5G MEC的网络安全研究

Research on Network Security of 5G MEC

王　凯，汪剑桥，卜　寅（中国联通江苏分公司，江苏 南京 210019）
Wang Kai，Wang Jianqiao，Bu Yin（China Unicom Jiangsu Branch，Nanjing 210019，China）

摘　要：
在5G MEC各类应用场景中，平台组成的复杂度和网络的暴露面均有所增大，网络安全防护是5G MEC需要重点考虑的能力之一。针对5G MEC系统各个功能模块的网络安全防护、端到端整体网络安全防护以及统一安全管控等多个维度进行了探究，并面向MEC 5G核心网域、云平台域、内联外联网络、安全运营等方向提出了相应的网络安全防护方案及整体网络安全防护架构。

关键词：
5G；MEC；UPF；边缘资源池；安全组件；安全运营平台
doi：10.12045/j.issn.1007-3043.2023.08.018
文章编号：1007-3043（2023）08-0081-04
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
In various application scenarios of 5G MEC，the complexity of platform composition and the exposure surface of network are increased，and network security protection is one of the key capabilities that need to be considered by 5G MEC. It explores multiple dimensions such as network security protection，end-to-end overall network security protection and unified security control of each functional module of 5G MEC system，and proposes corresponding network security protection schemes and overall network security protection architecture for MEC 5G core domain，cloud platform domain，internal and external network，security operation and other directions.

Keywords：
5G；MEC；UPF；Edge resource pool；Security component；Security operation platform

引用格式：王凯，汪剑桥，卜寅. 5G MEC的网络安全研究[J]. 邮电设计技术，2023（8）：81-84.

1 MEC网络安全防护面临的挑战和目标

5G MEC是5G面向2B垂直行业业务承载和应用的重要技术形态。5G MEC采用了5G转控分离能力。5G核心网UPF可下沉到所需位置作为MEC的一部分，大大增强了5G在面向2B业务承载时的灵活性和创新能力。5G MEC与云计算、人工智能、物联网、大数据、工业互联网、区块链、元宇宙等技术融合，推动5G 2B业务百花齐放。

在5G MEC各类应用场景中，网络边界多，暴露面大，极有可能引发网络安全事件。所以，5G MEC网络安全防护是5G MEC在部署时必须要综合考虑的问题之一。

5G MEC的安全防护目标须从设计、部署、运营端到端考虑，满足通信网络、云计算和业务应用等安全防护的要求，满足安全即服务的统一运营体系理念。

2 MEC网络安全研究

构建5G MEC网络安全防护体系需要深入理解5G MEC的构成、不同功能域的安全要求、功能域之间的安全关系、网络安全边界等。5G MEC从功能模块上可分为5GC部分（UPF）、云资源池部分（虚机/容器

收稿日期：2023-07-04

承载基础)、MEP部分(PaaS生产业务承载平台)、业务应用、对内对外网络、统一管理编排运营平台等。对于MEC不同功能模块的网络安全要求,首先需要研究清楚各自部分的网络安全要求,再端到端综合考虑衔接、边界、配合、隔离、防御等方面的网络安全要求。

2.1 MEC各个功能域的网络安全研究

2.1.1 UPF安全防护研究

UPF是5G MEC的5G本地分流模块,整个5G MEC的安全与UPF的安全联系非常紧密。UPF同属于5GC和MEC,起着承上启下的作用。从安全边界角度看,UPF域主要有2个网络边界,即N4和N6。从部署区域角度看,UPF可部署在可信的运营商边缘机房,也可部署在不可信的第三方机房。UPF的安全防护需要根据特定的场景差异化对待。

当UPF部署在可信边缘机房时,区别于部署在5GC核心机房,UPF网元的物理安全保护机制仍然是需要的。

当UPF部署在不可信机房时,UPF物理服务器需开启可信功能,保证UPF功能以及所在的主机处于可信状态。另外,可通过特定的技术确保网络安全,如N4流量采用IPSec等技术建立安全通道、开启防地址欺骗策略防止UPF上、下行流量中的地址欺骗、在物理端口执行ACL过滤策略、通过URL黑名单方式对WAP推入的恶意消息拦截过滤、通过GRE等隧道对不同业务类别流量进行控制和隔离、在UPF公网侧部署抗DDOS设备等。

2.1.2 MEC平台安全

MEC平台本身是一个云平台,其安全防护需按照云计算安全防护要求来考虑。安全防护的核心可参照立体防御体系架构,从网络边界、身份鉴别、数据安全、应用安全、行为监测等多个维度进行。另外,MEC平台安全防护体系需要面向XaaS服务、融合虚拟化/容器化、统一标准、资源整合、集中管控运营等,为MEC云服务交付、云资源访问、云平台维管等提供立体化安全能力。

2.1.3 MEC应用安全

MEC应用可以是运营商自有的边缘应用或者是第三方的边缘应用。MEC节点无论是部署在运营商环境内还是用户现场环境内,MEC应用均需进行安全评估,包括身份验证、安全合规检查和审核、基线扫描等,保证只有合法、合规的APP才能上线。

2.1.4 MEC编排和管理安全

MEC编排和管理涉及到MEC全生命周期的管理和操作,需要考虑安全防护,如管理员的鉴权、应用镜像安全等。另外,MEC的编排和管理模块在与其他功能模块通信时,也需对对端的身份进行认证,并对传输的数据进行加密和完整性保护,对涉及到的API接口的调用也需进行认证和授权。

2.2 5G MEC组网安全研究

5G MEC系统组网比较复杂,涉及到多个网络,包括5G承载网、用户网络(私网)、公网、互联专网(如VPN)等,同时,5G MEC内部各个不同域之间还有多个网络暴露面。组网安全需结合5G MEC具体的部署场景,本着对5G大网、信任域及业务保护等原则进行。对边缘UPF与5G核心网之间的N4接口进行安全隔离防护;对5G MEC信任域与不信任网络(如公网、用户私网)之间的网络暴露面(如N6)进行安全隔离防护;在运营商可信域与不可信域之间进行安全隔离防护;有互联网出口的,需在互联网出口进行安全隔离防护。具体的安全规划需按照5G MEC业务承载及部署场景差异化区分对待。

2.2.1 本地分流应用场景下的组网安全

该场景下UPF只为边缘应用/企业私网引流,其组网安全主要是要求UPF与边缘应用/企业私网间(N6)部署相应的安全防护能力,防止2个域之间的安全事件。该场景下如果MEC部署在不可信机房,则还需要对N4进行安全隔离,确保5G核心网的安全。

2.2.2 应用托管场景下的组网安全

该场景下MEC托管有第三方边缘应用或者自有边缘应用等,其组网安全要求如下。

a)较大的边缘机房(如端局),需要按照管理、业务和存储三平面物理隔离模式部署;较小的机房(如接入机房),至少支持管理和业务/存储平面的物理隔离的双平面部署模式。

b)划分不同的安全域,信任域与不信任域之间进行安全隔离。第三方应用可与UPF位于不同的物理服务器,之间使用防火墙进行隔离。不同应用之间通过逻辑网络隔离。

c)有互联网访问的场景,互联网出口边界按需部署抗DDoS等相应的安全能力。对于复杂的5G MEC,可通过部署内层防火墙进行双层异构安全隔离,严格区分AZ和DMZ等区域。从管理及经济性出发,5G MEC的互联网出口可集中部署并集中进行网络安全防护。

d）UPF通过设置专有DNN等隔离公网、私网流量。

e）UPF和5G核心网之间（即N4）需进行网络安全隔离，确保5G核心网的安全。

2.2.3 现场部署模式的5G MEC组网安全

该场景下，5G MEC部署在不可信区域（如用户机房），组网安全应考虑以下3点。

a）管理、业务、存储三平面的物理隔离，保证各个平面之间的独立性和安全性。

b）严格安全域的划分。该场景下第三方应用、私有平台等为不信任域，运营商UPF、MEP平台属于准信任域，二者之间通过部署内部防火墙进行安全隔离。同时，第三方应用和UPF、边缘计算平台需要部署在不同的服务器上。

c）UPF和5GC核心网控制面网元之间（N4）需使用防火墙进行安全隔离。从管理及经济性出发，可归集本地5G MEC节点的N4接口，集中部署N4接口隔离防火墙，统一进行安全隔离防护。

2.3 MEC的网络安全总体架构研究

2.3.1 MEC安全防护总体架构功能

综合上述对5G MEC各个功能域网络安全防护的研究，针对5G MEC的各个功能模块的安全差异性、连通性、依赖度等特点，结合MEC组网安全特点，在构建5G MEC总体安全架构时既要分层、分域、多维度、多梯次各自考虑，又要结合各个独立部分端到端综合考虑。

a）功能域需划分归属AZ、不信任域或DMZ，不同域之间需进行安全隔离。

b）N4需部署防火墙进行安全隔离，确保5G核心网的安全。

c）部署内部防火墙，隔离应用/用户私网对UPF的网络安全影响，隔离AZ与DMZ。

d）部署外部防火墙，阻止来自互联网的攻击、渗透等。

e）对标云资源池安全防护要求，部署相关安全组件，对边缘云资源池进行安全防护。

f）部署虚机安全/容器安全等防护能力，针对边缘云业务应用进行安全防护。

g）安全即服务自动化安全运营能力。

2.3.2 MEC安全防护总体架构组成

5G MEC安全防护总体架构如图1所示，包括安全模块及安全组件、集中式安全运营平台、安全运营使能模块。

2.3.2.1 安全模块及安全组件

安全模块和安全组件是实现各种安全防护功能的基础能力，可按需选择包括防火墙、抗DDoS、态势感

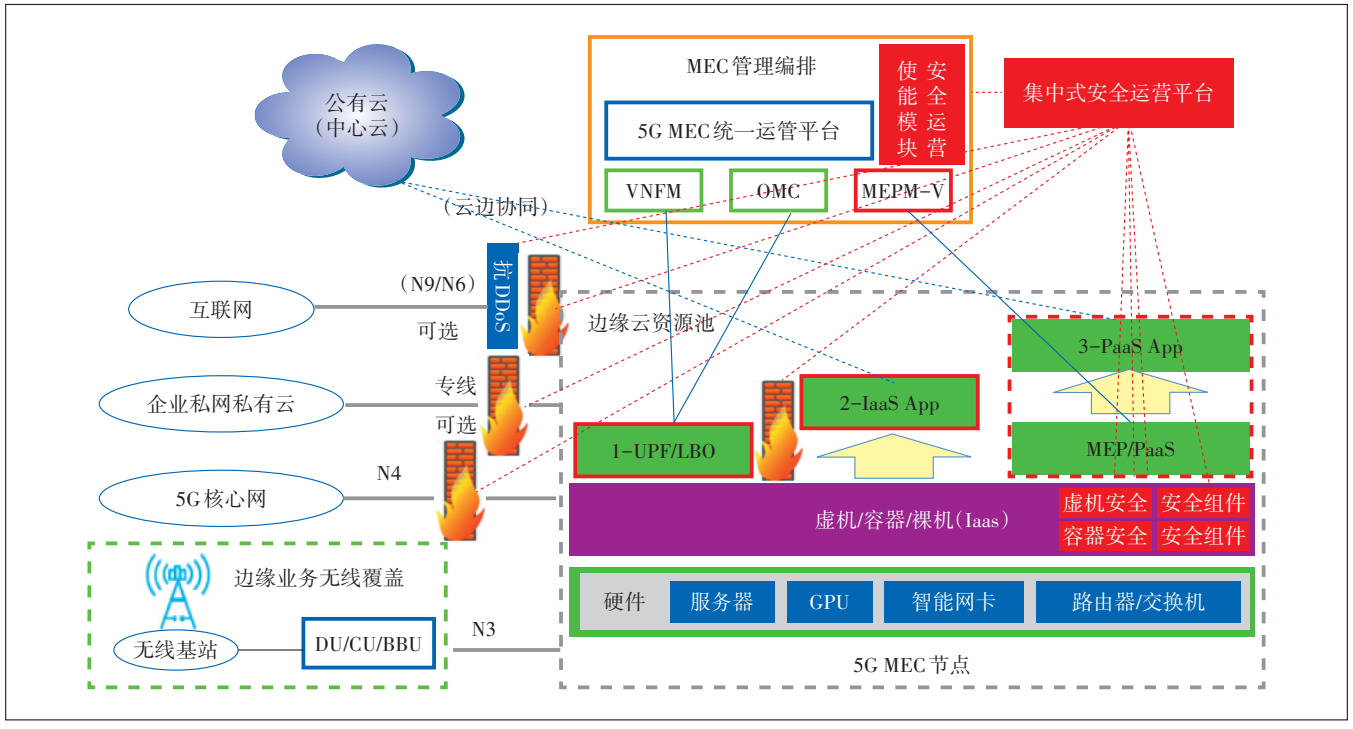

图1　5G MEC安全防护总体架构

知、虚机安全、容器安全、漏扫、基线核查、堡垒机、日志审计、WAF等特定的安全防护功能模块及组件。

2.3.2.2 集中安全运营平台

集中安全运营平台采用中心化部署，与5G MEC管理平台同级，提供安全运营能力的闭环，能自动纳管用户名下的安全组件，包括资产管理、防护配置、安全检测、安全事件告警等，提供北向接口与安全运营使能模块对接，支持应急响应能力。该平台是实现5G MEC自动化安全运营的调度指挥中心，也是实现安全即服务的重要部分。

2.3.2.3 安全运营使能模块

安全运营使能模块是集中安全运营中心与5G MEC实现安全自动化联动、安全能力开放的互通插件。

3 总结

5G MEC是5G面向2B市场的重要业务载体，其构成较为复杂、功能模块多、网络暴露面大，安全问题不可忽视。5G MEC每个功能模块的安全要求及其之间的安全隔离措施构成了整体网络安全防护架构，一般通过部署内墙和外墙的双层异构的防火墙隔离模式来实现不同域之间的网络边界安全隔离，资源池和边缘应用的安全防护需要对标云资源池安全防护要求来构建，安全功能组件按照集中管控+分布部署的模式按需部署。安全即服务是5G MEC安全防护体系架构的重要内容之一，是MEC编排管理平台与各安全组件安全模块实现联动所必需的。

5G MEC随着5G面向2B应用发展而不断快速发展，在部署5G MEC时，需要同步对5G MEC进行安全防护能力的部署，实现节点自身安全、5GC大网的安全、承载业务的安全等，为5G MEC的发展保驾护航。

参考文献：

[1] 3GPP. System architecture for the 5G System(5GS):3GPP TS 23.501[S/OL].[2023-05-04]. ftp://ftp.3gpp.org/Specs/.
[2] KEKKI S,FEATHERSTONE W,FANG Y G,et al. ETSI white paper No. 28 MEC in 5G networks[EB/OL].[2023-05-04]. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf.
[3] REZNIK A,SULISTIO A,ARTEMENKO A,et al. ETSI white paper No. 30 MEC in an enterprise setting: a solution outline[EB/OL].[2023-05-04]. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp30_MEC_Enterprise_FINAL.pdf.
[4] 华为.5G时代十大应用场景白皮书[EB/OL].[2023-05-04]. https://www-file.huawei.com/-/media/corporate/pdf/mbb/5g-unlocks-a-world-of-opportunities-cn.pdf?la=zh.
[5] 中兴通讯.5G安全白皮书[EB/OL].[2023-05-04]. https://res-www.zte.com.cn/mediares/zte/Files/PDF/white_book/201905291835_5G_Security_White_Paper_CN.pdf?la=zh-CN.
[6] 中兴通讯.5G行业应用安全白皮书[EB/OL].[2023-05-04]. https://www.vzkoo.com/document/9ae6fc0ce046e2769f56b98f353dd413.html.
[7] 庄小君，杨波，杨利民，等.面向垂直行业的5G边缘计算安全研究[J].保密科学技术，2020(9):20-27.
[8] 郝梓萁.5G新技术面临的安全挑战及应对策略[J].信息安全研究，2020，6(8):694-698.
[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.
[10] 朱京毅.面向5G网络边缘计算的安全技术方案与研究[J].通信技术，2020，53(1):210-214.
[11] 全国信息安全标准化技术委员会，通信安全标准工作组.5G网络安全标准化白皮书(2021版)[EB/OL].[2023-05-04]. http://www.chuangze.cn/attached/file/20210515/20210515135519081908.pdf.
[12] 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.
[13] 李杨飞，叶晶，杨睿.基于5G的MEC网络架构与部署策略[J].邮电设计技术，2021(1):50-54.
[14] 解晓青，余晓光，余滢鑫，等.5G网络安全渗透测试框架和方法[J].信息安全研究，2021，7(9):795-801.
[15] 刘云毅，张建敏，冯晓丽，等.5GMEC系统安全能力部署方案[J].电信科学，2022，38(11):143-152.
[16] 吴星培，李晗，王晨鹤，等.5G ToB边缘网络安全技术研究[J].通信电源技术，2021，38(16):147-149.
[17] 国家保密科技测评中心.面向垂直行业的5G边缘计算安全研究[EB/OL].[2023-05-04]. https://www.gjbmj.gov.cn/n1/2021/0909/c411145-32222461.html.
[18] 工业互联网产业联盟.5G边缘计算安全白皮书[EB/OL].[2023-05-04]. http://aii-alliance.org/upload/202102/0202_104527_347.pdf.
[19] 孙侃.面向融合媒体应用的5G安全风险分析与对策研究[J].广播电视信息，2022(S1):159-164.
[20] 奇安信.5G MEC云安全资源池解决方案[EB/OL].[2023-05-04].网络链接地址缺失.
[21] 沈景悦.5G定制网MEC与UPF部署方案[J].数字技术与应用，2022，40(5):196-198.

作者简介：
王凯，毕业于中国科学技术大学，工程师，学士，主要从事网络信息安全相关的技术和管理工作；汪剑桥，毕业于南京工业大学，助理工程师，学士，主要从事移动网数据采集的技术和管理工作；卜寅，毕业于南京邮电大学，高级工程师，学士，主要从事移动网通信管理工作。