运营商网络边缘云安全实践

张乐[1]，马洪源[2]
（1. 中国移动通信集团河南有限公司，河南 郑州 450008;
2. 中国移动通信集团设计院有限公司，北京 100080）

摘　要：在运营商边缘云建设的高峰期，为实现“三同步”建设策略，首先阐述了网络边缘云建设和运维管理模式，讨论了网络边缘云的安全风险和安全建设要求；然后，针对传统云安全建设模式在边缘云场景下的局限性进行了分析；最后，提出了创新型网络边缘云安全建设方案，统一进行省级边缘云安全建设，从实践应用角度完成对比，验证了创新型边缘云建设方案优势。

关键词：5G；边缘云；网络安全；to B 业务；UPF 安全
中图分类号：TN929.5
文献标志码：A
doi: 10.11959/j.issn.1000–0801.2023096

Practice on edge cloud security of telecom operators

ZHANG Le[1], MA Hongyuan[2]
1. China Mobile Communications Group Henan Co., Ltd., Zhengzhou 450008, China
2. China Mobile Group Design Institute Co., Ltd., Beijing 100080, China

Abstact: In the peak period of operator edge cloud construction, in order to realize the “three synchronization” construction strategy, the network edge cloud construction and operation and maintenance management mode were expounded, the security risks and security construction requirements of network edge cloud were discussed firstly. Then, the limitations of the security construction mode in the edge cloud scenario for the traditional cloud were analyzed. Finally, an innovative network edge cloud security construction plan was proposed, and the province’s edge cloud security construction was carried out uniformly. The comparison was completed from the perspective of practical application, and the advantages of the innovative edge cloud construction plan was verified.

Key words: 5G, edge cloud, network security, toB business, UPF security

0　引言

网络边缘云作为 5G 网络架构中的关键一环，具有低时延、广覆盖、大带宽的技术特点，运营商可以利用网络边缘云向用户侧不断下沉的建设优势，给 toB 用户提供更高品质的服务。基于网络功能虚拟化（network functions virtualization，NFV）技术的云化架构，已逐渐被应用到 5G 网络核心侧、边缘侧和接入侧。多接入边缘计算（multi-access edge computing，MEC）技术是云化

收稿日期：2022–09–08；修回日期：2023–04–15

架构在网络边缘的一种应用。5G 的网络边缘从移动核心网络内部迁移到移动接入网边缘，充分利用云计算技术优势为 CT/IT 业务提供了一个资源可弹性伸缩、流量可全局调度、能力可全面开放的分布式服务，但分布式和开放式的业务部署模式也产生了更多的安全风险[1]。

传统云安全建设方案为每个云独立建设安全防护体系，不足以支撑对全局所有 5G 边缘节点的信息安全分析管控。同时，区县以下边缘节点资源有限，传统云安全方案在经济方面和灵活性、差异性满足客户需求方面都存在不足[2-4]，因此需要寻求更契合边缘云场景的云安全解决方案。

本文针对运营商网络边缘云场景，构建“1+1+*N*”创新式边缘云安全架构，通过一个安全业务管理平台、一个安全数据运营分析中台和 *N* 个边缘流量防护节点，为运营商网络边缘云场景构建覆盖性、适应性架构。由集中平台统一安全运营分析，边界安全网元执行信息采集和风险处置，形成立体化安全防护策略，在保护用户、企业、国家网络安全的基础上实现开放、协同、联动能力。

1 网络边缘云安全建设分析

1.1 边缘云安全风险分析

参考《网络安全等级保护基本要求》[5-6]，运营商网络边缘云建设需要在基础设施、通信网络、区域边界、计算环境 4 个方面保证整体云平台安全性，同时提供安全运维管理和安全建设管理能力以保证云平台安全管理的合规性和安全性。根据网络边缘云控制与转发面分离、平台业务异构等特点，建设统一云安全管理平台，保障云上安全能力调度管理，云安全管理平台建设要求满足安全管理合规性、符合行业信息安全审计要求。

由于边缘云转发面直接暴露在整个运营商通信网络中[7]，且被多用户共享，其转发面安全建设需要关注用户安全隔离性要求。在对边缘云归属权划分中，一般认为，云平台基础设施及云平台提供的虚拟化业务承载单元等自建设施为运营商安全权责范围，云上用户业务应用及业务数据为用户私有产权。因此，针对不同的业务形态，安全行为管理需要有明确的划分。

网络边缘云将用户端口功能（user port function，UPF）网元下沉，将 5G 业务不断向用户侧延伸，建设模型的变化引入了更多的安全风险，可分为网络边界安全风险、云计算安全风险、行为管理安全风险三大类。

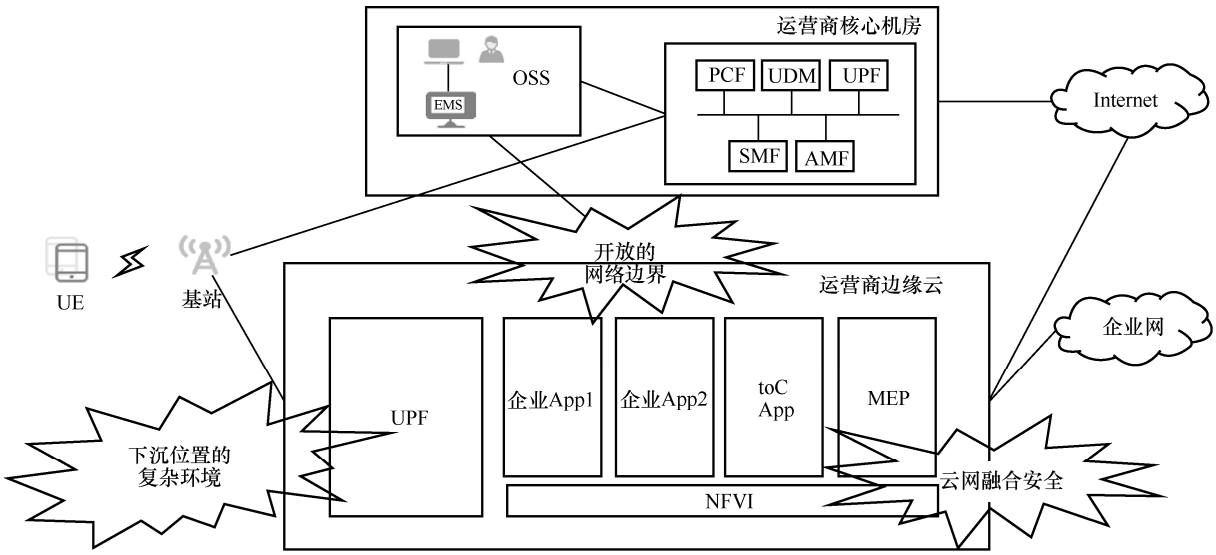
（1）网络边界安全风险

在云计算建设发展过程中，云环境边界安全一直都是关注重点，通过明确的云内外边界定义，收束安全暴露面，控制安全敞口，将云环境安全问题收束在明确节点上，边缘云安全风险示意图如图 1 所示，网络边缘云部署模型的变化带来了新的安全隐患。

从网络边缘云下沉位置分析，如图 1 所示，由于 5G 边缘计算节点部署位置下沉，部分网络设备会直接部署在用户侧机房或与用户侧网络直接连通。因此，相对于传统云独立机房部署场景，网络边缘云对外开放性更强、规范管控能力更弱，攻击者更容易通过开放接口接触到系统，通过非法连接获取网络传输数据。同时，下沉后的边缘机房环境多样，硬件防护和安全保障措施薄弱，易受断电、自然灾害等风险影响。

网络边缘云下沉带来大量网络信令交互的下沉，基于 5G 业务控制与转发分离的特点，UPF 下沉后，其与控制面存在多种信令交互，同时 UPF 仍保持与其他外部网络的互通，因此，网络边缘云与外部系统的数据传输模型更加多样，相应的安全风险更复杂。

综上，网络边缘云下沉位置环境复杂、网络边界开放的特点，会导致网络边缘云安全边界难以界定，难以做到精确的安全控制，这也是本文重点关注的网络边缘云安全要求。



注：用户设备（user equipment，UE）；运营支撑系统（operation support system，OSS）；策略控制功能（policy control function，PCF）；统一数据管理（unified data management，UDM）；用户面功能（user plane function，UPF）；会话管理功能（session management function，SMF）；接入和移动性管理功能（access and mobility management function，AMF）；网络功能虚拟化基础设施（network function virtualization infrastructure，NFVI）

图 1　边缘云安全风险示意图

（2）云计算安全风险

网络边缘云遵循云计算底层架构，引入虚拟化等新兴技术，以容器和虚拟机部署为主。在主机、应用、数据 3 个维度上，类似镜像模板的漏洞、虚拟机逃逸风险、租户间的非授权访问等问题依然存在。

（3）行为管理安全风险

安全防护的重要举措就是做好安全管理工作。相对于中心云池统一建设、统一运维管理模式，网络边缘云业务承载模式相对复杂，对云安全管理上存在粒度划分不明确、权责定义不清晰的问题，易导致安全威胁蔓延。

1.2　边缘云安全防护要求

在对边缘云权责归属划分中，通常认为，云平台基础设施、云平台提供的虚拟化承载单元等为运营商权责范围。主要以基于 UPF 转发网元和边缘计算平台（multi-access edge computing plat，MEP）的安全防护界定为平台安全范围，由运营商保证整体云平台运行安全性和稳定性。

边缘云组件连接示意图如图 2 所示，UPF 作为边缘云下沉路径中的关键网元，与周边系统存在复杂的连接关系。不同的部署环境存在不同的安全风险，所以需要对 UPF 相应接口做安全隔离[8-10]。

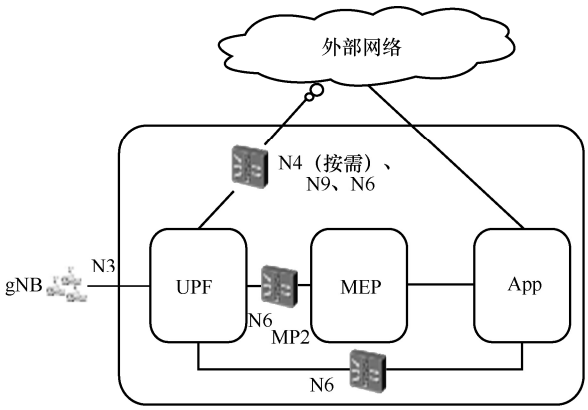
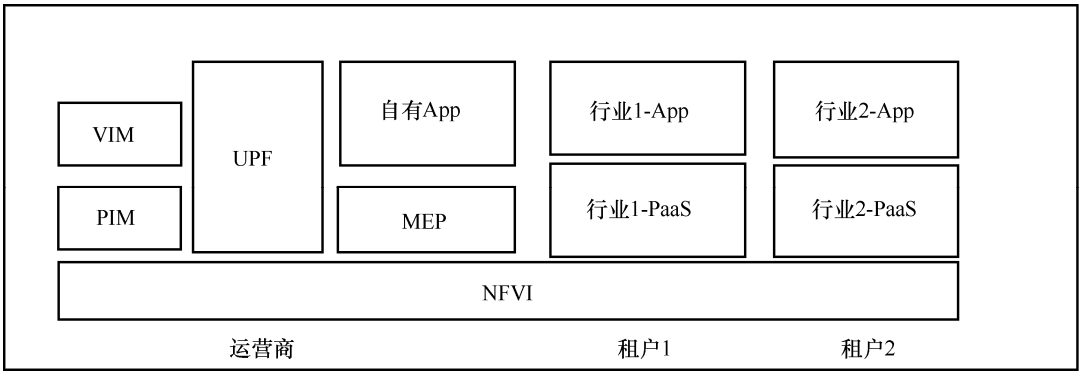


图 2　边缘云组件连接示意图

MEP 作为运营商为云平台用户提供基础业务承载平台，其管理面安全访问控制、业务面安全隔离和平台底座虚拟化安全稳定性都是防护要求。

在实际应用中，由于虚拟化技术快速发展，边缘云上可以创建承载多租户业务主机，执行各自的任务，但不可忽略的是各业务仍运行在同一个环境中。

租户业务模型如图 3 所示，边缘云租户业务



注：虚拟基础设施管理器（virtualized infrastructure manager，VIM）；物理基础设施管理器（physical infrastructure manager，PIM）；平台即服务（platform as a service，PaaS）

图 3　租户业务模型

基于云平台提供的资源进行部署，因此要考虑租户业务与平台间安全隔离、租户与租户间安全隔离。具体租户安全要求如下。

- 针对租户业务与平台安全隔离，规划 UPF 租户流量、MEP、业务应用之间安全隔离。
- 针对租户与租户间安全隔离，根据用户业务规范，规划云平台东西向流量进行安全隔离。
- 考虑不同层次业务系统的不同安全防护粒度要求，需要具备主机安全、数据安全能力。

2　边缘云安全建设方案

2.1　传统边缘云安全建设方案

传统运营商云平台建设有建设规模庞大、建设周期长等特点，同时有业务集中流量大、业务区域广的特点，在建设初期进行业务规划时，为了兼顾后期的业务发展，常常会采用高性能的安全硬件满足安全建设的需要。在一定的周期内会产生应用能力和资源消耗的错配。

在网络边缘云业务发展规划中，由于边缘计算节点有下沉位置较低、覆盖面广、部署点数众多的特点，传统边缘云安全建设模式相对而言会产生较大的冗余和沉没成本。

传统边缘云云安全建设模型考虑云上各类业务需求，会在每个云节点上划分业务与管理区域，并基于不同区域属性部署对应的安全组件，传统云安全建设架构如图 4 所示。因此传统云安全建设模式中各云节点安全建设相对独立，不存在跨云节点间的关联互动。

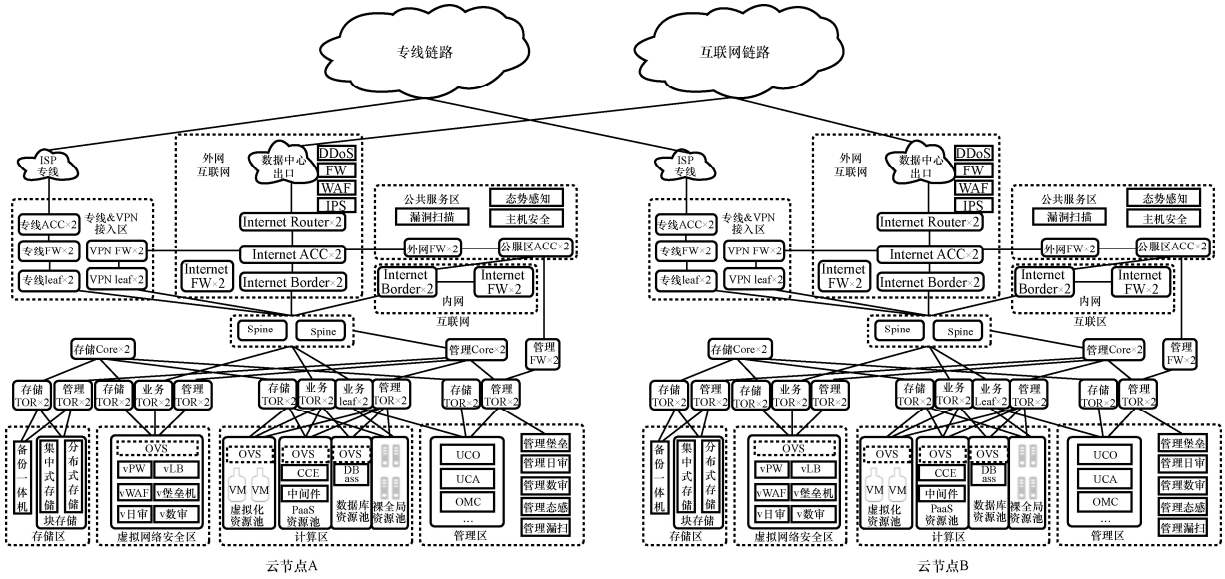
根据 IPDRR 能力框架模型，整体安全防御包括风险识别（identity）、安全防御（protect）、安全检测（detec）、安全响应（response）、安全恢复（recovery）五大能力，从以安全防护为核心的模型，转向以监测和业务连续性管理为核心的模型。因此传统边缘云安全只针对单个云内安全监测的模式，在网络边缘云业务统一调度编排的场景下，缺少安全管理的一致性，不利于执行统一监测、高效管控的安全策略。

2.2　边缘云安全创新建设方案

根据国务院《关于加快建立健全绿色低碳循环发展经济体系的指导意见》中全方位全过程推行绿色规划要求[11]，结合边缘云平台整体安全建设需要和现状，当前运营商边缘云安全建设对建设成本、低碳循环有明确的建设诉求。

因此，考虑整体边缘云业务安全及合规性、建设成本控制需求，遵循集约化、层次化、全覆盖原则，创新实践可采用“1+1+*N*”架构以省为单位建设，边缘云安全建设“1+1+*N*”架构如图 5 所示，将安全分析、安全监测、安全审计、安全运维等能力集中上收到省数据中心集中部署，将流量防护、拦截阻断等能力近源部署到边缘云。

省集中云节点部署云安全管理平台和集中安



注：网络业务提供商（Internet service provider，ISP）；虚拟专用网络（virtual private network，VPN）；分布式拒绝服务攻击（distributed denial of service attack，DDoS）；防火墙（firewall，FW）；应用控制网关（application control gateway，ACG）；开放虚拟交换机（open virtual switch，OVS）；用户控制操作（user control operation，UCO）；用户控制代理（user control agent，UCA）；运行管理控制（operation management control，OMC）

图 4　传统云安全建设架构

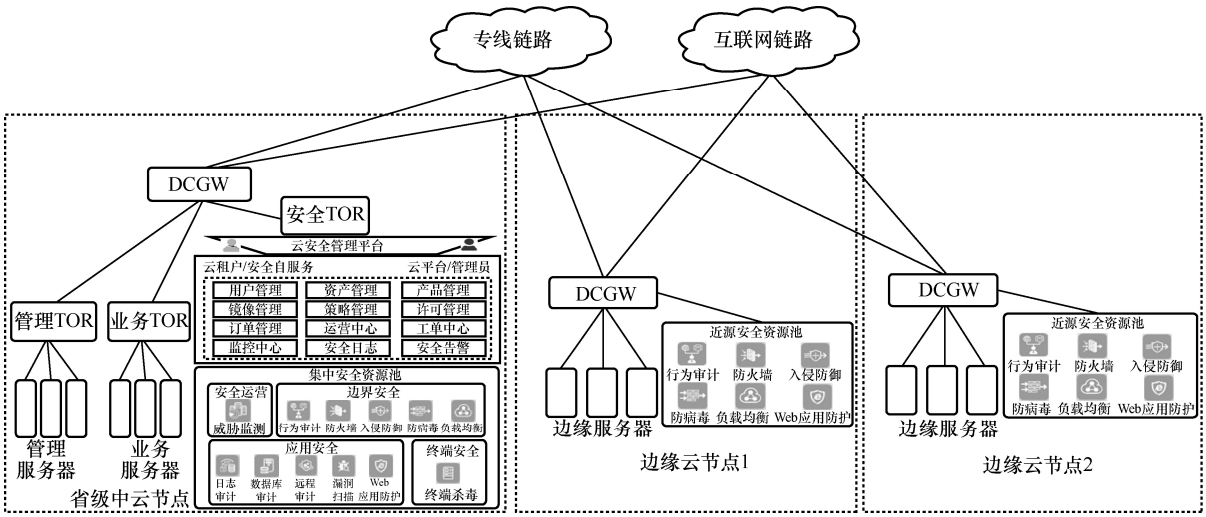


图 5　边缘云安全建设“1+1+*N*”架构

全资源池。其中云安全管理平台提供统一安全运营，并支持边缘云安全资源生命周期管理、策略配置管理和安全业务逻辑管理。集中安全资源池通过为全省所有边缘云及云上业务提供威胁监测、运维审计、日志审计（简称日审）、数据库审计（简称数审）、终端安全、漏洞扫描（简称漏扫）等安全监管能力，变被动为主动，能基于全省构建自适应安全体系。同时集中建设有效打破了传统云安全独立式部署限制，减少了每个节点的重复建设，实现了降本增效。

河南移动边缘云实践现状如图 6 所示，集中安全资源池部署于省内特色资源池，软件定义安全防护池近 UPF 侧部署，部署于郑州边缘云数据中心机房内。

省内特色资源池已完成硬件部署，资源池内设置有隔离区（demilitarized zone，DMZ）、可信域，满足公网业务需求及承载网互通需求。

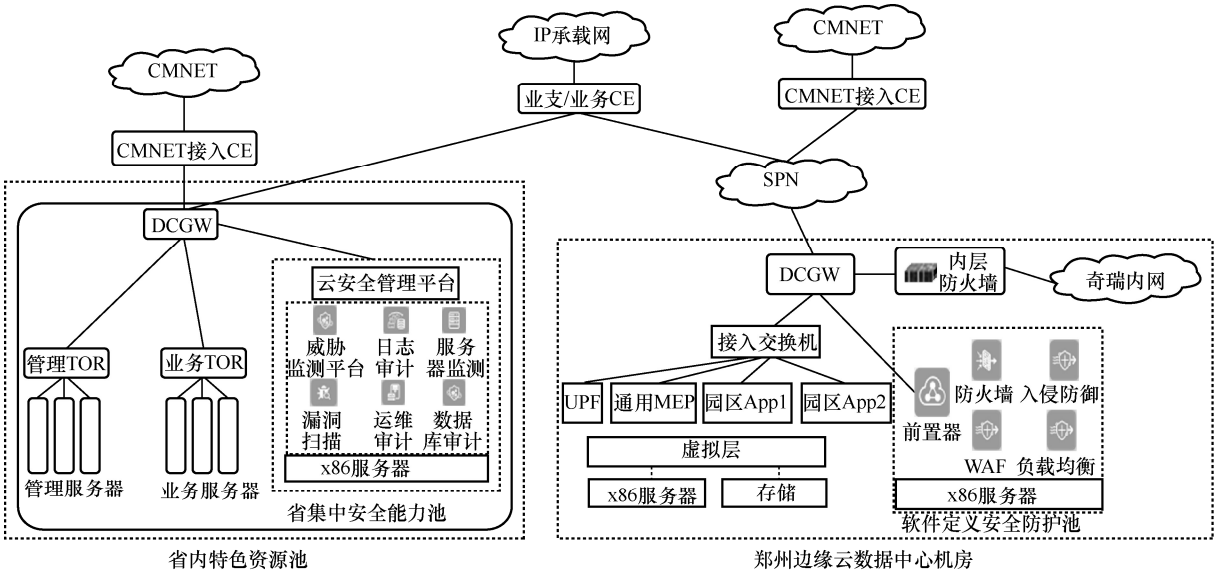


图 6　河南移动边缘云实践现状

安全管理平台和审计类安全资源池部署在省内特色资源池的 DMZ，可以通过中国移动互联网（China Mobile Network，CMNET）访问，集中安全能力池资源规格见表 1。

UPF 和边缘云安全资源池部署在郑州边缘云数据中心机房，对外连接信令侧 N2、N4 接口，以及网管。边缘安全资源池主要部署近 UPF 侧虚拟化防火墙、虚拟化入侵防御系统（intrusion prevention system，IPS）、虚拟化 Web 应用防火墙（Web application firewall，WAF）、虚拟化负载均衡（load balance，LB）等网元，软件定义安全防护池资源规格见表 2。

2.3　边缘云安全建设方案对比

云安全建议方案对比见表 3。

从管理效率来说，传统云安全建设模式下，每个云节点都有单独的云安全管理中心，提供安

表 1　集中安全能力池资源规格

部署位置	服务器用途	服务器规格			数量	服务器类型
		CPU	内存/GB	硬盘/TB		
省内特色资源池	安全管理平台	2×16 核	128	2	1	物理机
省内特色资源池	审计类安全资源池	2×16 核	128	10	2	物理机

表 2　软件定义安全防护池资源规格

部署位置	服务器用途	服务器规格			数量	服务器类型
		CPU	内存/GB	硬盘/TB		
郑州边缘云数据中心机房	边缘安全资源池	2×16 核	128	2	1	物理机

表 3　云安全建设方案对比

建设方式	管理方式	安全管控	建设模式
传统云安全建设	单个云节点独立服务运营	针对单个云节点进行信息采集和管控	专用安全硬件部署交付，规格灵活性差
创新型边缘云安全建设	多个云节点统一服务运营	统一采集多个云节点信息，统一分析与策略管控	通用性服务器设备，虚拟化软件交付灵活

全资源申请和应用能力[12]。但是在处理省内较多边缘云场景下的安全业务时，无法形成统一业务订购、业务开通、管理应用流程。不但每个节点的业务计费、应用能力都需要单独对接现有运营商服务门户，形成重复的开发对接工作，并且各云节点间用户信息不同步，易导致在云租户实际业务应用时，面临业务管理流程复杂、业务开展数据不一致等情况。

从安全管控来说，传统边缘云安全建设模式下，威胁监测和安全防护都局限在单一云节点内。安全能力依据 UPF 及行业客户需求按需配置，通过云环境区域间安全隔离管控和威胁监测处置能力，叠加安全管理规范，形成云环境安全体系[13-14]。但在网络边缘云架构下，安全能力独立部署，互相独立，无全省汇聚统筹网络会带来网络灵活性弱、资源集约度低的问题。相较而言，创新型边缘云安全建设方案中省中心部署的云安全管理平台可通过运营商专线网络对全省范围内所有安全网元进行统一配置管理能力，在批量对省内边缘云平台进行安全策略配置时具备高效性和一致性。同时集中安全能力池具备覆盖全省的监测和审计资源，会收集全省各边缘云节点业务流量信息和网络信息，通过更多的源信息输入，有利于建立更精确的异常流量、用户行为模型。同时省中心资源池可以为监测审计类安全组件提供丰富算力和存储空间。更多的信息输入配合更强的分析计算能力，有效提升风险流量识别的效率、威胁行为研判的准确性，实现对边缘云节点软件即服务（software as a service，SaaS）化安全赋能。基于全局风险监测与统一防护管控，可以建立对全省边缘云节点威胁识别、风险资产定位、精准处置的高效闭环安全体系。

从建设模式来说，网络虚拟化是目前网络发展的大趋势，传统边缘云安全建设多采用硬件形态部署，设备、空间、电源集约性差。以单个边缘云节点为例，传统形态安全能力需要占用 35U 机架空间和 11.7 kW 能耗。因此迫切需要将安全运维能力虚拟化、将安全审计类能力集中化，构建安全能力按需分发、灵活调配的体系。传统边缘 UPF 节点中安全能力需要在近 UPF 侧部署，设备集约性差。以单套 UPF 基础安全能力为例，投资为 10 万元，个性拓展安全能力投资约 5 万元。因此边缘 UPF 的安全能力以单套 15 万元线性叠加。从而造成设备利用率低、投资浪费的问题。基于上述传统边缘网络中安全能力的劣势，引入安全能力“集中+边缘”的防护架构，形成集约灵活网络，实现降本增效。采用虚拟化方式将安全服务能力上收至安全能力池内，随取随用，最大化提升设备使用率。同时对于 UPF 本身防护需求，仍部署于边缘侧，与集中能力池通过运营商专线链路互通。

3　结束语

边缘云是运营商建设重点，保障边缘云安全是全面建设边缘云及推广 toB 业务价值的基石。本文提出了集中+分布式的双层安全建设架构，与运营商 5G 边缘计算架构形成一致性，同时结合软件定义的安全能力池，保障网络边缘云业务正常开展，为 toB 用户提供了灵活选择的差异化安全服务，为运营商云网融合发展、实现政企业务转型提供有效的安全支撑。当前安全建设围绕网络边缘云业务面进行，5G 信令控制面精细化管控将是后续研究的重点方向。

参考文献：

[1] 马洪源, 肖子玉, 卜忠贵, 等. 5G 边缘计算技术及应用展望[J]. 电信科学, 2019, 35(6): 114-123.
MA H Y, XIAO Z Y, BU Z G, et al. 5G edge computing technology and application prospects[J]. Telecommunications Science, 2019, 35(6): 114-123.

[2] 冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83.
FENG D G, ZHANG M, ZHANG Y, et al. Study on cloud computing security[J]. Journal of Software, 2011, 22(1): 71-83.

[3] 李雨航, 郭鹏程. 云安全的发展与未来趋势[J]. 中国信息安全, 2022(5): 39-42.
LI Y H, GUO P C. The development and future trend of cloud security[J]. China Information Security, 2022(5): 39-42.

[4] 李莹, 张乐, 徐晓蕾, 等. 面向 5G 的云网融合发展探讨[J]. 电信工程技术与标准化, 2019, 32(11): 7-11.
LI Y, ZHANG L, XU X L, et al. Discussion on the cloud-network integration for 5G[J]. Telecom Engineering Technics and Standardization, 2019, 32(11): 7-11.

[5] 陈广勇, 祝国邦, 范春玲.《信息安全技术 网络安全等级保护测评要求》(GB/T 28448-2019)标准解读[J]. 信息网络安全, 2019, 223(7): 1-7.
CHEN G Y, ZHU G B, FAN C L. Information security technology—evaluation requirement for classified protection of cybersecurity (GB/T 28448-2019) standard interpretation[J]. Netinfo Security, 2019, 223(7): 1-7.

[6] 马力, 祝国邦, 陆磊. 《网络安全等级保护基本要求》(GB/T 22239-2019)标准解读[J]. 信息网络安全, 2019(2): 77-84.
MA L, ZHU G B, LU L. Baseline for classified protection of cybersecurity (GB/T 22239-2019) standard interpretation[J]. Netinfo Security, 2019(2): 77-84.

[7] 丁春涛, 曹建农, 杨磊, 等. 边缘计算综述: 应用、现状及挑战[J]. 中兴通讯技术, 2019, 25(3): 2-7.
DING C T, CAO J N, YANG L, et al. Edge computing: applications, state-of-the-art and challenges[J]. ZTE Technology Journal, 2019, 25(3): 2-7.

[8] 王琦. 5G 云化安全风险研究[J]. 信息通信技术与政策, 2021(2): 92-96.
WANG Q. Research on security risks of 5G cloud[J]. Information and Communications Technology and Policy, 2021(2): 92-96.

[9] 曹籽文. 边缘计算：框架与安全[J]. 保密科学技术, 2019(9): 44-48.
CAO Z W. Edge computing: framework and security[J]. Secrecy Science and Technology, 2019(9): 44-48.

[10] 尹东明. MEC 构建面向 5G 网络构架的边缘云[J]. 电信网技术, 2016(11): 43-46.
YIN D M. MEC build the 5G-oriented edge cloud[J]. Telecommunications Network Technology, 2016(11): 43-46.

[11] 关于加快建立健全绿色低碳循环发展经济体系的指导意见[J]. 中国产经, 2021(8): 19-22.
Guiding opinions on accelerating the establishment and improvement of green and low-carbon circular development economic system[J]. Chinese Industry & Economy, 2021(8): 19-22.

[12] 董亮, 阚新生, 胡伟雄, 等. 云平台安全技术架构研究[J]. 电信快报, 2021(6): 14-18.
DONG L, KAN X S, HU W X, et al. Research on security technology architecture of cloud platform[J]. Telecommunications Information, 2021(6): 14-18.

[13] 许暖, 韩志峰, 郑瑞刚. 基于分级分类的安全编排技术在网络安全应急响应中的应用探索[J]. 网络空间安全, 2021, 12(S1): 45-53.
XU N, HAN Z F, ZHENG R G. Practice and exploration in cybersecurity emergency response based on graded and classified security orchestration technology[J]. Cyberspace Security, 2021, 12(S1): 45-53.

[14] 赵粤征, 叶建伟, 员珊, 等. 基于 SOAR 的安全运营自动化关键技术构建及未来演进方向[J]. 信息技术与网络安全, 2021, 40(3): 19-27.
ZHAO Y Z, YE J W, YUN S, et al. Key technology construction and future evolution direction of safety operation automation based on SOAR[J]. Cyber Security and Data Governance, 2021, 40(3): 19-27.

[作者简介]

张乐（1976– ），女，中国移动通信集团河南有限公司高级工程师，长期从事中国移动网络云、核心网等领域的网络规划、设计工作。

马洪源（1984– ），男，中国移动通信集团设计院有限公司高级咨询设计师、高级工程师，长期从事云化核心网、边缘计算、5G 专网等方面工作。