中国联通
China unicom

中国联通 5G 核心网安全架构及关键技术白皮书

中国联合网络通信有限公司研究院
下一代互联网宽带业务应用国家工程研究中心

2024 年 8 月

版权声明

目录

前 言

5G 核心网引入了网络功能虚拟化、边缘计算、服务化架构等新技术，使得网络架构发生重大变化，也带来了新的安全挑战。

一方面，用户及产业对网络的要求越来越高，对网络的依赖性越来越强，使得网络承担了更多的使命和责任；另一方面，运营商自身的建设投资及运维压力较之前显著增大。如何既能保证业务体验，又能降低成本，既能保证网络的安全可靠，又可以灵活部署，降低压力，是当前运营商面临的重大课题之一。

5G 核心网容灾本质上是对网络运营成本和网络服务质量的平衡把控。对运营商网络安全和健壮性的考量也不仅仅是要求核心网应用层网元具备相应功能流程要求，而是一种基于网络整体的综合能力评估。本白皮书对 5G 核心网安全容灾架构及关键技术等多个方面提出部署策略、建议和要求，并提出对未来网络安全体系的思考和展望。

本白皮书由中国联通研究院牵头编制，联合编制单位（排名不分先后）：华为技术有限公司、中兴通讯股份有限公司、上海诺基亚贝尔股份有限公司。

一、网络安全面临的挑战

（一）网络多制式并存的复杂度到达新的水平

移动通信网络经过多年的演进，逐渐形成了一张四代同堂（2/3/4/5G）、三网并存（CS/PS/IMS）的超级复杂网络，在不同代际与不同业务网之间有多种不同组合。如果算上几乎同步演进的承载网、终端和基站，整个电信网的复杂程度已无以复加。此外，5G 核心网引入了服务化架构，实现简化部署和配置的同时也带来了集中注册和状态管理的风险。

（二）核心网部署集中故障容忍度低

5G 核心网逐步采用大区化部署，单大区数据中心规划容量过亿，故障影响巨大。5G 核心网多省份共享大区数据中心，两两容灾，单数据中心规模增长 2~3 倍，用户容量达到千万级规模，未来将超过 1 亿。

从应用层视角，由于 APP 要求永远在线，现代智能终端在不能连接数据网络时不断重试。由于大区数据中心集中，加剧了信令浪涌风险，大区间容灾倒换信令流量是平时 200 倍以上，业界重大恶性事故大多跟信令浪涌有关。

基站到大区控制面距离也超千公里，中间经过几十个传输路由设备，容易发生故障。如果是省干路由器故障将影响全省业务，业界已经发生过影响全省语音业务的严重事故。传输距离长导致传输时延大，

容易出现通信亚健康导致业务受损。

电信领域首次大规模采用云存储、SDN 等云化技术。新技术带来架构解耦和简化配置的同时也带来的网络高稳风险。集中部署或几种控制容易导致通信网络整体故障。

此外，在多代、多网络、多协议并存的场景下，电信设备及系统本身的业务复杂度和实现难度已经大幅提高。此时，再叠加上异厂家集成，系统可靠性就变得更加不可控了。

（三）网络安全影响生产安全

5G 网络大量应用在垂直行业，需要依赖大量的设备来实现其功能，这些设备在运行过程中可能会出现故障或异常。如果设备的安全性能不足或维护不当，将可能导致生产事故的发生。同时在 5G 网络中传输的数据量巨大且种类繁多，包括生产数据、用户信息等敏感信息。如果这些数据没有得到妥善保护，将面临泄露的风险。一旦数据泄露，将对企业的生产运营和用户的隐私安全造成威胁。因此，加强数据的安全管理和保护也是 5G 应用到垂直行业时必须重视的问题。

（四）智能化、数字化演进

随着技术的不断发展，网络复杂程度越来越高、遭受的攻击手段越来越复杂，传统的手段已经难以适应这种变化。随着智能化、数字化的演进，可以进一步探索网络安全体系的智能化演进，用各种新工具和手段实现网络的安全运营。

二、5G 网络容灾架构及关键技术

（一）网络可靠性架构

5G 网络的高可靠架构和高可靠产品是网络安全运行的基石。5G 云化核心网从网元内、网元间、网络级三个层面构建局部到整体的高可靠安全网络。

1. 网元内可靠性

云化核心网设备基于业务和数据分离的无状态架构设计，实现业务无损的资源弹性，弹性过程用户状态数据不丢失，保证业务连续性。

业务组件支持 1+1 或者 N+M 全负荷分担，一个组件故障其他组件可实时接管，业务无感。

网元内同类型虚机或容器互斥部署，分布在不同物理主机或裸机上，当主机运行故障时，虚机或容器可以进行本地自愈或异地重生，完成故障自恢复。

2. 网元间可靠性

5G 云化核心网支持网元间负荷分担（POOL）、1+1 互备等不同备份方式，根据网元类型确定合适备份容灾方式，当发生单网元故障时充分利用网元的容灾机制实现网元间容灾快速恢复业务。随着 AMF/MME、SMF/GW-C、UPF/GW-U 网元支持热备功能在网络中部署，接管效能进一步提升，实现终端无重连的平滑接管。

Bypass 功能也是一种有效的可靠性保障机制，在某类容灾网元

都发生故障时，邻接网元的 Bypass 功能生效，可以及时旁路故障网元，损失少量业务能力最大限度保障用户业务可持续。比如，AMF 在进入 Bypass 机制后，通过网络侧存储的安全上下文完成终端认证免鉴权，使用缓存的签约数据或本地配置最小签约数据，完成注册、切换等业务流程，使得 24 小时内用户重新注册、跨 AMF 移动、4/5G 互操作及常规在线业务均可用。SMF 在进入 Bypass 机制后，使用缓存的签约数据或本地配置最小签约数据，完成 PDU 会话的建立、更新等业务流程。

3. 网络级可靠性

为保障云化网络整体可靠性，在网络规划建设时满足多级容灾要求，资源池按照 DC 方案建设，DC 尽量部署在异地，实现异地容灾。一旦发生资源池和机房级故障，业务快速容灾到异地机房，实现业务快速接管。

此外，网元的对外网络也需要支持可靠性，包括不同功能的接口在 VPN 层面进行逻辑隔离，减少网络底层的互相影响。同一个逻辑接口，采用多链路组网、采用负荷分担或者主备进行链路级容灾，防止网络单点故障。

（二）通信云虚拟层可靠性

作为通信云的重要组成部分--虚拟化层，也必须支持高可靠性，才能满足上层网元的可靠性要求。

1．软件可靠性

通信云要求具备虚拟机热迁移能力，迁移期间保证虚拟机上业务连续性，保证在系统维护时做到业务不受影响。支持虚拟机看门狗功能，通过看门狗检测到虚拟机操作系统运行不正常时可以对虚拟机进行复位，使虚拟机尽快恢复正常。支持主动对虚拟机进行检测，在检测到虚拟机异常时对虚拟机发起复位操作，使虚拟机尽快恢复正常。

通信云要求支持虚拟机的异地重生，即系统可以主动检测物理机异常，并且在检测到物理机异常后，能够将该物理机上的虚拟机在其他物理机上重新启动，以减少业务损失。支持虚拟机的反亲和性部署。冗余备份的多个虚拟机需要部署在两台以上、不同的服务器上，以便在主用虚拟机所在的服务器故障时，其他服务器上的冗余虚拟机能够接管业务，例如，主备虚拟机和负荷分担虚拟机不能部署在同一块服务器单板上。

通信云要求支持虚拟机状态的检测和自愈功能。当虚拟化层检测到虚拟机故障或物理硬件故障时，需要能在本机恢复，或迁移至其他服务器上重生。支持控制节点的集群配置，在控制节点出现单点故障时能够及时切换，减少系统服务中断的时间，并且在控制节点发生异常并进行切换时，计算节点上运行的虚拟机不受影响。还应支持云系统配置数据以及数据库的定时自动及手工备份，保证在系统因硬件原因出现异常时，能够快速从备份的数据恢复正常运行。

2. 硬件可靠性

为了提供通信云的可靠性，组成通信云的硬件设备也必须有可靠性设计。

对于计算资源，要求机架、机框、服务器采用 N+M 冗余配置，电源/风扇采用 N+M 冗余配置，物理主机网卡 Bond，主备或负荷分担，BMC 支持开机和定时自检，对硬件进行主被动监视，并上报 PIM。服务器至少采用双网卡，主备或者负荷分担方式灵活进行配置，提高网络可靠性，当其中一块网卡故障，所有流量转移到另外一块网卡上处理。

对于存储资源，采用磁阵或分布式存储来实现。控制器、内置 SAS 交换等所有环节均采用冗余配置，磁盘采用 RAID 方式冗余。分布式存储支持 1+M 多副本方式，存储设备内置电池和监视模块，通过带外方式受 PIM 监视。存储资源需要配置多路径、冗余链路，防止单点故障，其中一块网卡或者链路故障，所有流量转移到另一条链路。存储设备必须为 APP 提供统一的云存储，替代本地磁盘，提升数据的可靠性。支持存储多路径访问、存储链路检测、及恢复后的路径自动补全；支持采用 1+1/1+M 多副本，提供数据的冗余保护。

对于网络资源，要求网络设备（包括 TOR，EOR，DC GW）采用 1+1 配置，采用设备 M-Lag 等技术组网，并采用多平面组网，在网络路径、接口、设备和路由上均采用负荷分担实现。网络设备需

要内置监视模块，通过带外方式受 PIM 监视。

（三）网络安全关键技术

5G 云化核心网处于可信域范围内，信息安全威胁较低。云化核心网产品采取可信的安全技术标准，将可信安全融入产品，构建可信安全网络架构，为云化环境中的核心网运行提供可信的安全保障。

1. 组网安全

VNF 内部平面包括管理面和控制面，采用 vNIC/VLAN/VXLAN 隔离。VNF 外部平面包括外部管理面、控制面、媒体面，采用 vNIC/VLAN/VXLAN/vRouter 隔离。

要求对网元进行必要的安全域划分，每个 NF 网元只能属于一个安全域，每个安全域分配专用的硬件资源池。用户安全域、接口服务安全域建议设置为非信任域，安全域之间访问要通过虚拟安全设备、防火墙等做防护。安全域内可根据网元种类、归属地区等划分子域。

通信云的资源池应提供 FW/VPN/WAF/IPS/IDS 等安全服务。针对 5G 网络中的 SBA 架构，部署 TLS 安全隧道传输保证信令面机密性与完整性。NF 与 NF 之间采用静态或动态授权认证，NF 与 NRF 之间静态或动态授权认证。NF 与 NRF 之间基于 Oauth2.0 授权认证，提高通信时的安全。

在漫游场景下，漫游运营商与归属运营商分别部署 SEPP，负责 HTTP 信令安全保护，拜访 SEPP 和归属 SEPP 之间采用静态配置，

网络内所有漫游相关 HTTP 信令均送往 SEPP。SEPP 实现网络拓扑隐藏，将 HTTP 信令中各 NF 的 FQDN 替换为 Telescopic FQDN，再转发至其他 PLMN。

根据部署场景方式不同，SEPP 可通过两种方式实现信令安全保护：通过 TLS 实现传输层安全加密传输，适用于 SEPP 间直连，无 IPX 转接场景；或者通过 ALS（ Application Layer Security ）实现应用层信令参数加密，适用于 SEPP 间通过 IPX 转接场景。

对于 5G 中的网络切片功能，要求支持分权分域，不同切片管理团队/合作伙伴/用户只能维护自已切片。对于共享网元，根据 Slice ID 提供 VNF 的隔离。切片之间采用资源隔离，包括基于 NFVI 提供物理隔离、逻辑隔离等。

2. MEC 安全

MEC 部署在网络的边缘，需要部署多维的安全防护手段。

应支持对物理网络设备认证防止非法链接。对各类物理口禁用，防止恶意接入和破坏。通过配置安全组、ACL 或部署虚拟防火墙对虚拟网络隔离，使用可信计算保证物理服务器的可信，实时监测虚拟资源的运行情况，检测恶意行为，并及时告警和隔离。支持对外数据流保密性和完整性，对相关交互的接口进行机密性、完整性和防重放的保护，支持对网元的配置数据及敏感信息（分流策略）进行加密存储。

平台的敏感数据应加密存储，禁止非授权访问。平台的 API 应进行认证和授权，与其它实体之间通信应进行相互认证。实现 APP 完整性验证、APP 之间隔离、资源 QOS/SLA 保证。MEC 编排管理系统从系统接入安全、账户、API 调用、ME APP 完整性校验、安全能力开放等方面进行安全防护。

3. 网络接入安全

3GPP 对 5G 网络认证做了要求，支持统一认证架构，提供用户和网络之间的双向认证，包括 EAP-AKA', 5G-AKA 认证。支持主流的加密和完整性保护算法，例如 AES, Snow 3G, ZUC。提供空口和 NAS 层信令的加密和完整性保护，按需提供空口和/或 UE 到核心网之间的用户面加密和完整性保护，支持层次化的密钥派生机制。

在无线网络与核心网之间 N2 接口支持从 RAN 到核心网的 IPSec 组网，可选择部署 DTLS，并启用 ACL 提升网络接入层面的安全性。提供机密性，完整性和防重放攻击保护。

N4 接口支持 IPSec 组网，提供机密性、完整性和防重放攻击保护。IPSec 实现 IP 地址绑定，只和配置的 IP 地址进行交互。

4. 数据安全

需要从终端、网络、业务提供商各个层面，对信息的请求、提交、传输、存储、处理、使用等操作，采用相应的技术和管理手段实现对关键数据的保护。需要严格定义每个网元处理业务所必须的信息，按

照定义对信息获取进行严格限制。

要求关键隐私数据和需要二次利用（大数据分析）的数据在网络传输中进行匿名替代。支持对数据进行加密传输，并进行完整性校验，防止窃听、篡改加密存储，对关键敏感数据进行加密存储。严格定义数据访问权限，防止非法访问、越权访问。

存储应采用数据增强技术，基于数据块来构建 RAID 组，使得数据均匀地分布到存储池的所有硬盘上，以数据块为单元来进行资源管理。删除虚拟机或删除数据卷，系统会进行资源回收，小数据块链表将被释放，进入资源池。存储资源重新利用时，再重新组织小数据块。通过这种方式防止重新分配的虚拟磁盘恢复原来的数据，有效做到剩余信息保护。

数据存储应采用多重备份机制，每一份数据都有一个或者多个备份，即使存储载体（如硬盘）出现了故障，也不会引起数据的丢失，同时也不会影响系统的正常使用。

系统对存储数据按位或字节的方式进行数据校验，并把数据校验信息均匀的分散到阵列的各个磁盘上。阵列的磁盘上既有数据，也有数据校验信息，但数据块和对应的校验信息存储于不同的磁盘上，当某个数据盘被损坏后，系统可以根据同一带区的其他数据块和对应的校验信息来重构损坏的数据。

5. 信令风暴预防

网络异常、发生故障可能会触发信令风暴，大量用户短时间内并发接入，由于设备处理能力无法及时处理而引发大量突发接入，此时会产生信令风暴，终端接入失败后会反复尝试接入，造成网络拥塞。

为了有效预防化解信令风暴，核心网需要采取源头控制的端到端流控方式，源端动态感知端到端能力，并依此适量放通用户，确保后端网元在能力范围内接纳用户，避免过载。要求数据网元 AMF/MME 以及语音网元 SBC 作为入口网元基于后端 UDM/HSS 网元能力联合部署端到端流控，建立防御信令风暴的坚实屏障。

网元的过载控制需要支持入向与出向的控制能力，可以基于 TPS、CPU 负荷、吞吐量、链路状态等对消息进行灵活的处理，保护本网元以及周边网元。

同时需要提供降质手段以保障基本业务，使得在紧急故障情况通过降低服务质量来保障基本网络业务，如发生网元级故障且无法容灾/无法恢复，可以提供对故障网元的旁路处理，临时采用本地策略或者惯性运行，等故障解决后，再解除旁路功能，恢复服务质量。

另外，熔断手段也是一种有效的手段，可以加快业务恢复，在故障已解决或隔离，但通过限流、降质等多种手段仍无法快速控制故障蔓延，可以考虑启用熔断机制，熔断冲击源（即终端 UE 和基站 NR）。

（四）5G 网络安全部署策略

1. 网元容灾

基础容灾及流控：具备虚机冗余机制、过载保护机制、抗雪崩能力、智能流控机制等安全能力。具备网元级池组、主备或互备能力，网元级抗信令冲击能力。5G 网元故障后可以在分钟级内快速完成容灾切换，尽量避免对业务的影响。

容灾热备：网元运行所需的数据，如用户数据、会话数据、NF 状态数据等实时备份，网元故障后备用网元迅速接管，会话不中断。

第三 DC 容灾：在大区双 DC 同城部署的现网条件下，全面论证跨大区容灾方案，规划适时引入跨大区容灾能力，提升大区级网络安全水平，避免双 DC 在战争、地震等极端自然灾害情况下同时故障带来的影响，保障用户及业务快速恢复。

2. 业务及数据逃生

1）基础设施故障逃生

存储故障 bypass：共享存储（共享磁阵或云存储）故障不影响业务正常运行。

管理面故障 bypass：管理面故障不影响业务正常运行。

网元 O&M 故障 bypass：保持网元功能惯性运行。

2）数据逃生

UDM 故障 bypass：UDM 资源池全故障，周边网元能够继续降

级业务，降级的含义是部分次要功能或可暂时不用的功能不可用，比如鉴权业务。该功能需要人工开启。

NRF 故障 bypass：NRF 资源池全故障，周边网元能够继续降级业务，周边网元本地缓存 NF 状态数据并进行下游 NF 故障探测。

PCF 故障 bypass：PCF 资源池全故障，周边网元能够继续降级业务，降级的含义是可会采用默认的承载 QoS 和流量配置策略。该功能需要人工开启。

NCG/CHF/OCS 故障 bypass：NCG/CHF/OCS 资源池全故障，周边网元能够业务降级继续处理，降级的含义是周边网元可以一段时间内缓存话单。

用户数据三方备份：用户数据三方备份，需要手工恢复数据。

3）业务逃生

新通话降级逃生：故障回落普通呼叫。

3. 亚健康恢复

1）网元 KPI 下降恢复能力

支持持续增加复杂故障场景（通信亚健康、资源异常、KPI 下降、多点故障等）恢复能力，在不需要新增数据和恢复操作条件下可以支持无码化发布恢复 UseCase。基础包已包括通信亚健康、CPU 异常的故障诊断、恢复。

2）电信云亚健康恢复能力

电信云恢复条件相比网元更严格，电信云恢复存在资源切换，业务网元业务可能短暂受损。支持持续增加复杂故障场景（通信亚健康、资源异常、多点故障等）恢复能力，基础包已包括通信亚健康、CPU 异常的故障诊断、恢复。

3）智能容灾辅助

倒换前评估容灾接管能力，判断容灾功能是否正常、是否有信令浪涌风险、接管后容量是否足够等。

4）浪涌仿真优化

产品支持配置静态出口流量阈值，通过浪涌仿真工具对现网局点进行浪涌仿真评估，优化各产品出口流量阈值，实现 30 分钟绝大部分用户能够上线，极少数行为异常用户需要等到周期性注册上线。

5）韧性评估服务

对现网网络进行风险评估并提出改进建议。包括不限于：组网合理性（避免故障单点等）；配置合理性（容灾倒换配置、浪涌流控参数配置等）；资源风险（关键资源占用率等）；运行状态风险（告警、Error 日志等）。

三、专网安全

（一）专网架构带来的安全风险

专网架构下边缘计算节点部署位置下沉，导致攻击者更容易接触到边缘计算节点硬件，攻击者可以通过非法连接访问网络端口，获取

传输数据，另外通过边缘节点可以进一步攻击大网，给企业和运营商带来安全风险。

对于企业，首先，专网用户由运营商管理，存在非本企业用户非法访问企业专网的风险，对此企业有用户接入专网进行二次鉴权的诉求，企业希望能自主控制用户专网访问的权限，另外为满足溯源的合规需求，需要能够关联用户访问日志到具体的人。其次，用户业务数据经过运营商网络，需要保障业务数据传输过程中的安全，防止数据泄露和篡改的风险。再者，运营商网络与企业网络存在对接关系，需要管控边界互相攻击的风险。

对于运营商，专网设备下沉部署，使得攻击者更容易接触边缘节点硬件，边缘节点安全暴露面扩大，安全风险增加。因此，首先需要做好机房安全和设备物理安全防护。其次，需要做好边界防护，进行安全域划分并进行跨域访问控制，再者，边缘设备需实现内生的安全，部署后需做好系统加固，对外接口使用安全协议，防止攻击者通过边缘节点进一步攻击大网。

行业对专网典型的安全诉求有，需要支持对用户接入专网进行可管、可控、可溯源。企业业务数据访问通道隔离，支持传输加密和完整性保护。

（二）专网安全解决方案

1. 专网用户接入安全方案

1)用户接入可管理

用户接入专网之前，除了进行 3GPP 标准的移动用户主认证之外，还需要支持专网的二次鉴权，通过在专网部署 DN-AAA 设备和安全网关，对用户访问专网的合法性进行管理。 二次鉴权流程中，可选支持验证用户的号码 MSISDN、设备号 IMEI、卡号 IMSI/SUPI, 以及接入位置等。基于用户的 IP 地址，可选支持 DN-AAA 与网关联动实现细粒度权限控制。

2)用户接入可控制

对于认证鉴权通过的用户，在识别到用户终端的异常时，支持强制终端用户下线，亦或者用户主动上报设备丢失等场景。

3)用户访问可溯源

用户的业务访问可通过 DPI 解析等方式记录日志,日志能够关联到具体的人，在用户终端动态获取 IP 情况下，不仅需要跟踪到终端 IP，还应支持通过终端 IP 关联到卡号或号码，进而关联到具体的人。

2. 专网传输通道安全方案

1)基站域安全

支持不同级别的无线切片隔离方案，如 5QI 软隔离，RB 资源预留硬隔离等。支持开启空口信令加密和完整性保护以及用户面数据加

密和完整性保护。

2)传输域安全

支持不同级别的传输隔离机制，如 VPN 软隔离，FlexE 硬隔离等。支持在基站与核心网用户面网元 UPF 之间的传输通道之上叠加启用 IPSec，保障传输通道的机密性，完整性以及防重放攻击。

3)核心网域安全

支持不同级别的切片隔离机制，支撑共享 UPF 或者专享 UPF 满足不同企业的网络隔离要求。同时支持网络分流机制，在满足用户灵活访问互联网和专网的同时，安全上保障专网访问通道与互联网访问通道的隔离。

支持通过 VPN，GRE 等专线技术与企业网络对接，支持叠加启用 IPSec 保障传输的机密性与完整性以及防重放攻击。

3. 专网边界安全方案

1)三面隔离

部署时，应支持管理面、控制面和用户面的传输通道隔离，建议实现物理通道隔离，当物理资源不足时，通过 VLAN（Virtual Local Area Network，虚拟局域网）实现逻辑隔离。三个平面不能相互访问，任何一个平面受到攻击不会影响其它平面，最小化攻击风险。应支持在管理面、控制面、用户面提供 ACL（Access Control List，访问控制列表）策略，拒绝来自非法地址或网络的访问，或只接受来

自信任地址或网络的访问，并对访问接口进行流控。

2)安全域隔离

构建专网网络时，运营商会部署接入网、核心网、传输网和操作维护网络等不同网络，也需要与企业网络 ，因此会存在不可控和不可预知的安全威胁。为了增强整个网络的安全性，在网络规划时需要根据每种网络的传输数据、业务、网络部署特点将其划分成不同的安全域，并在这些不同的安全域之间部署不同级别的安全策略。

在运营商与企业的边界应部署防火墙，设置不同安全域跨域访问的控制策略。

4. 专网设备自身安全

1)硬件安全

硬件服务器的本地串口、本地调试口、USB 接口等本地维护端口调试完成后应默认禁用，防止恶意攻击者的接入和破坏，对于所有开放的接口，应对任何试图接入该接口的用户或者通信对等端进行身份认证。对于不常用的端口应默认关闭，只有在需要使用的时候才打开，打开相应的端口应记录日志，并向网管上报告警事件。

机房安全：如果条件具备，边缘 UPF 所在机房可做一定的改造，应通过安全机柜、上锁、架设监控、定期巡检等人工手段保证其安全。

2)软件安全

产品开发过程应遵循业界最佳实践的安全开发流程，应通过权威

机构如 3GPP&GSMA 的 NESAS/SCAS 过程审计和产品安全测试。

产品发布前应进行安全加固(裁剪系统、移除冗余服务，关闭不使用端口及和最小化授权等)，病毒扫描，漏洞扫描；消除开源软件漏洞，减少攻击面，提升平台的安全性。

产品发布后应持续定期进行安全漏洞检测、扫描，通过安全补丁及时消除新漏洞。

3)业务安全

专用 UPF 具备上行流量防地址欺骗检查能力，若报文的源地址不是终端用户地址，融合设备丢弃该报文，并禁止将该报文转发出去。

专用 UPF 具备下行流量防地址欺诈能力，若目的地址与手机地址池不匹配，丢弃该下行流量。专用 UPF 具备对没有匹配 PDP 上下文/承载的下行流量执行丢弃的能力。专用 UPF 具备在转发移动用户分组数据流量时对数据流量进行 DDoS 攻击检测和过滤，防止恶意或者被控制的移动用户作为攻击源发起 DDoS 攻击。专用 UPF 具备禁止终端互访能力，需要互访时具备终端互访重定向到网关进行安全检测与防护的能力。

四、智能化网络安全体系

核心网是移动通信网络的中枢，负责整个网络的总体控制、管理和服务，积极探索 5G 核心网与 AI 的融合创新，实现网络智能化水平的提升，探索基于 AI 的网络智能化安全管理及检测，提升对核心

网性能和异常状态的实时感知和智能预测，有助于分析网络故障和安全隐患，从而提升核心网的健壮性和安全。

（一）5G 核心网智能化架构及演进

3GPP 在 Rel-15 阶段定义了核心网服务化网元网络数据分析功能 NWDAF 网元 (Network Data Analytics Function)，用于网络数据采集、网络数据分析，并可向其它网元提供分析结果和预测的建议。NWDAF 作为服务化网元，支持通过标准定义的服务化接口向 5G 核心网 NF、OAM 或 AF 进行事件订阅，以此获取分析所需要的原始数据。NWDAF 的分析结果信息可以反馈给 5G 核心网 NF 或 AF。当 NWDAF 的分析结果信息开放给 AF 时，需要通过网络开放功能网元 NEF 与 AF 进行交互。

3GPP 在 R16 阶段定义了基于单实例集中式的智能网络架构和能力，定义了完整的数据采集、数据分析、分析反馈架构和对应的网络流程，梳理了业务体验、网元负荷、网络性能、UE 移动性、UE 交互性、终端异常行为等场景和涉及的关键技术。

5G 核心网引入 NWDAF 后的智能化网络架构示意图如下：

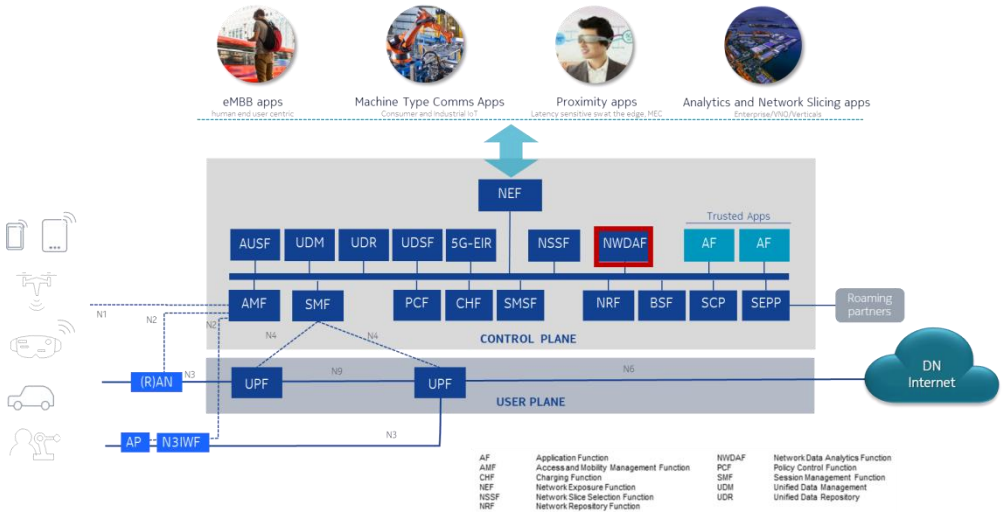

图 1 核心网引入 NWDAF 后的智能化网络架构示意图

3GPP 在 Rel-17 对智能网络架构进一步增强，包括 NWDAF 功能分解、数据采集效率提升、UE 数据采集、基于多实例分布式的智能网络架构和能力，梳理了业务分布情况分析、WLAN 性能、会话管理拥塞控制体验、DN 性能等更多的场景和涉及的关键技术。

NWDAF 功能分解如图 2，包括 DCCF(Data Collection and Coordination Function) 、 ADRF(Analytics Data Repository Function) 、 AnLF(Analytic Logical Function) 、 MTLF(Model Training Logical Function)等智能化网元，可为网络、业务、用户提供多样化的智能分析、训练和推理服务。

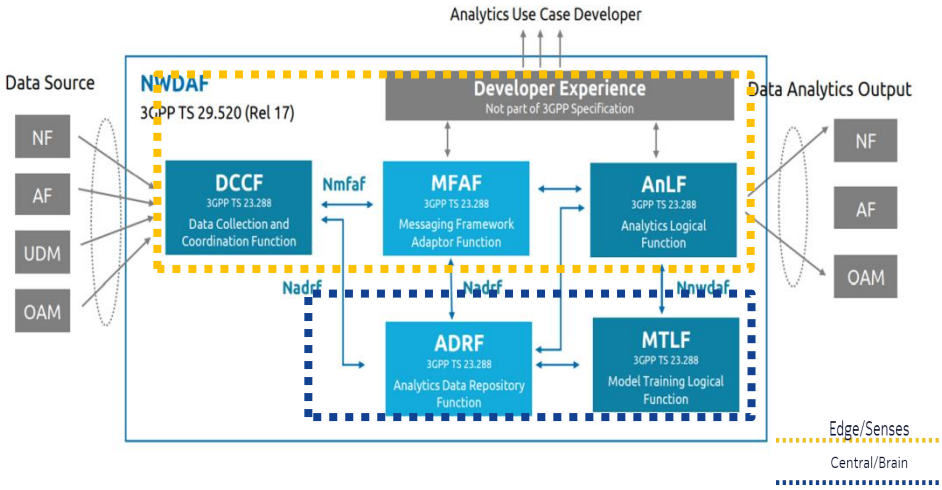

图 2 NWDAF 功能分解图

同时，NWDAF 支持多实例分布式部署，支持分离和聚合，支持集中和边缘部署。在同一网络中，多个 NWDAF 可以基于层级结构或树状结构进行部署，下级 NWDAF 可以和数据源 NF 合并部署或邻近部署，以实现快速实时性数据获取，而上级 NWDAF 汇总处理下级NWDAF的数据并生成总体的数据分析报告。或者多个NWDAF各自负责一片 NWDAF 服务区域，并将各自负责区域内的数据统一上报至上级 NWDAF，聚合生成针对更大管理区域的分析报告。

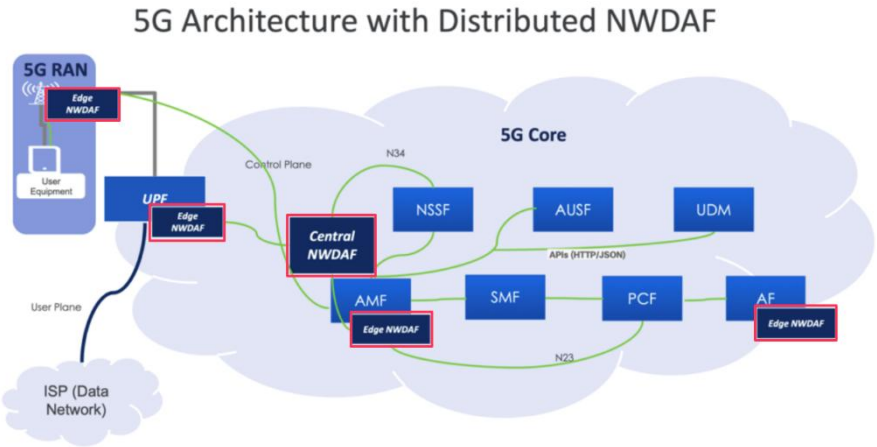

图 3 NWDAF 多实例分布式部署

3GPP R18 继续网络智能架构增强，包括如何缓解数据孤岛、漫游、网络优化策略推荐、网络部署建议等。

核心网引入分布式可信的人工智能技术，通过 3GPP 标准中制定的多 NWDAF 实例支持横向联邦学习的框架和能力，未来还将引入纵向联邦学习，跨域协同和跨层协同，跨域协同涉及 UE、RAN、CN、应用间数据、模型等共享和协同，跨层协同包括网元层与运维层协同，实现在保护数据隐私的前提下进行分布式训练，解决数据泄露、带宽短板等问题。

（二）5G 核心网智能化架构安全增强

随着 5G 网络智能化架构越来越复杂，网络的安全问题也会更多。一方面，需要关注网络智能化系统自身的安全，另一方面，对于网络数据的分析也可以包含对于安全数据的分析，分析结果反哺到网络中，对于提升网络的安全性有很大的帮助。

3GPP 引入 5G 核心网 AI 单元（NWDAF），现阶段已形成数据采集、训练、推理、闭环控制，以及支持多样化解决方案的网络大数据分析体系架构。作为 5G 网络自动化的核心网元目前 NWDAF 所需面临的安全问题与要求，并提供相应的解决方案，主要包括三方面关键问题：

1） NWDAF 从 UE 及网元收集数据时的安全保护，包括隐私保护，数据机密性保护，数据完整性保护，可访问性等。

2） NWDAF 及其相关功能支持检测的网络攻击和网元异常事件，特别是定义输入数据及输出结果。

3） NWDAF 实例间的数据及模型传输时的安全保护。

1．核心网智能化系统自身的安全

NWDAF 在设计、开发、测试阶段以及软件发布后都要考虑到安全问题。如用户身份的认证，基于角色的用户授权和访问控制，日志的管理等。NWDAF 也支持网络安全的功能措施，如 SBA 的安全，与 NWDAF 相关流量的隔离、数据的加密、流量的过滤等，针对 DDoS 攻击、MITM 攻击、IP 欺骗、端口扫描和数据包刺探等传统网络安全的防护，还有 OAM 的安全等。

NWDAF 收集网络中的各种数据进行机器学习，并输出相关的分析结果。训练和推理带来的安全问题也需要考虑。针对数据训练中存在的攻击（例如攻击者通过向模型的训练集中注入恶意样本，使得模型能够帮助攻击者完成预设的功能）、隐私攻击（攻击者在无法使用 AI 应用或者仅仅能调用 AI 服务的 API 时，推测相关信息）等，需要采用一些手段保证训练数据时的安全。而在推理过程中，如果不同的网络数据分析功能网元对于相同的数据输出了矛盾的结果，就有可能引起网络的 DoS 攻击，因此需要引入例如策略优先级、策略排序、元策略等策略冲突解决机制。

2. 利用 NWDAF 增强网络安全

5G 网络中有各类丰富的信息可以作为安全事件分析的宝贵数据源，NWDAF 可以有效利用这些数据实现网络安全智能化分析。例如，可以实现对网络内部异常行为进行检测分析，利用网络分析功能监控所有网元的行为，并在网元发生异常行为时报告异常。例如提高网络性能，通过 NWADF 提供有关特定区域的网络状态信息、网络资源使用情况等网络负荷统计或预测信息。例如提升用户体验，NWDAF 根据用户需求和业务场景提供个性化的 QoS 服务保障，提高用户满意度。也可以对外部网络攻击行为进行检测分析，核心网中的网元可以与 UE 合作，以收集相关数据作为输入，并将异常外部事件警报作为输出提供给网管或其他网元，以便对网络攻击风险进行缓解。

5G 标准中的网络自动化功能网元 NWDAF 的安全管理能力、安全策略制定和分发、自动化安全编排和调度机制等仍在不断研究和完善中。

3. NWDAF 在网络安全的应用场景举例

1）切片负荷分析

切片负荷分析(Slice Load Level Analytics)在 3GPP Rel-17 阶段完全定义。

NWDAF 在网络切片级别或网络切片实例级别或两者上向消费者 NF 提供切片负荷信息。NWDAF 不需要知道使用切片的当前订户。

NWDAF 将切片特定网络状态分析信息通知给订阅它的消费者 NF（例如 PCF、NSSF 或 AMF）。消费者 NF 可以直接从 NWDAF 收集切片特定网络状况分析信息。切片负荷的分析结果可以应用到网络切片的规划、部署、监控、优化的各个环节中，及时的调整切片资源分配。

2）服务体验的分析

服务体验的分析(Observed Service Experience Analytics)在 3GPP Rel-16 阶段定义。

NWDAF 可以提供观察服务体验的分析。例如，每个 UE 或 UE 组单独地，或者全局地，每个应用平均或者在网络切片上的一组应用上平均。服务消费者可以是 NF（例如 PCF、NSSF、AMF、NEF）、AF 或 OAM。

NWDAF 对服务体验的分析和预测，可以用于包括视听流以及非视听流等业务（如 V2X 和 Web 浏览服务）。

3）网元负荷的分析

网元负荷的分析(NF Load Analytics)在 3GPP Rel-16 定义。

NWDAF 可以统计或预测或两者兼有的形式把 NF 负荷提供给另一个 NF。输出诸如网元状态、网元资源使用、网元负荷、网元峰值负荷、指定区域的网元负荷等信息。服务消费者可以是 NF 或 OAM。

通过持续的采集监测和数据训练负荷分析还可以实现长期和短

期的预测模型输出提供给边缘或外部系统。

4）网络性能的分析

网络性能的分析(Network Performance Analytics)在 3GPP Rel-16 阶段定义。

通过网络性能分析，NWDAF 可以提供所选区域中 gNB 状态信息、gNB 资源使用情况、通信性能和移动性能的统计或预测（如 PUD session，HO 等）。此外，NWDAF 可以提供该区域中的 UE 的数量的统计或预测。

服务消费者可以是 NF（例如 PCF、NEF、AF）或 OAM。

5）UE 相关分析及网络异常行为分析

UE 相关的分析(UE related Analytics)在 3GPP Rel-16 阶段定义，并在 Rel-17 阶段增强和新增。

NWDAF 可以提供 UE 移动性的分析(UE mobility analytics)、UE 通信的分析（UE communication analytics）、预期 UE 行为参数分析（Expected UE behavioural parameters related network data analytics）、与异常行为相关的网络数据分析(Abnormal behaviour related network data analytics)、数据量分散/交易分散分析(Data volume dispersion /Transaction dispersion analytics)。

在符合国家的用户数据安全相关的法律法规和用户隐私的前提下，根据用户或客户需求，5G 核心网可以合理智能的分析利用这些

数据，来优化业务传输，提升网络资源利用率，还能通过 UE 行为分析及预测，大大提升用户体验。

例如，异常行为分析（abnormal behaviour analytics）可以对网络内部异常网元行为进行检测分析。5GC 支持分布式网元部署，以便网元从多个位置和多个执行实例提供服务。当这些网元分布在不同的云基础设施中时，网元可能会以未定义的方式运行。网元的未定义行为可能是由内部错误引起的，例如配置错误或内部数据损坏。根据网元的类型，这种不当行为可能会影响一个或多个 UE 的服务。在这种情况下，网络分析功能必须监控所有网元的行为并确保其行为符合定义，并在网元发生异常行为时报告异常。

侦测事件包括：UE 位置异常、乒乓切换、超大流量会话、异常唤醒、疑似 DDoS 攻击、异常目的地址、超频服务请求、异常 UE 空口断联等。

NWDAF 服务用于向消费者 NF（例如 PCF、SMF、AF 或 AMF）公开来自 NWDAF 的网元或 UE 异常行为的分析报告或告警。

6）网络拥塞的分析

用户数据拥塞的分析(User Data Congestion Analytics)在 3GPP Rel-16 阶段定义。会话管理拥塞控制体验分析(Session Mgmt Congestion Control Experience Analytics)在 3GPP Rel-17 阶段定义。

NWDAF 可以通过一次性报告或连续报告,以统计或预测或两者兼有的形式，向另一个 NF 提供与用户数据拥塞相关的分析。服务消费者可以是 NF（例如，NEF、AF、PCF）。

5G 核心网可实时采集用户在当前位置中经历的网络拥塞状态，并基于网络的历史负荷情况,通过机器学习预测网络拥塞的时间和等级,将预测的拥塞信息输出给策略控制功能用于调整特定用户和业务的 QoS 策略。除此以外，5GC 还可实时采集小区级别的负荷信息，进行小区级别的拥塞判断和预测，并将网络拥塞状态上报给 AF，指导 AF 进行业务层面的调整。

基于 5GC 的智能拥塞管控可充分实现对网络拥塞状况实时感知和智能预测，提升用户的业务体验，提高网络资源调度水平。

7）QoS 预测及可保持性分析

QoS 预测及可保持性分析(QoS Sustainability Analytics)在 3GPP Rel-16 阶段定义。

5G 网络的智能化分析网元通过采集网络特定时间或位置区域的 QoS 变化的历史信息,可以分析得到包括带宽,误码率等在内的 QoS 参数或性能的预测结果，或者特定的 QoS 参数是否超过了上报的门限值。该预测结果也可以针对未来特定的一段时间或者特定的位置区域。服务消费者可以是 NF（例如 AF）。

8）冗余传输体验分析

冗余传输体验相关的分析（Redundant Transmission Experience）在 3GPP Rel-17 阶段定义。

这些分析可由 SMF 确定是否应在 N3/N9 接口上执行冗余传输，或者（如果已激活）是否应停止；或由 PCF 计算冗余 PDU 会话的 URSP 规则中的路由选择组件。

服务消费者可以是 NF（例如 SMF、PCF）。

9）DN 性能分析

DN 性能分析(DN performance analytics)在 3GPP R17 定义。

NWDAF 可以提供 DN 性能分析，该分析以统计或预测的形式向服务消费者提供用户平面性能分析（即平均/最大流量率、平均/最大数据包延迟、平均数据包丢失率）。

DN 性能分析可以提供以下一个或多个信息的组合：

1）针对特定服务锚 UPF 上的 UE、UE 组或任何 UE 的特定边缘计算应用程序的用户平面性能分析。

2）针对特定 DNAI 上的 UE、UE 组或任何 UE 的特定边缘计算应用程序的用户平面性能分析。

3）针对特定边缘应用服务器实例上的 UE、UE 组或任何 UE 的特定边缘计算应用的用户平面性能分析。

服务消费者可以是 NF（例如，SMF）或 AF。

随着标准的演进以及 5G 智能化的推进，会有更多新的智能化、

联邦学习与网络健壮性和安全相结合的应用场景。

（三）网络能力开放安全架构

本白皮书重点讨论网络能力的开放安全(Network APIs)，针对3GPP 定义的标准能力开放架构 CAPIF 和安全。TMForum 的运营能力的开放(Operations API)侧重在 OSS/BSS/OCS 等 IT 流程 API 触发，不在本白皮书范围。此外，5G 网络安全能力的对外开放，建议通过能力开放平台实现。

随着 5G 与千行百业的结合不断深入，网络能力开放的业务场景不断涌现，网络软件化、网络服务化(NaaS)和网络代码化(NaC)推动网络和智能化分析挖掘出的各种价值数据给第三方，赋能行业和数字应用生态，随之而来的网络安全挑战，如何实现用户信息的脱敏，满足用户隐私、数据安全和合规等要求，如何在开展网络能力开放的过程中充分保障网络和第三方应用的安全，已成为运营商重点关注的问题。

3GPP 在 R15 标准中定义了通用 API 框架（Common API Framework，CAPIF），对 5G SA 网络中的能力开放架构和流程进行了规定，并在 R16/R17/R18 中对网络能力开放架构及安全进行了加强。

CAPIF 是 3GPP 定义的标准能力开放架构，可以视为 5G 网络能力开放的基石，其功能架构如下图所示。

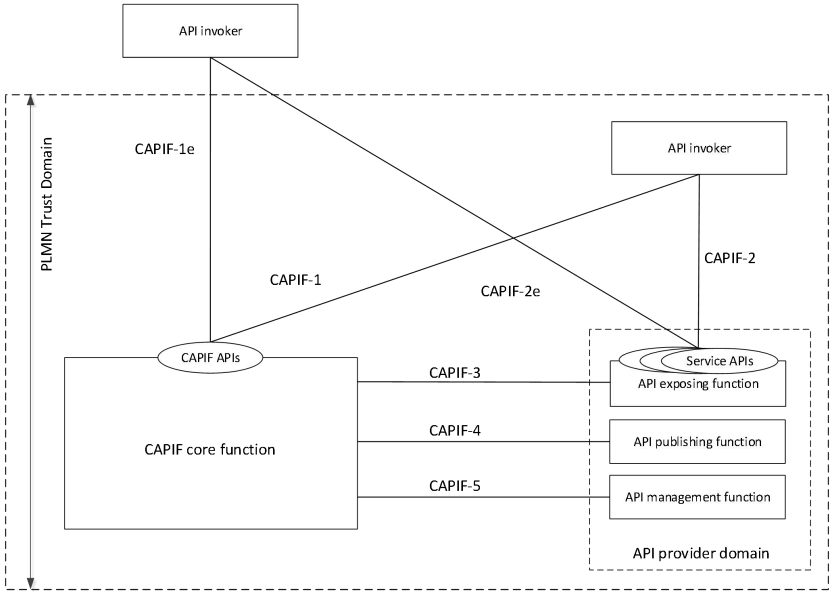

图 4 CAPIF 架构

API 使用者（API Invoker）是需要调用 5G 网络能力的第三方应用程序，可以在 PLMN 可信域域内，也可以在域外。属于 5G 核心网内部功能实体的包括CAPIF 核心功能(CAPIF Core Function)、API 开放功能（API Exposing Function）、API 发布功能（API Publishing Function）和 API 管理功能（API Management Function）这 4 个功能实体。在实际部署时，这 4 个功能实体可以根据网络情况和实际需求进行合设或者分设，例如可以选择将这 4 个功能实体合设并体现为网络开放功能（Network Exposure Function，NEF），也可以将 CAPIF 核心功能单独设置，并将其他 3 个功能实体合设为 NEF。

因为 CAPIF 架构肩负着对可信域外的第三方应用开放网络功能的职责，其安全防护的重要性也格外突出。针对 CAPIF 功能架构，

3GPP 定义的安全架构如下图所示。

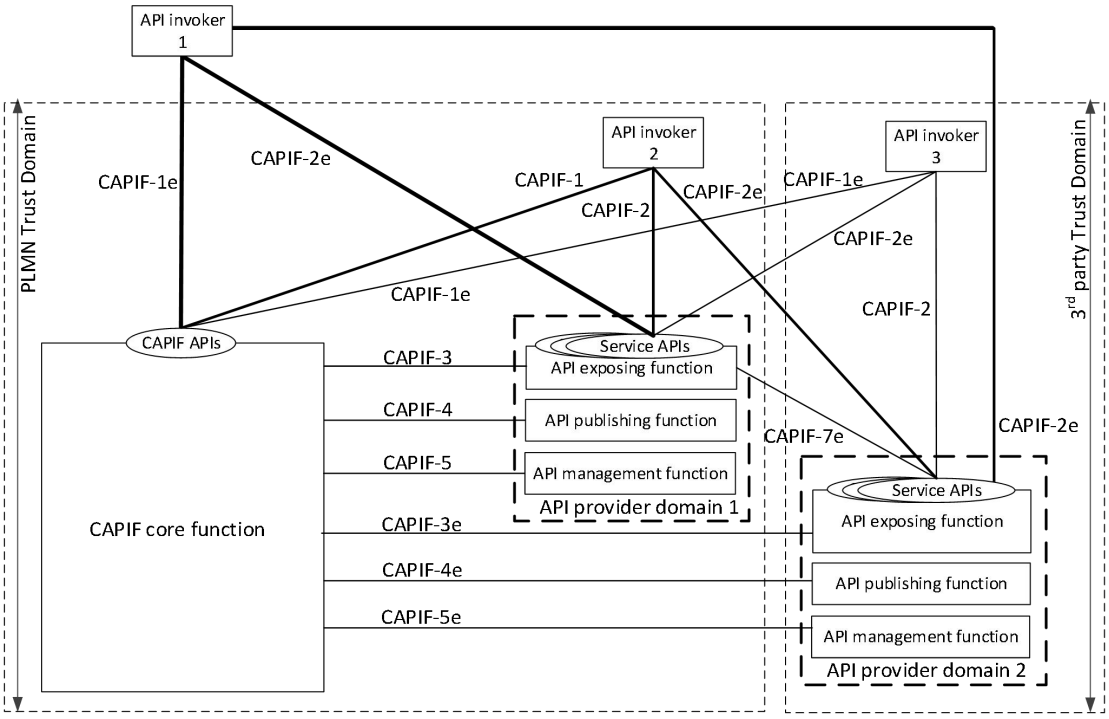

图 5 CAPIF 安全架构

CAPIF 安全架构涉及的接口众多，总体上可以分为两类：可信域内通信接口和可信域外通信接口，前者包括 CAPIF-1/2/3/4/5/7 接口，后者包括 CAPIF-1e/2e/3e/4e/5e/7e 接口。针对这些接口，其总体安全要求包括支持双向认证、消息传递需保证完整性和保密性、需保证通信中的用户隐私。

这些接口采用的协议都是 HTTPS/HTTP，CAPIF-1/2/3/4/5/7 接口的安全性强制支持传输层安全性协议 TLS（Transport Layer Security）。 CAPIF-3e/4e/5e 接口的安全性支持 NDS/IP 安全性，

以确保不同 IP 安全域之间的通信安全。通过利用规定的 NDS/IP 安全程序，避免了 API 提供域和 CAPIF 核心域之间的多个安全连接。

运营商在进行 5G 网络能力开放部署时，可能会选择将 CAPIF 中的 API 开放功能、API 发布功能和 API 管理功能合设为 NEF，作为 5G 核心网对外提供开放 API 的统一入口。同时，部署 5G 网络能力开放平台，作为运营商向外部第三方应用开放网络能力的统一门户。

该部署方案下，NEF 只需要与运营商网络内的能力开放平台进行对接，实现 API 开放。这样 CAPIF 的众多接口被收敛为 NEF 与能力开放平台之间的一个接口，因为该接口同处于运营商内部网络，接口安全可控度更高。而 API 使用者也是与能力开放平台对接，完成 5G 网络能力的调用。能力开放平台作为 IT 平台，在向外部 API 调用者开放能力时，可以更灵活地采用目前最先进的安全防护方案（例如在 3GPP 定义的安全策略之外增加安全网关等更多防护设备），实现更全面完善的安全防护能力。

随着标准的推进以及 5G 网络能力开放的不断发展，新的架构、接口和流程将不断出现，网络的服务化、代码化、软件化，能力开放的互联互通和漫游(GSMA 在 2023 MWC 发布了 Open Gateway 倡议，提出通用网络 API 框架)等也将带来新的安全挑战和防护需求，能力开放的安全也需要不断演进，以满足各种场景下的安全防护需求。

此外，为了帮助第三方应用更好地构建业务安全能力，5G 网络

除了可以提供开放的业务能力之外，还可以提供开放的安全服务能力。应用场景包括：运营商向第三方应用提供安全服务，如接入认证、授权控制、网络防御等服务，或者第三方应用通过对被授权的切片进行管理从而实现对网络安全能力的配置与调整。

5G 网络安全能力可以通过能力开放接口提供给第三方，以便第三方按照自身需求编排定制化网络安全服务。5G 网络可以建立独立于设备和应用的安全资源和能力，也可通过将安全能力进行抽象、封装，并结合其它网络能力和资源，动态按需组合，第三方行业应用可根据各自的安全需求，通过能力开放平台，灵活使用运营商网络的安全能力和安全资源，实现订制化的安全防护。

面向 6G 智能核心网，要构建定性高稳能力，实现自治网络，需要采用 AI 技术，即 NET4AI。关于自治网络，对于确定性网络需要结合模型驱动+数据驱动，前者提供闭环控制能力，后者提升故障感知能力。NET4AI 将实现网络高稳的确定性，故障后系统自己用“应急药箱”避免故障扩散甚至实现自愈，运维人员可以按部就班地进行善后修复处理，打造让客户放心的网络。

五、未来网络内生安全架构

未来核心网面临新业务、新架构、新模式等变化及演进所带来的新的安全风险及挑战，现有 3GPP 标准定义了网元安全配置及网元间互联互通安全，网元遵循标准要求实现相关安全能力。但随着网络暴露面增加、新型攻击手段不断演进，攻击者可以绕过传统边界防护设备，达到攻击网元的目的，甚至控制整个网络，现有传统边界防护设备已难以建立有效防护，已无法保障通信基础设施安全，网元成为最后一道防线。因此应通过在系统内构筑入侵检测能力来提升网络自身预防风险、发现入侵、响应恢复等安全韧性能力。

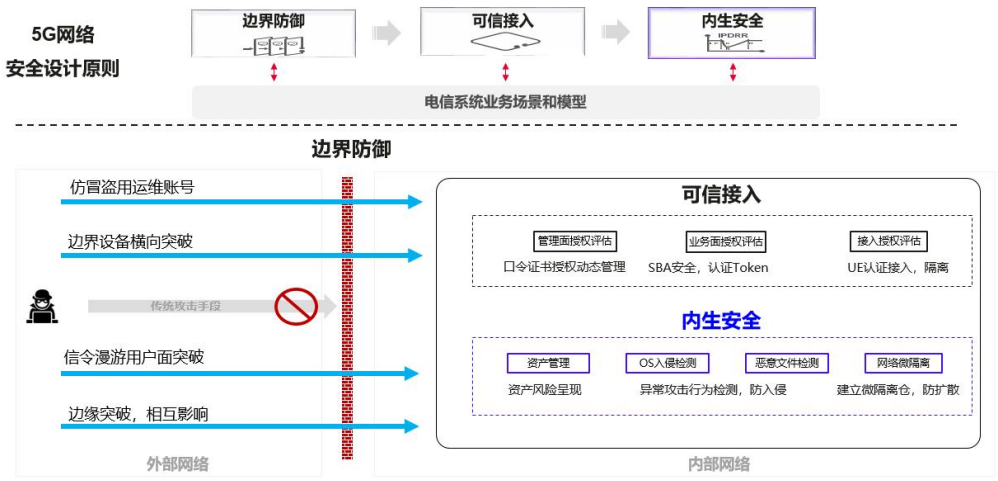

图 6 未来网络内生安全架构

未来核心网内生安全是将网络安全能力与网络设备融合内生，使得核心网设备具备“自主免疫力”，让核心网端到端网络环境具有更强健的“肌体”，从而能增强网络韧性，提高核心网网络抗攻击能力。通过提供资产管理、入侵检测、恶意文件检测和微隔离等功能，与传

统边界防护设备协同配合应对核心网面临的高级威胁。关键技术包括：

（1）内生安全资产管理，全栈资产可视可管：基于核心网业务拓扑开展全量资产采集。分钟级上报异常资产，资产变化自动同步。

（2）内生安全入侵检测，精准感知攻击行为：基于对核心网场景攻击知识库的积累，将安全风险与业务关联分析。通过高可靠、低开销的数据采集机制，结合白名单基线准确发现可疑行为，有效应对未知威胁。

（3）内生安全微隔离，准确限制风险扩散：基于对核心网业务理解，可视化拓扑呈现攻击风险，并构建业务视角的细粒度访问控制体系。实时感知业务变化，安全随行业务。基于通信白名单在极低开销下准确识别与处置风险扩散。

（4）内生安全高可靠，低开销，对网元业务无影响：充分考虑可靠性设计、CPU/内存开销设计、支持优雅降级，基于核心网确定性的运行机理可信构建白名单基线并全量预置，确保对业务零影响。

5G-A/6G 核心网内生安全通过检测、响应、处置、监控的闭环过程，对网络中潜在的安全风险和弱点进行发现、预警、定位和快速处置，保障 5G-A/6G 核心网网络安全运行。

未来5G-A/6G核心网内生安全相对比传统外挂式安全软件主要优势有：

（1）内生安全以电信业务模型库为基础，基于电信领域的确定

性知识，构建确定性的白名单和行为基线，提供全面精准的检测能力。

（2）内生安全可以在系统内部实时检测和响应威胁。通过使用内部的监控和分析工具，可以快速发现异常行为并采取相应措施，从而降低潜在风险造成的损害。

（3）内生安全是基于电信业务开发的安全能力，具备和业务模块相同的可靠性，对电信业务模块的运行不会造成影响。

（4）内生安全将安全机制融入整个系统中，为系统提供综合性保护，使系统能够自我保护并防御潜在攻击，可以有效减少潜在威胁造成的风险和损失，同时减少了对外部组件的依赖、配置和更新，并可随着系统的演进和升级而持续改进和更新，易于维护管理的同时提高系统的可靠性。

综上所述，内生安全将提供更全面、实时、高效和持续的保护，减少对外部组件的依赖性，成为系统安全的重要策略。同时，内生安全也需要在设计阶段充分考虑并且不断更新，以应对日益复杂和多样化的威胁。

六、总结及展望

随着网络架构的复杂性和数据流量的快速增长，网络安全问题日益突出。核心网作为网络的中枢，其安全性直接关系到整个网络系统的稳定运行和用户数据的安全。因此，采用一系列安全技术来保障核心网的安全性和可靠性，是确保 5G 业务发展的关键。

在未来，随着技术的不断进步和网络架构的不断完善，核心网安全架构将面临更多的机遇和挑战。我们可以期待更多智能化技术在核心网安全架构中的应用，如更高效的威胁检测、更精准的攻击防御等。随着网络安全问题的不断演变和复杂化，我们需要不断研发新的安全技术来应对新的挑战。未来，我们可以期待在加密技术、身份认证技术、访问控制技术等方面有更多的创新和突破。同时，智能化技术可能会带来新的安全风险点，如数据泄露、隐私侵犯等，需要我们进一步关注和研究。除了技术层面的创新外，我们还需要建立完善的安全治理体系来确保核心网的安全。这包括制定严格的安全管理制度、加强安全培训和意识教育、建立快速响应机制等方面。总之，采用一系列安全技术来保障核心网的安全性和可靠性，是确保 5G 业务发展的关键。

缩略语

缩写	英文全称	中文名称
3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
5G	5th Generation Mobile Communication Technology	第五代移动通信技术
AI	Artificial Intelligence	人工智能
BMC	Baseboard Management Controller	板级管理控制器
ADRF	Analytics Data Repository Function	分析数据存储功能
AnLF	Analytics Logical Function	分析逻辑功能
CAPIF	Common API Framework	通用 API 框架
DCCF	Data Collection and Coordination Function	数据采集和协调功能
HTTP	Hypertext Transfer Protocol	超文本传输协议
MTLF	Model Training Logical Function	模型训练逻辑功能
NRF	Network Repository Function	网络知识库功能
NWDAF	Network Data Analytics Function	网络数据分析功能
QoS	Quality of Service	服务质量
PDU	Packet Data Unit	报文数据单元
RAN	Radio Access Network	无线接入网
TLS	Transport Layer Security	传输层安全性协议
UE	User Equipment	用户设备
UPF	User Plane Function	用户平面功能
MITM	Man-in-the-MiddleAttack	中间人攻击
DDoS	Distributed Denial of Service	分布式阻断服务
RAID	Redundant Array of Independent Disks	独立硬盘冗余阵列

中国联通研究院是根植于联通集团（中国联通直属二级机构），服务于国家战略、行业发展、企业生产的战略决策参谋者、技术发展引领者、产业发展助推者，是原创技术策源地主力军和数字技术融合创新排头兵。联通研究院以做深大联接、做强大计算、做活大数据、做优大应用、做精大安全为己任，按照4+1+X研发布局，开展面向CUBE-Net 3.0新一代网络、大数据赋能运营、端网边业协同创新、网络与信息安全等方向的前沿技术研发，承担高质量决策报告研究和专精特新核心技术攻关，致力于成为服务国家发展的高端智库、代表行业产业的发言人、助推数字化转型的参谋部，多方位参与网络强国、数字中国、智慧社会建设。联通研究院现有员工近700人，平均年龄36岁，85%以上为硕士、博士研究生，以“三度三有”企业文化为根基，发展成为一支高素质、高活力、专业化、具有行业影响力的人才队伍。

战略决策的参谋者
技术发展的引领者
产业发展的助推者

态度、速度、气度

有情怀、有格局、有担当

中国联合网络通信有限公司研究院
地址：北京市亦庄经济技术开发区北环东路1号
电话：010-87926100
邮编：100176

中国联通研究院

中国联通泛终端技术