特殊行业5G独立专网安全需求及解决方案研究

Research on Security Requirements and Solutions for 5G Independent Private Networks in Special Industries

薛龙来，李　轲，许长峰，王殿亮（河南省信息咨询设计研究有限公司，河南 郑州 450000）
Xue Longlai, Li Ke, Xu Changfeng, Wang Dianliang (Henan Province Information Consultion Designing Research Co., Ltd., Zhengzhou 450000, China)

摘　要：
通过分析5G独立专网的安全需求，提出从整体网络安全架构、核心网安全、终端接入安全、数据安全、边界安全、安全审计等方面对特殊行业的5G独立专网安全解决方案进行研究与设计。该安全解决方案可进一步为运营商建设的园区5G独立专网提供安全、可靠的保障，并根据客户需求及安全隔离等级提供合理的网元下沉方案，使得投资效益、维护管理效益、信息安全保障都有所提高。

关键词：
核心网；高可靠组网；信息安全保障
doi：10.12045/j.issn.1007-3043.2025.02.008
文章编号：1007-3043（2025）02-0042-06
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:
By analyzing the security requirements of 5G independent private networks, it proposes to research and design 5G independent private network security solutions for special industries from the aspects of overall network security architecture, core network security, terminal access security, data security, boundary security, and security auditing. This security solution further provides secure and reliable guarantees for 5G independent private networks built by operators in industrial parks, and provides reasonable network element sinking solutions according to customer needs and security isolation levels, which improves investment efficiency, maintenance management efficiency, and information security protection.

Keywords:
Core network; High reliability networking; Information security guarantee

引用格式：薛龙来，李轲，许长峰，等. 特殊行业5G独立专网安全需求及解决方案研究[J]. 邮电设计技术，2025(2)：42-47.

0 引言

随着5G行业应用的推广，对于低时延、大带宽业务的需求逐步增多，核心网UPF、AMF等网元的下沉部署也将增加，如何根据客户需求及安全隔离等级提供合理的网元下沉方案将是专网研究讨论的焦点，这既需要考虑投资、维护管理效益，还要兼顾信息安全。5G专网面临的安全风险主要包括终端接入安全风险、网络链路安全风险、边缘计算MEC安全风险、边界安全风险和运维管理安全风险等。本文以某园区为例，重点研究5G独立专网安全部署与解决方案，运营商通过该方案为园区5G独立专网提供安全专用的5G通信管道，实现终端接入的安全认证和控制，提供边界安全保护、数据不出园区保护和网络安全韧性保护。

收稿日期：2024-12-12

1 5G独立专网安全技术保障措施

5G独立专网的安全需求一般较高，需要重点关注专网本身的安全能力，并结合行业用户的增强安全需求，提供定制化高可靠性的安全能力[1]。

1.1 终端接入控制

通过加入二次身份认证、双向鉴权、接入控制等机制，保障终端接入安全。在核心网认证的基础上，

通过AAA（Authentication、Authorization、Accounting）服务器，对接入终端进行增强的二次认证；通过5G AKA（Authentication and Key Agreement）为归属网络提供访问网络成功认证UE的证据，防止仿冒终端接入5G网络；通过封闭接入组（CAG）技术，限制特定物理区域内的合法终端接入专网。特别是，针对安全等级很高的专网用户，可通过专用SIM卡、定制化核心网与认证算法，确保终端接入与数据安全。

1.2 边界防护

在MEC安全防护方面，可通过安全即服务方式防护APP，通过网络审计/访问控制等手段实现流量出园及时告警。在基站和MEC间部署防火墙进行网络隔离，防止外网攻击，并基于UE IP保护防止恶意报文；在无线回传、基站共享等场景部署防火墙。在5GC、网络管理系统（NMS）和MEC间部署防火墙，启用IPSec保护，防止外网攻击以及信令或网管指令被非法篡改。防火墙可启用智能分析特性，以判断MEC节点的业务数据出园情况。同时，在MEC上APP边界防护方面，结合MEC云平台安全能力虚拟私有云（VPC）与虚拟局域网（VLAN）隔离技术，部署防火墙，防止不同APP之间的横向攻击。

在网络边界防护方面，通过构建隔离区（DMZ）提供边界防护，并在DMZ设置安全服务区，放置二次认证AAA、日志管理/态势感知系统等，在N6出口部署安全网关设备，结合二次认证AAA，实现基于角色的细粒度访问控制（RBAC）。

1.3 安全管理

针对安全运营和服务保障，构建5G网络的安全运维管理能力，确保园区5G专网的运维安全。通过堡垒机进行运维、记录和审计，对运维管理流量进行加密，对管理面所有运维活动日志进行审计与态势感知。配备虚机和容器层面的安全监测机制，在发现异常时可对虚机/容器进行隔离，并快速拉起新的虚机/容器，确保业务正常运行[2]。

2 5G独立专网安全需求及风险控制概述

5G网络终端使用SIM卡接入，具有很大的移动性，而对于园区自身来说，空口接入的完全本地化在园区还不常见，业务数据流甚至存储在运营商机房。园区的关键网络安全需求主要是确保园区终端和园区应用的安全，避免因网络安全问题造成业务中断和信息泄露。特殊行业园区5G独立专网的安全网络架构如图1所示。

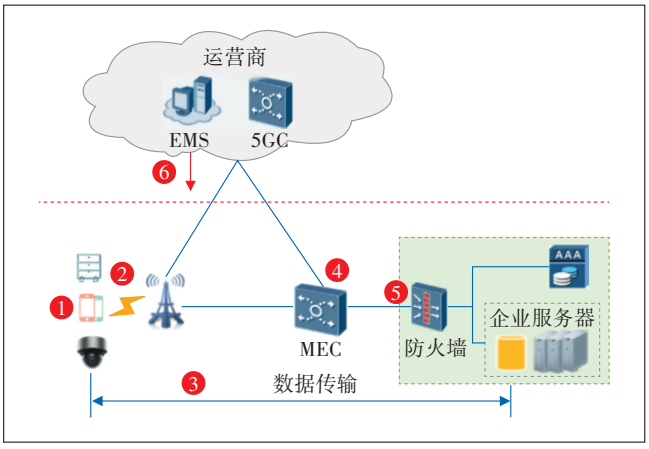

图1　园区安全网络架构

2.1 安全需求分析

园区安全需求及可能存在的安全风险及风险降低方案如表1所示。

表1　安全风险及降低方案

风险点	风险及影响	风险降低方案	可能性
1	非授权的SIM卡接入5G网络，攻击网络应用	5G网络对接入的终端进行身份认证	低
2	非授权终端滥用合法SIM卡接入5G网络	核心网及AAA对终端进行身份认证	中
	合法终端通过空口接入外部恶意网络	限制合法终端接入5G网络的地理位置	低
	终端业务数据通过空口泄露	空口信令和敏感业务数据空口加密	中
3	业务数据在5G网络中未加密，存在泄露风险	端到端业务数据加密传输	低
4	敏感业务数据通过MEC流出企业园区	边缘防火墙限制并监控MEC出园流量类型	低
5	外部攻击以MEC为跳板攻击园区内部网络	MEC到内网的流量需通过边界防火墙，边界入侵防御	低
6	通过运营商网管O&M入侵边缘节点，从而攻击园区内部网络	园区内部网络边界部署防火墙或IPSec进行入侵防御	低

2.2 安全架构设计

根据行业应用园区的安全需求以及典型业务场景分析和合规要求，5G端到端安全主要包括终端接入安全、数据安全、边界安全和安全审计四大部分。

a）终端接入安全。提供5G终端接入的网络准入和访问控制能力，多重的接入控制确保只有合法的终端才能接入园区5G网络。

b）数据安全。基于园区数据不离岸的原则，方案从组网和设计上保证了业务数据的安全，并通过E2E

加密等手段做到数据不泄露。

c）边界安全。确保MEC边界都做好隔离措施，运营商和园区内网边界隔离。

d）安全审计。留存一定时间段内的信令发送和后台运维等通信记录，对网络通信行为进行审计，做到事后可回溯。

3 特殊行业园区5G独立专网安全设计

3.1 园区5G专网整体架构及典型工作流程

某一园区为特殊行业应用，其5G专网主要应用为AGV小车物流系统、工业互联网数据采集分析处理等系统，由于该园区的特殊性，要求用户面数据和控制面数据均不出园区，且要满足长时间断连独立运行，对5G专网安全隔离度要求很高。图2为该园区5G网络结构以及终端认证信令流和业务数据流。

插有SIM卡的5G终端首先向5G网络发起注册流程（图2中红色虚线），完成注册后，5G终端接入到5G网络并发起建立用户面承载连接，以便使用数据业务。在网络为终端分配IP地址，并且建立终端与核心网相连的外部网络的专用通道后，5G终端可使用该IP地址访问外部网络上的业务。

用户面承载建立流程为：5G终端向核心网控制面发送用户面承载建立请求（图2中紫色虚线），并将终端签约的DNN（用来标识移动用户要使用的外部网络）发送给核心网控制面，控制面根据用户签约的DNN选择对应的用户面网元UPF，核心网控制面为用户分配IP地址，然后将用户的IP地址等相关信息发送给指定的用户面网元UPF、基站以及终端，UPF和基站侧建立起承载该用户的上下行专用隧道，最终完成端到端的用户面承载通道的建立（图2中绿色虚线）。

3.2 园区无线覆盖及接入保护解决方案

3.2.1 通过小功率设备精细化覆盖控制室分外泄

园区采用5G数字化室分，无线信号从pRRU发射，每个pRRU最大发射功率仅为250 mW，且发射功率可根据需求进行个性化调整，从而实现精细化覆盖，不会出现室内信号源泄露的情况。

3.2.2 通过接入电平控制限制边缘用户接入

数字化室分可通过定制最低接收电平（Minimum-RxLevel）来限制覆盖区域外边缘用户的接入。组网完成后，可通过对覆盖需求区域现场信号的测试获取MinimumRxLevel阈值，然后通过调整MinimumRxLevel来限制覆盖需求区以外的用户接入。

3.2.3 通过切换参数控制禁止外部用户切入

通过禁止切换（NoHoFlag）可控制外部用户向数字化室分进行切入，通过限制周边网络的移动性，保障数字化室分用户的安全。

3.2.4 通过物理扫频模式排查无线环境干扰

通过专业的5G扫频仪设备，可定期对指定范围内无线环境进行频谱监控，结合用户区域的5G基站工作频段干扰监控波形图，对比5G扫频仪测量到的干扰波形，确定无线环境干扰来源。

3.3 园区核心网方案

独立5GC本地主用方案，即核心网全量下沉和传输下沉。核心网全量下沉方案如图3所示[3-4]。

该方案部署2套下沉式5GC，在本地做主备，平日主用园区本地的5GC设备，最大程度不依赖大网。园区UDM需要定期与大网保持联系，用于数据同步以及版本升级。方案将用户数据业务局限在园区，取消进出园区互操作等业务能力。UPF用于实现用户面的数据分流能力，控制面使用园区本地AMF/SMF，本地数

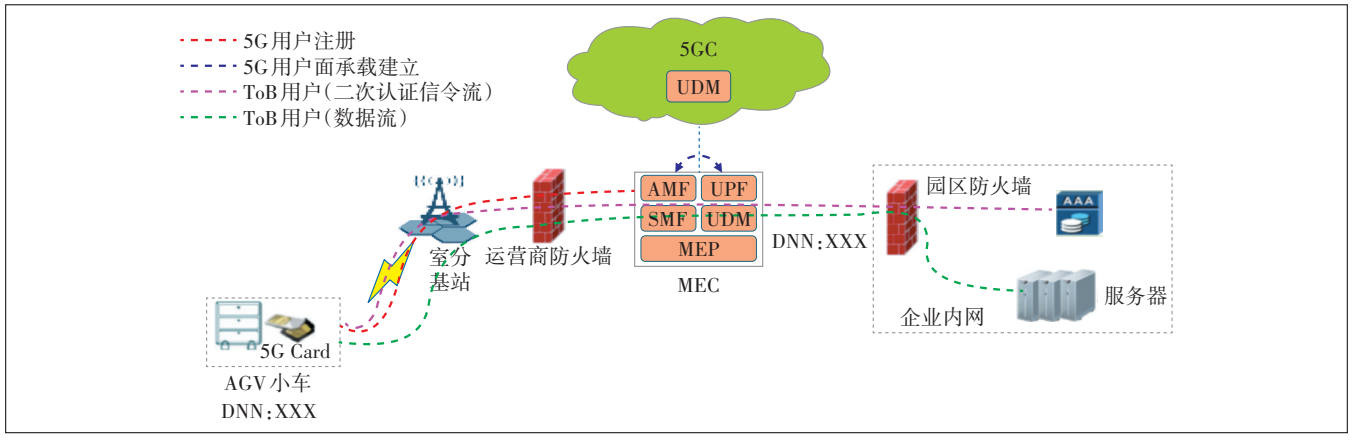

图2　工作流程示意

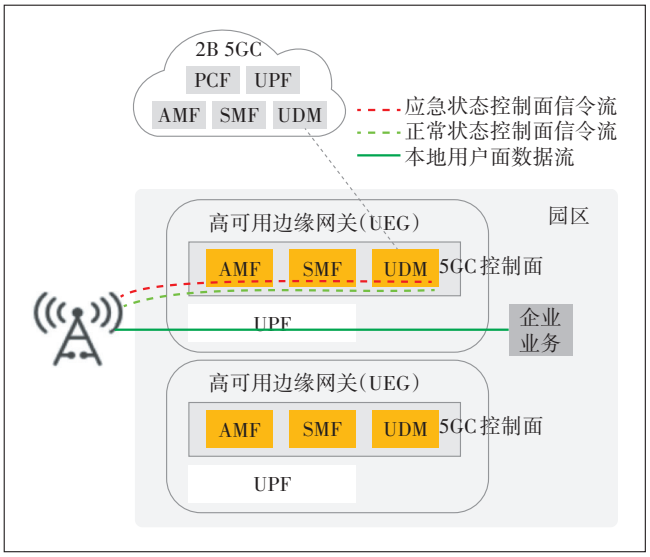

图3　园区核心网方案

据业务独立自主运行，数据和部分信令不出园区。园区UDM需定期与大网UDM进行数据同步，主要同步新开卡等用户信息，这提高了大网断连下的可靠性。方案落地后，园区可支持稳态用户不掉线，惯性运行；大网断连后，可支持用户移动切换以及新用户接入。终端在园区UDM完成注册流程，在园区AMF完成移动性管理，由园区SMF完成会话管理，流程最大程度集中在本地工作。园区与大网连接中断时，对已经开户的用户无影响，但无法支持园区自主运维，也无法支持新开户终端接入园区专网。大网断连前后对比如表2所示。

表2　大网断连前后对比

控制面	移动性管理（仅支持2B独享基站接入）	会话管理	用户面管理（UPF）
正常状态	本地接入运行	本地接入运行	标准UPF功能，如需计费，SMF对接大网CHF
断连状态	依赖本地AMF容灾数量，部署2套时支持重选接入	依赖本地SMF容灾数量，部署2套时支持重选接入	

方案实施运行后，园区UDM仍然需要对外与大网UDM保持联系，数据同步流程如下（见图4）。

a）大网UDM与本地UDM实现用户数据文件同步。

b）大网UDM定期导出本地UDM的用户卡/签约数据文件。

c）本地UDM定期下载园区用户数据文件到本地并加载生效，保证在大网失联时，用户可通过本地UDM实现用户的5G鉴权/注册/接入等基本业务。

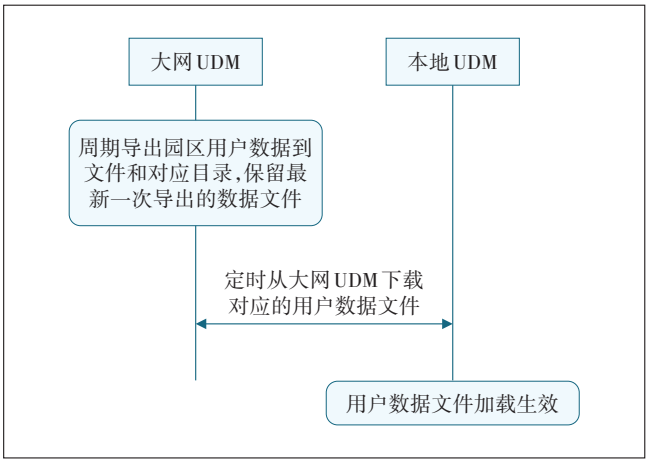

图4　UDM数据同步流程

3.4 终端接入安全设计方案

5G终端接入安全的整体设计如图5所示，终端多重接入控制能力如表3所示[5]。

3.4.1 5G终端主认证接入运营商

5G终端主认证是指终端接入本地运营商5G网络，其整体流程如下。

a）插有SIM卡的5G终端通过5G基站和5G承载网向5G核心网控制面发起注册流程。

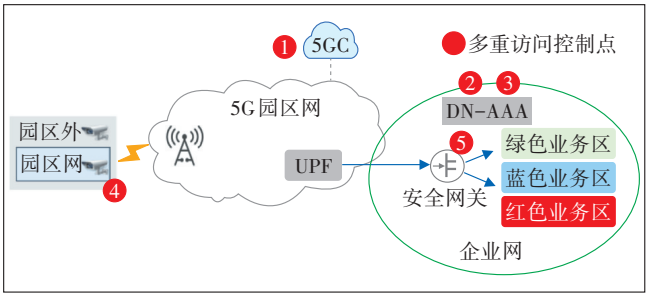

图5　5G终端多重接入控制

表3　5G终端多重接入控制能力说明

控制点	控制内容	安全能力	控制决策点
1	终端可否接入运营商5G网络	5G网络主认证	5GC（由运营商管理和控制）
2	终端可否接入园区5G网络	自主认证	DN-AAA（5GC和AAA协同，园区可自管理）
3	合法SIM卡是否在合法终端上使用	机卡绑定控制	DN-AAA（5GC和AAA协同，园区可自管理）
4	终端能在哪些位置接入到园区5G网络	电子围栏控制	DN-AAA（5GC和AAA协同，园区可自管理）
5	终端能接入园区哪个业务区	基于角色的访问控制	AAA、5G安全网关（园区可自管理，决定终端能够访问的业务）

b）终端通过注册流程对5G核心网进行鉴权，验证5G网络的合法性，5G核心网也会对用户进行鉴权以验证终端的合法性，双向鉴权保证了用户和5G网络之间的相互安全。

c）如果用户在核心网中已经签约，那么核心网会通过用户注册请求，完成注册。如用户未在核心网签约，核心网会拒绝用户接入。

3.4.2 5G终端二次认证接入园区内网

5G终端二次认证方案将终端接入园区的控制权放在园区网络中，给园区提供了更灵活自主的控制方式，园区可以基于设备识别码（IMSI）控制接入内网的终端。要支持二次认证等终端安全特性，需要在园区部署AAA服务器，并和5GC的SMF模块连接。

3.4.3 5G终端接入内网的多重控制

园区可以基于多种因素对接入内网的5G终端进行控制，当前可以控制的因素包括IMEI、接入位置等。

a）机卡绑定控制。园区用户开户时设置用户绑定IMSI和IMEI，将IMSI作为用户名唯一标识、IMEI作为设备唯一标识进行绑定。用户接入时AAA对用户IMSI和IMEI标识进行校验，对合法用户校验通过并予以接入，反之校验失败拒绝接入。

b）电子围栏控制。电子围栏方案基于SMF-AAA间园区自主鉴权机制实现。当用户在园区内移动时，SMF基于位置改变触发POD（Point Of Deployment）与AAA进行实时接入鉴权，SMF根据AAA的鉴权结果来决定是否准许用户的移动行为。AAA基于ULI地址池进行判断，ULI地址池为有效区域，越区则拒绝移动[6]。

3.4.4 5G终端精细化业务控制

开放的APP对应不同的终端，从安全性考虑，需要设定不同的访问控制策略。考虑到5G场景下5G终端的IP地址大部分是由运营商动态分配的，无法从IP看出其对应的终端，这就给以IP地址为基础的访问控制设备带来了挑战。5G终端精细化业务控制是在MEC边界部署接入防火墙，通过AAA系统从核心网同步终端IP信息，实现基于终端角色的精细化访问控制，从而减少园区应用暴露面（见图6）。

3.5 数据安全设计方案

园区数据安全主要如下。

a）园区数据不出园。UPF下沉到园区，通过SMF下发的分流策略，实现基于DNN本地分流，防止业务数据出园。同时，通过三面隔离，防止用户面数据通过管理面和信令面出园。

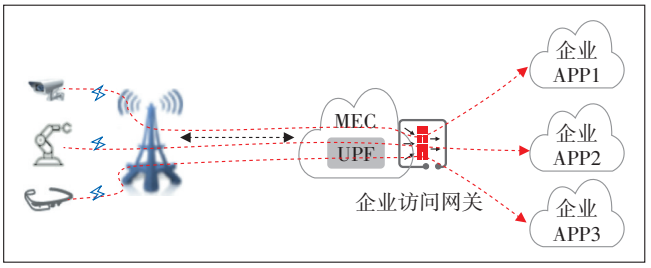

图6　5G终端应用精细化访问控制场景

b）数据端到端加密。为防止园区数据泄露，可以从网络和应用2个层面实现端到端加密，应用层加密如图7的c/h部分所示，需要在终端侧加密，在园区的应用服务器侧进行解密，其主要由园区应用支持。网络层加密如图7的a/b/d/e/f/g部分所示，可由运营商和园区共同提供，可以根据实际项目需要进行选择。其中，a为其他非5G终端连接CPE设备，该过程依赖CPE的加密功能。b/g为5G终端到MEC防火墙的IPSec加密（5G终端要具备IPSec能力）。d为5G终端通过空口传输的业务和信令数据，该部分数据通过3GPP空口信令面和UP面加密完保算法保障安全。5G空口加密和完整性保护的算法有SNOW 3G、AES（Advanced Encryption Standard）、祖冲之算法（ZUC），空口加密需要终端和基站同时支持才能生效。e为基站-MEC/UPF之间的业务数据，此数据通过GTP-U隧道进行传输，一般该段路径属于运营商机房内的可信网络，可以不加密，如果需要加密，则可以采用BBU到MEC之间的IPSec加密方案。f为MEC/UPF-园区内网之间的业务数据，可采用IPSec加密保护，以MEC/UPF侧的防火墙或路由器作为起点，终结在园区内网网关（防火墙或路由器），IPSec密钥由园区掌握。对本园区的一些特殊行业的合规要求，建议使用国密算法，通过MEC/

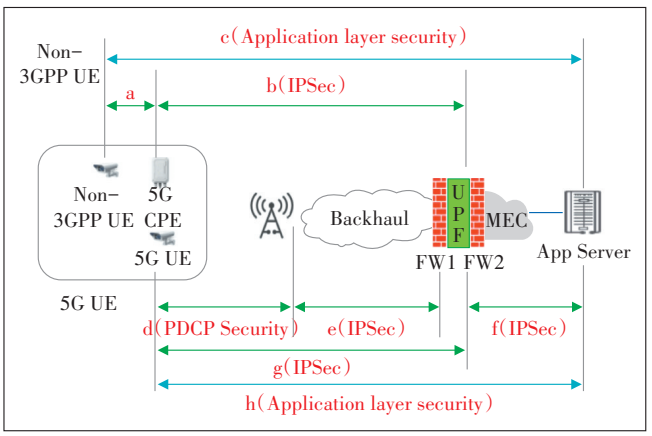

图7　端到端数据加密

UPF侧的防火墙或路由器来支持国密算法加密，建议采用均支持国密算法的防火墙和路由器产品。

3.6 边界安全设计方案

以MEC为中心的边界共有3类，分别是园区数据中心与MEC边界，接口为N6；MEC与接入区边界，接口为N3；园区MEC与大网核心网边界，接口为N8、N12以及O&M（见图8）。这些接口存在入侵威胁，需要与大网、园区网等进行隔离和保护。

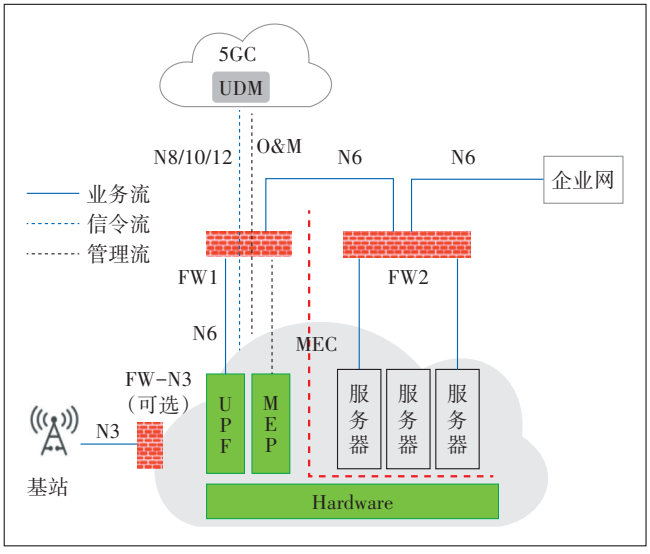

图8　边界安全设计

a）在基站与MEC间部署防火墙FW-N3，进行网络隔离，通过IPSec对数据进行加密。

b）在5GC与MEC间部署防火墙FW1，开启双向过滤策略，通过内置IPSec对数据进行加密；O&M采用TLS安全协议，利用防火墙FW1开启流量过滤策略。

c）在园区内网与MEC的边界，采用防火墙、入侵检测、抗拒绝服务、网络防病毒、网络审计等安全设备进行防护。如果MEC上无APP，则部署防火墙FW1，进行网络隔离，防止N6口的网络攻击；如果MEC上有APP，则增加部署防火墙FW2，隔离园区内网，防止不同APP之间的横向攻击。

3.7 安全审计设计方案

针对数据出园的风险，可通过防火墙实现访问控制以实现数据出园的控制；通过日志审计实现事后追查和审计。

3.7.1 访问控制

根据MEC各外部接口分别与gNodeB、园区内网和核心网UDM网元之间的五元组通信路由设定通信矩阵，进而生成防火墙白名单策略，防火墙基于这些白名单做双向流量控制，并需要根据现网运行情况逐步细化和丰富白名单。

3.7.2 会话和日志审计

a）会话日志记录。防火墙基于白名单策略做命中策略的记录，包括允许和拒绝的日志记录。针对拒绝的会话，记录其IP、端口的会话日志，并上报日志中携带流量的统计信息。

b）应用日志审计。日志系统收集网元执行高危命令的日志、分流策略等操作日志，用于进行后续溯源的日志审计。

通过审计员、管理员的权限分离，运营商可面向园区开放审计员账户，实现审计记录的透明化管理。

4 结束语

本文通过研究特殊行业的5G独立专网安全解决方案，从整体网络架构、核心网安全设计、安全架构设计、终端接入安全设计、数据安全设计、边界安全设计、安全审计设计等方面进行分析，由运营商为园区5G独立专网提供安全专用的5G通信管道，并根据客户需求及安全隔离等级提供合理的网元下沉方案。该方案提高了投资效益、维护管理效益以及信息安全。

参考文献：

[1] 郑舒. 5G定制专网的网络安全部署方案[J]. 电信快报，2022(7)：23-27.
[2] IMT-2020(5G)推进组. 5G行业专网安全技术研究[EB/OL]. [2024-06-30]. https://www.docin.com/p-4401601784.html.
[3] 中国联合网络通信有限公司. 中国联通轻量化5G核心网白皮书[R/OL]. [2024-06-30]. https://www.docin.com/p-2653115277.html.
[4] 周旸，吕艳芳，傅俊锋，等. 5G专网核心网高可靠组网设计与研究[J]. 邮电设计技术，2021(9)：77-81.
[5] IMT-2020(5G)推进组，中国信息通信研究院. 5G安全知识库[EB/OL]. [2024-06-30]. http://www.caict.ac.cn/kxyj/qwfb/ztbg//202112/P020211210558556929664.pdf.
[6] 麦欢怡，黄晓弟. 等保2.0下5G+工业控制系统的安全防护研究[J]. 电信快报，2022(7)：14-17.

作者简介：
薛龙来，高级工程师，硕士，主要从事无线网络规划设计及网络人工智能的相关工作；李轲，工程师，学士，主要从事传送网与物联网及移动网规划的相关工作；许长峰，高级工程师，学士，主要从事无线网络规划与优化相关工作；王殿亮，工程师，学士，主要从事无线网络规划设计及其相关工作。