

云计算环境网络安全隐患治理分析

鲁玉岭

新华联控股有限公司

DOI:10.32629/etd.v7i1.22226

[摘要] 云计算的普及应用重塑了传统网络运行架构,动态化、共享化的组网特征打破了固有防护模式,衍生出多种新型网络安全隐患。本文围绕云环境下虚拟化架构、多租户访问、网络边界与数据传输四大核心维度的安全风险展开梳理,结合云网络运行特性剖析各类隐患的形成原因与作用机制,针对性搭建适配动态云场景的防护治理体系,提出多维度、全方位的安全优化方案,能够有效弥补传统网络防护的短板,提升云平台整体安全运行效能。

[关键词] 云计算; 网络安全; 隐患治理

中图分类号: TP393.08 **文献标识码:** A

Analysis of Network Security Hazard Management in Cloud Computing Environments

Yuling Lu

Macrolink Holding Group Co., Ltd.

[Abstract] The widespread adoption of cloud computing has reshaped traditional network architectures. The dynamic and shared characteristics of cloud-based networking have disrupted conventional protection models and generated various new types of network security hazards. This paper systematically reviews security risks in four core dimensions of cloud environments: virtualization architectures, multi-tenant access, network boundaries, and data transmission. Based on the operational characteristics of cloud networks, it analyzes the causes and mechanisms of various security hazards and develops a targeted security protection and management system adapted to dynamic cloud scenarios. A multidimensional and comprehensive security optimization strategy is proposed, which can effectively address the shortcomings of traditional network protection and improve the overall security and operational efficiency of cloud platforms.

[Key words] cloud computing; network security; hazard management

引言

数字化技术的持续升级,推动云计算成为主流的网络资源调度与业务承载方式,灵活高效的资源调配优势,让云组网模式在各行各业广泛落地。组网架构的革新也彻底改变了传统网络的安全运行逻辑,虚拟化部署、多主体共享接入的模式,让网络安全防护面临全新挑战。传统静态防护体系难以适配云环境的动态运行特征,各类隐蔽的安全隐患持续影响网络运行稳定性。立足云网络架构特点梳理安全风险、完善治理手段,成为保障云业务长效稳定运行的关键。

1 云计算环境网络安全概述

网络技术持续更新迭代,行业调研显示国内超7%企业已落地云业务部署,云计算逐步成为各类网络资源调度和业务承载的主流运行形态。该运行方式依靠虚拟资源聚合、动态调度机制与分布式部署架构,改变了传统网络结构固化、资源利用率偏低的运行短板,实现网络资源的灵活分配与高效复用,整体提升

网络体系的运行效能。云网络体系具备资源开放共享、多用户并行接入、网络范围动态浮动的独有特征,整体运行环境更为开放灵活,原有封闭式网络防护体系已无法适应当前运行场景。这类全新的组网运行模式彻底改写了传统网络的安全运行逻辑,让防护工作的覆盖范围与管控维度发生根本性转变。传统网络防护手段多围绕静态网络架构设计,防护机制较为固定,适配场景有限,难以匹配云环境动态多变的运行属性。网络安全防护工作主要通过规范网络链路运行状态、维护程序与存储资源的运行秩序,保障整体网络运行状态稳定,减少各类网络异常问题对网络运行的干扰^[1]。依据云网络的架构特点优化安全防护模式,系统梳理网络运行过程中的各类安全隐患,搭建适配性更强的治理体系,可以持续优化云网络运行环境的稳定程度,为各类网络业务持续平稳运转提供保障,也是网络安全运维领域优化升级的重要趋势。

2 云计算环境主要网络安全隐患

2.1 虚拟化层面网络安全隐患

云计算整体架构的落地运行,高度依托虚拟化技术完成硬件资源的抽象重构与逻辑拆分,使单一物理设备能够拆分出多组独立的虚拟运行单元,以此提升硬件资源的利用效率。资源集约部署的运行模式重塑了传统物理网络的防护形态,也让底层网络防护体系产生了诸多新型风险点。虚拟化平台依靠底层管理组件完成各项资源的分配与单元隔离,这类基础程序若出现运行异常,会直接扰乱虚拟单元与物理设备的对应隔离关系,造成虚拟运行边界的管控失效。多组虚拟单元共用同一物理硬件资源的部署形式,使得单元之间的逻辑隔离机制存在可控性不足的问题,行业安全监测显示约6%云平台底层渗透风险源于隔离屏障被突破,可实现跨单元的网络侵入。虚拟运行单元支持动态迁移与灵活调配的运行特性,会持续改变网络拓扑的运行状态,固定的防护策略难以跟随运行环境动态调整,出现防护适配滞后的问题。此外,虚拟镜像可重复调用的部署形式,会让隐藏在镜像程序中的安全缺陷随批量部署扩散至整个虚拟化环境,持续干扰云网络底层架构的正常运转。

2.2 多租户网络访问安全风险

云平台开放式资源共享架构,可支撑多组用户主体同步接入网络体系,依托统一底层架构完成各类业务资源的调取与交互。资源共用的运行模式简化了网络部署流程,使平台资源得到充分利用,但也让访问管控体系面临更为复杂的运行环境,安全调研数据显示,近50%的云平台访问风险源于权限配置疏漏。云环境对不同用户的隔离约束完全依托软件逻辑实现,不存在硬性物理隔离屏障,逻辑化防护极易受系统程序波动影响,造成隔离约束失效。系统对用户访问权限的界定标准较为宽泛,细化管控力度不足,权限区分标准不够清晰,容易出现权限覆盖范围过大的情况。这类权限配置缺陷会造成访问管控松散,让未授权的资源读取和网络接入具备可行条件。系统常态化的身份核验与权限筛查机制较为固定,无法适配用户接入状态的动态变化,长期运行中会积累无效账号与过期权限,形成持续性的网络访问缺陷^[2]。不完善的访问管控体系会持续影响租户之间的网络交互安全,弱化云平台整体的访问防护水平,制约共享网络体系的平稳运行。

2.3 网络边界模糊防护漏洞

传统网络架构依靠硬件设施划定运行区间,区间划分相对固定,防护部署可精准对应网络外围区域,形成持续性的网络防护屏障。云场景下的网络架构依托软件化定义模式完成组网运作,整体组网结构可随业务运行需求灵活变更,网络覆盖区间处于持续变动的状态,彻底打破了传统静态边界的防护逻辑。网络资源跨节点流转与动态调配的运行特点,使得网络内外区间的划分标准不再明确,传统静态防护机制难以全面覆盖新型网络运行场景,行业监测显示,传统边界防护对云内横向流量的管控覆盖率不足40%。常规网络防护手段多针对固定网络出口设置管控规则,难以介入云环境内部各节点之间的数据交互流程,内部流量传输过程缺少完善的审核与管控依据。防护策略的更新节

奏无法匹配网络架构的变动频率,防护规则更新不及时会造成部分网络节点出现防护空白。这种防护层面的缺失会扩大网络风险的传播空间,使得各类安全隐患能够在云网络体系内快速蔓延,持续削弱网络整体的防护基础。

2.4 数据传输交互安全隐患

云平台业务运行依托跨节点的信息交互模式完成资源联动,各类信息内容在虚拟运行单元与物理硬件架构之间持续流转,支撑整体网络体系的正常运转。网络传输链路具备高度开放的运行特征,链路资源面向接入节点开放共享,防护配置不到位的传输通道极易滋生各类安全问题。通用型网络传输协议是当前云环境数据交互的常用载体,这类协议的原生防护设计偏向通用性,针对复杂网络环境的抗干扰与抗侵入能力存在明显不足。信息经过多级节点接力传输的运行形式,拉长了整体流转链路,安全监测显示跨节点传输的数据窃听风险较单节点场景高出近四成,更易受到恶意干预。不同类型的业务信息混合流转,整体构成较为复杂,部分隐蔽性的信息内容难以被常规防护体系全面覆盖,防护覆盖不全面的问题普遍存在^[3]。传输流程的校验机制存在完善空间,无法实现全流程的信息合规校验,信息内容被篡改、异常改动的情况无法及时甄别,整体降低了云环境信息交互的安全质量。

3 云计算环境网络安全隐患治理策略

3.1 强化虚拟化网络安全防护

云网络整体运行体系高度依赖虚拟化架构的支撑作用,底层防护体系的完善质量,决定着整体网络环境的运行平稳程度。为有效处置虚拟化架构层面存在的各类安全薄弱环节,需要从底层运行机制入手,系统性优化平台防护体系的适配能力,运维实践显示,分布式防护可使虚拟化层级风险处置效率提升近40%。可摒弃传统单一节点防护模式,采用分布式防护部署思路,对各虚拟单元之间的数据交互与流量往来实施细化管控,精准甄别并处置异常访问行为。围绕虚拟化平台底层管控程序,建立持续性的隐患排查机制,及时修复程序运行阶段产生的功能漏洞,规避组件运行异常导致的单元隔离失效问题。对各类虚拟镜像资源实行规范化准入管理,在资源部署前期完成全方位安全校验,从源头拦截存在安全缺陷的镜像文件。依据虚拟节点可动态迁移的运行特征,搭建可同步更新的动态防护体系,保障防护标准能够匹配网络运行状态的实时变动。系统性优化虚拟化层级的防护能力,可以有效弥补底层架构的防护缺口,持续提升云网络基础环境的安全运行水平。

3.2 规范多租户网络访问管理

云平台多用户并行接入、资源共用的组网形态,对访问管控精细程度提出更高标准,有序的访问管控是弱化共享架构安全缺陷的核心手段。网络访问管控体系的升级优化,需要依托权限分级、身份甄别、交互约束的全方位改造,完善整套接入管控运行逻辑。平台可结合不同接入主体的业务运行场景,精准划分网络资源的访问边界,落实最小权限运行原则,行业数据显示,落地该原则可使越权访问风险下降约60%。系统需要搭

载动态化的资质审核机制,对各类接入账号的访问资格进行周期性复核,及时清除长期未使用的无效权限配置,减少隐蔽性的接入风险。针对租户间横向流量交互行为,增设专项访问拦截与校验机制,收紧跨主体资源互通的准入条件,阻断非正常的横向接入行为^[4]。持续细化多用户场景下的网络管控细则,完善全流程访问约束机制,可以稳步提升共享网络架构的隔离防护能力,保障多用户并行接入模式的安全有序运转。

3.3 提升网络边界防护能力

传统网络依靠固定拓扑结构形成稳定的边界防护体系,这类静态防护逻辑无法适配云计算场景下拓扑结构灵活变动的组网特点,整体防护有效性会随网络架构迭代逐步下降。网络边界防护的优化升级,需要突破传统静态防护的局限,构建适配动态组网的新型防护体系。防护改造工作可以结合内外网分层防护的思路开展,针对外部接入端口和内部节点交互通道设置差异化防护标准,弥补传统防护体系对内网交互管控不足的问题。接入适配软件定义组网模式的智能防护模块,摆脱传统硬件防护设备的固定限制,使防护策略能够跟随网络架构的动态调整同步迭代更新,提升防护机制与云组网模式的契合度。着重加强内网数据交互过程的流量审核工作,规范节点之间的通信标准,实现全网流量的一体化防护管控。定期梳理整体网络的拓扑结构变化,及时更新边界防护范围,消除架构变动带来的防护空白。依托云网络常态化运行状态建立行为判定标准,精准识别各类异常接入行为,强化边界体系的主动防御属性。全新的动态防护架构可以充分适配云网络的开放运行特征,稳步提升网络边界的整体防护水准。

3.4 保障数据传输交互安全

云平台跨节点信息交互的运行形式,使各类业务资源持续在链路中流转,开放共享的传输通道天然存在防护薄弱点,整体交互流程需依托多层次技术优化强化安全基底。云环境的数据交互防护不应局限于单一环节的基础防护,需要结合链路运行特征构建全流程的保护体系。传统通用传输架构的防护标准较为基础,难以应对复杂网络环境下的各类网络干扰,可通过迭代专属传输架构的方式提升链路防护等级,增强网络通道自身的

抵御能力。依据业务信息的重要程度划分防护等级,对核心交互内容执行高标准加密处理,提升信息流转过程的保密性能,经实践验证,分级加密可使核心数据泄露风险降低近70%。在信息出入与节点转发的全流程中嵌入核验机制,及时识别内容改动与传输异常问题,保障所有交互资源的完整性。严格规范各类交互接口的接入标准,细化接口访问的准入条件,拦截未授权的接入行为^[5]。全方位升级数据交互防护体系,可以有效弥补云网络传输环节的防护漏洞,持续稳固云平台信息交互环节的安全运行基础。

4 结束语

未来,云计算技术会朝着更高效、更智能的方向持续迭代,网络组网形态与资源交互模式也会持续更新,随之衍生的网络安全风险也会呈现多元化、复杂化的发展特征。网络安全防护工作需要摒弃固化的防护思维,贴合云环境动态运行特征持续优化防护体系。持续完善虚拟化防护、租户管控、边界治理与数据保护等核心环节的治理手段,能够持续适配云网络的发展变化,逐步构建全方位、动态化的安全防护屏障,为云计算技术的常态化、规模化落地应用提供稳定的安全支撑。

[参考文献]

- [1]张羽芳,王振龙,陈星源,等.云计算环境下网络安全关键技术研究现状与展望——基于CiteSpace知识图谱的分析[J].应用数学进展,2025,14(6):55-63.
- [2]刘卫伟,李晓刚.云计算环境下网络信息安全技术发展分析[J].新潮电子,2025,(1):31-33.
- [3]李晓静,杨秀杰.云计算环境下多模态异构网络数据安全存储方法[J].现代电子技术,2025,48(6):63-67.
- [4]梁西陈.云计算环境下的虚拟机安全性分析与改进[J].集宁师范学院学报,2025,47(3):83-88.
- [5]廖芳,李雪松,李迪,等.云计算大数据环境下的信息安全技术分析[J].中国新通信,2025,27(5):42-44.

作者简介:

鲁玉岭(1987--),男,汉族,天津人,本科,中级工程师,研究方向:网络技术与云计算。