云计算环境下的网络安全防护技术研究

徐金萍
潍坊职业学院　山东　潍坊　261000

摘　要：云计算凭借弹性伸缩、资源共享等优势已成为信息化建设的主流模式，但其虚拟化、多租户、网络边界模糊的架构特征，也衍生出诸多新型网络安全隐患。传统网络安全防护技术受静态规则与固定边界限制，难以适配云端动态复杂的运行环境，存在防护盲区多、检测能力弱等问题。本文通过梳理云计算架构特点，系统分析云环境下的网络入侵、租户隔离失效、数据传输泄露等主要安全风险，对比研究传统防护技术的适配短板，重点探讨零信任访问、虚拟隔离、动态入侵检测及数据加密脱敏等新型防护技术。最后构建多层级安全防护体系与智能预警机制，为云计算网络安全防护建设提供可行的技术参考。

关键词：云计算；网络安全风险；安全防护技术；构建与优化

引言：随着数字化技术的持续普及，云计算在企业业务部署、数据存储与网络交互中的应用范围持续扩大，彻底改变了传统信息化的建设模式。云计算依托虚拟化资源池实现资源按需分配，有效降低了运维成本，提升了资源利用效率。但相较于传统封闭式网络，云环境网络边界开放、用户类型复杂、数据流转频繁，网络安全威胁呈现多样化、隐蔽化、动态化特征。传统防护手段已无法有效应对跨租户渗透、动态流量攻击、云端数据窃取等新型风险。在此背景下，研究适配云计算场景的网络安全防护技术，构建系统化、智能化的防护体系，对保障云端业务稳定运行与数据安全具有重要现实意义。

1 云计算与网络安全防护概述

1.1 云计算的核心概念与服务模式

云计算是依托互联网实现资源按需调度、共享与交付的分布式计算模式，打破了传统本地服务器算力、存储资源的局限，具备按需取用、弹性伸缩、资源共享的核心特点。该技术将网络、算力、存储、软件等资源整合为虚拟化资源池，根据用户实际需求动态分配资源，有效降低企业信息化建设的硬件投入与运维成本。现阶段行业通用的服务模式主要分为三类，分别是基础设施即服务、平台即服务和软件即服务。三种模式层级划分清晰，分别为用户提供底层硬件资源、开发运行平台、云端应用软件服务，覆盖了企业从基础架构搭建到业务系统运行的全场景需求，也是云计算安全防护分层研究的基础。

1.2 云计算环境的架构特征

云计算环境区别于传统本地网络架构，具备虚拟化、多租户、分布式部署的核心特征。虚拟化技术是云环境的核心支撑，通过对物理硬件资源虚拟化拆分，实现一台物理设备承载多个虚拟节点运行，大幅提升资源利用率。多租户架构为不同用户、企业提供隔离的云端服务空间，多个用户资源共存于同一物理集群。云计算采用分布式集群部署模式，数据与业务不再局限于单一服务器，而是分散存储、运行在不同云端节点。

1.3 网络安全防护的核心理论与评价标准

网络安全防护的核心理论围绕网络运行稳定性、数据安全性、访问可控性展开，核心目标是防范网络入侵、数据泄露、恶意攻击等安全问题，保障网络业务正常运行。在云计算场景中，防护核心延伸为云端资源隔离、数据传输安全、访问权限管控。对应的防护效果评价标准主要包含安全性、稳定性、高效性三大维度。安全性重点检测是否存在漏洞、攻击风险及数据泄露隐患；稳定性考察防护机制在高并发、动态资源调度场景下的运行状态；高效性衡量防护技术对云端业务运行速度、资源利用率的影响，是适配云计算轻量化、高效率运行需求的关键评价指标[1]。

2 云计算环境下网络安全风险与威胁

相较于传统网络架构，云计算环境具备边界模糊、资源虚拟化、多租户共存的特性，网络运行环境更为复杂，衍生出区别于传统网络的安全风险与威胁，各类安全隐患直接威胁云端业务与数据安全，具体可分为以下三类。（1）网络边界模糊引发的外部入侵风险。传统网络依托固定防火墙、网关构建封闭安全边界，防护范围清晰。而云计算资源具备动态伸缩、跨节点部署特点，网络边界呈现开放化、动态化状态，固定防护设备无法实现全域覆盖。攻击者可利用端口扫描、漏洞渗透、DDoS攻击等方式，针对云端公开网络接口、虚拟节点漏洞发起入侵，突

破网络防护屏障，干扰云端服务器正常运行，造成网络瘫痪、业务中断等问题。（2）多租户架构带来的内部隔离风险。多租户是云计算核心运行模式，多个用户与企业资源共享同一物理硬件集群，通过虚拟隔离技术划分独立运行空间。若虚拟化隔离技术存在漏洞、权限配置不当，会导致租户间网络隔离失效，出现跨租户数据访问、资源串扰问题。恶意租户可借助漏洞窃取其他租户的业务数据、用户信息，引发数据泄露风险，是云环境独有的核心安全隐患。（3）数据传输与节点交互的安全威胁。云计算数据需依托公共网络完成跨节点、跨区域传输，传输过程脱离本地内网保护，极易遭遇中间人攻击、数据窃听与篡改。云端大量虚拟节点频繁交互数据，节点数量多、交互路径复杂，部分隐蔽节点的安全漏洞难以排查，易被恶意程序利用，植入木马、病毒，持续窃取、篡改云端数据，破坏网络数据完整性与保密性[2]。

3 云计算环境下网络安全防护技术

3.1 云计算环境下传统网络安全防护技术适配性分析

3.1.1 传统防火墙技术适配性分析

传统防火墙以固定网络边界为基础，依靠预设静态规则过滤网络流量，广泛应用于拓扑、IP地址相对固定的传统局域网。云计算具备资源弹性伸缩、虚拟机动态迁移、多租户分区运行等特征，使得传统防火墙的缺陷逐步显现。（1）防护边界僵化。云端网络地址、端口随资源调度实时变动，静态防护规则无法同步更新，形成防护盲区。（2）吞吐量受限。多租户并发访问产生海量交互流量，传统硬件设备算力不足，易出现流量阻塞、规则匹配延迟。（3）管控粒度较粗。该设备仅能实现整体流量管控，不能对单个租户、虚拟主机设置独立权限，难以抵御租户串扰、内网渗透等风险。

3.1.2 传统入侵检测与防御技术适配性分析

传统入侵检测与防御系统依靠静态攻击特征库和流量分析识别攻击行为，适用于结构稳定、攻击路径明确的传统网络，在云环境中适配性不足。（1）特征库迭代缓慢。云端新型攻击、跨租户攻击手段不断变化，现有特征库难以及时收录，漏检、误检问题频发。（2）监测范围有限。检测设备部署在物理网络边界，仅可监控物理链路流量，无法穿透虚拟化架构，难以发现虚拟节点间的隐蔽攻击。（3）动态识别能力弱。虚拟机启停、迁移会产生大量临时流量，系统无法区分正常动态流量与攻击流量，频繁产生误报，干扰安全判断。

3.1.3 传统数据加密与身份认证技术适配性分析

传统加密技术普遍采用固定算法与静态密钥，多用于本地存储与内网传输防护；身份认证以账号密码、静态令牌为主，适配固定设备与固定访问场景，和云计算跨终端、跨网络的访问模式存在明显冲突。（1）密钥管理存在隐患。云端数据体量庞大、传输节点分散，静态密钥长期使用易发生泄露，也不支持动态更新与分级管控。（2）认证维度单一。静态认证方式无法结合设备、地域、时段开展多维度校验，账号冒用风险偏高。（3）运行效率偏低。传统加密算法运算复杂，在云端高频、大批量数据传输过程中，会占用较多算力，拖慢整体业务运行速度[3]。

3.2 云计算环境下新型网络安全防护核心技术

3.2.1 零信任网络访问防护技术

零信任技术摒弃传统边界防护思维，遵循“永不信任、始终验证”的核心原则，适配云计算无边界网络环境，是当前云网络核心防护技术。该技术不区分内网与外网，对每一次网络访问、每一条流量请求均进行全方位校验。（1）动态身份校验。结合设备信息、用户权限、访问场景、网络环境进行多维动态认证，摒弃静态账号密码认证模式，杜绝账号冒用、越权访问问题。（2）最小权限管控。基于租户业务需求分配最小访问权限，仅开放业务必需的网络端口与资源访问权限，从源头缩小攻击面，防范跨租户越权访问。（3）实时行为监测。持续记录用户与设备的网络访问行为，对异常访问、高频操作、跨区域登录等风险行为实时阻断，实现全流程动态防护。

3.2.2 虚拟化网络隔离防护技术

虚拟化网络隔离技术针对云计算多租户共享物理资源的架构特点，解决虚拟网络隔离失效、资源串扰问题，是云环境专属基础防护技术，核心实现虚拟网络与物理网络的双重隔离。（1）虚拟局域网隔离。通过虚拟网络划分技术，将不同租户、不同业务的虚拟节点划分至独立虚拟网段，阻断网段间非法访问，实现租户网络逻辑隔离。（2）虚拟防火墙部署。在每个虚拟租户网络内部部署分布式虚拟防火墙，替代传统物理防火墙，可跟随虚拟机迁移、资源扩容动态适配，实现精细化流量管控。（3）端口安全隔离。对虚拟端口进行权限绑定与状态监控，关闭闲置虚拟端口，限制端口非法映射，防范端口漏洞引发的内网入侵与数据窃取。

3.2.3 云动态入侵检测与防御技术

云动态入侵检测技术依托大数据挖掘与机器学习智能算法，适配云计算网络拓扑动态变化、虚拟节点灵活迁移的复杂网络环境，有效弥补了传统静态入侵检测技术响应滞后、覆盖范围有限、无法识别新型攻击的缺陷，能够对虚拟化网络中的各类恶意行为开展精准识别与主动防御。

（1）全网流量全景监测。技术实现物理网络、虚拟网络及租户内部网络的全链路流量深度监测，可精准捕捉虚拟节点内部漏洞攻击、跨租户横向渗透、资源耗尽型DDoS分布式攻击等隐蔽性较强的新型网络威胁。（2）智能特征迭代更新。依托云端海量安全样本数据库，持续汇总全网攻击数据，自动收录新型攻击特征并迭代算法模型，动态优化识别规则，显著降低未知攻击与变异攻击的漏检、误检概率。（3）联动主动防御。系统监测到异常流量与非法攻击行为后，可与云端虚拟防火墙、全局访问控制策略深度联动，实时阻断攻击链路、封禁攻击节点，形成检测、研判、处置、溯源的一体化闭环防御体系。

3.2.4 云端数据传输加密与脱敏技术

该技术针对云端数据跨节点、跨区域传输的安全风险，实现传输数据的全程防护，兼顾数据安全性与业务可用性，适配云计算高频数据交互场景。（1）动态密钥加密。采用临时密钥、分段加密模式，针对每一次数据传输生成独立密钥，传输完成后自动失效，规避静态密钥泄露风险。（2）数据脱敏处理。对用户隐私、业务核心数据进行脱敏替换，非必要场景展示模糊化数据，即使数据传输被窃听，也无法获取有效核心信息。（3）传输链路加密。对云端节点传输链路、用户访问云端链路进行全程加密，抵御中间人攻击、流量窃听与数据篡改行为，保障数据传输完整性与保密性[4]。

4 云计算网络安全防护技术体系构建与优化

4.1 多层级云网络安全防护体系架构设计

结合云计算分层架构特征，可构建物理层、虚拟层、数据层、应用层四层防护架构。（1）物理层聚焦服务器、交换机等硬件设备安全，做好设备准入、硬件漏洞检测与机房环境安全管控。（2）虚拟层针对虚拟化节点、虚拟网络开展隔离防护，依托虚拟防火墙、微隔离技术规避租户串扰与虚拟节点攻击风险。（3）数据层围绕数据传输、存储、调用全流程，落实加密、脱敏、备份等防护手段。（4）应用层针对云端业务系统、访问接口开展安全监测，拦截注入攻击、越权访问等行为，实现全维度覆盖防护。

4.2 防护技术的融合应用方案

各类云安全防护技术存在各自优劣，单一技术防护存在局限性，需推进技术融合落地。（1）边界防护与内网防护融合，结合零信任访问控制与虚拟网络隔离技术，兼顾外网入侵拦截与内网精细化权限管控。（2）被动防御与主动检测融合，将防火墙流量过滤、数据加密等被动防护技术，与动态入侵检测技术联动，形成拦截、监测、溯源的闭环防护模式。（3）多场景技术适配融合，针对不同租户、不同业务的安全需求，灵活组合防护技术，实现差异化防护。

4.3 基于大数据的智能安全预警优化机制

依托云端海量运行数据，可搭建智能化安全预警机制，优化传统人工排查、事后处置的防护模式。（1）采集全网流量、设备运行、用户访问等多维度数据，构建云端安全数据库。（2）通过大数据算法分析异常流量、违规访问、高频攻击等风险特征，实现安全隐患的提前识别。（3）建立分级预警机制，根据风险等级自动触发预警、流量阻断、权限冻结等操作，提升云网络安全防护的主动性与时效性[5]。

结束语：本文围绕云计算环境下的网络安全防护技术展开系统性研究，结合云计算特殊架构特征，总结了当前云网络面临的外部入侵、内网串扰、数据传输不安全等核心风险。通过分析传统防火墙、入侵检测、加密认证技术的适配局限性，梳理适配云场景的新型防护关键技术。从物理层、虚拟层、数据层和应用层完成多层级防护架构设计，结合技术融合方案与大数据智能预警机制，优化云端安全防御模式。

参考文献

[1]申捷.云计算环境下的网络安全防护技术研究[J].现代工业工程,2026(1):132-134.

[2]袁伟坚.云计算环境下的网络安全防护技术研究[J].IT经理世界,2024(8):17-20.

[3]马慧.网络安全技术在云计算环境下的应用与防护策略研究[J].现代工业工程,2026(4):128-130.

[4]莫善朋.云计算环境下网络信息安全技术发展研究[J].中国宽带,2026,22(1):69-71.

[5]时荣.云计算环境下的信息安全防护技术与应用研究[J].信息记录材料,2026,27(4):139-141.