自查，定期核查权限分配、设备策略、日志留存、数据分级管控等核心内容，及时整改各类不合规配置。为应对各类突发安全事件，运维团队针对病毒爆发、数据泄露、业务瘫痪、外网持续攻击等场景编制分级应急预案，明确完整处置步骤与岗位人员分工。除此之外，单位同步建立安全考核追责机制，把漏洞整改、日志管理、日常合规操作纳入绩效考核，逐层落实全员安全责任，避免管理制度流于表面形式。

3.3 人才、制度与运维综合保障

深入剖析基层运维瓶颈不难发现，人员专业能力不足、防护策略更新不及时、运维操作不规范三类问题，直接限制防护体系运行成效。为破解上述难题，单位可组建专职运维队伍，围绕态势感知、动态权限管控、数据防护、攻击溯源等核心模块开展专项培训，持续提升人员实战处置能力。日常运维过程中落实常态化值守巡查，在业务高峰、重点防护时段加大巡检力度，确保各类网络异常能够被快速识别处置[5]。单位同步定期优化设备策略，升级系统版本，更新防护规则，以此适配持续演变的新型网络攻击形态。全部防护建设内容严格遵循网络安全、数据安全相关法律法规，参照国家合规标准持续完善防护架构与内部制度。

4 结论

本文针对传统网络安全防护碎片化、被动化、落地性不足的现实问题，结合政企一线运维场景搭建多层级联动的闭环防护体系，优化四项核心安全防护技术，配套完善流程优化与制度保障措施。相较于现有单一技术与纯理论研究，本文构建的“架构-技术-保障”一体化方案，更适配基层网络安全实战场景，能够为常态化网络治理提供可行参考，具备一定的实践补充价值。后续可结合新型攻防技术迭代趋势，细化场景化防护策略，进一步提升防护体系的精细化与适配性。

参考文献：

[1] 郑吉龙,刘坚桥,王思羽,等.基于零信任架构的企业内网安全防护策略设计与实践[J].信息与电脑,2025,37(21):6-8.

[2] 郭宝霞,王佳慧,马利民,等.基于零信任的敏感数据动态访问控制模型研究[J].信息网络安全,2022,22(6):86-93.

[3] 卓柳俊,左鹏飞,胡国华,等.个人金融信息全生命周期安全管理实践[J].科技和产业,2024,24(22):184-189.

[4] 赵康.网络安全态势感知在企业应用中的研究[D].太原理工大学,2021.

[5] 孙峰,朱耿沛,孙艳,等.基于网络准入控制的企业内网终端安全防护研究[J].中国高新科技,2024,(9):72-74.