文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

云网融合网络架构安全防护关键技术研究

王稳
深圳白沙科技有限责任公司
DOI:10.32629/acair.v4i3.21354

[摘　要] 云网融合实现了计算、存储与网络资源的深度协同与统一调度,成为支撑数字化业务发展的核心基础设施。架构的根本性变革打破了传统网络的物理边界与安全防护体系,催生了跨域攻击、策略失配、响应滞后等全新安全风险。当前云网安全防护技术正处于转型阶段,各类防护手段逐步落地但仍存在明显短板。相关研究围绕云网融合的核心安全特征展开,梳理防护技术实施现状与核心问题,提出针对性的技术与管理措施,为构建一体化云网安全防护体系提供实践参考。
[关键词] 云网融合；网络安全；零信任；安全编排；策略动态适配
中图分类号：TN915.08　**文献标识码**：A

Research on Key Technologies for Security Protection in Cloud-Network Convergence Network Architecture

Wen Wang
Shenzhen Baisha Technology Co., Ltd.

[Abstract] Cloud-network convergence realizes the deep collaboration and unified scheduling of computing, storage and network resources, becoming the core infrastructure supporting the development of digital businesses. The fundamental transformation of the architecture breaks the physical boundaries of traditional networks and the security protection system, giving rise to new security risks such as cross-domain attacks, policy mismatch, and response lag. Currently, cloud-network security protection technologies are in a transitional stage. Various protection measures are gradually being implemented but still have obvious shortcomings. Relevant research focuses on the core security features of cloud-network convergence, summarizes the current implementation status and core issues of protection technologies, and proposes targeted technical and management measures to provide practical references for building an integrated cloud-network security protection system.
[Key words] Cloud-Network Convergence; Network Security; Zero Trust; Security Orchestration; Dynamic Policy Adaptation

引言

数字经济发展推动云网融合架构快速普及,业务系统逐步从传统数据中心向云端迁移,网络与云资源的边界逐渐模糊,云网融合通过资源池化与动态调度,大幅提升了业务部署效率与资源利用率,为各类数字化应用提供了灵活的支撑能力,传统安全防护体系基于固定物理边界构建,通过防火墙、入侵检测等设备在网络入口处实施集中管控,这种模式在静态网络环境中能够发挥有效作用,但在云网融合架构下,资源跨地域、跨平台分布,用户与设备可以随时随地接入网络,传统边界防护已经无法覆盖所有攻击面,攻击者可以利用云网架构的漏洞绕过边界防护,深入内部实施横向渗透,给业务安全带来严重威胁,云网安全是数字化转型的重要保障,面对架构变革带来的全新挑战,必须突破传统防护思路的局限,构建与云网融合特性相适应的安全防护体系,深入分析云网融合的安全特征,梳理当前防护技术存在的问题,探索有效的解决路径,对于保障云网环境下的业务稳定运行具有重要的现实意义。

1 云网融合网络架构安全防护技术的现状描述

1.1云网融合架构下资源动态调度与边界消融的安全特征

云网融合最核心的特征是网络与云资源的深度协同。传统架构中,网络与云是相互独立的两个层面,分别由不同的团队进行管理。云网融合实现了网络资源的云化与云资源的网络化,计算、存储与网络资源被统一纳入资源池,能够根据业务需求进行动态调度与按需分配。业务部署不再受物理地域的限制,资源可以在不同数据中心、不同云平台之间灵活迁移,极大提升了业务的敏捷性。

网络边界的消融是云网融合最显著的安全特征。传统网络

Copyright © This work is licensed under a Commons Attribution-Non Commercial 4.0 International License.

拥有清晰的内外网物理边界，安全防护主要围绕边界展开。云网融合环境下，业务系统分布在公有云、私有云、边缘云等多个节点，用户可以通过互联网从任何地点访问云资源。物理边界逐渐消失，取而代之的是随用户、设备与资源动态变化的虚拟边界。传统的边界防护设备无法跟随资源移动，导致大量资源暴露在公共网络中，攻击面大幅扩大。

流量流向也发生了根本性变化。传统网络中，南北向流量占据主导地位，大部分流量在内部网络与外部网络之间流动。云网融合环境下，云内服务之间的东西向流量成为主流，占比远超南北向流量。这些流量主要在数据中心内部流动，传统的边界防护设备无法对其进行有效监控与管控，给攻击者的横向渗透提供了便利。

1.2云网安全防护关键技术的实施现状

当前云网安全防护技术已经取得了一定的进展，各类新型防护手段逐步在工程实践中得到应用。安全能力池化是云网安全的重要发展方向，通过将防火墙、入侵检测、病毒防护等安全功能虚拟化，形成统一的安全能力池。安全能力可以根据业务需求进行弹性伸缩，按需分配给不同的租户与业务系统，解决了传统硬件安全设备扩展性差的问题[1]。

零信任安全理念在云网环境中得到广泛认可，现在很多公司开始在远程访问、云资源访问这些场景中使用零信任技术，主要是通过身份来进行访问控制，他们会不断验证用户和设备的身份，确保只有合法的人才能访问相应的资源，这样就能有效降低身份被冒用的安全风险，还有一些公司尝试把零信任的理念用到云内部服务之间的访问控制上，来构建一个服务级别的零信任防护体系。

云网安全运营中心的建设也在不断推进，把云服务和网络的安全日志和警报信息整合起来，就能集中监控和分析安全事件，有些企业用了大数据和人工智能技术，提高了发现安全问题的能力，缩短了应对威胁的时间，但总的来说，现在的云网安全防护还是有点乱，云服务和网络的安全设备各自行动，没有统一的协调和配合，很难应对跨领域的复杂攻击。

2 云网融合网络架构安全防护技术存在的问题

2.1云网边界消融导致跨域横向渗透攻击面失控

传统安全防护体系的核心是边界防护，所有的安全资源都集中部署在网络边界处，重点防范来自外部的攻击。对于内部网络的流量，大多采用默认放行的策略，缺乏有效的管控手段。云网融合环境下，边界消融使得攻击者可以通过多种方式绕过边界防护，进入云网内部。一旦攻击者获得了某个节点的访问权限，就可以利用内部流量管控宽松的漏洞，在不同云平台、不同业务系统之间进行横向渗透，逐步扩大攻击范围。

跨域资源共享进一步扩大了攻击面。云网融合环境下，不同租户、不同业务系统之间共享底层的物理基础设施。攻击者可以利用云平台的漏洞，从一个租户的系统渗透到另一个租户的系统，造成跨租户的数据泄露。同时，边缘节点的大量接入也增加了安全风险，边缘设备的安全防护能力相对薄弱，容易成为攻击者入侵云网核心的跳板。

横向渗透攻击具有很强的隐蔽性。攻击者通常会利用合法的账号与权限进行活动，其行为与正常用户的行为非常相似，很难被安全设备检测到。而且云内流量大多采用加密传输，传统的安全设备无法对加密流量进行深度分析，难以发现隐藏在流量中的攻击行为。很多企业在发生安全事件后，无法及时发现攻击者的横向移动，导致攻击范围不断扩大，造成严重的损失[2]。

2.2跨域跨层安全编排割裂导致端到端威胁响应滞后

云网融合架构涉及云、网、边、端多个层面，每个层面都装了好多安全设备，但这些设备都是不同厂商的，用的技术标准和接口也不一样，彼此之间没法有效配合，一旦有安全事件，这些设备只能单独行动，没法联合起来保护，云那边的设备发现威胁了，没法及时告诉网那边的设备，网那边的防护措施也延伸不到云那边去，所以响应速度很慢。

安全编排能力不足是导致响应滞后的主要原因，现在很多公司的安全设置还只是在一个层面上，不能做到不同领域和层次的统一管理，配置和调整安全策略需要人手动操作，一旦发生安全事件，管理人员得分别登录各种安全设备来处理，流程复杂还浪费时间，如果遇到大规模的攻击，人工响应的速度根本跟不上攻击的传播速度，结果就是威胁在短时间内迅速扩散。

威胁情报的共享机制也不完善，不同的安全设备和厂商之间不能实时共享威胁情报，所以同一个威胁在不同的地方被反复检测，浪费了很多安全资源，而且，没有统一的威胁情报分析和判断能力，无法对威胁进行全局了解，很难提前发现潜在的攻击风险。

2.3算网资源动态迁移导致安全策略一致性保障失效

资源动态调度是云网融合的核心优势，系统能根据业务量自动调整资源的分布，业务量增加时，系统会在其他节点自动创建新资源分担压力，业务量减少时，系统会自动释放多余资源，降低运营成本，动态迁移资源能有效提高资源利用率，但给安全策略管理带来了重大挑战[3]。

传统的安全策略基于静态的IP地址与端口进行配置，资源的位置是固定的，当资源移动到别的节点时，它的IP地址和网络结构都会变化，之前的安全设置就不适用了，如果安全设置不能跟着资源一起移动，新创建的资源就会没有保护，形成一段保护空白期，攻击者可以利用这个空白期攻击新资源，然后渗透整个云网系统。

安全策略的配置与更新速度无法跟上资源的动态变化，在业务忙的时候，系统可能会一下子创建好多新东西，安全管理人员来不及给每个东西都配上安全策略，而且业务总是变来变去，每次变化都可能要调整东西和安全策略，如果靠人工来配，效率太低了，还容易出错或漏掉，最后就可能留下安全漏洞。

3 云网融合网络架构安全防护技术的优化策略

3.1实施云网零信任跨域身份微隔离以遏制横向渗透

以身份为核心重构云网安全边界，构建全域零信任防护体系。为所有的用户、设备、服务与资源分配唯一的数字身份，

Copyright © This work is licensed under a Commons Attribution-Non Commercial 4.0 International License.

所有的访问请求都必须经过严格的身份验证与授权。无论访问请求来自内部还是外部，都遵循永不信任、始终验证的原则。通过持续的行为分析与风险评估，动态调整访问权限。当检测到异常行为时，立即撤销相应的访问权限，防止攻击者利用被盗身份进行横向渗透。

在零信任架构的基础上，实施细粒度的微隔离。将云网划分为多个独立的安全域，每个安全域包含一组具有相同安全等级的资源。不同安全域之间通过严格的访问控制策略进行隔离，只允许必要的业务流量通过。可以按照业务系统、数据敏感度、组织架构等维度进行安全域的划分，确保不同安全级别的资源之间相互隔离。微隔离能够将攻击限制在单个安全域内，即使某个安全域被突破，攻击者也无法渗透到其他安全域，有效缩小攻击的影响范围。

加强对云内东西向流量的全面监控，在云网里装上流量采集和分析设备，对所有来来回回的流量都进行仔细检查，通过分析流量的协议和行为模式，找出不正常的流量模式和攻击行为，建立内部威胁检测模型，持续监控用户和服务的活动，及时发现内部人员的违规操作和攻击者的横向移动[4]。

3.2构建云网跨层安全编排与自动化联动机制以加速端到端响应

建立统一的云网安全管理平台，把云、网、边、端的全部安全资源都集中管理起来，统一调度，平台通过标准化的接口连接不同厂商的安全设备，隐藏底层设备的差异，给安全管理人员提供一个统一的操作界面，把分散的安全能力整合成一个整体，实现安全策略的统一制定、统一下发和统一监控。

构建跨层安全编排引擎，自动处理安全事件，提前设定好各种安全问题的处理流程和办法，当安全管理系统发现安全问题，会自动启动对应的处理流程，协调云端和网端的安全设备一起处理，比如自动隔离受感染的主机、阻断攻击流量、撤销可疑用户的访问权限等，这样自动处理能大幅缩短响应时间，把攻击的影响降到最低。

建立统一的威胁情报共享与分析体系，把来自各种安全设备、不同厂商的威胁信息收集起来，统一分析判断，形成全面的网络安全情况图，让安全管理人员清楚地了解云网的安全状况，把威胁信息实时传给所有安全设备，提高它们的检测能力，通过信息共享和联动，提前预警攻击并主动防御。

3.3强化安全策略与算网资源调度的动态适配以保障策略一致性

实现安全策略与算网资源调度的深度联动，让安全策略跟着资源一起动，把安全策略和资源的身份绑在一起，而不是绑在IP地址上，资源从一个节点搬到另一个节点时，对应的安全策略也会跟着一起搬，保证资源在整个使用过程中都有统一的安全保护，这样彻底解决了资源搬家时安全策略不匹配的问题，避免了安全保护的中断。

采用模板化的方式管理安全策略，针对不同业务和资源，提前设定好安全策略模板，模板里包括了该类资源需要的所有安全规则和配置，创建新资源时，系统会自动给它分配对应的安全策略模板，自动完成安全配置，这样管理能大幅提高配置效率，减少人工配置可能出现的错误和遗漏[5]。

建立安全策略的全生命周期管理机制，全程管理安全策略的创建、发布、更新和删除，定期检查和优化安全策略，清除过时和冗余的策略，避免策略冲突和爆炸式增长，使用自动化工具检查安全策略的合规性，确保符合法律法规和企业的安全需求，建立安全策略变更的审计流程，记录所有变更操作，方便事后追溯和审计。

4 结语

云网融合架构的演进带来了业务效率的提升，也引发了一系列全新的安全挑战。边界消融、跨域协同与资源动态调度使得传统的安全防护体系难以适应新的环境，跨域横向渗透、威胁响应滞后与策略一致性失效成为当前面临的主要问题。实施云网零信任跨域身份微隔离能够有效遏制内部横向渗透，构建全域安全边界。构建跨层安全编排与自动化联动机制可以实现云网安全资源的协同响应，大幅提升威胁处置效率。强化安全策略与算网资源调度的动态适配能够保障资源全生命周期的安全防护，消除防护空窗期。通过这些措施的综合应用，能够构建起一体化的云网安全防护体系，为云网融合环境下的数字化业务提供坚实的安全保障。

[参考文献]

[1]余启明,吴爽,黄帅,等.云网融合下的安全能力池关键技术与应用[J].中兴通讯技术,2023,29(1):20-25.

[2]张悦.云网融合向算网融合演进的关键技术研究[J].中国宽带,2024,20(11):1-3.

[3]陆钢,陈长怡,黄泽龙,等.面向云网融合的智能云原生架构和关键技术研究[J].电信科学,2020,36(9):8.

[4]廖竣锴,程永新.云网融合的广域安全资源编排技术研究[J].通信技术,2021,54(12):9.

[5]李卓桐.面向云网融合的软件定义光业务网关键技术研究[D].北京邮电大学,2024.

作者简介：

王稳(1979--),男,汉族,湖南省双峰县人,本科,网络工程师,研究方向：网络安全。

Copyright © This work is licensed under a Commons Attribution-Non Commercial 4.0 International License.