面向5G专网的云原生安全技术研究与实践

Research and Practice of Cloud Native Security Technology for 5G Private Network

郭新海[1,2]，徐　雷[1,2]，张曼君[1,2]，丁　攀[1,2]，徐积森[3]（1. 中国联通研究院，北京 100048；2. 下一代互联网宽带业务应用国家工程研究中心，北京 100048；3. 中国联合网络通信集团有限公司，北京 100033）

Guo Xinhai[1,2]，Xu Lei[1,2]，Zhang Manjun[1,2]，Ding Pan[1,2]，Xu Jisen[3]（1. China Unicom Research Institute，Beijing 100048，China；2. Next Generation Internet Broadband Service Application National Engineering Research Center，Beijing 100048，China；3. China United Network Communications Group Co.，Ltd.，Beijing 100033，China）

摘　要：

5G和云原生技术的不断演进与发展，促进了5G专网的云原生化演进，云原生技术的应用也带来了镜像攻击、编排工具攻击、容器攻击等多种新型攻击行为。结合5G专网和云原生技术的发展趋势，分析了5G专网云原生演进情况和所面临的主要安全风险，研究了面向5G专网的云原生安全防护技术，并进行了实践验证，从而为业内的安全防护能力建设提供参考。

关键词：

云原生；5G专网；MEC；安全防护

doi：10.12045/j.issn.1007-3043.2024.08.014

文章编号：1007-3043（2024）08-0067-06

中图分类号：TP393

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

The continuous evolution and development of 5G and cloud-native technology has promoted the cloud-native evolution of 5G private networks. The application of cloud-native technology has also introduced a variety of new attack behaviors such as mirror attacks，orchestration tool attacks，and container attacks. Combined with the development trends of 5G private network and cloud native technology，it analyzes the cloud native evolution trend of 5G private network and the security risks faced，studies the cloud native security protection technology for 5G private network，and conducts practical verification，thereby providing insights for the industry.

Keywords：

Cloud native；5G private network；MEC；Safety protection

引用格式：郭新海，徐雷，张曼君，等. 面向5G专网的云原生安全技术研究与实践[J]. 邮电设计技术，2024（8）：67-72.

1 概述

随着数字经济的蓬勃发展，各行业的数字化转型进入关键阶段，5G技术因其大带宽、低时延、高可靠、大连接、泛在网等诸多优势，在工厂、能源、电力、交通、医疗等领域被广泛使用。工信部发布的《2023年通信业统计公报》显示，截至2023年末，我国的5G网络规模和质量已经处于世界领先地位，但为了更广泛、深入、安全地挖掘5G潜能，同时伴随着各行业的数字化转型进入关键阶段，5G网络需要持续向深度覆盖挺进，向行业融合应用深化拓展[1-2]。

1.1 5G专网的发展

云计算和网络功能虚拟化技术的发展，正在助推着5G网络向网元虚拟化、架构开放化和编排智能化方向发展，这些技术的应用和发展为5G专网提供定制化服务能力提供了保障，使其能够实现按企业客户需求对网络/网元功能等进行灵活编排、定制开发和快速部署。当前为了满足不同行业的需求，5G专网根据不同的场景进行设计，主要的组网模式包括5G虚拟专网、5G混合专网以及5G独立专网。其中，5G混合专网的UPF/MEC独立部署于行业用户的园区内，AMF以及SMF可选共用公众网络核心网资源或在行业用户园区

收稿日期：2024-06-25

内独立部署[3-4]（见图1）。由于UPF/MEC的独立部署，MEC侧的安全威胁会影响到运营商的核心网。

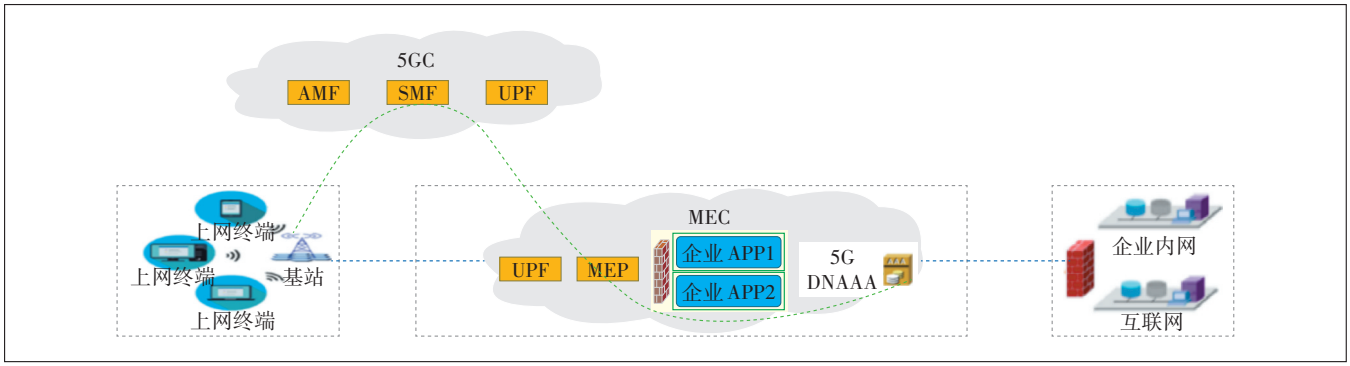

图1　5G混合专网部署逻辑

另外，5G核心网作为5G专网通信的基石，走向了全面云化的时代，通过虚拟化和云原生技术，5G核心网实现了网络功能虚拟化（Network Functions Virtualization，NFV），可以部署在通用X86服务器上，甚至直接部署在云端。核心网网元的NFV化部署，彻底打破了以往耦合封闭的设备形态，使5G核心网从封闭转向开放。同时，随着以微服务、容器、持续交付为代表的云原生技术的发展，国内外运营商已经开始网络云原生化的应用探索，美国AT&T明确NFV云原生演进路线，进行容器5GC（5G core）测试。Bharti Airtel公司以容器为虚拟化基础设施，构建NFV PaaS平台，已经实现vEPC容器化的小规模商用。中国电信正在研发网络云原生平台试点承载轻量化4G/5G网元和边缘云，中国移动正在进行边缘计算的容器技术试点，中国联通正在进行5G轻量化部署方案的研究。

1.2 云原生技术的发展

自开源Docker容器和K8S编排引擎出现以来，云原生生态不断扩大。当前，云原生作为云计算深入发展的产物，已经开始在5G、人工智能、大数据等各个技术领域得到广泛应用。2020年，云原生产业联盟发布《云原生发展白皮书》，指出云原生是面向云应用设计的一种思想理念，充分发挥云效能的最佳实践路径，帮助企业构建弹性可靠、松耦合、易管理可观测的应用系统，提升交付效率，降低运维复杂度，代表技术包括不可变基础设施、服务网格、声明式API及Serverless等[1]。

2 5G专网云原生演进分析

3GPP在R15、R16版本中规定，5G核心网需要支持服务化架构（Service-based Architecture，SBA）、微服务和跨平台等功能。SBA架构作为5G的基础网络架构，极大地推动了CT向IT的微服务的转变，并且与云原生技术中提到的微服务和容器十分契合。当前，中国的运营商已经规模部署5G核心网（5GC）设备，同时各种5GC应用主要以VNF形式部署，要实现5G核心网设备的云原生部署仍需要一定的时间，并且会在一定时间内存在虚拟机和容器并存的状态[2]。但是，在5G专网的混合模式下，UPF会下沉到边缘MEC侧，并且5G专网边缘侧与核心网侧相比，具有高度集成、快速安装、敏捷部署和按需扩容的特点，因此针对5G专网边缘侧的云原生化演进要优先于5G核心网侧。

边缘云的容器化将从现在的通过IaaS模式搭建虚拟机，然后在虚拟机上部署容器化业务或者直接部署业务，向通过CaaS模式提供服务的方式演进（见图2）[5-6]。

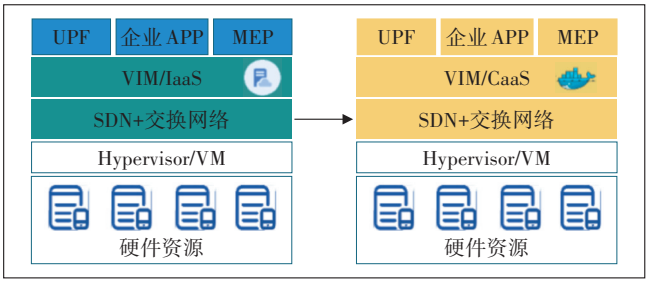

图2　边缘云容器化演进

核心网侧会从现在的虚拟机的方式逐步向以虚拟机和容器模式部署AMF、SMF和UPF的方式演进（见图3）。

3 5G专网云原生安全风险分析

由于云原生技术以DevOps、持续交付、微服务和

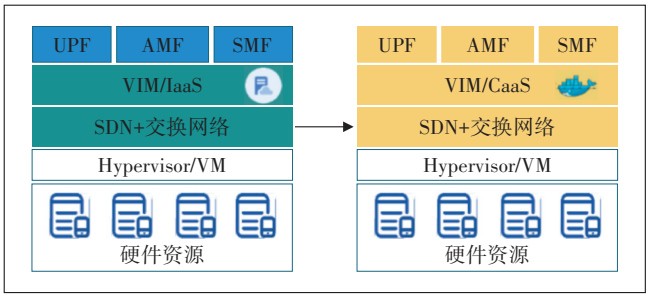

图3　核心网侧容器化演进

容器技术为代表，在5G专网部署架构的演进过程中，5G MEC环境中K8S和容器开始使用，随之而来也引入了新的安全风险，主要表现在镜像安全威胁、虚拟化安全威胁、编排工具安全威胁、微服务安全威胁以及应用安全威胁等（见图4）。

3.1 镜像和容器安全威胁

在5G专网的MEC环境中，虚拟机或容器是主要的部署模式，在通过镜像构建MEC计算环境、第三方APP和下沉的网元时，如果镜像存在安全漏洞，相关运行的容器可能会被攻击者利用发起攻击行为，并进一步控制容器和宿主机，从而威胁5G核心网络安全。

攻击者可以通过上传恶意镜像到公开仓库或受害者本地仓库，然后将恶意镜像伪装成正常镜像以引导受害者使用该镜像创建容器，具体的安全风险如图5所示。

3.2 编排工具安全威胁

当前，编排工具存在的安全漏洞，成为了攻击者发起攻击的主要手段之一，攻击者可以通过安全漏洞，实现对宿主机的入侵，主要的攻击手段包括K8S组

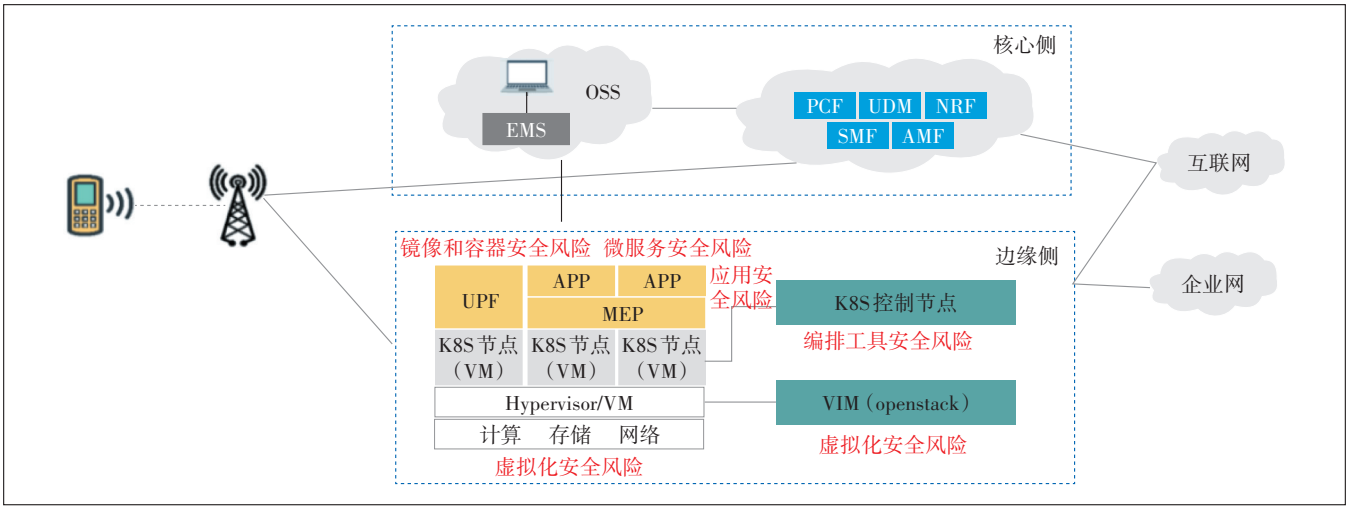

图4　安全风险分析

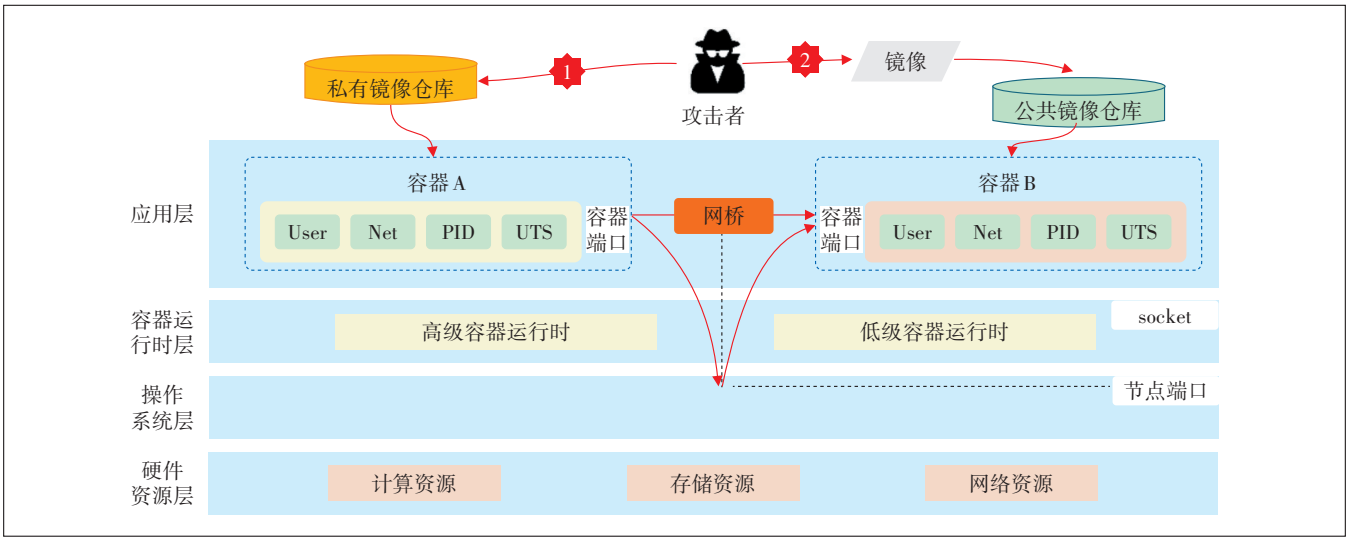

图5　容器镜像安全风险

件、服务对外暴露攻击、业务POD攻击、集群环境下的横向攻击、K8S管理平台攻击和第三方组件攻击等（见图6）。

攻击点1至攻击点4，展示了K8S各组件的不安全配置可能带来的安全风险，即API Server未授权访问、etcd未授权访问、kubelet未授权访问、kube-proxy不安全配置。攻击点5表示Node节点对外暴露的服务，由于管理员的疏忽或为了方便管理而故意留的一些接口，导致内部服务的暴露，使得编排组件存在一个潜在的攻击点。攻击点6显示的是攻击者利用Web服务的漏洞对POD发起的攻击。攻击路径7和8，展示了K8S集群中可能存在的横向攻击。

3.3 微服务安全威胁

微服务作为一种软件开发方式，允许将应用程序划分为更小、可管理的组件，并且可以根据需求进行独立扩展。在5G专网MEC环境中部署的业务应用，如果通过微服务的方式部署，会存在大量的API接口，并且开发者在开发微服务过程中引入的开源或第三方插件、加载库、模块、框架等（见图7），都可能成为被攻击者利用的点。

4 5G专网云原生安全防护技术研究与实践

针对5G专网使用云原生安全技术带来的镜像和容器安全威胁、编排工具安全威胁以及微服务安全威胁等，需要从计算环境安全和运行时安全开展5G专网的云原生安全防护能力建设。计算环境安全主要包

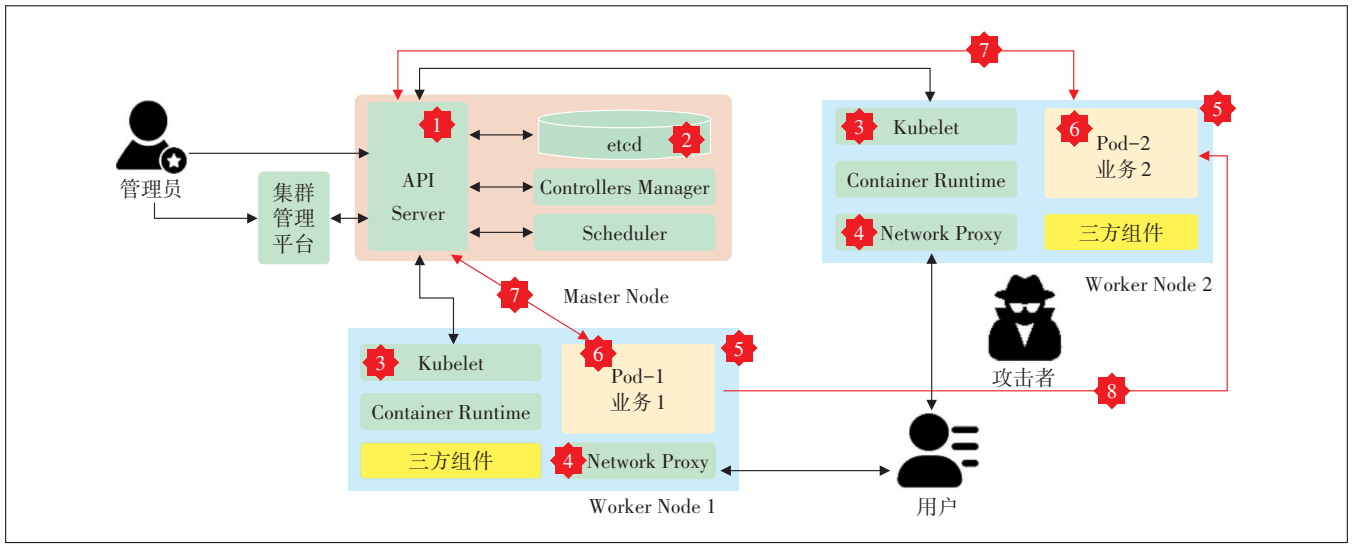

图6　K8S安全风险

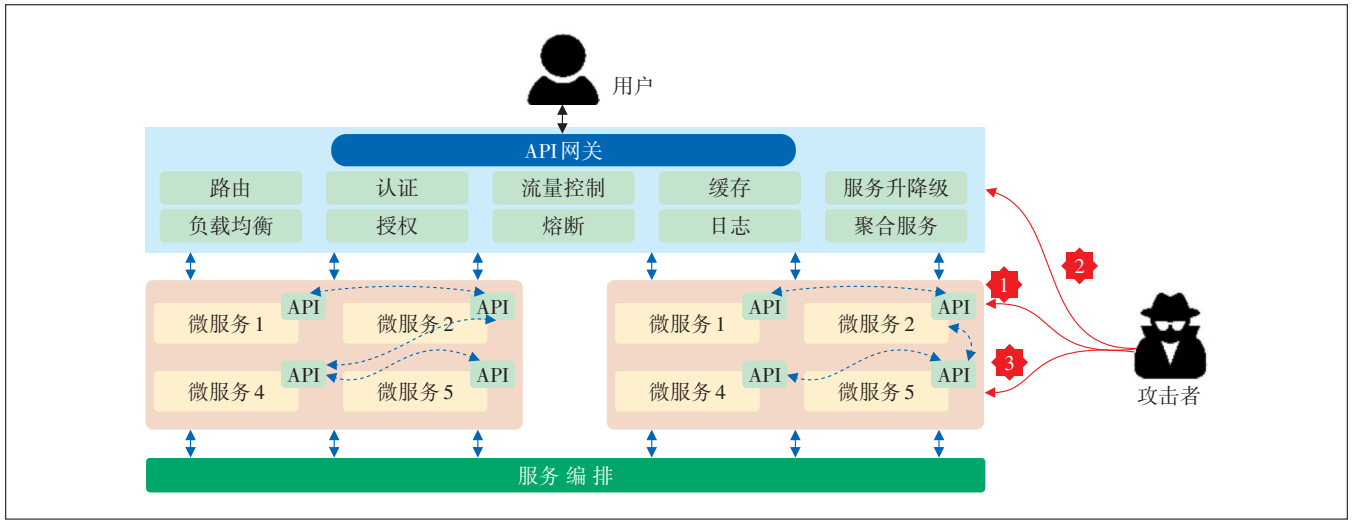

图7　微服务安全风险

括云原生资产安全管理、安全合规基线和漏洞扫描、虚拟化安全、容器安全和镜像安全等方面，运行时安全包括容器运行时安全以及网络微隔离等（见图8）。

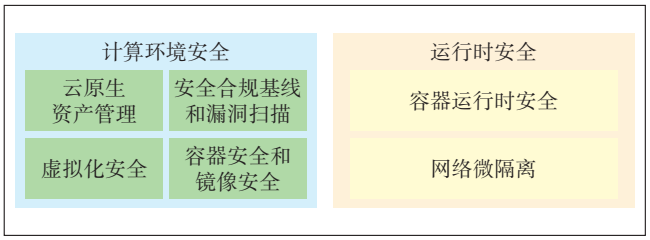

图8　计算环境安全和运行时安全

4.1 计算环境安全

当前5G专网的MEC计算环境中，存在物理机、虚拟机、容器、应用系统、边缘计算平台等，为了实现计算环境安全，需要从资产安全、虚拟化安全、容器安全和边缘计算平台安全等多个角度开展安全防护。

4.1.1 云原生资产安全管理

在云原生环境中，需要对物理机、虚拟机、集群、容器、集群中POD、Service、Namespace等资产进行统计，并进行关联性分析，形成多集群的统一可视化管理控制台。针对相关资产还应清点出关联关系，例如物理机上运行的虚拟机、虚拟机上运行的集群、集群中运行的POD、POD中包含的容器等。

4.1.2 安全合规基线和漏洞扫描

在云原生计算环境中，不安全、不合规的配置是引发安全问题的主要原因之一，为了提升计算环境的安全合规水平，需要建立面向Openstack、K8S和Docker等的基线合规配置检查和漏洞扫描能力，在业务系统上线运行之前，应对业务系统所在宿主机、容器、集群以及容器原镜像进行合规检测，以防止不安全的配置导致容器逃逸或者集群入侵事件，从而全面提升云原生计算环境的安全水平，防止不安全、不合规的配置以及已知的安全漏洞被攻击者利用对5G专网的MEC环境发起攻击。

4.1.3 虚拟化安全

为了避免虚拟机之间的数据窃取或恶意攻击，保证虚拟机的资源使用不受周边虚拟机的影响，Hypervisor要能够实现同一物理机上不同虚拟机之间的资源隔离，用户使用虚拟机时，仅能访问属于自己的虚拟机的资源（如硬件、软件和数据）。为了防止虚拟机逃逸，通过虚拟机隔离提升虚拟化安全，对于部署在虚拟化边缘环境中的VM，可以加强VM之间的隔离。另外，可以实时监测VM的运行情况，有效发掘恶意VM行为，避免恶意VM迁移对其他边缘数据中心造成感染。

4.1.4 容器安全

容器安全需要覆盖容器从开发、部署到运行的整个生命周期，在开发阶段需要对容器镜像进行漏洞扫描，同时对第三方和自己编写的代码进行代码安全检查。在部署阶段需要对部署的容器镜像进行漏洞扫描，控制有高危漏洞的容器镜像运行。在运行阶段应对容器运行时的行为进行实时监测，并实现容器实例和宿主机之间的内核隔离。

4.1.5 镜像安全

镜像作为容器运行的基础，提供了容器运行所需的序、库文件以及配置参数等。在日常运营使用的过程中，镜像多数会基于基础镜像构建，如果基础镜像存在大量漏洞，在生成业务镜像后，漏洞数量将会成倍的增长。所以为了保护镜像安全，需要建立黄金基础镜像，在黄金基础镜像仓库中的镜像文件，通过定期的病毒检测、恶意软件检测、软件成分分析、漏洞扫描、配置检查等方式，保护基础镜像的安全，从而从根源上防止风险和漏洞的引入。

4.2 运行时安全

由于5G专网的MEC环境中会部署MEC平台、业务应用系统和UPF网元，相关系统会以业务应用或微服务的方式存在，因此运行时安全需要从Web应用、网络隔离和容器运行时安全等几个方面考虑。其中Web应用的安全保护措施可以依靠防火墙、WAF和RASP等方式进行防护，本文中不再赘述，关于网络微隔离和容器运行时的安全防护能力建设包括如下内容。

a）容器运行时安全。为了保证容器运行时的安全，需要从容器运行时的资源监控、行为检测、数据留存等几个方面考虑构建容器运行时的安全防护能力。在资源监控方面，需要建立针对容器及主机的资源监控，并具备设定阈值告警的能力，以防止由于容器过度占用资源导致的安全问题；在行为检测方面，需要根据实际业务建立容器的行为基线模型，由于云原生环境下一个容器一般只会启动一个业务进程，其行为与主机相比变得极为简单，因此，对业务行为建立模型，在一定周期内，形成业务行为基线，从而发现模型外的异常行为，进一步发现未知漏洞攻击等行为。在数据留存方面，由于容器易消逝的特性，需建立对容

器基本信息以及运行过程中行为信息的监测和留存，包括可能存在的进程、文件、网络等多个方面，方便安全事件发生后的分析溯源。

b）网络微隔离。为了识别云内网络流量，并实现东西向和南北向流量的隔离，需要构建流量识别统计能力和流量隔离能力。在流量识别能力统计方面，可以通过特权容器的方式，实时监控云原生环境内的流量，并对网络流量进行分析和统计，以识别不同类型的网络流量、应用程序通信模式以及潜在的安全威胁，从而在发生安全风险时，快速定位风险影响范围。在流量隔离方面，对东西向以及南北向流量的隔离，对常用资源对象的出入站流量进行隔离，包括但不限于集群、命名空间、Service、宿主机、POD、容器等资源对象。

4.3 安全防护能力实践

由于当前5G专网MEC环境中云原生技术处于初步推进使用的阶段，镜像、容器和微服务等技术为相关业务的部署提供了便利，但是却缺乏相应的安全保护能力。基于此，我们结合现网实际情况，已经完成了面向5G专网MEC计算环境的安全保护能力的研发（见图9）。

相关安全能力在智能城域网的MEC环境中得到了部署应用，对MEC环境中的镜像资产、容器资产、节点资产和集群资产完成了清点纳管之后，对安全配置、镜像和容器进行了全面的安全检测，发现了安全配置缺陷、镜像漏洞和基于漏洞镜像所启动的容器，并提供了相关的修改建议，助力完成了安全问题的整改，提升了MEC环境的安全水平[7]。

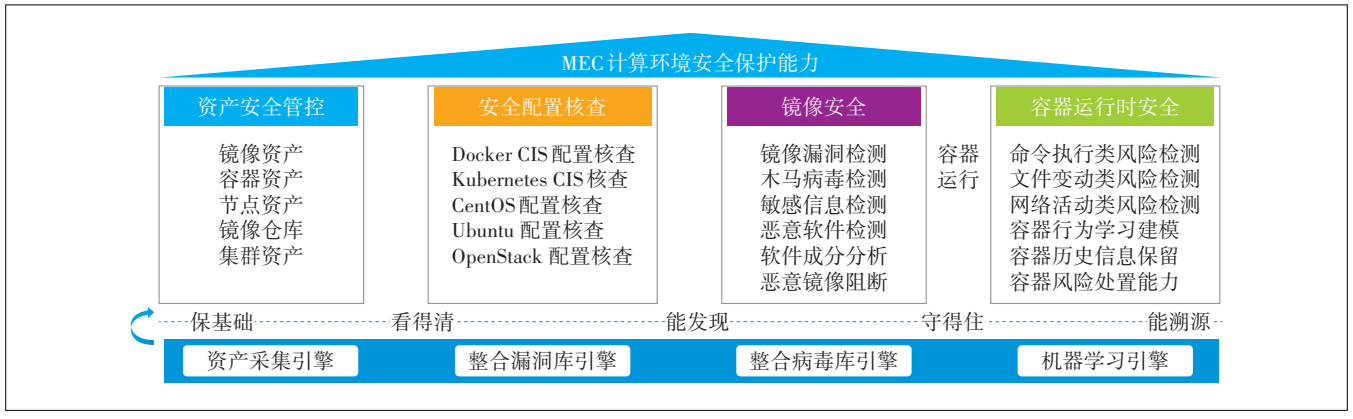

图9　MEC计算环境安全保护能力

5 结束语

随着云原生技术的发展和5G专网在垂直行业的广泛部署应用，基于云原生技术的5G专网将成为未来电信云网络演进的重点，同时基于云原生的轻量级5GC也将被广泛应用，本文全面分析了5G专网的云原生演进趋势和云原生演进后带来的安全风险，并基于目前较大的安全风险提出了相关的安全防护能力建设建议，验证了相关安全防护能力取得的安全效果，以期为业内5G专网云原生部署情况下的安全防护能力建设提供参考。

参考文献：

[1] 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.
[2] 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)：67-74.
[3] 中国联通. 中国联通5G行业专网白皮书[R/OL]. [2024-01-10]. https://www.digitalelite.cn/h-nd-2808.html.
[4] 中国移动. 中国移动5G行业专网技术白皮书V1.0[R/OL]. [2024-01-10]. https://www.sohu.com/a/403531864_468714.
[5] 史庭祥，徐法禄，章璐. 5G电信云网络的容器演进方案[J]. 中兴通讯技术，2021，27(6)：58-64.
[6] 陈长怡，陆钢，周丽莎，等. 基于云原生的轻量级5GC产品及关键技术[J]. 电信科学，2020，36(12)：89-95.
[7] 郑涛，谢泽铖，张曼君，等. 5G网络信令流量安全监测研究[J]. 邮电设计技术，2023(9)：75-78.

作者简介：
郭新海，工程师，硕士，主要从事网络与信息安全研究工作；徐雷，博士，主要从事网络与信息安全研究工作；张曼君，高级工程师，博士，主要从事网络与信息安全研究工作；丁攀，工程师，硕士，主要从事网络与信息安全研究工作；徐积森，高级工程师，主要从事网络安全运营工作。