5G专网接入安全管控方案

Security Management Scheme of 5G Private Network

邢建兵，史春磊，冉　萌，蔡　超，邱佳慧（中国联合网络通信集团有限公司，北京 100033）
Xing Jianbing, Shi Chunlei, Ran Meng, Cai Chao, Qiu Jiahui (China United Network Communications Group Co., Ltd., Beijing 100033, China)

摘　要：
随着5G随行专网业务的发展，行业客户对5G专网可管、安全可控、可溯源的需求越来越强烈。回顾了5G专网的发展和现有安全管控方案的局限性，并面向教育场景创新性地提出了基于VPP网关和AAA的5G专网接入安全管控方案，为5G专网接入安全管控能力建设提供了可参考、可复制的解决方案，满足了教育行业客户的可管、可控、可溯需求。探讨了该方案的实施细节，包括组网方案、认证流程和安全管控能力，并通过了应用场景验证，展示了其在教育行业的成功应用。

关键词：
AAA；5G专网；VPP网关；二次认证；自主运维
doi：10.12045/j.issn.1007-3043.2026.01.012
文章编号：1007-3043（2026）01-0055-05
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:
With the development of 5G accompanying private network services, industry customers have an increasingly strong demand for manageability, security controllability, and traceability of 5G private networks. It reviews the development of 5G private networks and the limitations of existing security management and control schemes, and innovatively proposes 5G private network access security management and control schemes based on VPP gateway and AAA for education scenarios, providing referable and replicable solutions for the capability building of 5G private network access security management and control, and meeting the manageable, controllable and traceable needs of customers in the education industry. It further discusses the implementation details of the scheme, including networking scheme, certification process and security control ability, and has passed the application scenario verification, demonstrating its successful application in the education industry.

Keywords:
AAA; 5G private network; VPP gateway; Secondary authentication; Autonomous operation and maintenance

引用格式：邢建兵，史春磊，冉萌，等. 5G专网接入安全管控方案[J]. 邮电设计技术，2026(1)：55-59.

1 背景

“十四五”规划纲要指出“加快5G网络规模化部署”，“构建基于5G的应用场景和产业生态”。5G技术作为新一代网络底座，为教育行业客户数字化转型提供了强大的支撑。从国家战略层面来看，党的二十大首次将“推进教育数字化”写进了党代会报告，强调加快构建“人人皆学、处处能学、时时可学”的学习型社会。教育数字化要求学校适应5G网络发展，加快建设服务全时域、全空域、全受众的高校智能学习体系，这对校园内网/期刊网等移动接入提出了明确需求。

5G专网的应用场景，从接入终端和访问业务分析，包括2B物联网终端和2C人网卡终端，访问的业务有行业客户内网也有互联网；从接入区域分析，有在

收稿日期：2025-12-08

特定区域内（如园区内）接入的场景，也有随行接入（如城市内或漫游）的场景，比较常见的需求是2B终端在特定区域访问行业客户内网（后续简称内网）以及2C终端随行接入既访问内网又访问互联网。面向2C用户通过5G专网无缝访问内网和互联网的需求，国内各大运营商积极进行了布局，分别对应中国联通的5G随行专网、中国电信的5G双域快网方案、中国移动的5G双域专网[1]。

本文重点讨论教育行业2C随行接入专网场景。教育行业用户既需要访问互联网，满足社交、购物等需求，又需要不换卡、不换号、随时随地访问校园内网资源，如校内网、教学管理、智慧课堂以及科研网站等[2]。在5G专网业务发展初期，5G专网具备智能分流能力，可实现用户不换卡不换号访问教育行业客户的内网和互联网，解决了传统VPN操作复杂、速率低等问题，是传统VPN网络技术演进发展的解决方案。随着5G专网业务的深入发展，教育行业信息化管理部门对5G专网接入安全管控能力和自运维管理的诉求逐渐强烈，如信息化管理部门需要满足师生良好的内网使用感知诉求，只允许授权终端接入校园内网，师生访问校园内网的数据配置实时生效，实时管控异常终端，建设具有IP地址溯源能力、自助可视及管理能力的5G专网系统等。满足客户可管、可控、可溯需求是5G专网深入教育行业、进行规模应用的关键。

文章首先分析了已有的网络安全管控方案，其次介绍了VPP网关和AAA的5G专网接入安全管控方案，最后进行了应用场景验证。

2 现有网络安全管控方案分析

在现有技术中，AAA可以实现二次鉴权认证，将5G专网的安全能力开放给行业客户，增强管控能力。AAA认证方案由核心网网元会话管理功能（Session Management Function，SMF）/用户面功能（User Plane Function，UPF）对接AAA，并在终端建立协议数据单元（Protocol Data Unit，PDU）会话之前发起认证。AAA认证方案需要依托签约的数据网络名称（Data Network Name，DNN）以及核心网的能力支持发起二次认证。鉴于当前技术环境中企业用户会同时访问互联网和企业网络，可以使用上行分类器（Uplink Classifier，ULCL）技术，根据UE访问的目的地址和目的域名，区分UE要访问的应用是内网还是公网。

这种场景主要存在的问题如下。

a）校园用户通常不会签约专用DNN，而是签约通用DNN，核心网能力不足以直接触发二次认证。即如果校园签约的是通用DNN，那么SMF就无法发起二次认证，无法满足企业对UE的接入权限进行控制的需求。

b）通常校园用户需要实现基于5G群组访问内网的策略管理，如学生和老师可以访问的资源权限，如对用户访问内网资源时间的管控。因5G AAA认证方案仅针对接入认证进行管控，无法满足企业的全面管控需求。

3 基于VPP安全网关和AAA的5G专网接入安全管控方案

3.1 方案概述

本文创新地提出了基于VPP（Vector Packet Processing）网关和AAA的安全管控方案，其中，VPP是一个模块化和可扩展的软件框架，用于创建网络数据面应用程序，5G专网VPP安全网关基于VPP进行开发设计。本文提供一种基于N4 XDR话单触发的5G用户二次认证的方法。5G用户二次认证指终端在成功接入到5G网络以后，在访问特定网络（如企业网络、敏感业务网络等）时，需要再次进行的认证过程。这一认证机制的主要目的是保障特殊网络的安全，确保只有经过特定认证的用户才能访问敏感的业务服务。这一认证过程通常由5G核心网在PDU会话建立期间发起，与外部的数据网络认证、授权和计费（Data Network-Authentication，Authorization，and Accounting，DN-AAA）服务器，基于扩展认证协议（EAP）等框架进行。与5G AAA认证相比，基于5G专网VPP安全网关和AAA的专网接入安全管控方案一方面是认证流程不同，另一方面是增加了策略控制机制（见图1），可以全面满足教育行业对5G随行专网可管、可控、可溯的需求[3]。

本章将介绍基于VPP安全网关和AAA的5G专网接入安全管控方案的组网方案、认证流程以及接入安全管控能力。

3.2 组网方案

为满足教育行业客户业务需求和安全需求，基于VPP安全网关和AAA的5G专网接入安全管控组网方案充分结合了CT强大的连接能力、IT的计算能力以及平台的OT运营能力，其组网拓扑如图2所示，主要组成部分包括MEC服务器、能力平台（5G专网自运维管

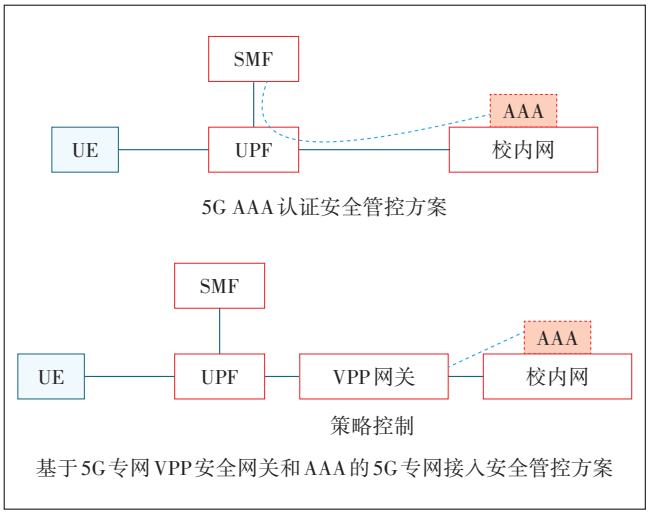

图1　安全管控方案对比

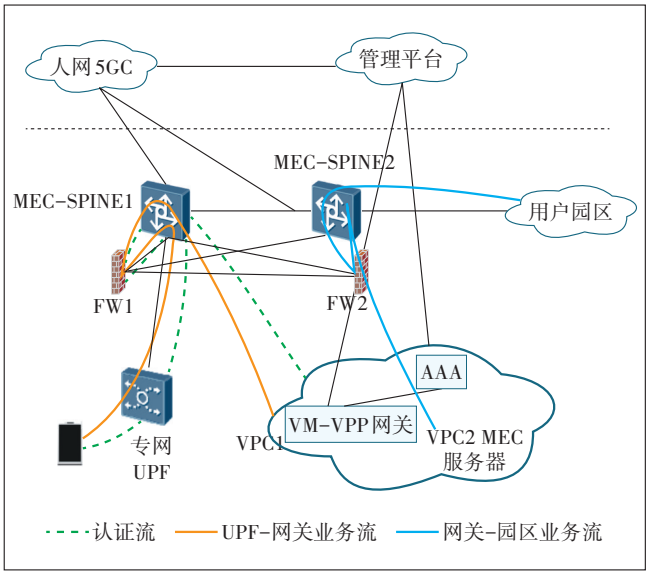

图2　基于VPP安全网关和AAA的5G专网接入认证组网方案

理平台和短信网关平台）、人网5G核心网络（5G Core，5GC）以及用户园区云。

3.2.1　MEC服务器

MEC平台上部署5G专网VPP安全网关和AAA服务，为VPP网关和AAA提供基础算力资源及网络连接。MEC平台主要由MEC SPINE（SIPNE-LEAF为一种数据中心网络架构）交换机、防火墙（Firewall，FW）、MEC服务器和云平台组成。通过采用在MEC平台上部署网络能力和应用能力的解决方案，运营商确保用户数据在专网内，实现专网专用，从而保障专网数据的安全性和私密性；MEC平台位于移动核心网的边缘，同时保障了网络访问的低时延特性[4]。

5G专网VPP安全网关为用户面策略执行组件，实现了准入控制、策略控制。5G专网VPP安全网关作为软网关，部署在中国联通MEC底座上，能够在不对5G大网网元进行配置的前提下，面向行业客户提供专网安全等专网能力服务，实现行业应用的自主精细适配和业务配置实时生效。

AAA实现用户鉴权信息数据库的终端二次鉴权管理，它接收5G专网VPP安全网关发起的Radius认证消息并响应，验证用户身份，满足行业客户自主认证的安全要求。只有行业客户认证合法的终端，才允许接入专网。

3.2.2　能力平台

5G专网自运维管理平台是基于5G专网创新能力的业务服务平台，为客户提供自服务触点以及可管、可控、可溯融合的管理界面。图3是5G专网自运维管理平台的架构，本文重点阐述了5G专网自运维管理平台中的用户黑白名单（认证）以及IP地址溯源功能。

3.2.3　人网5GC

人网5GC是为2C用户提供服务的5G无线通信系统的核心部分，负责提供高速、低延迟、高可靠性的5G网络服务。

3.2.4　用户园区云

用户园区云是构建校园专属、高效、安全的数字化生态环境，提供校园所需的数字化应用，包括不限于教学管理、数字课堂、科学研究等应用系统。

3.3　认证流程

基于组网方案，本文进一步构建了无感知认证，以优化用户体验并确保认证过程的安全性与便捷性。

在该业务流程中，UE首先通过5G核心网的网络鉴权流程，以确保其身份的合法性与网络接入的安全性。与验证码认证方式不同的是，UE在尝试发起对用户面数据的访问，接入行业客户的内部网络时，自动触发认证机制，如果认证MSISDN为用户的白名单号卡，即可认证成功。此认证过程对UE是完全无感知的，即用户无需执行任何额外的认证操作或等待认证成功消息，即可访问内网[5]。

无感知认证技术架构如图4所示。5G专网自运维管理平台采集并解析SMF至UPF之间的N4信令。将信令作为输入，N4信令采集解析设备从其中的PFCP协议信令中解析出N4 PFCP Session Establishment、N4 PFCP Session Modification、N4 PFCP Session

图3　5G专网自运维管理平台架构

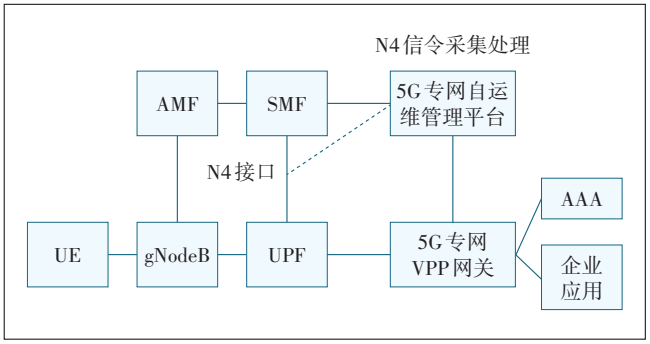

图4　无感认证技术架构

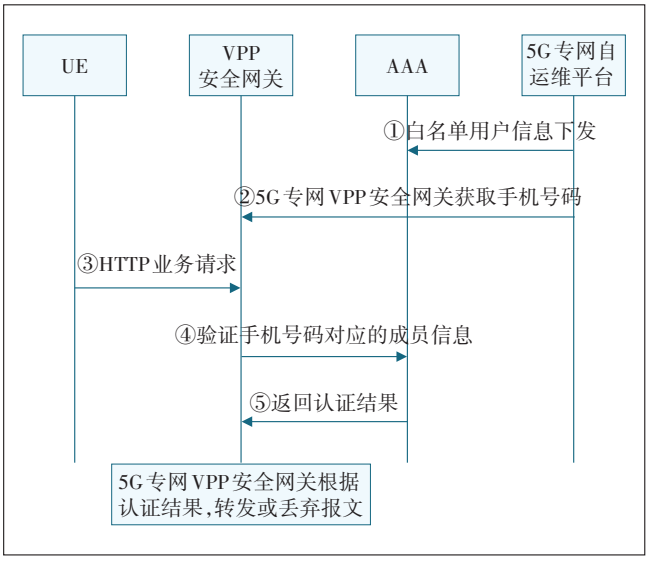

图5　无感认证业务流程

Delete、N4 PFCP Session Report等4种流程的关键信息，输出为N4 XDR话单记录，并从中提取出UE的IMSI、MSISDN、UE IP address信息，并下发给5G专网VPP安全网关。5G专网VPP安全网关是认证处理单元和策略执行单元，它构建Radius报文并向AAA发起认证请求，认证字段为MSISDN，并对鉴权认证结果进行策略处理和数据处理。AAA实现UE二次鉴权管理[6]。

合法用户信息的管理与验证流程主要分为5个部分（见图5）[7]。

a）白名单用户信息下发。管理平台负责将已审核并确认为合法的用户信息下发给AAA系统。

b）5G专网VPP网关获取MSISDN。5G专网VPP网关通过与管理平台的交互，动态获取当前网络中MSISDN与其对应IP地址的映射关系。

c）HTTP业务请求。UE作为数据请求的发起端，按照既定的网络协议向目标服务器发送HTTP请求，以获取所需的数据或服务。

d）验证MSISDN对应的成员信息。在接收到UE

的HTTP请求后，5G专网VPP网关首先依据IP地址关联出MSISDN信息，并向AAA系统发起验证请求。

e）返回认证结果。AAA系统在完成用户身份验证后，将认证结果及时回传给5G专网VPP网关。5G专网VPP网关根据认证结果判定是否允许UE的HTTP请求通过。

通过以上5个步骤，无感知认证流程确保了内网只能被合法用户所访问。这个流程不仅提高了系统的安全性，还进一步提升了用户体验的便利性。

3.4 安全管控能力

通过5G专网自运维管理平台，学校信息管理部门可以实现5G专网接入安全管控。此方案具备基于5G专网VPP网关和AAA的5G专网接入安全管控接入认证能力、IP地址溯源能力，也具备当用户访问内网业务时用户面数据配置实时生效的能力，如一键断网等功能[8]。

a）AAA认证管理能力[9]。学校信息管理部门可以给特定的5G手机号卡授权，授权的号卡通过自运维管理平台发送至AAA平台；可以查看号卡的认证日志以及授权日志。教育行业客户可自主控制准入的号卡清单，并在管理界面上设置认证模式[10-12]。

b）IP地址溯源能力。通过5G专网自运维管理平台，学校信息管理部门可以通过用户使用的IP地址及访问时间范围，来查询IP地址分配的MSISDN，进而溯源出具体的IP地址使用者，可查询在线IP地址溯源和历史IP地址溯源记录。因为5G专网VPP网关只针对UPF分流至校园内网的数据流，所以IP地址溯源功能仅限于访问内网的IP地址。系统的这一机制很好地实现了保护网络安全的目标，同时也达成了保护用户数据安全的要求[13]。

c）一键断网能力。对有安全风险的用户或手机遗失的场景，学校信息管理部门可以设置学生和老师能够访问的资源权限，如对用户访问内网资源时间的管控等。

3.5 应用场景验证

本文所提出的基于5G专网VPP安全网关和AAA的5G专网接入安全管控方案，在部分高校完成了业务场景验证，测试用例包括MSISDN与IP地址对应关系获取、号卡白名单授权设置、无感二次认证以及IP溯源等，测试情况良好，方案可行，具有实际应用价值。该方案目前已经在河北、山东、吉林、福建等多个省份落地实施，为教育信息化场景提供了可参考、可复制的解决方案。

4 结语

安全可控的5G随行专网的诞生，顺应了5G扬帆政策引领、5G科技革命和产业变革的潮流，实现了将移动通信网络、互联网络和行业客户内网的融合，体现了IT、CT、OT深度融合的新生态，为社会发展带来了变革和价值[14]。

参考文献：

[1] 中国联通. 中国联通5G行业专网白皮书(2020)[R/OL]. [2025-08-21]. https://www.digitalelite.cn/h-nd-2808.html.
[2] 王杉，傅俊锋，李宏平，等. 5G专网混合组网方案研究与应用[J]. 信息通信技术，2022，16(1)：34-39.
[3] 余晓光，余滢鑫，阳陈锦剑，等. 安全技术在5G智能电网中的应用[J]. 信息安全研究，2021，7(9)：815-821.
[4] 王俊，田永春. 一种面向关键行业应用的广域5G安全专网设计[J]. 中国电子科学研究院学报，2021，16(10)：964-972.
[5] 高功应，平军磊，刘凡栋，等. 5G SA VPDN业务继承方案研究[J]. 邮电设计技术，2021(9)：11-16.
[6] 江魁，肖泽宇，何维兵，等. 5G校园专网的安全接入和授权管理研究[J]. 福州大学学报(自然科学版)，2023，51(5)：596-603.
[7] 董芸，何余锋，王菲，等. 基于DN-AAA的5G专网接入安全管控方案研究及应用[J]. 信息安全研究，2023，9(8)：784-791.
[8] 郝立谦. 5G随行专网的安全技术研究与应用[J]. 邮电设计技术，2023(4)：1-4.
[9] 肖洪，方嘉宇，曾礼荣. 基于软件定义边界技术的5G专网二次鉴权研究[J]. 广东通信技术，2023，43(2)：64-66，70.
[10] 王建英，吕俟林，许建明. 可应用于5G网络的垂直行业二次认证方法浅析[J]. 通信技术，2020，53(10)：2538-2542.
[11] 孔令义. 面向5G的网络优化和重构[J]. 电信科学，2020，36(2)：117-125.
[12] 温三宝，辛冰，陈思翰，等. 5G行业专网典型应用场景的二次认证方案[J]. 电信工程技术与标准化，2024，37(2)：64-71.
[13] 赵恒梅，冷昕. 基于5G专网的智慧校园建设应用[J]. 信息与电脑，2024，36(3)：42-46.
[14] 李迪生，袁朋，吴培，等. 5G专网发展瓶颈及6G展望[J]. 电信工程技术与标准化，2023，36(4)：84-87.

作者简介：
邢建兵，高级工程师，博士，主要从事智能终端、网络与应用相关技术研究工作；史春磊，高级工程师，硕士，主要从事5G网络的创新产品研发工作；冉萌，高级工程师，硕士，主要从事移动网络创新产品研发工作；蔡超，毕业于西安电子科技大学，正高级工程师，硕士，主要负责中国联通面向5G网络的创新产品研发工作；邱佳慧，毕业于北京交通大学，正高级工程师，博士，主要研究方向包括车联网、5G通信、高精度定位等。