面向未来安全架构的5G核心网内生安全设计与实现

Design and Implementation of Endogenous Security for 5G Core Network in Future-Oriented Security Architecture

马田丰[1]，贺晓博[2]，尚　楠[2]，王　荣[3]（1. 中国联合网络通信集团有限公司，北京 100033；2. 中讯邮电咨询设计院有限公司郑州分公司，河南 郑州 450007；3. 中国联通山东分公司，山东 济南 250001）

Ma Tianfeng[1]，He Xiaobo[2]，Shang Nan[2]，Wang Rong[3]（1. China United Network Communications Group Co.，Ltd.，Beijing 100033，China；2. China Information Technology Designing & Consulting Institute Co.，Ltd. Zhengzhou Branch，Zhengzhou 450007，China；3. China Unicom Shandong Branch，Jinan 100029，China）

摘　要：

内生安全作为未来安全架构下的网元安全新手段，可以实现风险预防、入侵发现、事件响应和系统恢复等功能。这种全新的防护机制不仅能够提升网络的整体安全性，还能形成内外兼容、纵深防御的统一安全防护机制。对5G核心网内生安全技术进行研究探索，为5G核心网提供了一种有效的安全防护手段，确保5G网络的稳定运行和数据安全。

关键词：

5G核心网；内生安全；入侵检测

doi：10.12045/j.issn.1007-3043.2026.07.012

文章编号：1007-3043（2026）07-0068-05

中图分类号：TN915

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

Endogenous security, as a novel network-element-level security approach within future security architectures, enables capabilities for risk prevention, intrusion detection, event response, and system recovery. This entirely new protection mechanism not only enhances the overall security of networks, but also establishes a unified security framework featuring compatibility between internal and external defenses with layered protection. Endogenous security technologies for 5G core networks are explored, providing an effective security protection method for 5G core networks, and ensuring the stable operation of 5G core networks and data security.

Keywords：

5G core network；Endogenous security；Intrusion detection

引用格式：马田丰，贺晓博，尚楠，等. 面向未来安全架构的5G核心网内生安全设计与实现[J]. 邮电设计技术，2026（7）：68-72.

1 概述

5G技术的快速发展和广泛应用，正在推动社会经济的数字化转型[1]。但5G业务的开放性和5G网络的复杂性，也对网络安全提出了新的技术需求。5G核心网不仅承载了更高的流量和更复杂的应用，还支持网络切片、边缘计算等先进技术，以满足不同业务场景的需求[2]。5G核心网改变了传统网络的安全边界，进而引发了一系列新的安全风险。

5G网络的开放性和连接性使攻击者有了更多的机会和手段。例如，物联网（IoT）设备的广泛接入使得攻击者可以通过这些设备对网络发起攻击，甚至利用网络中的脆弱环节进行更高级别的攻击，如拒绝服务（DoS）攻击和信令嗅探。根据相关报告，有38%的云攻击针对电信公司[3]，攻击者可能会入侵电信云系统，进而在云内进行横向移动，获取敏感信息或扩大攻击范围，给经济和日常生活带来灾难[4]。因此，研究如何增强5G网络的安全性，尤其是信令安全、入侵检测等关键领域，具有重要的现实意义。

将网元安全作为最后一道防线，通过在核心网中

收稿日期：2026-05-20

构建内生安全能力，实现风险预防、入侵发现、事件响应与系统恢复。这种全新的防护机制不仅能够提升网络的整体安全性，还能形成内外兼容、纵深防御的统一安全防护机制。

本文通过对网元内生安全的技术研究，解决当前5G核心网面临的多种安全挑战，提升网络的安全韧性与抗攻击能力，为未来的网络安全发展奠定基础，为通信行业提供切实可行的安全解决方案。

2 5G核心网的安全威胁及挑战

5G核心网作为关键基础设施，在部署建设后，其网络新架构、部署新模式、新业务等给网络安全运营带来了新的挑战。关键基础设施对国民经济和社会发展起到基础性的支撑作用，而通信网络作为关键基础设施的“基础设施”，为金融、能源、交通、供水、医疗卫生和应急服务等与国计民生密切相关的重要系统及政府事务管理提供关键支撑，事关国家安全。

a）网络新架构带来的挑战。云化和IT化的网络架构，引入了虚拟化软件漏洞被利用、虚拟机逃逸、容器逃逸、虚拟机和容器镜像被篡改等问题；网络切片之间隔离失败导致切片被非法访问，切片之间相互攻击；在服务化架构中，服务化接口存在非法访问、敏感数据泄露问题；离开封闭的物理环境，安全需求更加个性化，责任界定也更加困难[5]。

b）部署新模式带来的挑战。边缘计算增加了5G核心网的暴露面，UPF下沉后易遭受物理接触攻击，并且攻击者可通过攻击UPF进一步攻击核心网；切片管理向第三方开放，会引入敏感数据泄露、非法访问等问题。

c）新业务带来的挑战。在边缘计算节点中，被攻击者劫持的第三方应用或者恶意第三方应用，对边缘计算平台、5G核心网发起DDoS攻击或者进行非法访问；海量终端接入网络，攻击者可利用终端存在的漏洞，对终端进行恶意劫持利用，或者恶意构造非法终端反复接入网络等，对5G网络发起信令风暴或数据面的DDoS攻击，导致网络瘫痪。

现有边界防护手段不再坚不可摧，当前边界防护手段FW/IDS/IPS/WAF等都是基于已知特征进行安全防护和检测，并且依赖正确的安全配置。但是当攻击者利用安全产品本身存在漏洞、开源/第三方零日漏洞或者利用边界防护设备配置不当的弱点时，可以绕过或者突破边界安全设备防护入侵核心网。

3 运营商5G网络安全防御现状

全球运营商根据自己的实践经验，已采用多种技术手段来保护5G网络不被入侵，确保用户数据不被窃取，例如通过划分网络安全域，实现分层分域的纵深安全防护。在网络安全域划分的基础上，运营商在各安全域的边界部署多种安全防护、安全检测、安全监测等网络安全设备，一是通过部署防火墙、堡垒机、4A系统、零信任接入网关等限制非法的网络访问；二是通过入侵防护系统（IPS）基于流量分析发现网络攻击行为并进行阻断，通过抗DDoS攻击设备防范各类拒绝服务攻击流量；三是通过部署网络安全扫描器、Web应用扫描器、安全配置核查系统等发现网络和系统的各类安全漏洞、设备配置不合规等；四是通过部署入侵检测、态势感知、安全审计等技术手段动态分析入侵行为、安全事件、违规操作等。

5G网络包括海量的基站、UPF、边缘云等网络暴露面资产，大量的垂直行业应用终端，同时还有位于运营商电信云上的核心网网元等，资产数量多，暴露面风险突出。传统的网络安全防御体系限于尽力而为的惯性思维，挖漏洞、打补丁、查病毒、杀木马乃至设蜜罐，附加式、外挂式、边界防护等安全建设思路难以应对新的安全风险。

4 内生安全框架设计

由于5G网络业务运行在确定性硬件、确定性系统、确定性软件、确定性进程、确定性文件、确定性端口的确定性资产和状态的特点，很多安全问题和风险难以通过传统外挂式安全产品解决，只有结合5G网络半开放的特点将安全特性下沉到产品功能中，实现贴合业务的安全，才能更好地降低安全风险。因此，本文提出5G设备内生安全设计三大原则（见图1）。

a）纵深防御。纵深防御主要是在外部威胁和内部关键资产之间，构建多层次的安全防护体系，不同的层次采用不同的安全技术，避免出现突破一点即突破全局的情况。

b）零信任。基于网络时刻处于危险之中，任何接入或访问的流量在认证前都不可信这一假设，需要对任何访问进行逐次验证，动态授权，持续评估，实现动态的访问控制。

c）自适应。依托IPDRR（识别〔Identify〕，防护〔Protect〕，检测〔Detect〕，响应〔Respond〕，恢复〔Re-

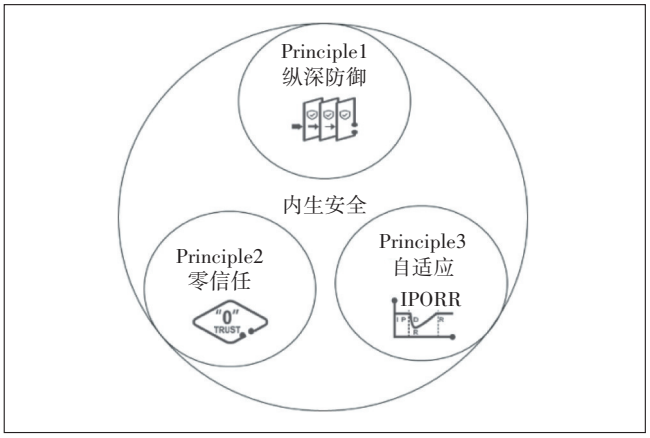

图1　内生安全设计原则

cover〕)安全理念，构建网元内生安全的管控能力，提升安全运维效率，并构筑相关5G核心网网元攻击感知能力。

(a) 识别(Identify)。通过网元合规风险管理实现网元业务面、系统面(OS、中间件、DB等)安全基线核查全覆盖，快速消减弱配置风险，缩小攻击暴露面。对网元资产进行安全风险评估，根据资产价值、脆弱性、威胁等因素进行综合判定，识别高危风险资产和风险账号，并上报告警事件。

(b) 防护(Protect)。通过纵深多级防御实现进程/文件、网络级隔离，防止网元间的横向攻击以及恶意软件、病毒的内部扩散。通过ASLR、KCFI、NX、堆栈保护等多种内核保护技术来提升漏洞利用难度，保护操作系统不受黑客攻击。

(c) 检测(Detect)。通过系统面全栈入侵检测实现5G网络中的Host OS以及以虚拟机或容器的方式部署虚拟化网元的入侵检测能力，包括恶意软件检测、进程提权检测、关键文件篡改检测等。5G网络管理面(OM面)是主要威胁来源，5G网元及网管均应实现OM入侵检测，如黑客账户暴破、内鬼异常登陆、越权/高危操作检测等。

(d) 响应与恢复(Respond&Recover)。安全响应处置系统通过剧本(Playbook)将不同系统或一个系统中不同组件的安全能力按照一定的逻辑关系整合到一起，用以实现某个或某类威胁事件的自动化处置闭环。

5 网元级内生安全设计方案

内生安全的防护设计强调动态纵深防御机制，致力于核心网最后一道防线的安全防护。依据内生安全设计原则，内生安全关键架构方案如图2所示。

网元内生攻击感知是以业务为中心，基于白名单机制，通过网元自身检测，并协同OMC/NFVO中的网元生命周期管理，配套安全管理模块，来检测网元操作系统以及运维相关的安全攻击，其框架如图3所示。

网元内生攻击感知框架包括2个部件，分别为安全管理模块和攻击感知组件。

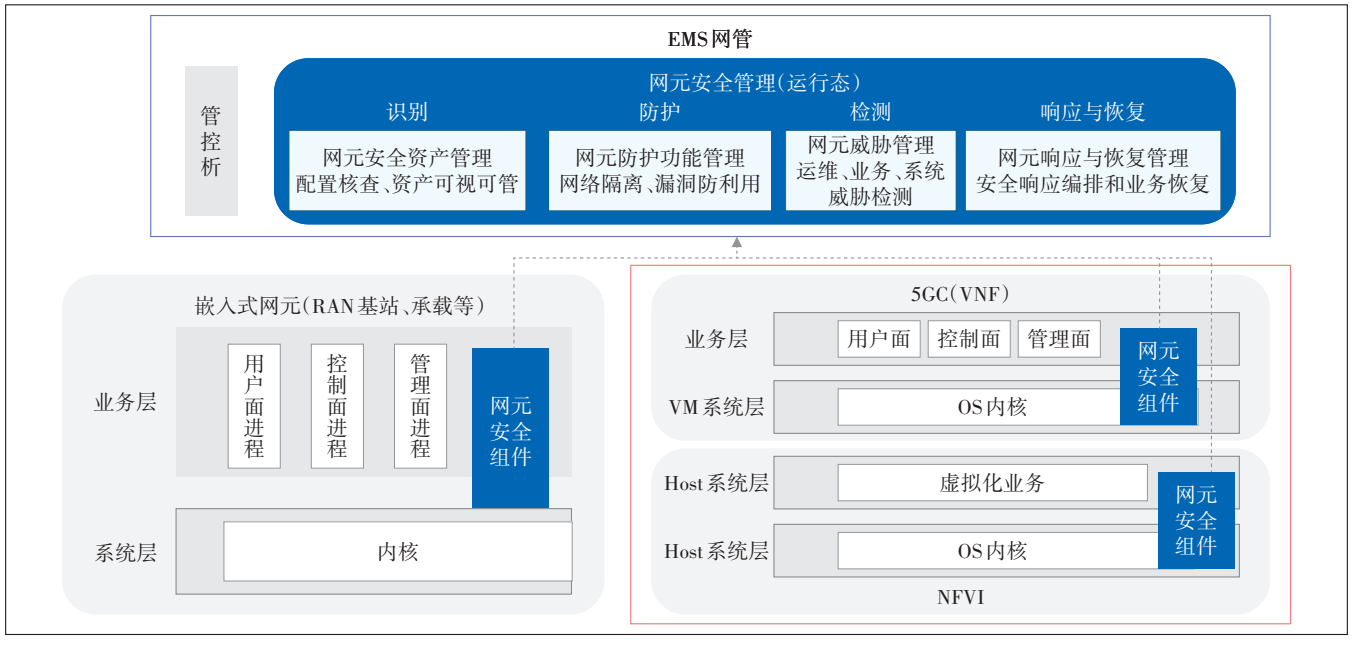

图2　内生安全关键架构

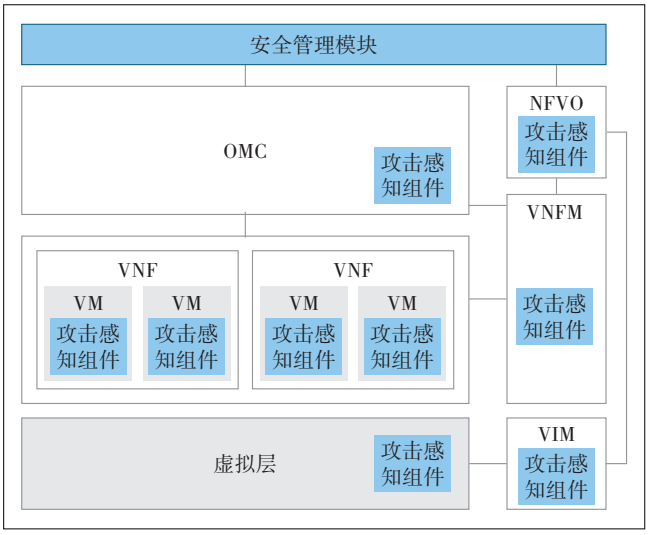

图3　网元内生攻击感知框架

a）安全管理模块。安全管理模块支持对网元（包括通信云云平台、网管、VNF等）上报的日志、安全事件进行分析，识别暴力破解、反弹shell等攻击，并进行网元安全态势展示。安全管理模块支持灵活部署，可与OMC共部署以管理VNF网元的安全事件，与NFVO共部署以管理NFVI虚拟层的安全事件。安全管理模块也支持独立部署，以管理通信云VNF网元以及NFVI虚拟层中的全部安全事件。

b）攻击感知组件。网元内置攻击感知组件，攻击感知组件可感知文件权限提升、非root用户权限提升、关键文件篡改等攻击，并将操作系统日志、OM日志以及异常文件等上报给安全管理模块，由安全管理模块进行分析。目前通信云中的网元一般以虚机或者虚机容器的形式进行部署，为了减少在每个容器中部署攻击感知组件带来的资源消耗，本方案在承载容器的虚拟机上部署攻击感知组件，实现对该虚拟机上所有容器的攻击检测。

6 内生安全关键能力

6.1 安全配置合规检查

弱配置是现网多数安全事件的主要诱因，需要在设备运行阶段提供自动化安全配置合规检查管理手段，缩短弱配置的暴露期，避免现网“弱配置”低级错误引发安全事件。

针对云化系统的NFVI层，需要对操作系统、openstack等关键能力项涉及的安全加固内容进行合规检测；针对云化系统Guest层，需要对操作系统、中间件、容器、数据库等关键能力项涉及的安全加固内容进行合规检测；针对VNF层，需要进行如加密算法强度、安全日志类开启、安全防护等必要性安全参数的检测。

安全配置合规检查能力通过自动化、标准化、持续化、可视化的手段，在设备和业务上线安全检查、合规安全检查、日常安全检查和安全服务任务中协助查找设备在安全配置方面的不足，并与安全整改与安全建设相结合，提升各类业务系统的安全防护能力，达到整体合规要求，实现复杂网络多设备的自动化和周期性检查，大大缩短人工检查的时间。

6.2 系统恶意入侵检测

电信云物理主机、网元虚拟化VM、网管等应支持入侵检测能力，具体包括恶意软件检测（包括Rootkit、反弹shell）、异常账号检测（包括暴力破解、非法账号、非法登录）、权限提升检测（包括账号、文件和进程权限提升检测）、信息破坏检测（包括关键文件篡改、关键文件删除、shell文件篡改、非法文件下载等）以及行为异常检测（包括账号异常更改、非授权新增账号、登录异常行为）。物理主机的虚拟层应支持虚拟化逃逸攻击检测，防止虚拟机获得底层平台控制权等。

6.3 防病毒能力

内生安全能力应支持病毒检测能力。通过在网元虚拟机、电信云宿主机中内置病毒检测组件，支持检测木马病毒、蠕虫病毒、僵尸网络、后门病毒、勒索软件等恶意软件；支持手动扫描能力，包括快速扫描、全盘扫描；支持黑白名单处理，若确认为病毒恶意文件，则加入黑名单，若检测结果经分析确认为非病毒恶意文件，则加入白名单，黑白名单可提升检测有效性。

6.4 安全事件处置与响应

由于CT网络对可靠性要求高，若在出现安全事件后直接进行处置，会给系统稳定性带来风险。为确保系统优先稳定运行并保证业务可用，网元内生攻击感知仅产生病毒检测安全事件，不进行自动处置，而是安全运维人员进行分析评估后，手工操作进行相应的处置，　例如检测到非法登录事件后，可选的处置措施包括添加黑名单、禁用账号等；检测到恶意文件后，可选的处置措施包括杀进程、删除文件、隔离文件等，或将其进行组合。

6.5 资产安全风险可视化

安全风险管理以预防为先，而构建安全预防体系的基础是先要有安全风险的评估体系。基于整个网

络系统提供的各类基础数据，构建风险评估体系，从该评估体系中可以知道整个系统中因自身脆弱性导致容易被攻破的部分、因对外暴露而容易被攻击的部分以及已经处于经常被攻击的场景下的部分。安全风险评估体系对整个系统有一个从定性到定量的风险呈现。

风险评估的范围包含网元和网管，其纵向将云化的Guest层与VNF层相结合，同时针对NFVI层进行风险评估，并将资产风险可视化。

6.6 轻量化、高可靠、安全性

由于ICT基础设施的电信级业务属性，网元对性能消耗、高可用性等方面有着更严格的要求。所以，入侵检测能力还需要具备轻量化、高可靠、开放化等特征。

a）轻量化：资源消耗小，CPU占用率最高不超过3%~5%；功能组件化，可按需开启和停用。

b）高可靠：高达5个9的电信级可靠性设计。

c）安全性：安全面自身的安全性、日志审计能力、安全面与内生攻击组件的通信安全等。

7 内生安全方案在某运营商的应用

5G核心网内生安全方案研究构建网元内生安全的管控分析能力，提升安全运维效率，并构筑5G核心网网元风险识别、纵深防御、入侵检测、响应与恢复的攻击感知能力。同时，协同OMC/NFVO中的网元生命周期管理，配套安全管理模块，实现对网元操作系统及运维相关安全攻击的检测识别。

本方案已在某运营商现网5GC资源池进行部署并完成业务测试，其架构如图4所示。内生安全策略中心与部署在网元上的Agent交互，采集内生安全相关的告警。在OMC上可以统一监控网元本身的告警和内生安全的告警。通过OMC现有的北向接口，将内生安全相关的告警上报给厂家NFVO+，NFVO+再通过现有的运营商MANO-OSS接口将内生安全相关告警上报给运营商一级NFVO，并在一级NFVO上实现告警的统一监控。

8 结束语

本研究针对5G核心网在新安全形势下面临的安全威胁，提出5G核心网内生安全解决方案，解决外挂式安全技术难以为网络通信提供保障的问题。内生安全的引入突破了传统的边界防护思路，它充分结合

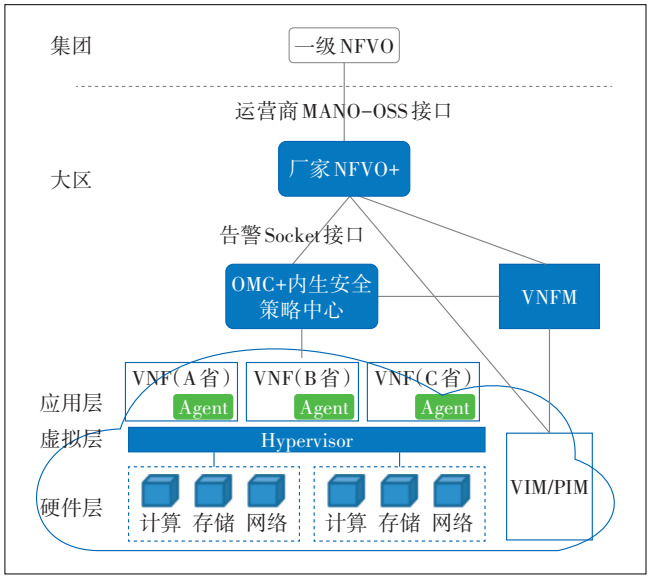

图4　某运营商内生安全部署架构

核心网超高可靠性运行要求和技术特点，为运营商5G核心网安全防护积累了宝贵经验。这些研究成果不仅将为通信行业提供切实可行的安全解决方案，也将推动相关技术的进步，为整个社会的数字化转型与发展保驾护航。

参考文献：

[1] 张阳．记者手记：商用五周年，数说5G高质量发展[EB/OL]．[2026-03-18]．https://tech.huanqiu.com/article/4I6K34AfasW．

[2] 江小平．基于智慧家庭应用的组网方案[J]．物联网技术，2021，11（1）：39-41．

[3] Sysdig. Twenty 23：global cloud threat report[EB/OL]．[2026-03-18]．https://sysdig. com/content/c/pf-2023-global-cloud-threatreport? x=u_wfri.

[4] 曹刚，关先锋．利用网络微分段技术增强5G电信云安全性的研究[J]．邮电设计技术，2025（5）：62-68．

[5] 王瀚洲，周洺宇，刘建伟，等．5G网络安全威胁发现及解决方法综述[J]．信息安全研究，2024，10（4）：340-346．

作者简介：

马田丰，北京邮电大学博士在读，工程师，主要从事移动核心网、5G专网、物联网等专业的研究和建设工作；贺晓博，毕业于北京邮电大学，高级工程师，学士，主要从事云核心网规划、设计、咨询及相关新技术跟踪研究及行业标准编制工作；尚楠，毕业于重庆邮电大学，高级工程师，硕士，主要从事移动核心网、通信云、创新业务平台等专业的研究和设计工作；王荣，毕业于山东大学，高级工程师，硕士，主要从事移动核心网、通信云、创新业务平台等专业的研究和建设工作。