5G MEC 系统安全能力部署方案

刘云毅[1]，张建敏[1]，冯晓丽[2]，张丽伟[2]
（1. 中国电信股份有限公司研究院，北京 102209；2. 中国电信集团有限公司，北京 100033）

摘　要：多接入边缘计算（multi-access edge computing，MEC）作为 5G 网络的核心差异能力，是电信运营商为企业客户打造 5G 专网的关键技术。随着 5G MEC 节点数量的增多，安全风险和安全防护方案等问题也日益受到关注。首先介绍了 5G MEC 系统架构，对其潜在安全风险进行了分析。在此基础上，提出了 5G MEC 系统安全能力部署架构和方案，并介绍部署案例。最后，针对目前边缘计算安全能力部署存在的问题与挑战进行了讨论，为后续研究开发提供了参考。

关键词：5G；多接入边缘计算；安全能力；部署方案
中图分类号：TN929.5
文献标志码：A
doi: 10.11959/j.issn.1000–0801.2022265

5G MEC system security capability deployment scheme

LIU Yunyi[1], ZHANG Jianmin[1], FENG Xiaoli[2], ZHANG Liwei[2]
1. Research Institute of China Telecom Co., Ltd., Beijing 102209, China
2. China Telecom Group Co., Ltd., Beijing 100033, China

Abstract: Multi-access edge computing (MEC), as the core differentiated capability of 5G, is the key technology for telecom operators to build private 5G networks for enterprises. With the increase of 5G MEC nodes, security risks and protection schemes are increasingly concerned. Based on the description of 5G MEC system architecture, the potential security risks were analyzed. On this basis, the security capability deployment architecture and scheme of the 5G MEC system were proposed, and the deployment case was introduced. Finally, the current problems and challenges in the deployment of MEC security capabilities were discussed to provide references for subsequent research and development.

Key words: 5G, MEC, security capability, deployment scheme

0　引言

多接入边缘计算（multi-access edge computing，MEC）作为 5G 网络的关键技术，可将计算能力和网络能力按需下沉到靠近用户的网络边缘，从而有效提升用户的业务体验，推动网络与业务深度融合[1]。随着 5G 技术在垂直行业中的广泛应用，MEC 在解决低时延、大带宽、数据不出场等业务问题或客户需求中发挥着日益重要的作用，已成为运营商 5G 定制专网的核心能力和产品之一[2]。

收稿日期：2022−03−23；修回日期：2022−09−23

随着边缘计算产业发展和边缘节点的大规模部署，未来大量的边缘节点将下沉到地市、区县、客户园区等网络边缘。边缘应用和网络能力的开放作为边缘计算系统的核心能力，需要边缘计算系统与 5G 网络、运营管理系统进行频繁交互，实现基于用户个性化业务需求的灵活调度。5G 边缘计算可能会给运营商网络引入一定安全风险，因此，需要对 5G 边缘计算系统的潜在安全风险进行全面分析，从而制定相关方案进行安全能力建设和管控。

国内外研究机构和标准组织针对边缘计算领域的安全问题也展开了一系列研究。欧洲电信标准组织（European Telecommunications Standards Institute，ETSI）发布 MEC 安全性白皮书，分析了与 MEC 安全相关的用例和要求，强调了边缘云和边缘设备带来的安全挑战[3]。文献[4]分析了 MEC 架构中不同类别的安全威胁以及保护措施，建议 MEC 提供商实施多层安全控制机制，以降低针对性的攻击风险。文献[5]重点研究了 5G 网络中 MEC 典型应用场景的安全漏洞，并提出相应的安全流程和解决策略。文献[6]对 5G 边缘计算中 10 个安全关键问题进行了分析，并提出安全解决方案。工业互联网产业联盟面向运营商和 5G 行业用户，提出了 5G 边缘计算安全防护策略，指导行业提升边缘计算的安全能力[7]。

1　5G MEC 系统架构

5G MEC 系统架构如图 1 所示，包括 MEC 业务管理平台（集团级）、MEC 业务管理平台省级汇聚层、MEC 边缘节点 3 级架构。

1.1　MEC 业务管理平台（集团级）

MEC 业务管理平台（集团级）负责边缘计算系统和业务的统一管理和控制，主要包含合作方门户、运营支撑门户、运维管理门户，为用户、运营和运维人员提供服务；能力管理、运营支撑、云边协同、编排管理、安全管理和运维管理子系统，为前端门户提供支撑；同时搭建应用仓库，用于存储应用镜像文件。

MEC 编排器（MEC orchestrator，MEO）作为系统核心控制组件，负责维护 MEC 系统的总体视图，包括边缘资源、应用服务以及网络拓扑等，加载 MEC 应用数据包、检查镜像完整性、验证 MEC 应用的规则和需求，并负责 MEC 应用部署、生命周期管理和迁移。

为支撑 MEC 业务统一运营和管理需求，MEC 业务管理平台需与业务支撑系统（business support system，BSS）、云网运营系统、云管平台对接。与 BSS 对接，实现订单信息及计费话单传递。云网运营系统承接 MEC 产品套餐开通需求，将其分解为相关专业的编排需求，包括 5G 核心网（5G core，5GC）、承载及云资源。对接云管平台实现对边缘资源的统一纳管。

1.2　MEC 业务管理平台省级汇聚层

MEC 业务管理平台省级汇聚层是 MEC 业务管理平台（集团级）在省级的延伸，负责完成本省内边缘节点的汇聚管理，包括 MEC 平台管理器（MEC platform management，MEPM）和 5GC proxy。MEPM 负责执行 MEC 平台（MEC platform，MEP）监控、配置、性能等管理，承接 MEO 编排下发的边缘应用生命周期管理和配置需求。MEC 系统通过 5GC proxy 与 5GC 对接，实现对 5GC 网络原子能力的调用，提供网络协同和能力开放。

1.3　MEC 边缘节点

MEC 边缘节点是 MEC 系统的业务节点，包括虚拟化层、MEC 平台和 MEC 应用[8]。其中，虚拟化层为 MEC 系统提供平台、应用、服务的部署环境。MEC 平台作为边缘节点的核心组件，支持网络能力和业务能力的统一开放，接受 MEC 业务管理平台的管理调度，执行和实现相应能力调用和管理策略。MEC 应用通过与 MEC 平台交互提供或使用边缘服务[9]。

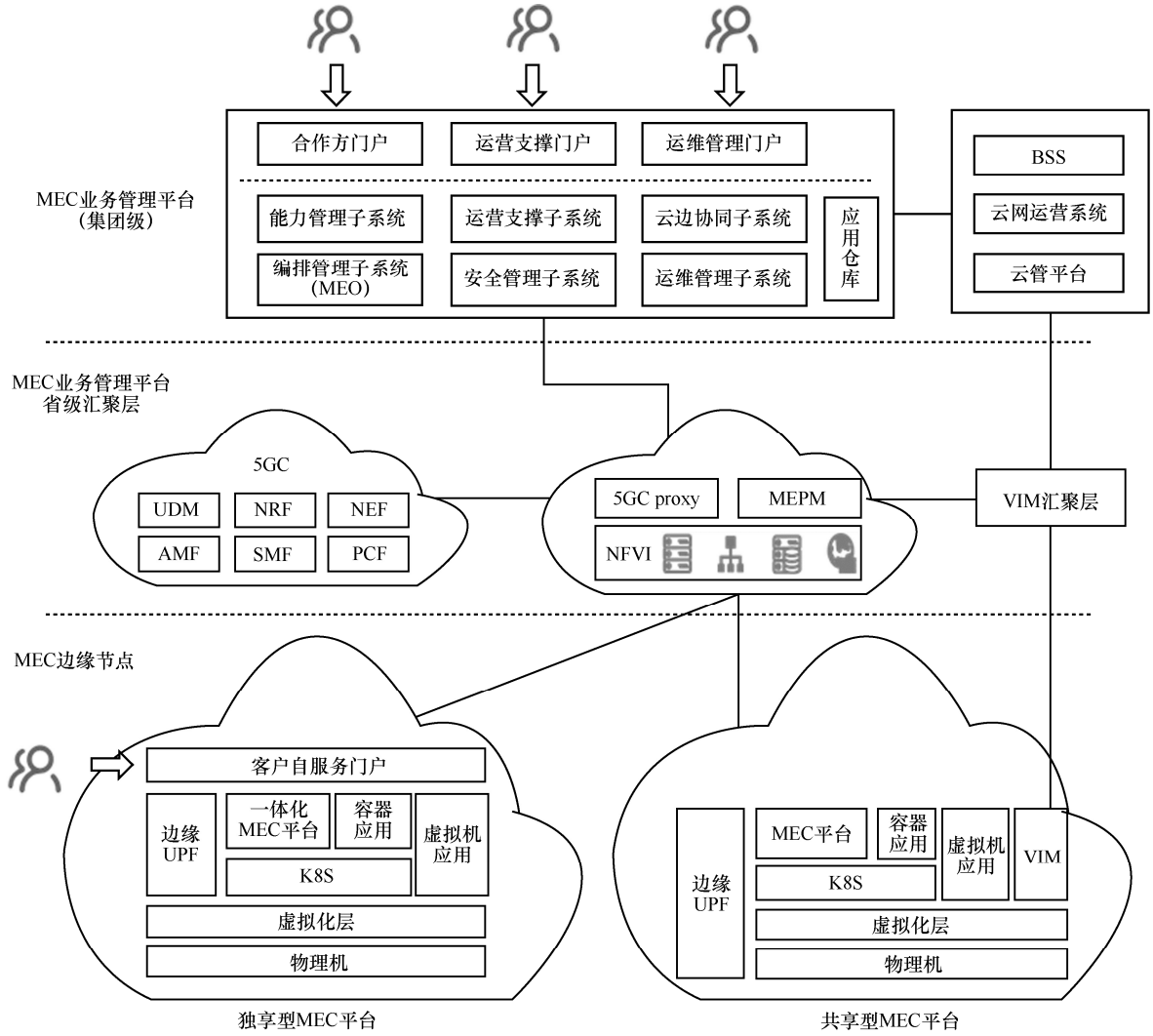


图 1　5G MEC 系统架构

按照部署场景、交付形式不同，MEC 平台分为共享型 MEC 平台和独享型 MEC 平台两类。共享型 MEC 平台通过 MEC 业务管理平台实现集约管控，在同一资源池为不同用户分配逻辑隔离的计算和网络资源；独享型 MEC 平台为客户专享，提供自主管理的自服务门户，满足客户的本地化部署、数据不出场、高安全、私密性等需求，实现快速、灵活的边缘节点集成交付。

2　5G MEC 系统安全风险分析

基于 5G MEC 系统架构，本文对其潜在的安全风险进行分析，为安全能力部署方案提供依据。本文重点关注边缘计算系统安全风险分析及部署方案，5G NR、承载网、5G 核心网等安全问题不作重点讨论。

2.1　MEC 业务管理平台（集团级）安全风险

MEC 业务管理平台（集团级）作为 MEC 系统的核心及“大脑”，其潜在安全风险如下。

（1）门户风险：MEC 业务管理平台为用户、运营支撑人员、运维人员提供可公网访问的门户，存在恶意流量攻击、恶意入侵、网站高危漏洞被利用等风险。

（2）编排管理风险：MEO 编排系统存在权限滥用、非授权使用、管理失效、鉴权接口漏洞等安全风险，攻击者可以非法控制 MEC 系统和资源[10]。编排管理网络存在消息不可达、命令被劫持及恶意篡改等风险。

2.2 MEC 业务管理平台省级汇聚层安全风险

（1）5GC 风险：省级汇聚层与 5GC 相关网元互通，有可能将安全风险引入 5GC，从而影响 5G 网络的正常运行，需要进行重点安全保障。

（2）编排管理风险：MEPM 存在与 MEO 类似的编排管理安全风险。

2.3 MEC 边缘节点安全风险

（1）物理安全风险

MEC 边缘节点大多部署在无人值守的边缘机房，存在恶意人员入侵、设备断电、网络中断等风险。

（2）虚拟化基础设施安全风险

虚拟机间恶意攻击风险：由于同一服务器上的虚拟机共享计算、存储等资源，虚拟机之间存在相互挤占资源或恶意攻击的风险。

容器间渗透风险：由于容器应用共用宿主机内核资源，若进程、文件系统等隔离不当，存在容器间相互渗透的安全风险。

（3）MEC 平台安全风险

平台权限漏洞：若 MEC 平台存在权限设置或安全漏洞，MEC 平台可能被攻击者非授权访问，从而影响平台正常运行。

数据安全风险：存储在边缘节点的数据存在被损坏、篡改、泄露的安全风险。

（4）MEC 应用安全风险

资源挤占风险：MEC 应用共享边缘节点资源，若某一应用占用的计算、存储等资源过高，就可能会对其他应用的正常运行造成影响。

安全漏洞风险：若 MEC 应用存在中高危安全漏洞，该应用上线后，可能发生由于自身漏洞被攻破，向其他应用或 MEC 平台进行恶意攻击的安全风险，从而影响整个边缘节点的安全性。

（5）MEC 能力开放安全风险

能力开放风险：能力开放作为 MEC 的核心能力，可以将业务能力和网络能力通过开放应用程序接口（application programming interface，API）的方式，开放给用户使用，提升业务体验。如果能力开放的权限控制不当，或者认证鉴权手段存在漏洞，可能存在能力被滥用或恶意使用的风险。

（6）网络安全风险

边缘用户面功能（user plane function，UPF）安全风险：部署在边缘机房或客户机房的 UPF 需要与 5GC 连接实现信令面控制，一旦 UPF 被非授权接入，将对 5GC 造成威胁。

网络边界安全风险：MEC 在企业内网及互联网边界存在恶意访问、分布式拒绝服务（distributed denial of service，DDoS）攻击等风险。

3 5G MEC 安全能力部署方案

基于 5G MEC 系统架构以及安全风险分析，本节提出 5G MEC 安全能力部署架构和方案，并给出部署案例。

3.1 总体原则

5G 边缘计算安全能力部署需要统筹考虑相关法律法规及客户实际需求，以国家网络安全法律法规和监管要求为指导，以满足企业安全运营和客户安全的需求为落脚点，并按照上级单位监管、等保 2.0、定级备案等安全要求，进行同步规划、建设和使用。同时，应根据集约化原则，在满足安全需求的情况下，通过调用集中安全能力池或边缘安全能力池的安全能力，实现 5G 边缘计算安全防护。

5G 边缘计算系统安全防护需要将安全能力部署与内部安全加固相结合，通过安全域划分、隔离、基线配置规范、漏洞安全管控、权限管控等方式，提升 MEC 平台自身安全防护能力；通过镜像安全管控、应用安全隔离、细粒度的授权控

制、应用生命周期管理、容器安全监测等技术手段，降低第三方应用引入的安全风险；此外，辅以相应的安全维护管理手段，构建全方位的边缘计算安全防护体系。

3.2　部署方案

5G MEC 系统安全能力多级部署架构与边缘计算系统多级架构相匹配，包括安全管理平台、集中安全能力池、边缘安全能力池 3 级架构，如图 2 所示。

（1）MEC 业务管理平台（集团级）安全

门户安全防护：建议优先复用所在资源池已具备能力，进行网站应用防护系统（Web application firewall，WAF）、DDoS 防护、入侵防御系统（intrusion prevention system，IPS）、防病毒、防火墙的安全配置。

编排管理安全加固：MEC 业务管理平台（集团级）与 MEPM 间实施双向认证和白名单接入，对 API 调用进行认证授权、安全审计；通过专用虚拟专用网络（virtual private network，VPN）通道传输数据，并进行机密性和完整性保护，防止编排管理系统或网络被入侵。

应用镜像安全管理：MEC 系统提供安全加固后的公共虚拟机镜像供用户使用，用户也可自行上传私有镜像。在应用仓库部署镜像漏洞扫描系统，只允许通过漏洞扫描的应用进行部署，避免带病入网；镜像传输通道加密传输，并开启完整性校验。为保证边缘应用部署流程的完整性，建议镜像漏洞扫描系统与 MEC 业务管理平台集成部署。

自身安全加固：复用集中安全能力池已有能力进行安全加固，在 MEC 业务管理平台部署代理客户端，集中安全能力池部署管理端。对接数据库审计系统，提供数据库安全保护和审计能力；对接敏感数据控制系统，提供敏感数据脱敏、控制能力；对接主机入侵防护系统，提供主机微隔离等综合能力；对接漏洞扫描系统，定期进行平

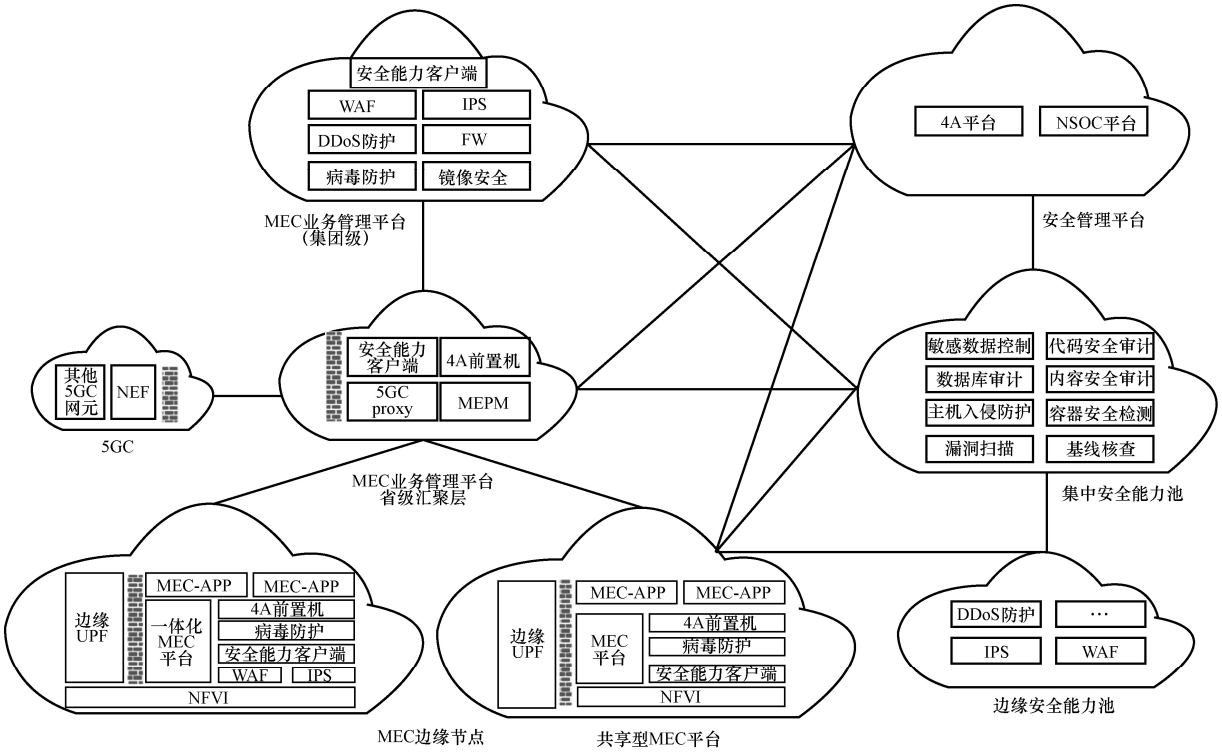


图 2　5G MEC 系统安全能力多级部署架构

台漏洞扫描和加固工作；对接基线核查系统，提供系统基线配置标准化核查能力。

（2）MEC 业务管理平台省级汇聚层安全

5GC 安全隔离管控：5GC proxy 与 5GC 通过专用 VPN 通道对接，对传输数据进行机密性和完整性保护；实施双向认证，并启用白名单，不允许白名单以外的 IP 地址或用户接入；5GC proxy 与 5GC 设置防火墙进行安全隔离；只允许 5GC proxy 访问网络开放功能（network exposure function，NEF）或只访问特定网元（不具备 NEF 时）；在进行网络能力调用时，不允许直接传递 5GC 参数信息，或对其进行机密性保护。

编排管理安全加固：同 MEC 业务管理平台（集团级）加固方案。

自身安全加固：同 MEC 业务管理平台（集团级）安全加固方案，复用集中安全能力池已有能力进行安全加固，如数据库审计、敏感数据控制、主机入侵防护、漏洞扫描、基线核查等安全能力。

（3）MEC 边缘节点安全

MEC 边缘节点建议按不低于其所承载应用的等保级别进行定级备案和安全能力匹配。

① 物理安全

机房环境安全：由于 MEC 边缘节点部署在边缘机房或客户机房，应在物理访问控制、防盗窃、防破坏、防雷击、防火、防水防潮、温湿度控制和电力供应等方面对所在机房提出相关要求，并通过加锁、远程监控、人员管理及定期巡检等方式保证物理环境安全。

物理设备安全：应要求边缘设备具备物理安全增强功能，包括默认关闭本地维护端口、启用密码保护、对服务器 I/O 访问控制、具备远端集中监控告警功能。

② 虚拟化安全

三平面安全隔离：划分管理、存储、业务三平面，并在物理服务器网卡上为各平面分配独立物理网口，采用交叉互联方式，保证三平面之间彼此隔离，提高可靠性。

虚拟机安全隔离：配置宿主机资源访问控制权限，对 Host OS、虚拟化软件、Guest OS 进行安全加固；设置虚拟机操作权限及资源使用限制，对同一物理机上不同虚拟机之间的资源进行隔离，并对资源使用情况进行监控[11]；同时，部署主机入侵防护系统，提供入侵检测和主动防护能力。

容器安全检测：部署容器安全检测系统，对容器运行进行安全检测，及时发现容器运行的异常行为。

③ MEC 平台安全

加强对 MEC 平台自身安全、数据防护和接口管控，规范 MEC 节点配置，提升 MEC 平台安全性，具体措施如下。

平台安全加固：对接集中安全能力池漏洞扫描系统，对 MEC 平台进行安全扫描与评估，修复中高危漏洞，保障平台安全；对接基线核查系统，对平台的运行环境参数、自身配置、开发端口等进行安全基线管理和定期核查，并及时修复整改；在边缘节点内部部署防病毒软件，进行病毒防护。

数据安全防护：通过对接数据库审计系统、敏感数据控制系统、内容安全审计平台进行数据库保护、敏感数据脱敏、内容安全监测等，保护数据安全。

④ MEC 应用安全

MEC 应用安全需要通过应用隔离、资源监控、镜像安全等手段，统一融合在 MEC 应用生命周期安全管理中。

应用隔离：MEC 应用之间可采用虚拟扩展局域网（virtual extensible local area network，VxLAN）、虚拟局域网（virtual local area network，VLAN）或虚拟私有云（virtual private cloud，VPC）等方式实现逻辑隔离；MEC 应用之间的访问启用授权机制；MEC 虚拟化基础设施对 MEC 应用使

用的 CPU、内存、存储等资源进行隔离。

资源监控：对 MEC 应用的资源情况进行实时监控，并对资源消耗配置限额。

镜像安全：对于共享型 MEC 平台应用，MEC 业务管理平台作为应用部署的唯一入口，可复用应用仓库镜像扫描能力进行处理；对于独享型 MEC 平台应用，可通过部署镜像扫描插件或复用集中安全能力池的漏洞扫描能力，对应用镜像进行漏洞扫描和加固。

⑤ MEC 能力开放安全

认证授权管控：规范 API 的安全调用，对 MEC 应用发起的 API 调用采用证书等方式进行认证与鉴权，防止 API 非法调用；通过访问列表 ACL 限制 MEC 应用对 API 的访问；开启 API 白名单，同时 API 调用请求应进行合法性验证。

⑥ 网络安全

边缘 UPF 安全：边缘 UPF 通过 5G 承载网专用 VPN 与 5GC 连接，进行双向认证与鉴权，对非授权设备通信进行限制；双方配置互访白名单，仅允许白名单内的设备与 5GC 互访。

网络边界安全：通过复用边缘节点所在机房或边缘安全能力池的防火墙、IPS、DDoS 防护等能力，实现 MEC 平台与边缘 UPF、企业网和互联网边界的安全隔离和访问控制，对 MEC 边缘节点进行数据保护、高级威胁防御、僵尸网络防护等。原则上不建议 MEC 边缘节点直接开放互联网出口。

⑦ 运维管理安全

边缘计算系统及各节点通过对接集团/省级安全管理平台，实现统一安全维护管理。

边缘计算系统各节点内部部署 4A 前置机，纳入集中 4A 平台，实现运维管理人员的集中账号管理、认证授权、访问控制和行为操作审计，遵循最小授权访问原则，建立权限分离机制[12]。

边缘计算系统通过对接集中 NSOC 平台，对边缘计算系统安全基础信息、配置变更等信息收集管理，对边缘资产进行存活识别和管理，对各类设备日志信息收集分析，实现配置安全管理、资产安全管理、日志安全审计等安全管理功能。

根据以上分析和安全部署方案，除平台、虚拟化等自身安全加固外，对 5G 边缘计算系统需要部署的安全能力进行了梳理，见表 1。

3.3　部署案例

为了更好地支持 5G 业务应用的本地化部署，运营商某省公司建设共享型 MEC 边缘节点，并与省级汇聚层、UPF、5GC、安全等系统进行对接，某共享型 MEC 边缘节点组网架构如图 3 所示。

根据实际情况和需求，在资源池出口核心交换机部署防火墙、IPS、WAF 等流量型安全能力，实现安全隔离、高级威胁防御及 Web 应用保护，防止信息泄露和外部入侵。MEC 节点内部划分 VLAN，建立 VLAN 配置访问控制列表，细化安全控制粒度。通过 STN 承载网 VPN 加强访问通道安全，同时也防止外部终端直接对系统进行攻击。根据项目实际情况，资源池同局址部署数据库审计服务器，进行数据库安全防护。

非流量型安全能力方面，MEC 平台中云化部署容器安全检测系统、漏洞扫描器、防病毒软件、基线扫描代理软件。具体部署方式为在服务器、虚拟机中安装相关 Agent 软件，进行中间件、漏洞、基线等信息采集；在资源池内部署前置机进行信息采集汇总，通过 Nginx 反向代理服务与集中安全平台对接。

运维管理方面，通过 DCN 与省内集中 NSOC 平台和 4A 平台对接，实现运维安全管理。

本地化部署建设完成后，由外部第三方安全公司对该边缘节点进行安全测评，以识别 5G 边缘节点系统可能存在的安全风险，为安全加固以及安全防护等保障工作提供依据，保障 5G 边缘节点的安全稳定运行。本次测评从 MEC 边缘节点物理安全、计算环境安全、边界安全、通信网络安全、运营管理等方面进行评估，并评估边缘节点系统安全防护策略的全面性及执行情况等，共涉及测评项

表 1　5G MEC 系统安全能力部署对应

分类	安全能力	覆盖范围	部署方案	功能简述	需求等级
虚拟化安全	容器安全检测	MEC 业务管理平台、省级汇聚层及边缘节点	分级部署，MEC 系统各节点内部部署客户端，集中安全能力池部署管理端	容器运行时对其进行安全检测	必选
	主机入侵防护系统	MEC 业务管理平台、省级汇聚层及边缘节点	分级部署，MEC 系统各节点内部部署客户端，集中安全能力池部署管理端	提供攻击入侵检测和主动防护能力	可选
	代码安全审计	MEC 业务管理平台、省级汇聚层及边缘节点	集中安全能力池部署	对平台和应用代码进行安全审计，发现潜在风险	可选
平台安全	基线核查系统	MEC 业务管理平台、省级汇聚层及边缘节点	分级部署，MEC 系统各节点内部部署客户端，集中安全能力池部署管理端	提供设备配置标准化核查能力	必选
	漏洞扫描设备	MEC 业务管理平台、省级汇聚层及边缘节点	分级部署，MEC 系统各节点内部部署客户端，集中安全能力池部署管理端	提供设备或者虚拟化设备的漏洞扫描和加固指导能力	必选
	防病毒系统	MEC 业务管理平台、边缘节点	MEC 业务管理平台及 MEC 边缘节点内部部署	提供主机安全保护和防病毒能力	必选
网络安全	防火墙	MEC 业务管理平台、省级汇聚层及边缘节点	MEC 系统各节点所在资源池内部部署	实现 MEC 系统的安全隔离、MEC 边缘节点与 UPF、企业网、互联网等网络边界的安全隔离	必选
	IPS	MEC 业务管理平台、边缘节点	MEC 业务管理平台资源池、边缘安全能力池或 MEC 边缘节点内部部署	对 MEC 业务管理平台门户及边缘节点进行数据保护、高级威胁防御、僵尸网络防护等	必选
	DDoS 防护	MEC 业务管理平台	MEC 业务管理平台资源池	保护 MEC 业务管理平台门户免遭 DDoS 攻击	可选
应用安全	镜像扫描	MEC 业务管理平台、独享型边缘节点	MEC 业务管理平台集成部署，独享型 MEC 边缘节点内部部署	对应用镜像进行漏洞安全检测	必选
	WAF	MEC 业务管理平台、边缘节点	MEC 业务管理平台资源池、边缘安全能力池或 MEC 边缘节点内部部署	保护 MEC 业务管理平台门户和 Web 应用免遭当前和未来的安全威胁攻击	业务管理平台必选，边缘节点可选
数据安全	数据库审计系统	MEC 业务管理平台、省级汇聚层及边缘节点	分级部署，MEC 系统各节点内部部署客户端，集中安全能力池部署管理端	提供数据库安全保护和操作审计能力	可选
	敏感数据控制系统	MEC 业务管理平台、省级汇聚层及边缘节点	分级部署，MEC 系统各节点内部部署客户端，集中安全能力池部署管理端	提供敏感数据脱敏、控制数据流转	可选
	内容安全审计	MEC 业务管理平台、省级汇聚层及边缘节点	集中安全能力池部署	对内容进行安全监测，及时发现并阻断数据泄露	可选
管理安全	4A	MEC 业务管理平台、省级汇聚层及边缘节点	分级部署，MEC 系统各节点内部部署前置机，复用省/集团已有 4A 平台	对操作人员进行统一认证授权管理和操作审计	必选
	NSOC 平台	MEC 业务管理平台、省级汇聚层及边缘节点	分级部署，MEC 系统各节点内部部署客户端，复用省/集团已有 4A 平台	配置安全管理、资产安全管理、日志安全审计	必选

30 项，其中符合 30 项，不符合 0 项，安全测评结果显示安全能力建设满足相关建设指引要求。

4　问题及挑战

综上所述，基于集约化原则和多级部署架构的5G边缘计算安全能力部署方案可以实现安全能力部署与边缘计算系统的融合，解决边缘计算场景中的安全防护问题。然而，上述安全能力部署架构和方案也有很多问题与挑战亟待解决。

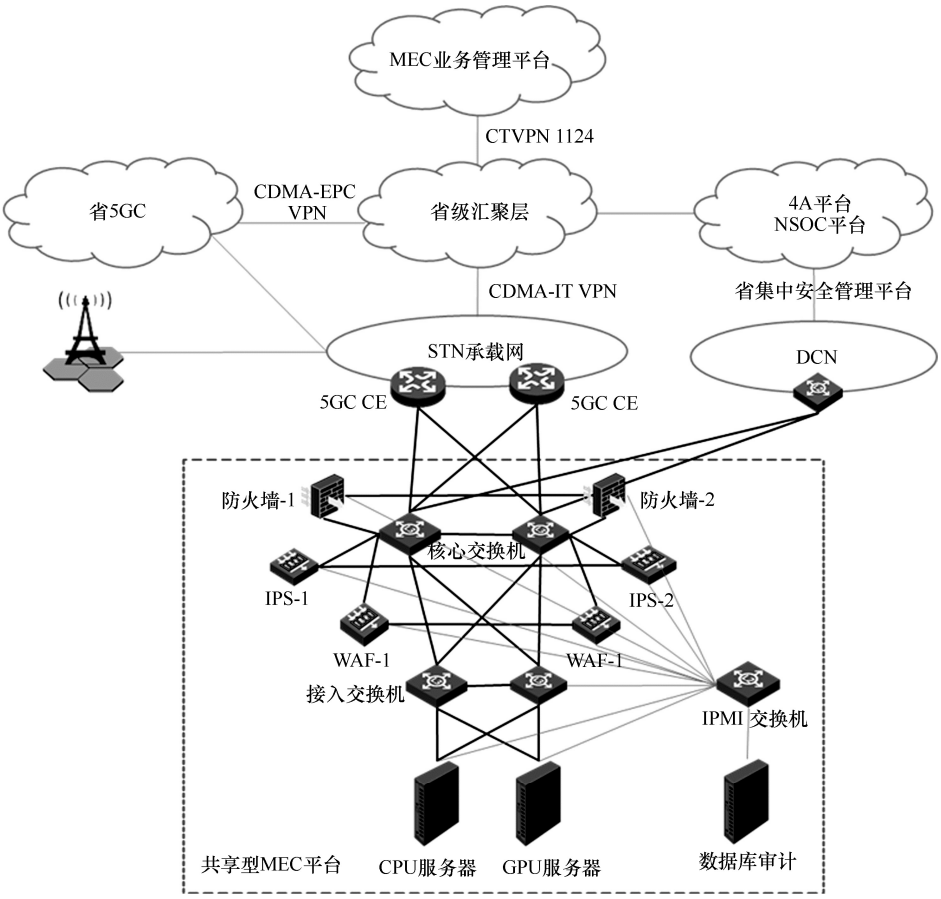


图 3　某共享型 MEC 边缘节点组网架构

（1）安全管理系统繁多，对接流程复杂，缺少集约管理平台

根据集约化建设原则，5G 边缘计算系统通过对接集团、各省级安全管理平台（如 4A 平台、NSOC 平台、资源管理平台等）实现安全维护管理功能，降低建设投资成本。由于各个安全管理平台分散独立，5G 边缘计算系统需要分别与各省安全管理系统进行对接，并分别打通平台、网络、管理流程等，对接流程复杂，缺少集约管理平台进行统一管理。

（2）安全能力池集中部署模式对智能化引流技术提出较高要求

从集约化角度出发，在边缘或集中安全能力池进行安全能力部署有利于安全能力统一管理、节省投资和维护成本，但 WAF、IPS 等安全能力需要对业务流量进行引流和清洗，对智能引流、智能路由技术等要求较高，需要云、网、业紧密协同，实现边缘计算业务与安全防护。

（3）不同业务的安全防护能力需求各不相同，需要进行灵活编排

不同租户、不同业务的安全能力需求差异较大。例如，某些业务安全防护要求较低，仅需要某几项安全能力，而某些业务安全防护要求较高，希望可以专享某些安全能力，而不与其他租户共享。因此，需要对安全业务链流量进行灵活编排，将安全管理编排服务与 MEC 业务相融合，实现边缘计算应用、边缘安全能力、安全业务链的统一编排管理，实现不同租户和不同业务所需安全能力的定制化加载和灵活管控。

5　结束语

5G 边缘计算可将网络能力和计算能力延伸

到网络边缘和用户边缘，并与 5G 专网相结合，在垂直行业客户的数字化转型升级中发挥重要作用。本文对 5G 边缘计算安全风险进行详细探讨，并提出相应的安全能力部署架构和方案，并对存在的问题及挑战进行了思考，建议未来可从智能化引流、安全能力编排等方面展开深入研究与实践，期望本文可以为 5G 边缘计算的安全防护及建设部署提供一定的借鉴。

参考文献：

[1] 刘云毅, 张建敏, 杨峰义. 基于 MEC 的移动网络 CDN 增强及部署场景建议[J]. 电信科学, 2019, 35(S2): 36-43.
LIU Y Y, ZHANG J M, YANG F Y. MEC-based mobile network CDN enhancement and deployment scenario recommendations[J]. Telecommunications Science, 2019, 35(S2): 36-43.

[2] 张建敏, 杨峰义, 武洲云, 等. 多接入边缘计算（MEC）及关键技术[M]. 北京: 人民邮电出版社, 2019.
ZHANG J M, YANG F Y, WU Z Y, et al. Multi-access edge computing (MEC) and key technologies[M]. Beijing: Posts and Telecom Press, 2019.

[3] ETSI white paper No.46. MEC security: status of standards support and future evolutions[R]. 2021.

[4] ALI B, GREGORY M A, LI S. Multi-access edge computing architecture, data security and privacy: a review[J]. IEEE Access, 2021(9): 18706-18721.

[5] RANAWEERA P, JURCUT A, LIYANAGE M. MEC-enabled 5G use cases: a survey on security vulnerabilities and countermeasures[J]. ACM Computing Surveys, 2022, 54(9): 1-37.

[6] 杨红梅, 王亚楠. 5G 边缘计算安全关键问题及标准研究[J]. 信息安全研究, 2021, 7(5): 390-395.
YANG H M, WANG Y N. Study on security key issues and standards of 5G MEC[J]. Journal of Information Security Research, 2021, 7(5): 390-395.

[7] 工业互联网产业联盟. 5G 边缘计算安全白皮书[R]. 2020.
Alliance of Industrial Internet. 5G edge computing security white paper[R]. 2020.

[8] 张建敏, 谢伟良, 杨峰义, 等. 移动边缘计算技术及其本地分流方案[J]. 电信科学, 2016, 32(7): 132-139.
ZHANG J M, XIE W L, YANG F Y, et al. Mobile edge computing and application in traffic offloading[J]. Telecommunications Science, 2016, 32(7): 132-139.

[9] 张蕾, 刘云毅, 张建敏, 等. 基于 MEC 的能力开放及安全策略研究[J]. 电子技术应用, 2020, 46(6): 1-5.
ZHANG L, LIU Y Y, ZHANG J M, et al. Research on capability exposure and security strategy based on MEC[J]. Application of Electronic Technique, 2020, 46(6): 1-5.

[10] 何明, 沈军, 吴国威, 等. MEC 安全探讨[J]. 移动通信, 2019, 43(10): 2-6.
HE M, SHEN J, WU G W, et al. Discussions on the security of MEC[J]. Mobile Communications, 2019, 43(10): 2-6.

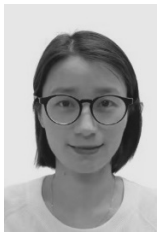
[11] IMT-2020(5G)推进组, 中国信息通信研究院. 5G 安全知识库[R]. 2021.
IMT-2020(5G) Promotion Group, CAICT. 5G security knowledge base[R]. 2021.

[12] 何明, 沈军, 吴国威. MEC 安全建设策略[J]. 移动通信, 2021, 45(3): 26-29, 34.
HE M, SHEN J, WU G W. Strategy on the security construction of MEC[J]. Mobile Communications, 2021, 45(3): 26-29, 34.

[作者简介]

刘云毅（1993− ），男，中国电信股份有限公司研究院中级工程师，主要研究方向为移动通信与边缘计算。

张建敏（1983− ），男，中国电信股份有限公司研究院教授级高级工程师，主要研究方向为移动通信技术与边缘计算等。



冯晓丽（1983− ），女，中国电信集团有限公司高级项目经理、5G MEC 产品运营经理，主要研究方向为 5G MEC。

张丽伟（1982− ），女，中国电信集团有限公司云网运营部政企智能服务运营中心室主任，主要研究方向为 5G 移动通信、5G 定制专网等。