DOI: 10.54254/3050-2187/2025.27911

基于微隔离的私有云访问控制研究

李 涛

（国能数智科技开发（北京）有限公司，北京市，100006；20037293@ceic.com ）

摘 要：随着数字化转型改革的推进，业务信息系统云化部署，私有云安全成为关乎生产业务运行的重要风险点，网络安全等级保护制度中对云计算环境提出了针对性扩展要求，而现有技术对于日益凸显的私有云内部安全问题存在明显的防护盲区。为实现对私有云服务器东西向访问控制，建设完成具有混合异构环境统一管理需求的自适应私有云微隔离访问控制平台具有重要意义。

关键词：微隔离；私有云；访问控制；东西向安全

引言

信息化时代下，随着虚拟化、云计算技术的普及，传统网络边界保护模式已难以应对日益复杂的新型网络攻击,需要探索全新的网络安全保护措施 [1]。因云化数据中心基础架构发生巨大变化，虚拟机、容器等工作负载将随时发生克隆复制、扩缩容、漂移或消亡，其“飘忽不定”的特性严重影响了私有云的安全性。云数据中心75%的网络流量均由内部工作负载间的横向连接而产生，东西向流量已然成为安全措施难以覆盖的“空白地带”[2]。东西向流量的管理缺失，给私有云数据中心、业务应用和数据带来了巨大安全风险。

1. 研究背景和意义

1.1. 微隔离技术背景

微隔离把一个无结构无边界的网络分成多个逻辑上的微小网段，以确保每个网段上只有一个计算资源，而所有需要进入微网段的流量都需要经过访问控制设备 [3]。微隔离是一种安全策略，通过将网络划分为多个小的、独立的区域(段)，限制数据横向移动，从而减少攻击面 [4]。微隔离技术的使用打破了传统基于边界防火墙为主的安全配置策略。零信任架构下的微隔离（Micro-Segmentation）概念最早于2014年由VMware在应对虚拟化环境的安全需求时提出，旨在通过在数据中心内部实现细粒度的逻辑隔离，限制不必要的网络通信，防止内部威胁的横向扩散和敏感数据的非法访问 [5]。

“隔离”技术是最早、最基础，也是最为核心的安全技术手段之一。而在隔离技术被更广泛和迫切需求的同时，虚拟化技术的引入使得传统隔离技术无法在现代数据中心内部有效运用，微隔离即是在这样的背景下诞生的。微隔离用于提供主机、容器间安全访问控制，并对东西向流量进行可视化管理。近年来，零信任理念得到广泛认可和加速落地，微隔离技术被同步纳入零信任技术框架的必要结构性要求之列，并被定义为实现数据中心内部业务资源调用场景下零信任访问控制的核心组件。

1.2. 微隔离应用现状研究

微隔离主要有四种技术路线，分别是基于私有云原生组件、基于第三方防火墙、混合模式及基于主机代理（Agent）的微隔离实现。

1.2.1. 基于私有云原生组件

利用虚拟化平台内置的网络管理组件完成微隔离。该路线与私有云管理结合紧密，但控制对象通常仅面向基础设施（如主机名、IP地址），且仅适用于自身平台，难以适应同时采用多种虚拟化架构的跨平台场景统一管理需求。

1.2.2. 基于第三方防火墙

通过与私有云虚拟化层的适配，将平台内部的东西向流量引流至传统的防火墙系统实现访问控制。该路线理论上可利用防火墙系统较完整的安全功能，对东西向流量进行较全面的安全检测，但由于其将同步产生较大的延迟，故该特性鲜有运用。同时，该路线具有较明显的性能劣势，一方面需要将较高的性能压力集中于防火墙系统单点，另一方面虚拟化防火墙部署于私有云内部，还将对私有云产生额外的资源占用。此外，该技术路线的环境适应性受其与虚拟化架构兼容程度的制约较大。故该路线同样难以适应云网复杂场景下的微隔离管理需求。

1.2.3. 混合模式方案

指上述两种路线的结合，即利用第三方防火墙进行南北向（内网和外网之间）的安全管理，而利用私有云原生组件进行东西向管理，此模式本质上是一种解决方案。对于偏向于传统架构（流量构成以南北向为主、安全需求主要面向南北向流量）的云数据中心可提供较全面的管控效果，但其提供的并非云工作负载间流量的控制能力。

1.2.4. 基于主机代理（Agent）的微隔离方案

通过在云工作负载上部署运行代理程序（Agent），监听云工作负载连接信息，并通过控制云工作负载操作系统的主机防火墙程序（如IPTABLES）实现东西向流量的可视化管理。该路线具有基础架构无关的特性，可在混合异构环境中规模化部署，并广泛纳管各类云工作负载。同时，其采用集中策略计算、分布式策略执行的方式，可较好应对规模化部署场景下策略自适应计算能力及云工作负载性能风险的问题。主机代理模式凭借其灵活性与普遍适用性，在众多微隔离实施手段中占主导地位。它直接嵌入操作系统层面，易于定制化策略并适应多样安全需求。

2. 微隔离私有云访问控制平台

基于微隔离的访问控制平台采用基于主机代理(Agent)的微隔离方案，适用于私有云、公有云、混合云等多种业务场景下所涉及的物理机、虚拟机、容器等多种类型工作负载间的安全防护。平台通过对工作负载东西向流量采集分析、基于角色的工作负载资产管理、面向业务的策略管理和安全策略自适应计算等关键技术，实现东西向流量可视化、构建私有云内网屏障、降低内部访控运维成本、满足等级保护2.0云计算环境安全扩展要求，同时建立健全支撑微隔离访问控制平台常态化运营的工作负载管理、连接需求审批、异常连接核查等管理流程。

2.1. 基于微隔离的私有云访问控制平台设计方案

微隔离访问控制平台包括云工作负载标签化管理、业务连接可视化分析、东西向流量精细访控、全局策略自适应计算4大核心功能。

2.1.1. 工作负载标签化管理

工作负载标签化是基于工作负载的业务属性，通过多维标签（如位置、环境、应用、角色等）标定工作负载实体身份的资产管理能力。标签化是实现基于业务的互访流量可视化、面向业务的访问控制和自适应策略计算的基础能力。

2.1.2. 业务连接可视化分析

对工作负载的连接信息进行学习采集和统计分析，以图形化呈现出易于理解的东西向流量访问模型。该功能主要解决管理者对数据中心东西向流量不可视、无感知的难题，同时也是建立业务访问基线、部署访问控制策略的支撑能力。

2.1.3. 东西向流量精细访控

私有云访问控制平台的策略管理模型，对工作负载间的东西向流量制定基于业务角色的访问控制规则。该功能通过更加接近自然语言的描述方式定义复杂的东西向流量策略，并实现安全策略与基础设施解耦的零信任管控模式。

2.1.4. 全局策略自适应计算

通过自适应策略计算引擎，根据工作负载的变化而实时自动调整符合其业务角色的安全策略。在工作负载规模庞大、资产变化高频普遍的云化数据中心场景中，该功能有效地保障了业务上下线、扩缩容、工作负载漂移等情况下安全策略的高效更新及同步。

2.2. 基于微隔离的私有云访问控制平台实施步骤

2.2.1. 评估需求、划定资源，完成管理平台部署

首先确定私有云工作负载的范围，基于纳管规模评估微隔离访问控制平台（安全计算中心）所需的算力、存储、网络等资源需求。同时，对访问控制平台应保障的可靠性、可用性提出具体指标要求，输出微隔离访问控制平台安全计算中心集群化部署方案设计，并完成部署实施和联调测试。通过安全计算中心部署，为平台整体推进奠定基础。

2.2.2. 兼容异构、同台纳管，云工作负载统一接入

开展私有云所涉及云工作负载的微隔离Agent（安全管理终端）的批量、规模化部署，通过充分验证，确保其能够在不损害云工作负载稳定可靠、不造成云工作负载性能明显衰减的前提下，对私有云内物理机、虚拟机、容器云工作负载，尤其是部分基于国产操作系统和硬件平台的服务器主机实现同台统一纳管，从而实现微隔离访问控制平台侧与私有云打通。

2.2.3. 理清资产、摸清家底，建立业务访问基线

对照微隔离访问控制平台云工作负载列表，基于现有业务运维数据，梳理云工作负载部署位置、所处环境、所属业务、所承载的应用等信息，完成资产的业务属性标定。进而基于微隔离访问控制平台对云工作负载系统信息、连接信息的学习采集，结合其业务属性，分析其监听端口、互访关系，并对照实际业务访问需求，建立业务访问基线，为制定东西向流量访控策略提供依据支撑。

2.2.4. 精细访控、缩减暴露，执行按需授权访问

在云工作负载业务属性梳理及业务访问基线建立的基础之上，以“最小特权（Least Privilege）”为原则，制定基于角色的访问控制策略，并通过一段时间的策略执行效果模拟仿真、调整优化，最终实现安全策略向云工作负载主机防火墙的下发执行。

2.2.5. 数据打通、高效协同，对接内部相关系统

通过开放API接口，打通微隔离访问控制平台与安全运营中心（SOC）系统的东西向连接数据通道，建立面向内部流量的异常分析、威胁预警能力。

2.2.6. 优化管理、简化运维，建立运营管理流程

以微隔离访问控制平台的部署运行为抓手，优化云工作负载资产管理相关流程，以安全规划前置、安全能力左移为原则，建立一套符合微隔离访问控制平台运营管理逻辑的云工作负载申请、资产注册及纳管管控流程，满足平台运营需求。

3. 微隔离技术在安全运营的应用和思考

利用大数据建模、神经网络和深度学习技术，通过数据聚合、关联分析、智能感知等多种技术手段，将微隔离私有云访问控制平台的多项系统数据进行预处理、整合、建模、多维分析，实现对私有云平台生产数据的统一查询、安全预警的综合分析与智能判断，有效提升异常事件的高效处置能力，为私有云各个系统的应急处置与安全防护提供技术支撑，实现云平台的大数据分析和智能化处置。

进一步挖掘私有云东西向流量的数据价值，实现对运营系统运行效果的量化评估、关键业务异常监测、内部威胁分析预警能力。通过流量监测、智能预警、异常流量分析等技术，快速准确地发现业务系统异常情况，实现服务器流量监控指数和业务连续性指数可视化，构建私有云业务系统的安全监测预警及应急处置模式，提升私有云安全管控及流量监管水平。

微隔离私有云访问控制平台预警机制将整合终端历史数据，提供长期历史数据、短期历史数据查询，追溯异常服务器；对各系统将根据业务特征进行建模、分析，建立各系统业务流量监控逻辑，精准定位异常告警；与资产类、管理类系统对接，实现私有云的服务器在线和运行状态的查询展示，增强平台可扩展性；集

成流程管理模块，并根据私有云异常告警和安全事件类型建立匹配的异常报警及处置流程，配置处置任务派发、跟踪、管理功能；支持私有云业务系统定期的服务器和业务合规性自动检查，确保重点系统平稳运行。

4. 结语

微隔离技术实现了私有云主机内部流量的可视化分析和细粒度的安全策略管理；加强了私有云内部的环境隔离、域间隔离以及端到端隔离；完善了私有云东西向和南北向的纵深安全管控，实现了安全策略精细化管理；提高了系统应用层安全防护能力，全面提升了私有云信息化网络安全运维及安全防护保障能力。

参考文献

[1] 黄亮浩. 基于微隔离技术的网络安全纵深防御优势探析 [J]. 数字技术与应用, 2025, 43(4): 82-84.

[2] 徐春利, 刘鲲, 孟庆晨, 等. 基于微隔离技术的数据中心云网络安全研究 [J]. 中国口岸科学技术, 2025, 7(z1): 79-86. DOI: 10.3969/j.issn.1002-4689.2025.z1.013.

[3] 张世倩, 李沛谕, 许丹丹, 等. 统一身份认证中的微隔离方案研究 [J]. 网络安全技术与应用, 2024(6): 15-19. DOI: 10.3969/j.issn.1009-6833.2024.06.006.

[4] 杜彪, 苗青鹏, 石凯, 等. 人工智能技术在零信任架构下的应用研究 [J]. 信息安全与通信保密, 2025(7): 66-74. DOI: 10.3969/j.issn.1009-8054.2025.07.007.

[5] 刘青, 刘千仞, 李长连, 等. 云原生环境高性能微隔离策略管控方案研究 [J]. 邮电设计技术, 2024(8): 62-66. DOI: 10.12045/j.issn.1007-3043.2024.08.013.