网络安全技术在网络安全维护中的应用分析

李　可　聂昱昕　唐懋钧
北京计算机技术及应用研究所　北京　100854

摘　要：网络安全维护聚焦数据、网络运行、终端三大安全目标，需适配需求、精准防控、闭环防护。本文介绍了身份认证、数据加密、边界防护等核心技术在维护中的应用，指出存在技术适配、协同、更新迭代及应用门槛问题。提出提升技术适配性、强化协同性、推动更新迭代、降低应用门槛等优化对策，以提升网络安全维护水平，保障网络环境安全稳定运行。

关键词：网络安全维护；核心目标；技术应用；问题优化

引言：在数字化时代，网络已深度融入社会各领域，成为关键基础设施。网络安全不仅关乎个人隐私与财产安全，更影响企业运营安全与社会稳定。随着网络攻击手段日益复杂多样，网络安全维护面临巨大挑战。在此背景下，深入分析网络安全技术在维护中的应用，找出存在问题并提出优化对策，对构建安全可靠的网络环境、推动网络技术健康发展具有重要意义。

1 网络安全维护的核心需求与技术应用导向

1.1 网络安全维护的核心目标

网络安全维护的核心目标围绕数据安全、网络运行安全、终端安全三大维度有序展开，三者相互支撑、有机衔接，共同构筑网络安全的基础防线[1]。数据安全聚焦各类信息资源的完整与保密，防范数据泄露、篡改与丢失，确保数据在采集、传输、存储、使用全流程处于安全可控状态。网络运行安全侧重保障网络基础设施稳定高效运转，规避网络中断、拥堵、被非法入侵等异常情况，维持网络服务的连续性与可靠性。终端安全针对各类接入网络的终端设备实施防护，涵盖计算机、移动终端等，抵御恶意程序入侵、非法访问等安全威胁，筑牢网络接入端的安全屏障。三大目标协同发力，构成网络安全维护的核心支撑，缺一不可。

1.2 网络安全技术的应用核心导向

网络安全技术的应用核心导向紧密贴合网络安全维护的实际需求，立足防控实效，构建全方位、多层次的防护体系。适配维护需求是技术应用的首要导向，各类安全技术的选型与部署需紧扣数据安全、网络运行安全、终端安全的实际要求，摒弃脱离实际的技术堆砌，确保技术应用与维护需求高度契合，发挥技术的实际防护价值。精准防控风险要求安全技术具备精准识别、快速响应的能力，精准研判网络环境中的各类安全隐患，针对性采取防控措施，减少无效防护投入，提升风险防控的精准度与效率。保障网络闭环防护强调构建“识别-防控-响应-优化”的完整防护链条，确保各类安全技术协同联动，实现从风险识别到隐患处置、再到防护优化的全流程覆盖，形成持续防护、动态优化的良性循环，全面提升网络安全防护的整体性与长效性。

2 网络安全维护中核心网络安全技术的具体应用

2.1 身份认证与访问控制技术

身份认证技术在维护中主要用于实现主体身份合法性校验，通过预设的验证机制核对接入主体的身份信息，筛选非法接入行为，为网络安全筑牢第一道身份防线。身份认证技术不断发展，从最初的简单密码认证，到如今的生物识别、多因素认证等多种方式，大大提高了身份认证的准确性和安全性[2]。访问控制技术在维护中侧重限制主体访问权限，依据身份认证结果分配对应访问范围，杜绝未授权主体接触敏感资源，防范未授权访问引发的安全风险，进一步强化身份认证后的防护效能。

2.2 数据加密技术

数据传输加密技术的应用重点保障数据传输过程中的安全，对传输中的数据进行加密处理，避免数据在传输环节被窃取、篡改，确保数据从源头到接收端的完整与保密。随着网络带宽的增加和传输速度的提升，数据传输加密技术也在不断优化，以满足高速传输下的安全需求。数据存储加密技术的应用聚焦保障数据静态存储的安全，对存储在各类设备中的数据进行加密保护，即便存储设备出现安全漏洞，也能避免数据被非法读取，守护静态数据安全。

2.3 网络边界防护技术

防火墙技术在维护中用于隔离网络边界，筛选网络接入请求，过滤不安全访问行为，阻止非法数据跨越网络边界传输，划分网络安全区域。防火墙技术不断升级，从传统的包过滤防火墙到状态检测防火墙，再到下

一代防火墙，功能越来越强大，防护能力也越来越强。入侵检测技术在维护中专注识别网络边界异常行为，实时监测边界数据流转与接入行为，及时发现超出正常范围的操作，为后续防控措施提供精准依据。入侵防御技术在维护中负责阻断边界入侵行为，针对检测到的异常入侵行为快速采取拦截措施，强化边界防护强度，弥补防火墙与入侵检测技术的防护短板。

2.4 终端安全防护技术

终端杀毒与恶意代码防护技术的应用主要针对终端设备中的病毒、恶意脚本等威胁进行查杀与拦截，定期扫描终端运行状态，清除潜在恶意代码，防范恶意程序对终端设备造成破坏。随着恶意代码的不断变异和增多，终端杀毒与恶意代码防护技术也在不断更新病毒库和检测算法，以提高查杀效果。终端安全管理技术的应用用于规范终端运行状态，统一管控终端接入网络的参数与行为，排查终端设备的安全隐患，防范终端层面风险扩散至整个网络。

2.5 数据安全防护技术

数据备份与恢复技术的应用通过定期备份各类重要数据，存储备份文件并建立恢复机制，当数据出现丢失、篡改等问题时，能够快速恢复数据，降低数据安全事件造成的损失。数据备份与恢复技术不仅要考虑备份的频率和方式，还要考虑备份数据的存储位置和安全性，以确保在需要时能够顺利恢复数据。数据脱敏技术的应用聚焦保护敏感数据安全，对各类敏感信息进行脱敏处理，隐藏核心敏感内容，避免敏感数据泄露。数据泄露防护技术的应用实时监测数据流转过程，识别数据泄露的潜在风险，采取防控措施阻止敏感数据非法外泄，全方位守护数据安全。

2.6 网络安全监测与响应技术

网络安全监测技术的应用用于实时捕捉网络异常状态，全方位监测网络运行参数、数据流转情况与设备运行状态，及时发现网络中断、非法入侵等异常现象，精准定位异常源头。网络安全监测技术需要具备高度的敏感性和准确性，能够及时发现微小的异常变化，为后续的应急响应提供准确的信息。安全事件应急响应技术的应用针对监测到的网络安全隐患快速处置，启动预设应急流程，采取针对性处置措施，遏制安全隐患扩散，降低安全事件对网络运行的影响，快速恢复网络正常运行状态。

3 网络安全技术在网络安全维护应用中存在的核心问题

3.1 技术适配性问题

技术适配性问题主要体现在不同维护场景下技术应用的匹配度不足。网络安全维护场景呈现多样化特征，不同场景的防护重点、风险类型、基础设施条件存在明显差异，各类安全技术的设计与研发往往具有通用性倾向，未能充分兼顾不同场景的个性化需求[3]。例如，在一些对实时性要求极高的金融交易场景中，如果采用通用的安全技术，可能会导致交易延迟，影响业务的正常开展。部分技术部署时未充分考量场景实际情况，盲目套用统一标准与模式，导致技术功能无法充分发挥，既难以有效应对场景特有的安全风险，也可能造成技术资源浪费，无法形成针对性的防护效能，间接削弱整体网络安全维护水平。

3.2 技术协同性问题

技术协同性问题集中表现为各类安全技术联动防护效果不足。当前网络安全维护中应用的各类技术多处于独立运行状态，缺乏有效的联动机制与统一的管控标准，不同技术之间难以实现信息共享与功能互补。比如，防火墙检测到异常流量后，不能及时将信息传递给入侵检测系统，入侵检测系统就无法根据这些信息进一步分析是否存在入侵行为，从而延误了防护时机。一种技术检测到安全隐患后，无法及时将相关信息同步至其他防护技术，导致防护环节出现脱节，部分安全风险能够借助技术联动漏洞突破防护体系。各类技术各自为战，无法形成全方位、一体化的防护合力，使得防护效果大打折扣，难以应对复杂多变的网络安全环境。

3.3 技术更新迭代问题

技术更新迭代问题核心是技术发展与网络安全风险变化不同步。网络安全风险始终处于动态演变之中，新型风险类型、攻击手段不断涌现，对安全技术的防护能力提出更高要求。例如，近年来出现的量子计算攻击，对传统的加密技术构成了巨大威胁，需要研发新的抗量子计算的加密技术来应对。部分安全技术更新迭代速度缓慢，研发与升级投入不足，技术功能难以跟上风险变化节奏，仍停留在应对传统安全风险的层面，无法有效抵御新型网络攻击与安全隐患。老旧技术长期应用，不仅防护效能有限，还可能因技术漏洞成为网络安全维护中的薄弱环节，增加安全事件发生的概率。

3.4 技术应用门槛问题

技术应用门槛问题主要表现为技术落地与实操过程中的难点。各类网络安全技术具有较强的专业性，对实操人员的专业素养、技术能力有较高要求，部分维护主体缺乏专业的实操人才，无法熟练掌握技术的操作方法与维护技巧，导致技术难以充分落地应用，即便完成部

署也无法发挥应有防护价值。例如，一些复杂的网络安全监测系统，需要专业的技术人员进行配置和管理，如果缺乏相关人才，系统就无法正常运行。同时，部分安全技术的部署与维护成本较高，操作流程复杂，缺乏简洁高效的实操指引，进一步提升技术应用难度，阻碍技术在网络安全维护中的广泛落地与有效应用，影响整体防护体系的构建与完善。

4 优化网络安全技术在网络安全维护中应用的对策

4.1 提升技术适配性

提升技术适配性需结合维护需求优化技术选型与应用方案，打破技术应用的通用性局限，兼顾不同维护场景的个性化特征。深入梳理各类维护场景的防护重点、风险类型与基础设施条件，精准梳理场景所需的技术功能的核心要点，避免盲目选型与部署[4]。可以通过建立场景化的安全技术评估体系，对不同场景下的安全技术进行评估和筛选，选择最适合的技术方案。优化技术应用方案，根据场景差异调整技术参数与运行模式，让安全技术能够精准对接场景需求，充分发挥技术防护效能，减少技术资源浪费，让每一项技术都能适配对应场景的防护需求，提升技术应用的针对性与实用性，推动技术与维护场景深度融合，夯实网络安全维护的技术基础。

4.2 强化技术协同性

强化技术协同性关键在于构建一体化联动防护体系，打破各类安全技术独立运行的壁垒，实现技术之间的信息共享与功能互补。建立统一的技术管控标准，规范各类技术的运行流程与数据交互模式，搭建高效的信息同步机制，确保一种技术检测到安全隐患后，相关信息能够快速传递至其他防护技术。例如，可以通过建立安全信息共享平台，实现不同安全技术之间的信息实时共享和交互。整合各类技术的防护功能，形成全方位、一体化的防护合力，弥补单一技术的防护短板，消除技术联动漏洞，让各类安全技术协同发力、无缝衔接，提升整体防护体系的完整性与有效性，更好应对复杂多变的网络安全环境。

4.3 推动技术更新迭代

推动技术更新迭代要主动跟进网络安全风险变化，持续升级防护技术，确保技术发展与风险演变保持同步。密切关注网络安全领域的新型风险类型与攻击手段，加大技术研发与升级投入，聚焦新型风险防控需求，优化现有技术功能，研发适配新型风险的安全技术。及时淘汰老旧落后技术，替换存在漏洞、防护效能不足的技术，避免老旧技术成为网络安全维护的薄弱环节。建立技术更新迭代的长效机制，定期评估技术防护效能，根据风险变化及时调整技术升级方向，让安全技术始终保持较强的防护能力，有效抵御各类新型网络攻击与安全隐患。

4.4 降低技术应用门槛

降低技术应用门槛需简化技术实操流程，提升技术应用效率，破解技术落地与实操过程中的各类难点。优化安全技术的操作设计，删减繁琐的操作步骤，简化部署与维护流程，打造简洁高效的操作模式，降低技术实操的复杂度。完善技术实操指引，梳理清晰的操作流程与维护技巧，为实操人员提供明确指导，帮助快速掌握技术应用方法[5]。加强实操人员专业培训，提升专业素养与技术能力，弥补专业人才缺口，确保技术部署后能够得到规范操作与有效维护。合理控制技术部署与维护成本，推出简洁易用、性价比高的安全技术，推动技术在网络安全维护中广泛落地、有效应用，完善整体防护体系。

结束语

网络安全技术在维护中发挥着关键作用，但当前应用存在诸多问题。通过提升技术适配性，让技术精准对接不同场景需求；强化技术协同性，构建一体化联动防护体系；推动技术更新迭代，紧跟风险变化；降低技术应用门槛，促进技术广泛落地，能有效提升网络安全维护水平。只有不断优化技术应用，才能应对复杂多变的网络安全挑战，保障网络空间安全有序运行。

参考文献

[1]冯汀杉.网络安全技术在网络安全维护中的应用研究[J].网络安全技术与应用,2022(9):174-176.

[2]唐德浩,王慧敏,胡敬明.网络安全技术在网络安全维护中的应用[J].数字技术与应用,2024,42(7):71-73.

[3]王海鹏.网络安全技术在网络安全维护中的应用研究[J].电脑爱好者（普及版）,2022(8):142-144

[4]刘成.计算机网络安全技术在网络安全维护中的应用分析[J].网络安全技术与应用,2022(4):169-170.

[5]王伟.基于网络安全维护的计算机网络安全技术应用探讨[J].网络安全技术与应用,2023(8):164-165.