零信任架构下企业网络访问控制优化研究

黄景涛
广东中科实数科技有限公司　广东广州　511455

摘　要：在当下数字化转型以及网络安全威胁变得日益严峻的大环境里，传统的边界安全模型已经没办法应对新型网络攻击以及内部风险了，企业网络访问控制体系急需进行革新。零信任架构是一种新兴的安全范式，它把“永不信任，持续验证”当作核心原则，为企业网络访问控制的优化给出了根本的思路。这项研究重点关注零信任架构下企业网络访问控制的优化途径，全面剖析了零信任理念给访问控制模式带来的深刻变革，探讨了其关键的实施组件以及技术支撑体系，并且针对企业实际部署时可能会遇到的技术整合、策略动态化以及管理复杂性等挑战，提出了一套包含架构设计、策略引擎优化、身份治理以及持续监测的综合性优化框架。依靠理论阐释以及路径分析，这项研究可为企业构建适应动态业务环境、精准管控访问权限、提高整体安全韧性的新一代网络访问控制体系提供理论参考以及实践指引，对于推动企业网络安全架构的演进与升级有着关键的现实意义。

关键词：零信任架构；网络访问控制；动态授权

引言

随着云计算、大数据、物联网以及移动办公技术的广泛普及，企业网络边界日益模糊，传统基于边界的那种“内网可信、外网危险”的静态防护模式暴露出明显缺陷：高级持续性威胁、内部人员违规、供应链攻击等风险，致使依赖单一网络位置划分信任等级的安全策略难以发挥作用。在这样的背景状况下，零信任安全理念顺势而生，并且快速成为网络安全领域的关键演进方向。我国网络安全领域的权威专家、中国科学院院士冯登国教授在其相关研究和论述当中，大多时候强调：零信任的本质是“从不信任，始终验证”，还指出其核心是建立以身份作为基石、以访问控制作为关键技术的动态可信体系。这一深刻的见解明确了零信任架构从根本上否定了网络位置与信任之间的自动关联，主张对所有访问主体以及请求进行严格且持续的身份验证与授权评估。就像冯登国院士所阐述的那样，其核心以便构建一种以身份为中心、以最小权限为基准、有动态适应能力的精细化和智能化访问控制体系，实现从静态边界防护向动态身份与行为信任评估的根本性转变。探索零信任架构下企业网络访问控制的优化策略，是应对当前复杂威胁环境的必然需求，也是企业实现数字化转型与业务敏捷性的关键安全保障。

作者简介：黄景涛（1995.12——），男，汉族，广东惠东人，大学本科学历，中级职称，研究方向：网络安全。

一、零信任架构对网络访问控制模式的根本性变革

（一）从静态边界防护到动态身份中心的安全范式转换

传统网络访问控制模型主要依靠防火墙、VPN等边界设备，在网络有明确内外之分的基础上开展防护工作，它默认内部网络是可信的，访问权限的给予大多时候依据用户所在的网络区域或者IP地址等静态属性，这种模式在固定办公环境中曾起到关键作用，不过在资源云化、终端多样化、业务移动化的当前，其僵化和粗放的问题变得日益明显。零信任架构完全颠覆了这种范式，把安全重点从网络边界转移到访问主体自身，强调“身份”成为新的安全边界，在这种模式下，每一次访问请求，不管是来自企业内部网络还是互联网，不管访问的以便数据中心应用还是云端服务，都要依据对用户身份、设备状态、应用上下文等多方面因素的实时、动态评估来进行认证和授权。这种转变让访问控制策略不再依赖固定的网络拓扑，而是围绕身份及其关联属性动态生成，实现了从基于位置的“网络中心化”控制到基于身份的“访问中心化”控制的重大变革，它可更精准地反映业务需求与安全要求，有效应对边界消失带来的挑战。

（二）持续验证与最小权限原则的深度贯彻实施

零信任架构的关键之处在于严格执行其两项基本原则，也就是“持续验证”以及“最小权限”。传统的访问控制一般是在初始登录的时候开展一次性的强认证，之

后就会给予较为宽泛的会话权限，一直到会话超时，这样就给攻击者利用窃取的凭证或者会话劫持来进行横向移动留下了很大的空间。零信任要求对访问行为持续进行信任评估，在连接建立的时候进行验证，而且在会话存续期间会按照周期或者基于敏感操作触发重新验证，以此保证访问主体在整个过程中都符合安全策略的要求。“最小权限”原则规定给予每个用户、设备或者应用完成其特定任务所需要的最低级别的访问权限，并且权限分配是动态且即时的，并非长期固定不变的。访问权限不再是依靠静态角色绑定就能一劳永逸的，而是要依据具体访问请求的上下文来进行实时计算并授予，任务完成之后权限马上就会被回收。这种深入贯彻较大缩小了攻击面，限制了潜在威胁在系统内部的扩散能力，使得访问控制从粗放的“通道管理”转变为精细的“交易级管控”。

二、零信任架构下访问控制优化的关键技术支撑体系

（一）身份与访问管理（IAM）的增强与泛化

身份作为零信任架构的关键基石，强化并泛化身份与访问管理系统成为优化的关键技术支撑，这并非仅关乎单点登录以及基础的用户生命周期管理，还需要打造一个统一、权威且覆盖所有人员、设备、应用及服务的身份治理框架。具体优化方向囊括：运用强身份验证机制，像多因子认证、基于风险的适应性认证；构建细粒度的、基于属性的访问控制模型，把用户属性、设备属性、环境属性等当作策略决策的输入；达成身份联邦与标准化协议支持，以便无缝集成混合云环境与第三方服务。对于非人类实体，例如服务账户、API、物联网设备等，同样要赋予其可管理的数字身份，并纳入统一的IAM体系实施管控，保证所有访问主体可被唯一标识、认证和授权，为精细化策略执行奠定稳固基础。

（二）软件定义边界与微隔离技术的应用

软件定义边界作为一种达成零信任网络访问的具体技术模型，借助于在资源周边构建起一个基于身份的逻辑安全边界，以此来取代物理网络边界，让应用以及服务在网络中呈现出“隐身”状态；唯有经过严格验证与授权的用户和设备，才可借助SDP控制器搭建起通往特定应用的单点加密连接。如此一来，便切实有效地防范了网络扫描以及横向探测。微隔离技术主要聚焦于数据中心或者云环境内部，依据工作负载的安全等级以及业务逻辑，实施更为细致的网络分段以及流量控制，以此来阻挡威胁在东西向流量中的扩散。在零信任架构的环境下，微隔离的策略制定同样应当以身份以及工作负载属性为依据，而非传统的IP地址，达成动态且精细的隔离策略。SDP与微隔离相互结合，共同搭建起了从用户到应用、从应用到应用之间的精细化访问控制通道，这是达成网络层零信任的关键技术方式。

（三）持续风险评估与策略引擎的动态决策

动态且智能的策略决策，乃是零信任访问控制不同于传统静态规则的关键特性。此特性依赖于一个策略引擎，它可整合多源数据，开展实时风险评估，并输出动态授权决策。该引擎需持续接收来自终端安全代理、网络设备、身份提供者以及威胁情报平台等多方面的信号，涉及用户行为分析、设备合规状态、漏洞信息、地理位置异常以及时间因素等，构建一个全面的访问上下文。依据预设的风险评估模型与策略规则，引擎针对每次访问请求进行实时风险评分，并依据评分动态调整访问权限，如允许访问、要求进行附加认证、仅限只读操作或者直接拒绝。这种持续的风险评估与动态授权机制，让访问控制策略拥有了情境感知和自适应能力，可更为灵活、智能地应对不断变化的安全态势与业务场景。

三、企业实施零信任访问控制优化的核心挑战与应对路径

（一）现有系统与技术栈的整合复杂性

企业通常拥有大量遗留系统、传统网络设备和异构的IT环境，这些系统并非为零信任理念设计，可能在身份协议支持、API开放性、日志格式等方面存在差异，导致与零信任组件集成困难。优化过程面临如何在不中断业务的前提下，逐步将旧有应用和基础设施纳入零信任体系的技术挑战。应对路径在于采用渐进式演进策略，而非颠覆式替换。先通过API网关、反向代理或SDP网关等“包装”方式，为传统应用提供零信任访问入口。优先从新建应用、云上应用或高价值数字资产开始实施零信任控制，形成示范效应。同时，投资建设统一的数据总线与标准化接口，促进各安全组件与IT系统之间的数据互通与能力集成，逐步降低架构复杂性。此外，企业需在规划阶段就建立明确的互操作性标准与集成规范，通过引入适配层或中间件来桥接新旧技术鸿沟，并建立跨部门的联合技术团队，统筹管理集成项目中的技术依赖与进度协调，确保整合过程有序可控。

（二）动态策略的管理与运维难度提升

零信任环境下的策略管理从相对静态的防火墙规则和网络ACL，转变为大量基于身份和上下文的动态策略。策略的数量、复杂度以及更新频率都可能急剧增加，给

策略的定义、部署、验证、审计和生命周期管理带来巨大运维负担。应对此挑战，需要构建集中化、可视化的策略管理平台。该平台应支持策略的直观定义（如自然语言或图形化），具备策略模拟与影响分析能力，能够在部署前预测策略效果；同时，需实现策略的版本控制、自动化分发与一致性检查。更重要的是，应结合机器学习技术，对访问日志进行持续分析，自动识别异常模式并提出策略优化建议，甚至实现一定程度的策略自适应调整，从而提升策略管理的智能化水平与运维效率。

（三）用户体验与安全效能之间的平衡

严格的持续验证和最小权限控制可能会增加用户访问资源的步骤和频率，如果设计不当，易引发用户抵触，影响工作效率。优化目标是在保障安全的同时实现无感知或低摩擦的用户体验。应对路径包括：采用风险自适应的认证机制，对于低风险访问场景，简化认证流程；对于高风险操作，则自动升级认证强度。实施单点登录与无缝的会话管理，减少用户重复登录次数。利用设备信任状和生物识别等技术，实现更自然、便捷的身份验证。同时，加强用户安全教育，让员工理解零信任措施的必要性，并通过优化交互设计，使安全流程尽可能顺畅地融入日常工作流，从而在安全强化与用户体验之间找到最佳平衡点。

四、面向未来的企业零信任访问控制综合优化框架构建

（一）以数据资产为核心的分层分级保护架构

零信任优化的最终目标是保护企业核心数据资产。因此，应构建一个以数据分类分级为基础，层层递进的访问控制防护架构。对企业所有数据进行发现、分类和敏感度标记。其次，将访问控制策略与数据标签深度绑定，确保策略决策引擎能够识别所请求访问数据的敏感级别。在此基础上，实施差异化的控制强度：对于非敏感数据，可采用相对宽松的策略；对于核心敏感数据，则强制执行最严格的持续验证、最小权限和操作审计。这种以数据为中心的方法，使得安全控制力能够精准聚焦于最关键资产，实现安全资源的最优配置，确保即使在复杂环境中，核心数据也能得到最强有力的保护，从而将零信任原则落到实处。

（二）融合人工智能的智能化安全运营闭环

为了应对日益复杂的威胁和庞大的数据量，未来的零信任访问控制优化必须深度融入人工智能与自动化能力，形成智能化的安全运营闭环。通过机器学习算法对海量身份行为数据、网络流量日志和威胁情报进行关联分析，建立正常行为基线，实时检测偏离基线的异常访问行为，并自动触发策略调整或响应动作。利用自动化编排与响应技术，将风险识别、策略计算、权限调整、威胁遏制等流程串联起来，实现从威胁感知到策略自适应的快速闭环。例如，当检测到某个账户存在凭证泄露风险时，系统可自动提升该账户的认证要求、临时限制其访问范围并通知管理员。这种智能化闭环不仅极大提升了威胁响应速度与策略的精准性，也显著降低了安全团队的人工运维压力，使零信任体系成为一个能够自我学习、动态演进的主动防御系统。

结语

零信任架构代表着网络安全范式的一次深刻演进，其为企业网络访问控制体系的优化与重构提供了根本性的指导原则与实践框架。需要明确的是，零信任并非单一的产品或项目，而是一个持续演进的安全战略与体系化工程。其实施成功依赖于清晰的顶层设计、分阶段的务实推进、跨部门的紧密协作以及对技术与流程的不断调优。展望未来，随着技术的持续发展与威胁态势的不断变化，零信任架构下的访问控制优化将更加注重智能化、自动化和业务融合，从而为企业构筑起一道适应数字时代发展需求的、弹性而精准的动态安全防线。

参考文献

[1]李碧贵，彭秀兰，童翌运，等.基于零信任模型的网络访问控制机制探讨[J].网络安全技术与应用，2025，(09)：3-5.

[2]刘建清.零信任模型在企业网络安全中的应用研究[J].中国宽带，2024，20(09)：40-42.

[3]蔡东赟.零信任安全[M].机械工业出版社：202403：228.

[4]周潮洋，谢琴.零信任理念下的企业新型安全技术防护体系研究[J].网络安全技术与应用，2022，(02)：99-101.

[5]张如旭.如何通过零信任边缘确保安全[J].计算机与网络，2021，47(17)：48-49.