云原生环境高性能微隔离策略管控方案研究

Research on High-performance Micro-segmentation Policy Control Solutions for Cloud-native Environments

刘　青[1]，刘千仞[2]，李长连[1]，蔺　旋[1]，王贺龙[1]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联合网络通信集团有限公司，北京 100033）

Liu Qing[1], Liu Qianren[2], Li Changlian[1], Lin Xuan[1], Wang Helong[1]（1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 2. China United Network Communications Group Co., Ltd., Beijing 100033, China）

摘　要：

针对云原生环境日益严峻的安全挑战，深入探讨了微隔离技术在云原生安全领域的应用。首先分析了微隔离技术的背景及其在云原生环境的需求特性，随后确立了无侵入式部署、自动化运维、高性能流量管理等核心目标。通过云原生组件集成eBPF技术，同时引入标签化管理机制，实现了适应云原生场景下复杂多变的网络环境的细粒度安全策略管理体系，在提升隔离效能、资源优化、策略灵活性及多场景适应性方面效果显著。

关键词：

云原生安全；零信任；微隔离；工作负载；K8s

doi：10.12045/j.issn.1007-3043.2024.08.013

文章编号：1007-3043（2024）08-0062-05

中图分类号：TP393

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

In response to the increasing security challenges of cloud-native environments, it deeply explores the application of micro-segmentation technology in the field of cloud-native security. Firstly, it analyzes the background of micro-segmentation technology and its demand characteristics within the cloud-native environments, subsequently it establishes central objectives such as non-intrusive deployment, automated operational management, and high-efficiency traffic management. Through the integration of eBPF technology with cloud-native components and the concurrent adoption of a label-driven management scheme, the study realizes a granular security policy management framework that is adaptable to the complex and mutable network ecosystems inherent to cloud-native scenarios, which has significant effect in improving isolation efficiency, resource optimization, strategy flexibility, and multi scenario adaptability.

Keywords：

Cloud-native; Zero-trust; Micro-segmentation; Workload; Kubernetes

引用格式：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.

0 引言

随着云计算技术的飞速发展，云原生已成为现代企业IT架构的核心特征。云原生环境以其敏捷开发、快速迭代、弹性伸缩和高效资源利用等优势，极大地推动了业务创新与数字化转型[1]。然而，这种高度动态、分布式、容器化和微服务化的环境也带来了全新的安全挑战。

在传统的单体应用架构中，应用程序通常运行在相对封闭的环境中，网络边界相对清晰，安全性的管理相对容易。然而，在云原生环境中，应用程序被拆分为多个微服务，运行在共享的基础设施上，传统的边界防护机制在云原生架构下显得力不从心，单一的安全防线难以有效应对复杂多变的威胁态势。微服务之间的通信、数据的流动和共享资源的使用，使得安全隔离变得尤为重要[2]。特别是内部横向攻击、未授权访问以及容器逃逸等安全风险显著增加，凸显了对细粒度、实时、自适应的安全隔离措施的需求。

收稿日期：2024-06-16

1 微隔离技术背景与现状

近年来，微隔离技术作为一种解决云原生安全问题的关键技术，受到了越来越多的关注。微隔离技术能够在保证应用程序运行效率的同时，有效地隔离不同微服务之间的网络流量和数据访问，提升整个系统的安全性。

1.1 微隔离技术背景

零信任架构（Zero Trust Architecture，ZTA）是一种现代网络安全框架，其核心理念是默认不信任任何网络内外部实体，无论它们是否位于企业网络内部，均需通过严格的身份验证、授权和持续监控来确保对资源的访问安全[3]。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[4]。

随着云原生技术的发展，微隔离技术逐渐从单纯的网络层面扩展到涵盖应用、数据等多个维度的全面隔离。它与容器技术、服务网格、API管理等紧密结合，形成了一套适应云环境特性的安全模型。微隔离技术可以将计算资源划分为多个隔离的微段，并通过安全策略来控制不同微段之间的通信，从而实现对关键业务系统、数据和应用的保护。微隔离技术在云计算环境下的应用场景包括保护关键业务系统、数据和应用，实现合规性要求，以及提升云计算环境中的运维效率。微隔离管控数据中心内东西向流量如图1所示。

1.2 微隔离研究现状

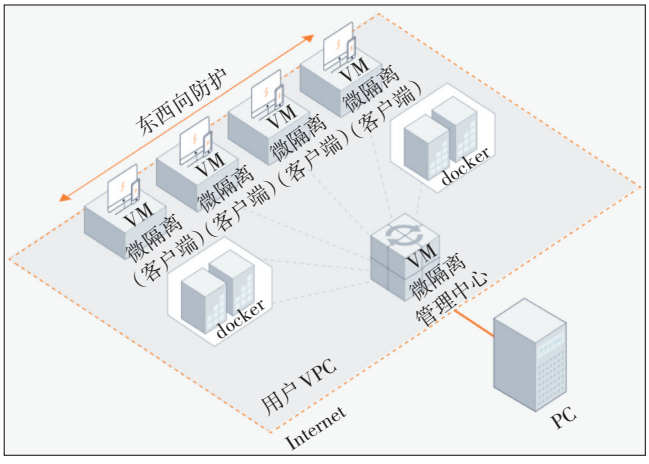

图1　微隔离管控数据中心内东西向流量

微隔离是目前安全领域研究的热点之一，在Gartner的2017年报告中提出了微隔离的4种技术路线，其中基于云平台、基于第三方防火墙、主机代理模式是目前的主流方案[5]。最早被提出的是基于第三方防火墙的方案，该方案将虚拟化环境中的专用第三方防火墙嵌入到虚拟网络层面，通过策略来划分和控制不同工作负载间的通信[6-7]。这些防火墙通常具有更丰富的安全功能和深度包检测能力，但可能增加资源消耗和潜在延迟；基于云平台的方案利用云服务提供商的内置安全功能可以在IaaS层面上实现基于标签、实例ID或其他属性的微隔离[8]。该方案与云原生集成度高，可利用云服务商的API自动配置和调整策略，但应用灵活性受到云平台的限制；主机代理模式下可根据网络环境内部实际网络防护需求配置不同细粒度的安全策略并下发到客户端，通过本地代理快速响应和执行策略变更，实现实时的细粒度隔离能力[9-10]。

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。然而，伴随其优势而来的是部署复杂度增加、资源消耗问题凸显，同时侵入性部署方式可能影响业务系统的性能与稳定性，需权衡利弊，寻求更优解。

2 研究目的与方法

虽然目前微隔离解决方案已日趋成熟，但仍存在一些亟待解决的问题，如部署侵入性强、策略管理复杂、性能瓶颈明显等，在大规模容器化场景下，微隔离策略编排与写入的时延可达到分钟级。同时，iptables四表五链的复杂结构和串行执行方式使得其策略执行开销与延时会随规则条数增多而增大，实验数据表明当配置100条策略时，其新建连接速率的衰减将接近10%，这与云原生架构下业务发布的敏捷性相悖。因此本文旨在研究并提出一种零信任架构下的高性能、无侵入、自适应的云原生微隔离安全策略管控方案。通过分析微隔离技术的发展趋势，结合当前主流的实现方式，本文设计并实现了一种新的微隔离解决方案。本方案采用了无侵入的DaemonSet方式，实现了自适应的标签化管理，利用eBPF（Extended Berkeley Packet Filter）技术实现了高性能的数据包过滤。

本文将详细探讨上述方案的设计原理、关键技术、性能评估与实际应用效果，为云原生环境下的微隔离技术研究与实践提供新的思路与参考，推动云原

生安全技术的进一步发展和应用。

3 云原生微隔离方案设计

本章节所提出的高性能云原生自适应微隔离安全策略管控方案，旨在为云原生环境提供一种细粒度、实时、智能且适应性强的安全策略管理机制。方案融合了现代云原生技术、eBPF高性能网络过滤、标签化管理理念以及前后端解耦设计，以应对云原生架构下的复杂网络流量、动态资源变化以及多样化安全需求。

3.1 方案概述

本方案采用了Client/Server（C/S）架构模式，该架构主要由客户端代理（Agent）与服务器端管理控制台（Manager）构成。客户端代理作为K8s集群节点（Node）上的守护进程，其核心职责在于实时捕获Node层面的K8s资源状态及网络流量数据，并将这些信息精准传递至服务器端管理控制台进行深度处理与分析。与此同时，客户端代理还需具备响应管理控制台下发的安全策略更新指令的能力，确保策略的即时生效。管理控制台则部署于服务器环境中，专注于接收并高效处理由各客户端代理推送的海量数据流。在实时分析的基础上，管理控制台能够根据需要向客户端代理发出相应的控制指令，实现对全局安全态势的灵活调控。

3.2 无侵入代理部署与实施

高性能云原生自适应微隔离安全策略管控方案采用DaemonSet部署模式，实现微隔离代理的透明安装与维护，同时结合自动化运维与故障恢复机制，并与云原生组件Kubernetes（K8s）进行深度集成。

3.2.1 无侵入部署模式

DaemonSet是Kubernetes中一种资源对象，用于确保在每个符合条件的节点上运行一个（或多个）Pod实例。对于微隔离安全策略管控方案，采用DaemonSet部署模式可以在不影响现有系统结构和业务运行的前提下，安装和配置微隔离代理。这种部署方式旨在减少对应用容器的直接修改，保持应用的原始形态和性能，同时确保安全策略的有效实施。由于微隔离代理作为守护进程部署在集群的所有工作节点上，确保每个节点上的容器实例都能受到统一的策略管控，消除安全盲点。当节点加入或离开集群时，DaemonSet会自动在新节点上启动微隔离代理，或在节点移除时停止代理，保持与集群规模的动态同步。无侵入微隔离客户端部署如图2所示。

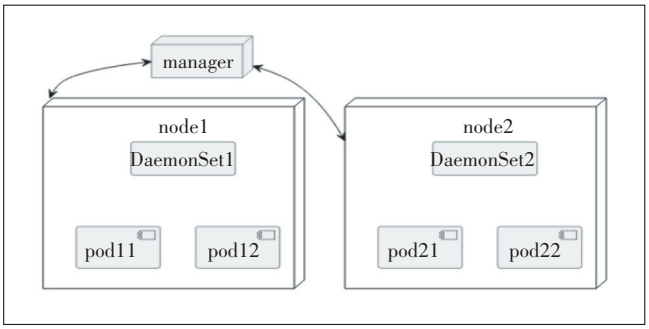

图2　无侵入微隔离客户端部署

3.2.2 自动化运维机制

部署在各个Node上的微隔离代理通过Kubernetes API将中央策略管理系统生成的微隔离策略自动分发至各个节点上的微隔离代理，无需人工干预。支持在线更新策略配置，代理能够实时接收并应用新策略，确保策略变更即时生效，无需重启服务或中断网络流量。管理控制台通过收集微隔离代理的日志、指标数据，实现日志集中存储、性能监控与告警通知，便于运维人员及时发现和解决问题。此外，Kubernetes编排层能够根据节点状态和微隔离代理版本需求自动调整代理实例数量，执行滚动升级，确保服务连续性和最小化业务中断。

3.3 高性能流量采集与管控

本方案中采用eBPF的方式取代传统的基于iptables的方式进行策略的管理与执行，以提高微隔离解决方案在大规模场景下的性能。具体来说，服务端策略引擎负责策略的编译、存储、更新、撤销等操作，同时收集系统状态、策略执行结果、网络流量等数据，并进行实时监控和告警。部署在各节点上的代理负责监听Kubernetes API Server和其他数据源（如eBPF上报的事件），处理标签变更、资源创建/删除、策略更新等事件，触发策略的自动同步，并将策略转化为eBPF程序部署到各节点，确保策略在内核中实时执行。

3.3.1 eBPF方案选择

eBPF是一种在Linux内核中运行的高效、安全的程序，能够在不引入额外数据拷贝和上下文切换的情况下处理网络数据包。Cilium是一个开源的网络可观测解决方案，底层基于eBPF技术，可完全适配高敏捷的云原生环境。Cilium作为容器网络接口（CNI）插件，为容器化工作负载提供网络连接、安全策略实施

以及深入的网络流量监控能力。它适用于大规模、高度动态的容器部署，能够无缝集成到现有的 Kubernetes 集群中。Cilium 利用 eBPF 实现近乎线速的网络性能和极低的延迟。

3.3.2 系统集成设计

Cilium 作为一个功能完备的网络与安全解决方案，内建了详尽的监控、配置与告警接口及组件，旨在实现跨平台的无缝集成与统一管控。微隔离管理控制台通过利用 Cilium 提供的 RESTful API 接口，与部署在各个 Kubernetes 节点上的 cilium-agent 建立直接通信通道。

首先进行节点状态监控，实时获取各节点的服务运行状态信息，确保对整个集群健康状况的精准把控，并在此基础上动态识别并纳管 K8s 中的各类工作负载，对工作负载间的访问流量进行采集，并上报至管控平台，确保微隔离策略能精准映射到实际业务场景。

管控平台基于收集到的流量信息分析并呈现业务间访问关系，根据业务需求制定基于白名单或黑名单的安全策略，并以标准化的方式向 cilium-agent 分发，确保已下发策略的及时、准确执行，主动捕获 cilium-agent 上报的异常事件与告警信息，为策略优化与故障排查提供数据支撑，确保对潜在风险的快速响应与妥善处置。流量采集与管控流程如图 3 所示。

3.4 标签化策略制定与执行

方案中的标签化策略制定与执行流程涵盖了从面向业务的标签体系构建，到基于标签的策略生成与更新，再到实时策略生效与反馈机制的全过程。

3.4.1 面向业务的标签体系构建

首先定义结构化的标签分类体系，支持按资源类型、环境属性、业务特性、地理位置、团队归属等维度划分标签类别。通过标签对纳管的工作负载进行分组、分类管理，管控平台根据客户端代理上报的负载标签信息（本方案中采集的标签为 Pod 的 app 字段），实时更新和同步全局信息，确保标签信息随资源状态变化实时同步至策略管控系统。

3.4.2 基于标签的策略生成与更新

管控平台可直接基于标签创建自定义策略规则，字段包括策略生效范围、源/目的标签、协议/端口等要素，同时支持黑白名单 2 种策略机制以及出入站 2 个方向流量管控。白名单机制用于基于零信任概念的常态化管理，黑名单机制用于应急场景下非法流量快速阻断与恢复，双向流量管控提供更灵活的策略制定方式。策略的自适应更新由多种事件触发，如资源标签变更、环境扩缩容时进行全局策略同步更新等。

3.4.3 实时策略生效与反馈机制

策略管控系统将生成或更新的策略实时推送到各个执行节点 cilium-agent，实现动态策略分发，确保策略即时生效。管控平台实时监控和记录所有策略执行结果，包括连接和阻断的连接请求，为安全审计、故障排查和策略优化提供依据。同时，通过管理控制台集成的拓扑展示、事件告警等功能模块，可实时展示策略执行状态、流量统计、异常访问等指标，并设置告警规则，以便在触发告警时及时通知相关人员作出

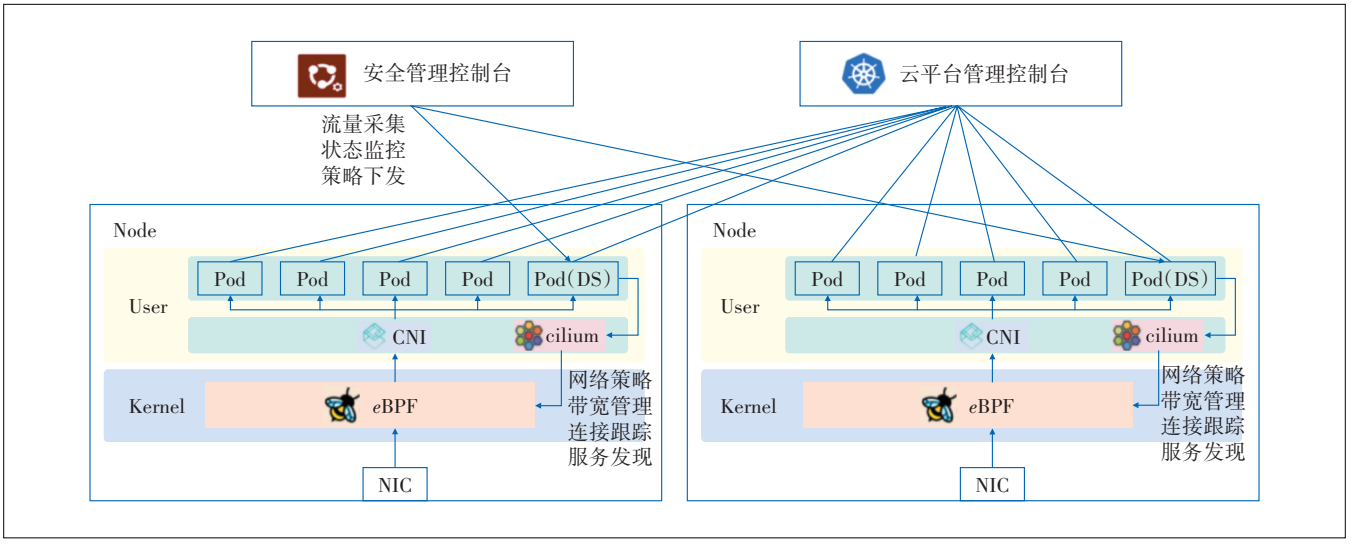

图 3　流量采集与管控流程

响应。

4 方案应用效果与优势分析

本文提出的云原生环境的高性能微隔离解决方案符合现代企业IT架构安全需求，在安全策略管理、性能表现与运维自动化方面相较于主流方案存在显著优势（见表1）。

表1　方案多维度优势分析

方案	现有微隔离方案（主机代理模式）	基于Daemonset的云原生高性能微隔离方案
部署无入侵性	需要修改应用或系统配置，对业务系统存在一定的侵入性	采用Daemonset部署模式，无需修改应用代码或大量配置，自动与云原生基础设施集成，减少对现有应用架构的干扰
高性能	对业务系统存在资源消耗，同时可能引入网络延迟	利用eBPF技术直接在内核层级执行策略，绕过传统的iptables，极大降低处理延迟，提高数据包过滤性能
云原生环境适应性	与云原生生态集成度不高，有可能不完全匹配云原生环境的动态特性，需额外适配	自适应标签化管理，随Kubernetes资源状态实时更新策略，与云环境动态变化同步，自动扩展和收缩，同时与Kubernetes原生API深度整合，充分利用云原生能力，如自动化运维、滚动升级
自动化策略管理	策略更新和管理有可能依赖手动操作或不够灵活	策略自动分发与更新，支持在线更新配置，无需重启服务，减轻运维负担，提高响应速度
细粒度流量管控	细粒度控制程度不一，部分方案仅能支持较粗粒度的隔离	基于标签的策略制定，实现微服务级别、进程级别的隔离，满足云原生环境下微服务间复杂交互的需要

方案采用DaemonSet部署模式确保微隔离代理的透明安装与全节点覆盖，实现了对云原生基础设施的零影响，同时利用了云原生组件K8s的自动编排机制，确保策略随集群动态调整，减少人为错误，提升了运维效率，降低了安全风险；引入标签化管理理念，构建灵活的标签体系，实现基于标签的策略动态生成与实时生效和端到端的细粒度策略控制；依托cilium eBPF技术，有效加速数据包过滤，减少资源消耗，保障了高并发下的隔离效果；管理控制平台集成的监控与告警系统，有利于实时观测网络安全健康状态，及时响应安全事件。该方案与云原生技术深度集成，适应性强，支持业务扩展，为云原生环境提供了高效、安全、易管理的微隔离策略实施办法。

5 总结

本文设计了一种适用于云原生环境的零侵入、自适应、高性能的微隔离解决方案。方案创新性地融合了eBPF、标签化管理和DaemonSet部署模式等先进方法，为微隔离技术在云原生环境中的应用提供了新的技术范式，有助于推动微隔离技术的持续创新与进步。

虽然，本文提出的微隔离方案已展现出显著的技术优势和应用价值，但随着网络技术和应用的快速发展，零信任和微隔离领域仍存在诸多挑战。为了进一步降低复杂动态环境运维的难度与成本，需要更加智能化的策略生成与优化方案。在后续的工作中将探索运用机器学习、人工智能等技术，根据实时流量、威胁情报等数据自动调整和优化微隔离策略，为网络环境提供更可靠更高效的安全防护。

参考文献：

[1] 李亮. 云原生应用开发与部署面临的挑战及其应对方案[J]. 软件工程，2024，27(1)：6-9.
[2] 代仕勇，吴跃隆，汪绪先，等. 基于微隔离技术的网络安全纵深防御研究[J]. 网络安全技术与应用，2024(5)：4-5.
[3] 李惟贤，张建辉，曾俊杰，等. 基于软件定义边界的零信任匿名访问方案[J/OL]. [2024-01-30]. http://kns.cnki.net/kcms/detail/50.1075.TP.20240409.1032.004.html.
[4] 陆英. Gartner：2018年十大安全项目详解(二)[J]. 计算机与网络，2018，44(23)：48-50.
[5] 管纪伟，朱凌君，张文勇. 基于零信任的公有云微隔离安全研究[J]. 电信工程技术与标准化，2021，34(12)：46-50，56.
[6] 朱洪武. 基于NSX网络虚拟化的微分段机制探讨及应用[J]. 西南民族大学学报(自然科学版)，2022，48(4)：428-432.
[7] 左一男. 基于微分段的数据中心网络安全隔离技术研究与运用[J]. 现代信息科技，2024，8(1)：185-188.
[8] 黄庚，郑剑武，王子璇，等. 云原生环境中零信任安全架构的研究与实践[J]. 网络安全和信息化，2023(8)：139-142.
[9] 那宝玉，丁晨，董圳林，等. 基于微隔离技术的数据中心云平台安全策略自适应系统设计[C]//第十一届中国指挥控制大会论文集. 北京：中国指挥与控制学会，2023：352-356.
[10] 张伍全，扈飞. 基于主机微隔离技术的网络安全纵深防护探索[J]. 中国金融电脑，2023(2)：85-87.

作者简介：
刘青，毕业于北京邮电大学，硕士，主要从事网络安全技术与产品规划研究工作；刘千仞，毕业于北京邮电大学，高级工程师，主要从事云计算、数据通信等规划相关工作；李长连，毕业于西北工业大学，高级工程师，主要从事网络安全技术方向的研究工作；蔺旋，毕业于西安交通大学，硕士，主要从事网络安全技术的研究工作；王贺龙，毕业于西安电子科技大学，硕士，主要从事网络安全技术与产品研发工作。