 DOI: https://doi.org/10.12345/bdai.v7i3.38177

Research on Collaborative Protection Mechanism Construction for Network Engineering and Information Security

Yanjun Ping

Beijing Zhongqi Times Technology Co., Ltd. Horinger Branch, Horinger, Inner Mongolia, 029200, China

Abstract

Against the backdrop of deepening digital transformation, network engineering has become the core foundational support for the operational development of various organizations, while information security serves as the critical line of defense to ensure the smooth operation of network engineering. Current cyber attacks exhibit diverse, covert, and intelligent characteristics. According to the "2024 China Cybersecurity Report," domestic enterprises have experienced a 47% increase in advanced persistent threat (APT) attacks compared to 2023, making single-network construction or security protection models insufficient to counter complex cyber threats. At present, most organizations face the issue of network engineering and information security operating in isolation, directly leading to reduced protection effectiveness. The annual average vulnerability remediation cycle reached 28 days, significantly higher than industry standards, with a 32% year-on-year increase in security incident rates. Based on practical application scenarios, this paper explores the core logic and practical challenges of collaborative protection between network engineering and information security from the perspectives of network engineering structural characteristics and information security protection requirements. It proposes practical and implementable collaborative protection methods to break through the traditional perception that "network construction focuses on connectivity while security protection emphasizes isolation," promoting deep integration and coordinated cooperation between network engineering and information security to enhance cybersecurity protection capabilities across organizations.

Keywords

network engineering; information security; collaborative protection; protection mechanism; implementation

网络工程与信息安全协同防护机制构建研究

平彦军

北京中企时代科技有限公司霍林郭勒分公司，中国·内蒙古 霍林郭勒 029200

摘　要

在数字化转型深度推进的背景下，网络工程已成为各单位运营发展的核心基础支撑，信息安全则是保障网络工程平稳运行的关键防线。当前网络攻击呈现多样化、隐蔽化、智能化特征，据《2024年中国网络安全报告》显示，国内企业遭遇的高级持续性威胁（APT）攻击较2023年增长47%，单一的网络建设或安全防护模式已难以抵御复合型网络威胁。现阶段多数单位存在网络工程与信息安全“各自为战”的问题，直接导致防护效果下降，全年平均漏洞修复周期达28天，远高于行业合理标准，安全事件发生率同比上升32%。本文立足实际应用场景，从网络工程结构特征与信息安全防护要求出发，阐述二者协同防护的核心逻辑与现实困境，提出兼具实操性与落地性的协同防护方法，突破“网络建设重连接、安全防护重隔离”的传统认知，推动网络工程与信息安全深度融合、协同配合，助力各单位提升网络安全防护水平。

关键词

网络工程；信息安全；协同防护；防护机制；落地实施

1 引言

互联网技术的普及使网络深度融入政府、企业及民众日常生活，网络工程规模持续扩大、结构日趋复杂，已从传统局域网逐步演进为云网络、物联网异构网络融合的复合型网络架构，所承载的核心数据与重要资产价值呈指数级增长，据统计，大中型企业年均网络数据存储量超 500TB，核心业务网络依赖度达 98%。与此同时，网络攻击的危害性、隐秘性与传染性显著提升，攻击形式从简单病毒入侵升级为 APT 攻击、勒索病毒、供应链攻击等复合型手段，攻击路径从外部渗透延伸至内部数据泄漏，2024 年国内企业因内部安全漏洞引发的信息泄露事件占比达 61%，信息安全风险遍布网络全生命周期。

当前诸多单位在网络工程建设中存在“重建设、轻安全”的误区，网络建设仅追求连通性与便利性，忽略安全体系的同步集成；安全防护则局限于单一设备部署，未结合网络结构进行系统性设计，最终导致防护系统与网络运行严重脱节，呈现“防不住、响应慢、难追溯”的三大痛点，超

【作者简介】平彦军（1977–），男，中国内蒙古呼伦贝尔人，本科，工程师，从事网络工程研究。

70% 的中小企业曾因网络与安全体系脱节遭遇过实质性网络攻击。因此，构建网络工程与信息安全一体化防护体系，推动二者有机结合、协同联动，改变各自为战的现状，是解决当前网络安全难题、保障网络工程稳定运转的有效途径，也是数字化时代下各单位亟待研究与落地的重要课题。

2 网络工程与信息安全协同防护的核心逻辑与现实困境

2.1 协同防护的核心逻辑

网络工程与信息安全协同防护的核心，是消除“网络建设”与“安全防护”的壁垒，践行“建设与防护并举、运行与管控结合”的理念，实现二者的深度融合、相互支撑。一方面，网络工程是信息安全的基础载体，脱离网络工程的结构特征、业务流程与节点布局，安全防护将成为“无的放矢”，无法精准识别网络架构中的潜在漏洞，据测算，未结合网络结构的安全防护，漏洞识别准确率不足 40%；另一方面，信息安全是网络工程的保障屏障，缺少信息安全的防护体系，再完善的网络结构、再高效的互联能力，也无法规避信息泄露、系统崩溃、业务中断等风险，2024 年因缺少安全防护导致网络工程瘫痪的企业占比达 29%。

协同防护的核心目标主要包含两层：一是防御黑客非法入侵，依托病毒查杀、入侵检测、行为分析等先进技术，构建全流程入侵防御体系，目前主流防护技术可实现 85% 以上的常规攻击实时拦截，有效保障个人与行业的正常用网质量；二是保障个人、行业实体的信息与系统安全，通过全维度的网络信息安全管理，防范系统故障、数据丢失与隐私泄露问题，实践证明，建立协同防护体系的单位，内部数据泄露风险可降低 76%，系统运行稳定性提升 90% 以上。

2.2 协同防护的现实困境

“先建设、后防护”模式导致体系脱节：多数单位在网络工程建设中，核心目标为设备互联、业务互通，往往在网络工程竣工后才考虑增设安全设备，超 60% 的传统企业网络工程未预设安全接口，后续加装的防火墙、入侵检测等设备无法与原有网络设备兼容，形成“设备孤岛”，安全防护与网络运行难以形成合力。

设备异构性引发数据与联动障碍：目前国内企业的网络硬件与安全硬件超 80% 采购自不同厂家，各厂商产品的通信协议、数据格式存在显著差异，导致设备间无法实现数据实时传输与联动处置。例如网络交换机检测到异常流量后，无法即时向入侵防御系统传递日志信息，安全产品发现漏洞后，也无法自动通知网络设备修改访问规则，需人工介入完成操作，平均处置延迟超 4 小时，且人工操作失误率达 15%，为黑客攻击创造了可乘之机。

缺乏集中式管理平台导致运维低效：超 75% 的中小企业未建立集中式网络与安全管理控制台，运维人员需登录 5 个及以上的设备管理界面才能实现全维度监控，不仅耗时耗力，工作效率降低 60% 以上，还难以全面掌握网络运行状况与安全威胁态势，极易遗漏关键安全预警信息。

3 网络工程与信息安全协同防护机制的构建原则

3.1 实用可行原则

协同防护机制的设计需紧密契合各单位的实际情况，综合考量网络工程的规模、结构复杂程度、业务类型，结合单位人力资源、财力物力等条件，避免采用过于繁琐的技术手段。对于网络规模小、业务单一的小型企业（占国内企业总数的 90% 以上），无需构建复杂协同防护体系，仅需做好接入层防护、终端安全与核心数据加密，即可满足基本安全需求；对于网络架构庞大、业务类型多样的大中型企业与政府单位，需建立多层次全方位协同防护体系，实现设备、技术、管理的深度配合。同时，机制设计需简单易懂，便于维护人员掌握使用，避免操作步骤过多、难度过大影响实际应用效果，保障防护体系的落地性与可操作性。

3.2 全面覆盖原则

协同防护机制需贯穿网络工程全生命周期、全层次，覆盖信息安全各方面、各环节，实现全方位无死角防护。在网络工程立项、设计、建设、运维的全流程中，同步融入风险评估、漏洞修复、攻击阻止、应急预案等安全工作；防护范围既包含内部网络、外部网络、云环境等各类网络环境，也覆盖终端设备、服务器、数据库等所有重要信息系统组件。例如在立项阶段同步明确安全防护要求，设计阶段预留安全接口、划定安全区段，建设阶段同步安装安全硬件，运维阶段实现 7×24 小时实时监控，从源头规避安全漏洞，据统计，实现全流程覆盖的防护体系，可将安全事件发生率降低 82%。

3.3 协同联动原则

协同联动是协同防护的核心基础，需实现设备、技术、管理、人员、部门的全方位协同。设备层面，打破不同厂家、不同类型设备的壁垒，实现信息共享与联动处置；技术层面，推动网络技术与信息安全技术深度融合，使网络结构设计符合安全防御要求；管理层面，建立跨部门沟通合作制度，明确各部门、各岗位的配合职责，实现上下联动、左右协同；人员层面，强化运维人员的协同防护理念，提升跨岗位协作能力，确保安全事故发生后，相关人员能快速响应、联合处理，将事故处置时间缩短 50% 以上。

3.4 动态优化原则

网络攻击方式与网络技术的更新迭代速度持续加快，据监测，全球平均每天新增网络攻击手段超 100 种，云网络、物联网等新技术的应用也不断改变网络工程结构，因此协同防护措施并非一成不变，需建立动态优化机制。在网络工程建设升级、业务需求变动或出现新型网络攻击方式时，及时调整优化防御措施：例如企业新增云业务时，同步在云端部署云防火墙、数据脱敏等安全防护措施；出现新型勒索病毒攻击时，立即更新防火墙、入侵检测设备的规则库，调整联动处置流程，确保协同防护体系始终适配最新的网络安全形

势，提升防护的有效性与准确性。

4 网络工程与信息安全协同防护机制的具体构建路径

4.1 规划建设协同：实现“建设与防护同步”

在网络工程前期规划阶段，组建由网络运维、安全运维、业务部门人员组成的联合工作组，根据业务需求确定网络结构设计、设备选型、区域划分方案，同步开展安全防护需求分析，明确安全设备安装位置、防护级别与联动机制。针对不同业务类型进行安全区隔，将核心业务服务器及数据库部署至隔离区，同步制定防火墙、入侵检测设备的部署计划，保障隔离区防护到位；设计远程登录功能时，同步采用零信任认证、VPN 加密等防护手段，将远程登录安全风险降低 90%。

网络架构设计需充分考虑安全防护需求，预留标准化安全接口，便于后期接入各类安全产品；采用分层设计思路，将网络分为接入层、传输层、核心层，在各层针对性布置安全设备，接入层部署接入控制设备，传输层部署加密设备，核心层部署入侵防御设备，实现各层级防护的相互配合。网络协议选择以高安全性为核心，优先采用 HTTPS、SSH 等安全协议，关闭无用服务端口与服务，据测算，合理关闭非必要端口可使网络攻击入口减少 70%，有效降低潜在安全隐患。

4.2 技术协同：构建“设备联动、数据共享”的防护体系

搭建一体化智能管控平台，整合网络运行监控、安全风险监控、设备管理、应急响应等核心功能，实现对网络设备、安全设备的统一管理，消除设备与系统间的“信息孤岛”。管控平台需具备 7×24 小时实时监控能力，可精准掌握全网运行状况与安全态势，及时发现网络故障与安全隐患并发出报警信号，报警响应时间控制在 1 分钟内。

实现平台与所有设备的信息交互与自动联动处置，建立“一处报警，全网联动”的防护机制：当接入层设备检测到非法终端连接时，管控平台立即发出警报，同步联动防火墙阻止该终端登录，通知入侵检测设备对其进行实时监视；当核心层检测到 APT 攻击时，平台迅速切断攻击路径，联动数据备份系统保护核心数据，同时启动攻击溯源分析。通过设备间的无缝联动，将安全事件处置时间从小时级缩短至分钟级，大幅提升防护效率。

4.3 管理协同：建立“责任明确、流程规范”的保障体系

制定《网络工程与信息安全联合防御管理规定》，明确联合防御的目标、原则、程序，划分各部门、各岗位的职责边界：网络运维人员负责网络设备日常巡检、维护、升级改造，确保网络设备运行稳定性；安全运维人员负责安全设备安装配置、策略调整、监控报警，及时处置安全隐患；业务部门负责本部门终端设备安全管理与信息保密，落实人员安全培训责任。

4.4 应急处置协同：实现“快速响应、高效处置”

根据安全事件的影响范围、危害程度，将其划分为一般事件、较大事件、重大事件三个等级，针对性制定应急预案与响应机制，明确各类事件的响应时间、处置程序、责任划分。一般事件（如单个终端病毒感染）由终端管理员配合安全运维人员处置，1 小时内完成病毒清除与终端恢复；较大事件（如局部网络入侵）由网络运维与安全运维部门联合处置，2 小时内切断攻击路径、修复漏洞；重大事件（如全网入侵、核心数据被盗）立即成立应急指挥部，统一指挥调度网络、安全、业务等所有相关部门，4 小时内完成应急处置，阻止攻击扩散。

5 结论

网络工程与信息安全协同防护是适配当前复杂网络安全形势、保障网络工程安全稳定运行的必然选择，其核心在于打破二者“各自为战”的局面，实现建设与防护并举、技术与管理结合、硬件与软件配合、人员与部门协同。本文立足实际应用场景，阐述了协同防护的核心逻辑与现实困境，围绕实用可行、全面覆盖、协同联动、动态优化四大原则，从规划建设、技术、管理、应急处置四个维度提出了具体的构建路径，为各单位构建协同防护机制提供了清晰的实施框架。

参考文献

[1] 王尧,杨志垚.网络工程信息安全技术的优化分析[J].电子技术,2025,54(05):410-412.

[2] 张海民.以问题为导向的项目式教学方法探究——以“网络工程专业导论”课程为例[J].辽东学院学报(社会科学版),2024,26(06):124-131.

[3] 黄伟锦.广播电视网络工程建设与管理策略[J].卫星电视与宽带多媒体,2024,21(23):130-132.

[4] 尹智.计算机网络工程与信息安全策略分析[J].集成电路应用,2024,41(03):182-183.

[5] 汲方君.网络工程中的信息安全与对策分析[J].集成电路应用,2024,41(03):380-381.