GTI

5G MEC Security White Paper

5G MEC Security White Paper

Version:	V1.0
Deliverable Type	□**Procedural Document** ☑**Working Document**
Confidential Level	☑**Open to GTI Operator Members** ☑**Open to GTI Partners** ☑**Open to Public**
Working Group	Terminal Working Group
Task	Task-T-PM3-PJ5-7: 5G MEC Security
Source members	CMCC
Support members	CTCC, CUCC, Ericsson, Nokia, Huawei, ZTE, Sany, China Southern Power Grid (CSPG), BUPT, BJTU, Qihoo, DBAPPSecurity, Neusoft, etc.
Editor	Le Yu (CMCC)
Contributors	Bin Zhang(CMCC), Jie Yuan(CMCC), Feng Zhang(CMCC), Xiangjun Li(CMCC), Hongyang Zhang(CMCC), Yaodong Tao(BJTU), Qin Qiu(CMCC), Baoyu An(CMCC), Bo Cheng(BUPT), Shuai Zhao(BUPT), Guoyi Zhang(CSPG), Yang Cao(CSPG), Shiying Zheng(CMCC), Qiguang Fan(CMCC), Guofeng He(CTCC), Jianyu Zhang(CTCC), Feng Gao(CUCC), Xiulong Liu(Huawei), Bing Zhu(Huawei), Na Li(Ericsson), Zhiyuan Hu(Nokia), Yonggang Xue(Huawei), Xianqiao Chen(Huawei), Jingjing Hao(Huawei), Zhimeng Teng(ZTE), Gaofeng Xu(ZTE), Linna Ge(ZTE), Liping Wei(ZTE), Yi Xin(ZTE), Kai Chen(Sany), Yi Zhang(Qihoo), Jianfeng Li(DBAPPSecurity), Jiuhong Gu(Neusoft)

Last Edit Date	02-02-2021
Approval Date	13-07-2021

Document History

Date	Meeting #	Version #	Revision Contents
02-02-2021		V1.0	
DD-MM-YYYY			
DD-MM-YYYY			
DD-MM-YYYY			
DD-MM-YYYY			

Table of Contents

Preface

5G multi-access edge computing (MEC) is a new model for 5G network architecture that moves cloud computing capabilities and IT service environments to the edge of mobile communications networks, providing nearby services for users. This establishes a carrier-class service environment with high performance, low latency, and high bandwidth [1].

5G MEC enables new applications by moving core network functions to the network edge. However, it also brings new security challenges and increases security supervision difficulty. In fact, conventional security protection solutions do not cover edge scenarios, while 3rd Generation Partnership Project (3GPP) and other international standards organizations are still working on edge computing standards [2-6]. This white paper proposes 5G MEC security protection policies for operators and 5G industry customers by drawing on successful industry practices. The goal of these policies is to help industry customers implement the three sync requirements (synchronous planning, synchronous construction, and synchronous maintenance) on security while developing 5G MEC applications, as well as guiding the industry to improve MEC security capabilities.

1 5G MEC Overview

1.1 Introduction

5G MEC provides nearby MEC services where closing to the source of user service data, meeting the industry's basic requirements on low latency, high bandwidth, security, and privacy protection. For example, it offers real-time, secure data processing and etc. closer to users.

The 5G empowering vertical industries [7] white paper, published by the 5G Public Private Partnership (5G PPP), explains that 5G uses MEC to deploy applications to the data instead of sending all data to a centralized data center, thereby ensuring real-time applications. This paper shows that MEC is most typically employed for smart factory, smart grid, smart driving, healthcare, entertainment, and digital media scenarios, and these industries represent the largest potential future markets for MEC. Currently, operators are closely cooperating with customers in these industries to meet user requirements and promote MEC development, in order to deliver secure and reliable MEC services to users. According to the MEC Security White Paper [1] published by the Edge Computing Consortium (ECC) and the Alliance of Industrial Internet (AII) in 2019, MEC offers resource-constrained, distributed, and real-time performance. Therefore, security protection should consider these factors, along with massive terminals and heterogeneous systems typical of MEC. To this

end, the MEC Security White Paper proposes a lightweight and targeted MEC security protection architecture.

1.2 5G MEC Scenarios

MEC is mainly deployed in aggregation equipment rooms and on campuses due to the latency, cost, and enterprise data security requirements of different services. This means that there are two typical MEC deployment scenarios: wide area network (WAN) MEC and local area network (LAN) MEC.

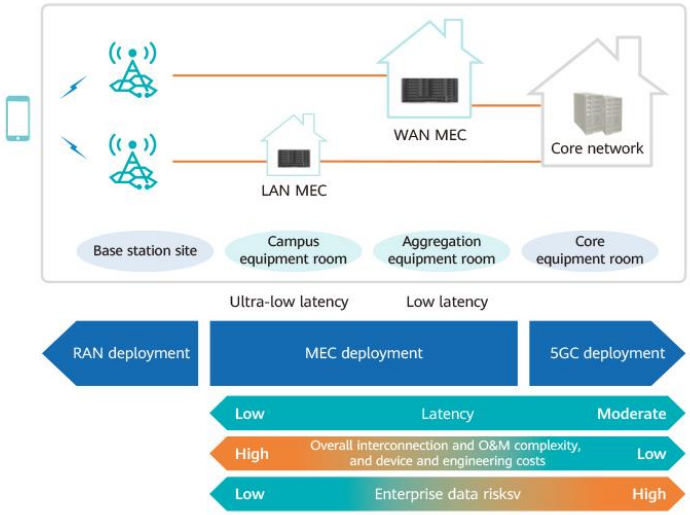

Figure 1-1 MEC deployment scenarios

1.2.1 WAN MEC Scenarios

WAN MEC ensures low latency services through two-way latency below 1 ms over 100 km of transmission. This indicates that the 5G public network based on WAN MEC has the capacity to offer 5G network

services to a variety of vertical industries. The MEC deployment in aggregation equipment rooms with security control is the mainstream WAN MEC solution for operators, considering factors such as application interconnection, O&M complexity, and device and engineering costs.

WAN MEC mainly applies to OTT connections on public networks (such as cloud VR and cloud gaming), group connections on public networks (such as bus advertisement and public security protection), ultra-reliable low-latency communication (URLLC) private networks (electric power, etc.), and private line connections (enterprise private lines). In these cases, MEC can be deployed in aggregation equipment rooms to meet low-latency service requirements.

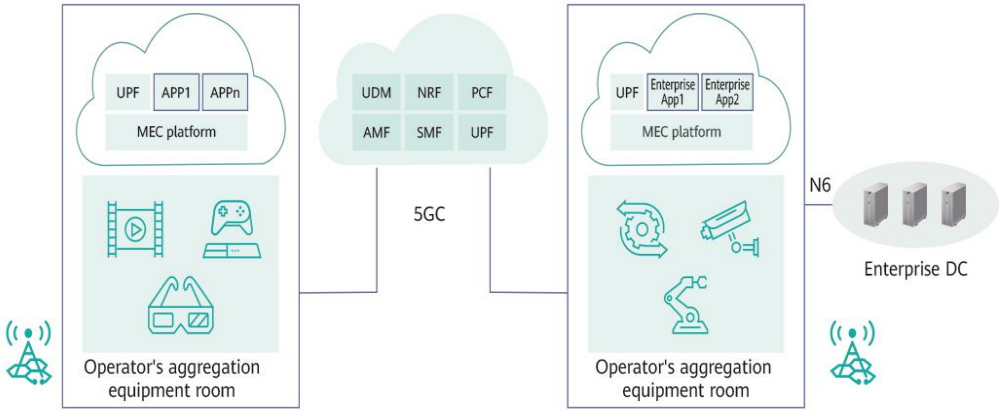

Figure 1-2 WAN MEC scenario

1.2.2 LAN MEC Scenarios

For industries that are highly sensitive to security and privacy protection,

MEC can be deployed on campus to ensure data within campus.

Typical LAN MEC scenarios include remote control of gantry cranes in ports and bridge cranes in steelworks, and most manufacturing, petrochemical, education, and healthcare campuses and factories. LAN MEC deployment is suitable for URLLC services. It can also support local breakout (LBO) of enterprise service data, providing local network pipes for campus customers. In addition, isolation and authentication capabilities can be enhanced to prevent unauthorized access to the enterprise intranet from public networks, helping build 5G private networks for enterprises.

- An enterprise subnet can be set up by using a data network name (DNN), slicing, or other solutions. This assures that only enterprise UEs have access to campus networks.
- Device and SIM card binding, enterprise AAA secondary authentication, and other methods can be used to allow only specified UEs to access campus networks.
- The base station can broadcast the campus-specific combination of public land mobile network (PLMN) ID and nework identifier (NID) or closed access group (CAG) ID to allow only enterprise UEs to access dedicated campus networks.

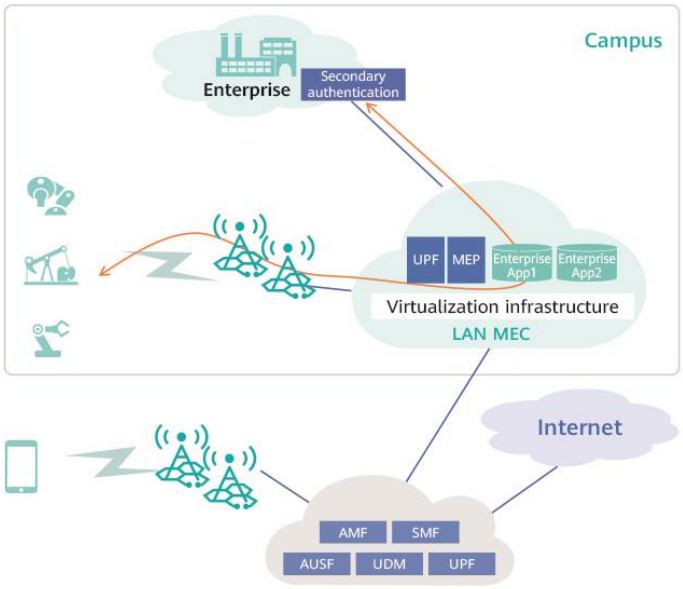

Figure 1-3 LAN MEC scenario

2 5G MEC Standards and Policies

2.1 5G MEC Standards

MEC standards are developed by both the European Telecommunications Standards Institute (ETSI) and 3rd Generation Partnership Project (3GPP). ETSI focuses on defining standards related to MEC platforms, virtual machines (VMs), and API management, while 3GPP addresses the interaction between MEC and other 5G core network elements. In terms of architecture, MEC belongs to the core network. Typically, ETSI specifies that the location of a user plane function (UPF) is where MEC is located in the 5G network architecture.

In March 2016, ETSI released ETSI GS MEC 003 that defines the MEC

framework and reference architecture. It later on released GS MEC 009, GS MEC 010-2, GS MEC 011, GS MEC 012, GS MEC 013 and ohter standards, covering topics which include application lifecycle management, mobile edge application support, radio network information and location and etc..

At the same time, 3GPP TS 23.501 (Release 15) also defines support for edge computing of 5G MEC. Currently, 3GPP Release 17 standards on MEC enhancement and secure boot are scheduled for delivery after March 2021.

Furthermore, the International Telecommunication Union (ITU) proposed two international edge computing security standard projects: ITU-T X.5Gsec-netec "Security capabilities of network layer for 5G edge computing" and ITU-T X.5Gsec-ecs "Security framework for 5G edge computing services".

It also shows that China Communications Standards Association (CCSA) also proposes a 5G MEC system architecture in the General Technical Requirements for 5G Core Network MEC, as illustrated in 错误!未找到引用源。.

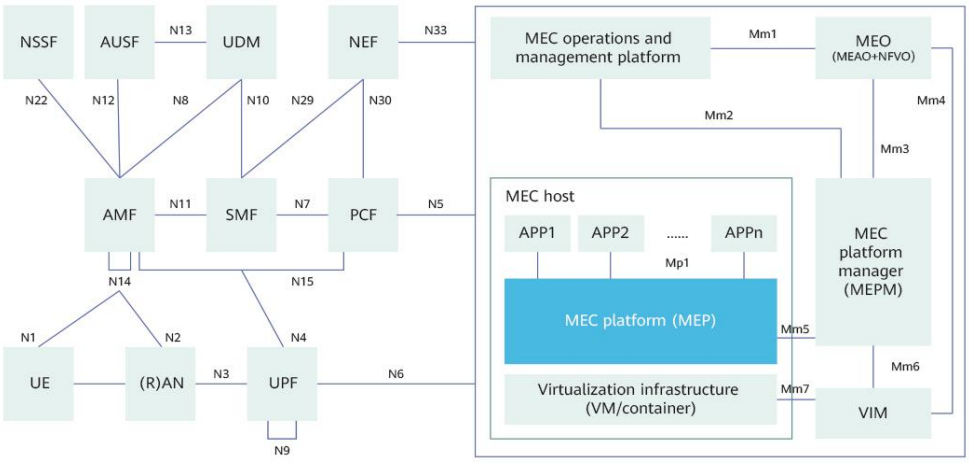

Figure 2-1 Logical architecture of the 5G MEC system

In this architecture, the 5G UPF is the MEC data plane; the MEC platform (MEP) provides the environment to run edge applications and manages them. The 5G MEP functions as the application function (AF) + data network (DN) for 5G core networks, and connects to the UPF through standard N6 interfaces.

In addition, CCSA is currently working on the 5G MEC Security Technology Research and 5G MEC Security Protection Requirements.

2.2 5G MEC Security Boundaries

3GPP specifications clearly distinguish between core and non-core networks. Even though some 5G core network functions (such as UPF) move closer to applications, they are still part of the 5G core network and comply with its traffic distribution policy. 5G MEC and RAN have

different security levels, and therefore must deploy security gateways or firewalls to secure the interconnected interfaces. Both 5G MEC and RAN interfaces are defined in 3GPP specifications, so different vendors that comply with 3GPP and ETSI can provide MEC and RAN to implement decoupling and interoperation.

The CCSA security architecture defines MEC security boundaries. In addition to meeting general UPF security requirements, CCSA expects MEC to be deployed in equipment rooms that operators can control and have a basic physical security environment. In addition,these infrastructures where the physical or virtual UPF is located should have physical security protection mechanisms (for example anti-dismantle,anit-theft,anti-tamper, the device powers off or restarts, link-down and etc. should be triggered the alarm). All this to say that MEC is deployed in a different geographic location and security zone compared to distributed RAN, and therefore it requires a totally different level of security. In principle, MEC should be deployed in equipment rooms with a secured physical environment, such as campus and aggregation equipment rooms, with clear security boundaries for both MEC and RAN base stations.

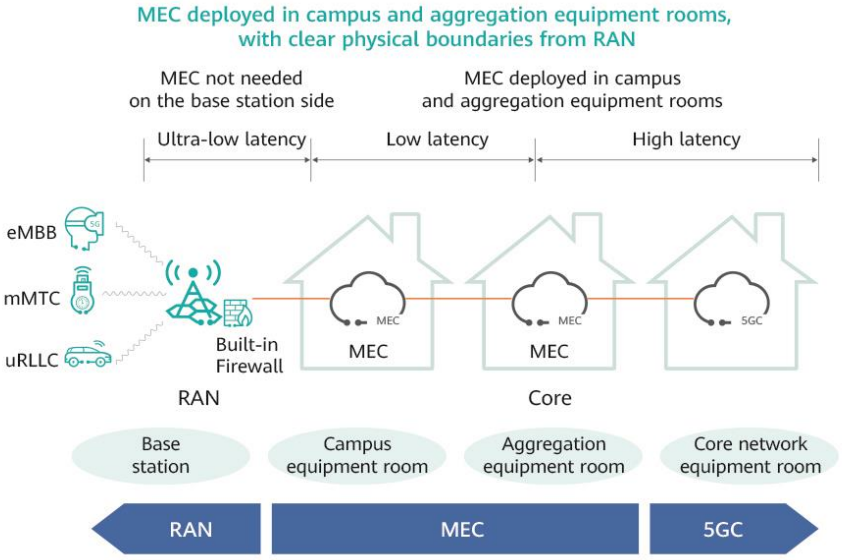

Figure 2-2 Typical 5G MEC deployment location

3 5G MEC Security Threats

5G MEC has an abundant of computing, communication, and storage resources. It can therefore provide sensitive data storage, communication applications, and computing services for many enterprises. However, if attackers were to manipulate MEC nodes and perform lateral or vertical attacks, they would severely compromise the confidentiality, availability, and integrity of applications, communications and data. This signals new security threats to users and our society. The fact that MEC nodes are usually deployed in unattended equipment rooms with multiple operators and owners throughout the security lifecycle that also brings further challenges to physical security protection and security operation and management.

3.1 Threats to Network Service Security

In the mobile edge architecture, there are a large number and various types of access devices, along with multiple security zones. This increases security risks, exposing networks to distributed denial of service (DDoS) attacks. Since 5G MEC is deployed at the network edge, it is easier for attackers to access MEC node hardware. Attackers can access network ports through unauthorized connections and obtain data transmitted over the network. In addition, MEC systems are still under the threat of conventional network attacks, such as malicious code intrusion, buffer overflow, and data theft, tampering, loss, and forgery.

3.2 Threats to Hardware Environment Security

Different from core networks that are deployed in the central equipment room with well-established physical security measures, MEC nodes may be deployed in unattended or customer equipment rooms, or even in less obvious spaces, with complex environments and weak protection and security measures. This exposes MEC nodes to devices power-off, network broken, and other security risks caused by natural disasters. It also makes them even more vulnerable to physical contact attacks, such as attackers physically accessing hardware infrastructure and tampering with device configurations. In this case, attackers could gain unauthorized access to I/O interfaces of physical servers to obtain sensitive information.

Attackers can gain unauthorized access to I/O interfaces of physical servers to obtain sensitive information.

3.3 Threats to Virtualization Security

Containers or VMs are the mostly deployed. Devices in MEC infrastructures. Attackers can tamper with container or VM images, exploit vulnerabilities in host operating systems (OSs) or virtualization software to launch DDoS attacks against containers or VMs, and exploit container or VM escape to attack the host or its other containers or VMs.

3.4 Threats to MEP Security

The 5G MEP is deployed based on virtualization infrastructure. It provides interfaces for application discovery and notification. Attackers or malicious applications can have access service interfaces on the MEP without authorization. They can intercept or tamper with communication data between the MEP and applications, and launch DDoS attacks on the MEP. Attackers can also use malicious applications to access, steal, tamper with, and delete sensitive privacy data on the MEP.

3.5 Threats to Application Security

MEC nodes connect with a large number of heterogeneous UEs and carries applications for multiple industries. These UEs and applications communicate through diverse protocols, mostly connection-oriented and

reliable, but not as secure as conventional communication protocols. Therefore, attackers can exploit vulnerabilities in such protocols to launch denial of service (DoS) attacks, perform unauthorized access, and exploit software vulnerabilities, abuse privileges, forge identities and other risks

At the same time, there may be multiple third-party applications deployed on the MEP, leading to potential unauthorized access security risks. Third-party applications may also exhaust MEC system resources, making them unavailable.

Industrial enterprises have various types of applications. Carrying high-reliability and low-latency applications over the MEP makes it more vulnerable to DoS attacks, which could lead to great losses. In addition, MEC nodes have limited resources. So, if they lack effective data backup, restoration, and audit measures, attackers may modify or delete user data on the nodes to destroy evidence.

3.6 Threats to Capability Exposure Security

MEC provides a platform to carry applications. To facilitate applications development, MEC needs to provide a series of open APIs for users to access MEC-related data and functions. These APIs facilitate applications development and deployment, which in turn makes them targets for attackers. If there are no effective authentication and authorization methods, or API security is not fully tested or verified, attackers may

access through bogus terminals, exploit vulnerabilities, or launch side-channel attacks to achieve unauthorized API invoking, unauthorized access, or user data tampering.

3.7 Threats to Management Security

Management security threats mainly include unauthorized access by malicious insiders and the use of weak passwords. Since MEC is deployed in distributed mode, operators have to manage and maintain several MEC nodes. To make the process less labor-intensive, operators reply on remote O&M. In this case, if upgrades and patching are not done in time, attackers may exploit vulnerabilities to launch attacks.

3.8 Threats to Data Security

The 5G MEP can collect and store data of an interconnected device, including application data, user data, and the like. Such data may be destroyed or leaked.

Data destruction may occur when the 5G MEP is destroyed or attacked, important data is not backed up, or no data recovery mechanism is available.

The 5G MEP platform can obtain and process the sensitive privacy data of users during service development. This may cause security risks (such as data leakage) if this data is not classified and managed by level,

encryption or anonymization methods are not deployed, or data is opened up and shared in a non-compliant manner.

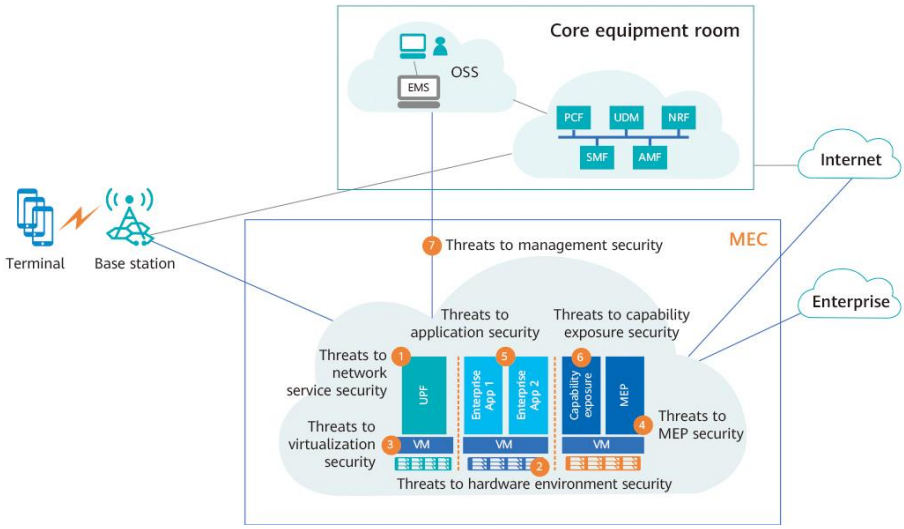

Figure 3-1 MEC security risks

4 5G MEC Security Protection

4.1 5G MEC Security Protection Architecture

There are different ways to deploy the UPF and MEP, depending on the specific requirements of each industry.

- For WAN MEC, customers do not usually have particular requirements on the deployment location of MEC. Therefore, the UPF and MEP can be deployed in operators' aggregation equipment rooms with security control to provide services for users.
- For LAN MEC, customers have highly sensitive data, so they require

operators to deploy the UPF and MEP on campus. This enables the customers to have control over the infrastructure, ensuring that sensitive data stays within the campus.

For both WAN and LAN MEC, customers may require the edge UPF to also forward their service data traffic along with the MEP. The level of surface exposure of operators' networks depends on the MEC deployment mode. As such, it is essential to determine MEC security requirements in relation to its deployment mode and customer service requirements. Security solutions should then be designed accordingly, providing secure operating environments and security services for industry customers while ensuring the security of operators' networks.

The 5G MEC security system includes infrastructure security (hardware and virtualization security), network service security, MEP security, application security, capability exposure security, and management security, as shown in **错误!未找到引用源。**.

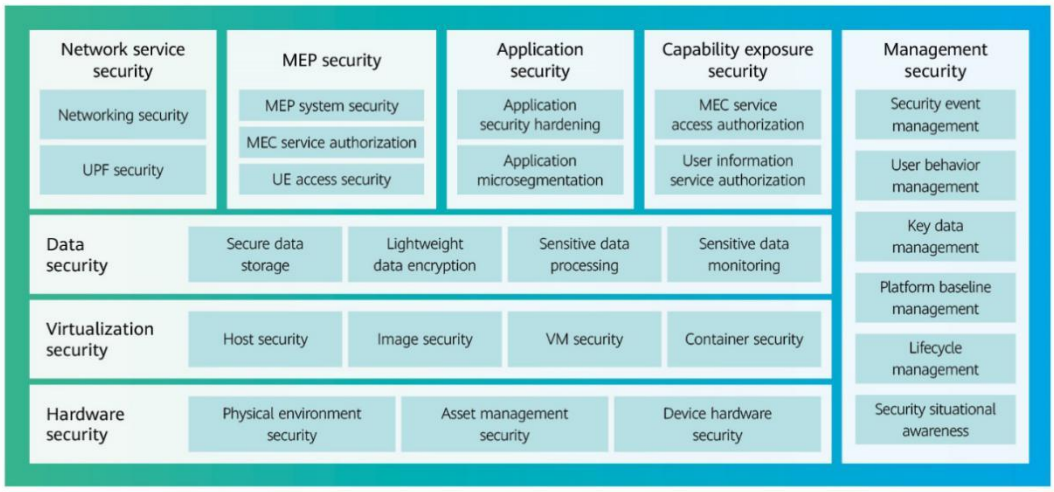

Figure 4-1 5G MEC security protection architecture

4.2 5G MEC Security Protection Requirements

4.2.1 Network Service Security

4.2.1.1 Networking Security Requirements

In addition to the UPF and MEP, 5G MEC requires the deployment of third-party applications. In this context, there are four basic networking security requirements:

(1) Three-plane isolation: Servers and switches should support physical/logical isolation of the management, service, and storage planes. If the scenario requires high service security and there are sufficient resources, physical three-plane isolation is ideal. However, scenarios that do not require high service security can adopt logical three-plane isolation.

(2) Security zone division: The UPF and the MEP that communicates with the UPF through MP2 interfaces should be deployed in a trusted zone, one that differs from the security zone of proprietary and third-party applications. The decision to implement physical or logical isolation depends on service requirements.

(3) Internet security access: If Internet access is required, a demilitarized zone (DMZ) should be set up based on service access requirements

(for example, portals whose IP addresses are exposed to the Internet should be deployed in the DMZ). In this case, security capabilities such as anti-DDoS, intrusion detection, access control, and web traffic detection should be deployed at the border for border security protection.

(4) UPF traffic isolation: The UPF should support the configuration of a whitelist and VRFs specific to the N4, N6, and N9 interfaces. A firewall should be deployed to control the security of traffic transmitted over the N6 interface of the UPF.

5G MEC networking security is closely related to the locations of the UPF, MEP, and applications, and depends on the MEC deployment mode.

(5) For WAN MEC where the UPF and MEP are deployed in the operator's aggregation equipment room, the UPF and MEP are deployed on the operator's edge cloud, and customer applications are deployed on the operator's MEP. This networking needs to meet the four basic security isolation requirements listed above.

(6) For LAN MEC where the UPF and MEP are deployed on the campus network, there are two additional security requirements to the four basic security requirements mentioned above. In terms of security zone division, the UPF and the MEP that communicates with the UPF through MP2 interfaces should be isolated from the applications, and

the applications should also be isolated from each other (for example, by dividing VLANs). In terms of UPF traffic isolation, security access control measures should be configured on the N4 interface of the UPF to control the security of traffic transmitted between the UPF and session management function (SMF).

In MEC on dedicated networks, the UPF is deployed in the operator's aggregation equipment rooms or in campus equipment rooms, and forwards traffic only. However, it still needs to meet the four basic security requirements.

4.2.1.2 UPF Security Requirements

Since core network functions are deployed at the 5G network edge along with the UPF, the core network faces increased security risks. To counter these, the UPF deployed at the edge of the 5G network should provide carrier-class security defense capabilities. The UPF should comply with 3GPP security standards and industry security specifications, and obtain NESAS/SCAS security certifications and industry security certifications in China. The UPF deployed at the network edge should be able to interoperate with mainstream core network devices and their interfaces should be compatible. UPF security requirements include network security and service security.

1. The UPF should support the following network security requirements:

(1) Isolation of different security zones

The UPF should support VLAN division for network management, core network, and RAN. The data, signaling, and management planes of the UPF can be isolated to prevent them from impacting each other.

(2) Built-in interface security functions

The UPF deployed in the customer's campus equipment room should support built-in interface security functions. For example, it needs to support IPsec to secure any data being transmitted by establishing IPsec tunnels with the N3, N4, N6, N9, and N19 interfaces of the core network element.

(3) Traffic control of signaling data

The UPF should limit the rate of signaling traffic received from and sent to the SMF to prevent signaling DDoS attacks.

2. The UPF should support the following service security requirements:

(1) Defense against DoS attacks initiated by mobile terminals

The UPF should be able to defend against DoS attacks initiated by UEs and filter data packets of UEs based on the configured packet filtering rules (ACLs).

(2) Protocol control

The UPF should have a protocol control function to determine the protocols whose IP packets are allowed or denied access to the 5G core network, thereby ensuring network security. This function can also be implemented by deploying firewalls.

(3) Detection of bogus mobile terminal addresses

The UPF should be able to detect bogus mobile terminal addresses. To do so, it matches the UE addresses of uplink and downlink traffic in a session. If the given UE address of a packet transmitted over the session does not correspond to the session, the UPF discards the packet.

(4) Policies for mutual access between UEs attached to the same UPF

The UPF determines whether to allow inter-UE access based on the operator's policy. The UPF should also be able to redirect inter-UE access packets to an external gateway, which then determines whether to allow or deny inter-UE access.

(5) UPF traffic control

The UPF should limit the rate of abnormal traffic received from UEs or applications, preventing DDoS attacks.

(6) Built-in security functions

The UPF has a built-in virtual firewall function for security control (for

example, the UPF denies the forwarding of packets sent from MEC applications to the UPF on core networks) and etc..

(7) Detection of abnormal traffic of massive UEs

The UPF and core network control plane need to detect abnormal behavior of massive UEs. This helps them promptly identify and block attacks from malicious UEs, ensuring network availability and security. They can also identify legitimate UEs hijacked by attackers, and then provide security detection and attack defense capabilities for legitimate UEs.

3. The UPF can take the following security measures for abnormal UE behavior:

- Conduct big data analytics of signaling and data traffic to detect abnormal UE traffic, filter out abnormal signaling, and control signaling overload.
- Parse data traffic features and profile the signaling behavior of UEs in attack scenarios where legitimate UEs are hijacked. This helps identify UEs with malicious traffic and abnormal signaling behavior and then implement targeted restriction and management.
- Perform security detection on UE signaling through the core network control plane. Use AI algorithms and other technologies to analyze

signaling DDoS attack characteristics based on traffic statistics, CHRs and other data to locate the malicious UEs that cause DDoS attacks.

- Provide UE micro-segmentation to prevent its unauthorized access to resources and isolate abnormal UEs or applications.

4.2.2 Hardware Environment Security

Hardware environment security includes physical environment security, asset management requirements, and device hardware security.

1. Physical environment security: The equipment room of MEC systems should be equipped with an electronic access control system at the entrance/exit to control, identify, and record people entering/leaving the equipment room. The cabinets should have an electronic anti-dismantle function, and anytime a cabinet is opened or closed, this should be recorded and audited. MEC systems should be trusted and protected against unauthorized access.

2. Asset management requirements: The infrastructure should have asset management capabilities, including:

- Physical asset management, including discovery, deletion, change, and display of physical assets. The infrastructure should support auto-discovery of hosts, or auto-discovery or manual addition of asset libraries for switches, routers, and security devices.

- Asset fingerprint management, which supports collection, analysis, recording, and display of four types of fingerprint information: listening port, software asset, running process, and account asset. Asset fingerprint management should support set collection refresh rate of listening port, software asset, running process, and account asset. And it Asset fingerprint management can also set the frequency with which fingerprint information data is collected and updated.

3. Device hardware security

The MEC server is booted and runs securely with the TPM hardware root of trust (RoT), ensuring the secure boot chain and preventing backdoors. At trusted boot, remote attestation can be used to verify the software security and trustworthiness. In the boot phase, the MEC server calculates the hash value (measurement value) layer by layer and compares the measurement value recorded by the TPM with the reference value preset on the remote attestation server (the remote server is not subject to local tampering). This process ensures that that the software runs properly.

4.2.3 Virtualization Security

1. Host security technical requirements

Unnecessary devices or functions, such as USBs, serial ports, wireless access and etc. must be disabled on hosts; unnecessary system components must not be installed; and unnecessary applications or

services, such as email agents, graphics desktops, Telnet, compilation tools and etc. must not be enabled.

Host resource access requests are controlled by user identities to prevent unauthorized operations, privilege escalation, and data leakage of the host OS.

Security hardening is required for the host OS. Different user names are allocated to administrators with different roles, and management rights vary depending on the user identity. Therefore, sharing an account among multiple administrators is prohibited. A proper password policy should also be configured for the host OS, with the password complexity, length, and validity period meeting security requirements and passwords being encrypted for storage. In addition, an OS-level mandatory access control (MAC) policy should be configured. Remote login to the host using its super administrator account is prohibited, and the IP addresses for logging in to the host should be restricted.

Secure protocols should be enabled for remote login to the host, and insecure protocols such as Telnet and FTP should be disabled. The host should be able to process login failures, and the policies for login timeout, processing consecutive incorrect password inputs, and single sign-on (SSO) should be configured.

The host system should log all OS-level access control operations and be

configured to allow only authorized users to access logs.

2. Image security

VM images, container images, snapshots and the like should be securely stored to prevent unauthorized access. The infrastructure should ensure the integrity and confidentiality of these images. The virtualization layer should support VM image integrity verification using SHA256, SM3 and the like digest algorithms as well as signature algorithms. Standard cryptographic technologies or other technical means commonly used in the industry should be employed to protect uploaded images. The infrastructure should support the use of protected images to create VMs and containers.

A constraint should be configured to ensure that images are uploaded to a fixed path, preventing users from accessing directories in the system without restriction. Users should be prohibited from switching the directory using ../ when uploading images through the CLI. They should also be prohibited from switching to other directories using the browser windows when uploading images on the GUI. In addition, the at and cron commands should be disabled to prevent any insecure operations.

Images should pass vulnerability scanning check before release. At the minimum, they should not contain high-risk or ultra-high-risk security vulnerabilities made public in authoritative vulnerability databases, such

as Common Vulnerabilities and Exposures (CVE), China National Vulnerability Database (CNVD), and China National Vulnerability Database of Information Security (CNNVD).

3. Virtualization security

To prevent data theft or malicious attacks between VMs and ensure that resources of a VM are not affected by other VMs, the hypervisor should be able to isolate resources of different VMs on the same physical server, including:

- vCPU scheduling isolation
- Storage resource isolation
- Intranet isolation

Users can access only resources allocated to their own VMs (hardware, software, and data), ensuring secure VM isolation. A VM cannot detect the existence of other VMs.

Security hardening should be performed for the hypervisor, and only the minimum necessary services should be enabled for the security management and configuration of the hypervisor.

If the hardware supports the input/output memory management unit (IOMMU), the hypervisor should support this configuration item to better

manage direct memory access (DMA) of VMs.

VM operation permissions and resource usage restrictions (e.g. minimum/maximum vCPU and memory usage) can be set, and resource usage can be properly monitored.

The hypervisor should support multi-role definition and assign different permissions to different roles to perform operations at different levels.

Access control policies, such as security groups, are migrated along with the migration of virtualized applications.

To prevent VM escape, VM isolation is used to improve virtualization security. Inter-VM isolation can be enhanced for VMs deployed in the edge virtualization environment, strictly isolating insecure devices and preventing user traffic from entering malicious VMs. In addition, the running status of VMs can be monitored in real time to effectively detect malicious VM behavior and prevent malicious VMs from migrating to other edge data centers.

4. Container security

Container security should cover the entire lifecycle of containers, and security protection can be implemented during development, deployment, and operation.

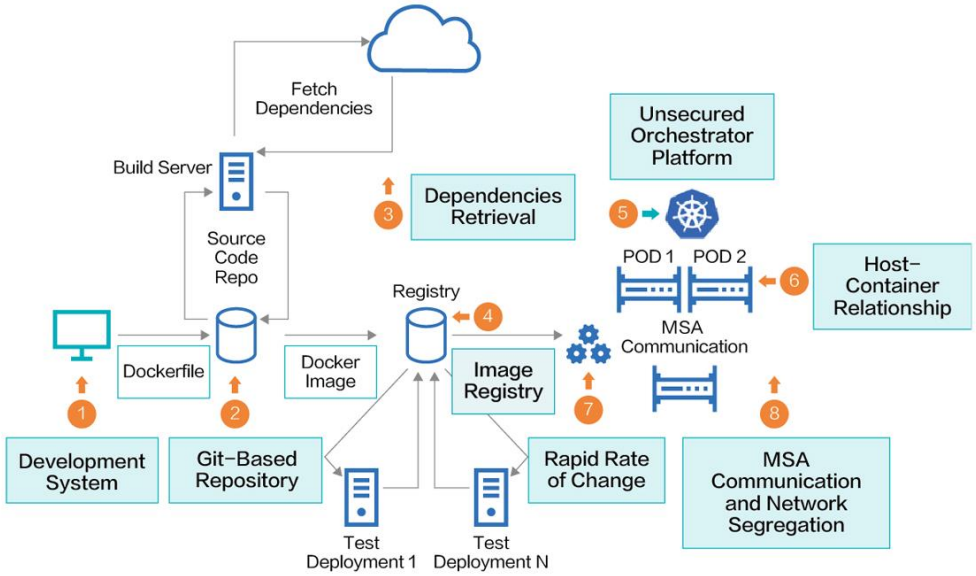

Figure 4-2 Gartner's container attack surface analysis throughout lifecycle

In the development phase, developers are required to scan for vulnerabilities in base container and intermediate images, as well as performing security checks on third-party applications or even proprietary applications or code.

In the deployment phase, the MEP monitors the security of the image repository, scans for vulnerabilities in the uploaded third-party or proprietary container images, and controls the running and use of container images with high-risk vulnerabilities.

In the operation phase, the following requirements need to be met: kernel isolation between container instances and the host; firewall mechanism deployed in the container environment to prevent unauthorized access

between containers (for example, using the NetworkPolicy that functions as a network firewall of containers to control network access between container instances); process or traffic monitoring to identify illegal/malicious behavior of container instances at runtime; API security gateway deployed at the platform layer to monitor the API invocation of the container management platform.

The system should also support host-based container behavior awareness and detection of malicious behavior such as container escape.

4.2.4 MEP Security

4.2.4.1 MEP System Security

The MEP provides registration and notification services, as well as DNS request query, route selection, and NAT for MEC applications. In addition, it has control and management capabilities based on mobile subscriber identities, ensuring user access control after service distribution. The MEP also enables service registration, making services on the MEP discoverable by other services and applications. MEP capabilities can also be exposed through APIs.

In the MEC architecture, the MEP is deployed based on the virtualization infrastructure, which is required to provide security assurance. Specifically, security hardening needs to be performed on the host OS, virtualization software, and guest OS, and virtual network isolation and

data security mechanisms need to be provided inside the MEP. The MEP provides application discovery and notification interfaces to external systems, and therefore interface and API invocation security are essential. Access to the MEP should be authenticated and authorized to prevent unauthorized access by malicious applications. In addition, to prevent communication data between the MEP and applications from interception and tampering, it is necessary to enable confidentiality, integrity, and anti-replay protection for data transmission. The MEP should also be protected against DoS and DDoS attacks. Security protection should be enabled for its sensitive data to prevent unauthorized access and tampering.

Standard interfaces in the MEC system should support mutual authentication between communication parties, and if authenticated, use secure transmission protocols (such as SSHv2, TLSv1.2 and later versions, and SNMPv3) to protect the confidentiality and integrity of communication content. Using Telnet, FTP, or SSHv1 is prohibited.

4.2.4.2 MEC Service Authorization

Mobile network operators need to authorize UEs to use MEC services, and only authorized users can use MEC services. If operators are not the ones to deploy 5G MEC services, the MEC service provider should also adopt a similar authorization mechanism to prevent unauthorized access.

For example, when a user accesses an MEC application, the core network needs to obtain the user's subscription data, and denies user access if the user has not subscribed to the application. Alternatively, the core network interacts with an application accessed by the user to obtain user authorization information, and allows user access to 5G MEC services only if the user has been authorized.

4.2.4.3 Service Authentication and Authorization during Application Switching

Applications may select different edge application servers (EASs) due to factors such as UE mobility or load balancing. Necessary context needs to be securely transferred from the source EAS to another server (EAS or cloud application server) to ensure user service continuity. Application switching can be triggered by the EAS, edge enabler server (EES), UE-side application client, or UE-side enabler client. For example, if the EAS triggers switching, the application context is transferred to a target EAS via the source and target EESs, so that the target EAS can authenticate and authorize the UE. This ensures service continuity of the UE during the application switching process.

4.2.4.4 UE Access Security

UE access security is the process of identifying UEs that are trying to access the operators' core networks and MEC to determine whether UEs

should be permitted or denied access based on preset policies. A large number of heterogeneous UEs may access MEC. These UEs communicate through various protocols, and their computing capabilities and architectures vary greatly. For example, in industrial, enterprise, and IoT MEC scenarios, many insecure communication protocols (such as ZigBee and Bluetooth) are used between sensors and MEC. At the same time, there is a lack of encryption, authentication, and other security measures, making the communication content vulnerable to eavesdropping and tampering. Therefore, a security policy should be set to allow access of specific UEs and deny access of unauthorized UEs.

In addition, it is important to perform dynamic and continuous security and trust assessment on UEs that access key core services based on the zero trust concept, as well as taking appropriate control measures upon the detection of security and trust exceptions.

4.2.5 Application Security

MEC applications can have different service types, such as operators' NEs, operators' value-added services, and third-party vertical industry services. Different types of services have different security requirements and capabilities. Third-party vertical industry applications impose particularly high security risks to the MEC environment. It is therefore essential to isolate applications with different service types and monitor

security during inter-application access. In addition, security management is required for applications throughout their lifecycle.

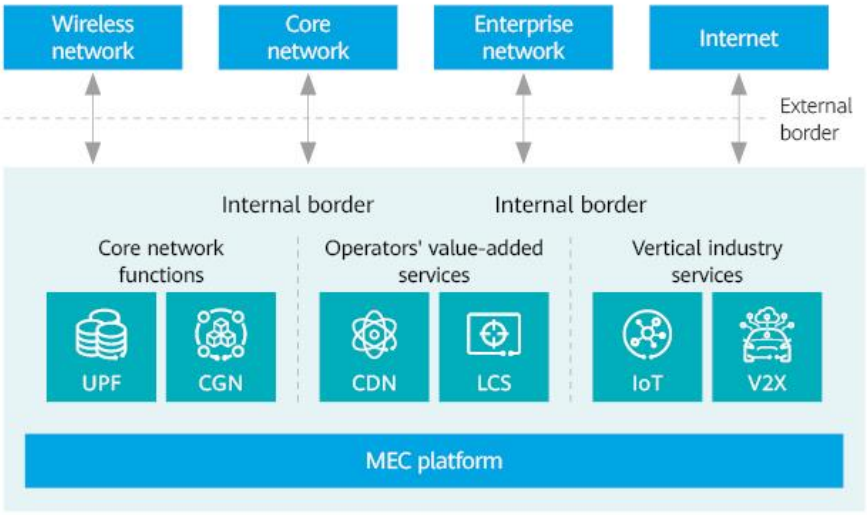

Figure 4-3 MEC application security

MEC applications are deployed on the NFV infrastructure as virtualized network functions. When MEC applications are deployed on a VM or container, the virtualization infrastructure should be able to isolate the vCPU, virtual memory, and I/O resources used by the MEC applications from those used by other VMs or containers. It should also ensure the integrity and confidentiality of application images and image repositories, as well as performing access control. For details, see the security requirements of the virtualization layer and containers.

4.2.6 Capability Exposure Security

MEC applications should be able to invoke operators' network capabilities, such as user location and QoS information, to achieve

business values. In response, operators' networks need to expose network capabilities to applications, thereby providing better services to MEC applications. However, despite its benefits, this network exposure also leads to new security threats. As such, it is essential to securely manage, publish, and expose APIs. MEC applications that function as API invokers should be authenticated and authorized to ensure the security of MEC network capability exposure. The common API framework (CAPIF) for API service invocation specified in 3GPP TS 23.222 [5] defined by the 3GPP SA2 is used for capability exposure. 错误!未找到引用源。 shows the business relationships in CAPIF.

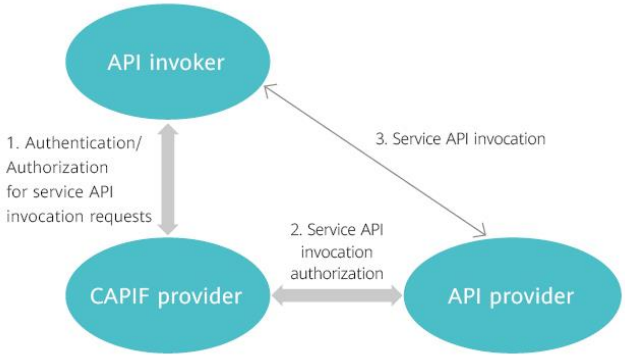

Figure 4-4 Business relationships in CAPIF

The CAPIF provider provides CAPIF core functions, processes the API invoker's requests and authorization, and manages the service APIs of the API provider.

4.2.6.1 CAPIF Architecture Adaptation

CAPIF can be deployed centrally or in a distributed manner. In distributed deployment, in addition to the CAPIF core function deployed in the PLMN, each edge data network is deployed with an independent CAPIF core function, enabling the API invoker to invoke service APIs. In centralized deployment, the CAPIF core function deployed in the PLMN manages service invoking on edge data networks, and the CAPIF core function is not deployed in a distributed manner.

With this architecture in place, the above-mentioned security mechanism can be used during API invocation between MEC servers, or if MEC servers invoke northbound APIs exposed by 3GPP networks.

4.2.6.2 User-Authorized Capability Exposure

The EAS needs to invoke the exposed capabilities of the operator's network, which involves sensitive information about the UEs, such as location information. The use of such information requires user consent, and users shall have full control over which applications can obtain the specified information of users or user devices and at what frequency. For example, when the core network receives a user location request from an MEC application, it sends the location request to the user via signaling, and returns the obtained user location information to the MEC application only after user consent is obtained.

4.2.7 Management Security

In the MEC environment, there are a large number of small-scale MEC nodes, and it is important to consider the secure operation and management of the limited edge resources. Technical means, such as cloud-edge collaboration and Security Orchestration, Automation and Response (SOAR) should be used to ensure service-oriented, intelligent, and collaborative security of the MEP.

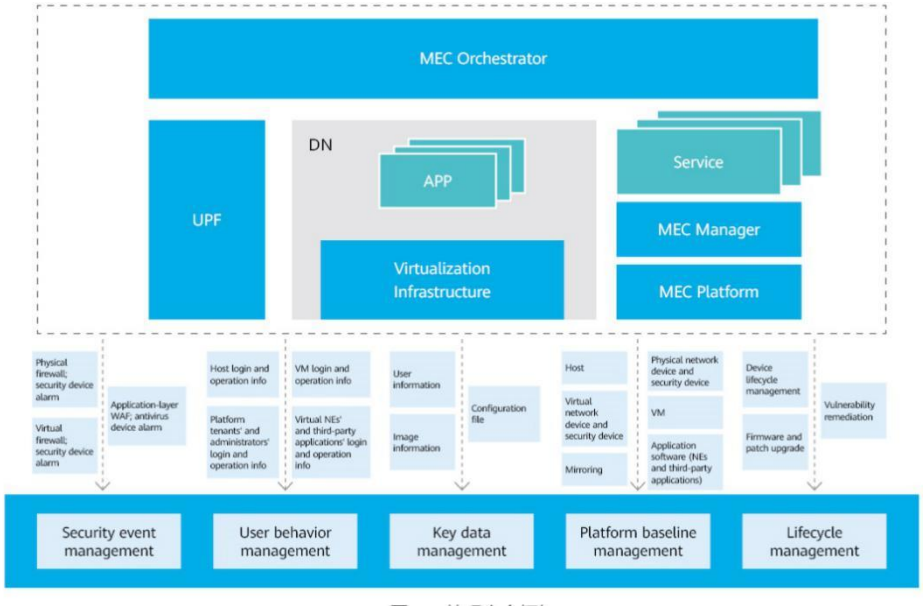

Figure 4-5 Framework for management security

Management security includes:

1. Security event management: Traces security events in the MEC system, improves the utilization of alarm logs, and generates warnings for security events. Security event management collects

alarm logs of physical, virtual, and application-layer security devices, and reports them to the situational awareness system for analysis and security warning. In addition, the alarm information is archived to facilitate subsequent log tracing.

2. User behavior management: Traces users' operations and issues warnings of risks caused by manual operations. Approval procedures are established and implemented for system changes, importance operations, physical access, system access, and other activities. A universal access portal allows to centrally manage the hosts, VMs, cloud management platforms, MEC platform managers, virtual NEs, and users of third-party applications. User behavior management records logins, logouts, and command operations, as well as using the user and entity behavior analytics (UEBA) technology to profile user behavior and generate security policies. In the case of abnormal user operations, an alarm is generated and related operations are blocked.

3. Key data management: Traces key data flow paths to prevent data leakage. The transfer of key data, such as information about users, configurations, images, and software packages, is recorded to form a data flow path. In the case of a data breach, evidence can be provided for incident tracing.

4. Platform baseline management: Ensures the reliability and security

protection capabilities of the MEP. A baseline check is performed on hosts, VMs, physical and virtual network devices, images, and application software packages (NEs and third-party applications), ensuring the security of the platform and upper-layer applications, reducing security risks, and improving the level of security protection.

5. Lifecycle management: Manages the lifecycle of UEs that access MEC, periodically updates all MEC nodes over remote connections, maintains and manages patch and firmware updates, and promptly fixes vulnerabilities. If the latest patches are not installed, or MEC nodes or terminal sensor firmware are not upgraded on time, new and complex attacks that emerge every day will pose significant risks. Equipment vendors should be able to provide sustainable vulnerability system governance and emergency response capabilities. They need to:

- Establish an end-to-end governance, response, and support organization for security vulnerability incidents.
- Establish a comprehensive vulnerability awareness channel and analysis system to ensure quick and accurate tracing.
- Define a vulnerability remediation baseline that complies with industry practices and customer needs to support rapid remediation and deployment.

- Provide timely, open, and transparent security vulnerability disclosure policies and channels, ensuring the customers' equal right to know and support downstream customers in decision-making and vulnerability handling.
- Build engineering system capabilities to ensure that the process is visible and traceable and that vulnerability-related sensitive information is secure and controllable.
- Build an organizational and personnel development system.

6. Situational awareness capability building: Implements situational awareness of edge-cloud collaboration through unified security situational awareness and collaborative defense capability building. Central cloud intrusion detection technologies can also be applied to MEC nodes to detect malicious software and attacks. In addition, distributed edge intrusion detection technologies can be used to identify the distributed edge situational awareness, and then the security situation can be presented on the management plane of the central cloud.

Unlike in legacy network scenarios, it is impossible to apply heavyweight defense capabilities in MEC scenarios because of their deployment at the network edge, capability exposure, and limited resources. Therefore, MEC scenarios face greater security threats. In response, technologies

such as whitelist, rule, and AI algorithm can be used to build lightweight security situational awareness capabilities into edge scenarios. These should be based on the service characteristics of MEC nodes to achieve high-performance threat detection and a high detection rate.

The lightweight security situational awareness capabilities built into edge scenarios implement security configuration check and system hardening before device access to reduce system vulnerabilities, achieve real-time intrusion detection and scheduled configuration check and hardening when the platform is running, and promptly detect abnormal behavior such as network attacks and system configuration tampering and quickly respond to reduce the adverse impact.

The orchestration management system architecture of MEC is similar to that of NFV. As shown in the ETSI MEC reference architecture referenced in 错误!未找到引用源。, the MEC orchestration management system consists of the MEC orchestrator (MEO) and MEC platform manager (MEPM). Its southbound interfaces connect to the virtualization infrastructure manager (VIM) and MEP, and northbound interfaces connect to the operations support system (OSS) of operators. Interfaces connecting the OSS, MEO, and MEPM are involved in API invocation and are not directly available to users or the Internet. In addition to strict access control, API gateways can be deployed to implement security

control on API invocation.

Management and maintenance interfaces in the MEC system should be able to authenticate the identity of UEs that are accessing the system, and if authenticated, use secure transmission protocols to protect the confidentiality and integrity of communication content.

4.2.8 Data Security

In the MEC environment, the service mode is complex; it runs in real time, processes heterogeneous data from various sources, features perception, and has limited UE resources. As such, data security and privacy protection mechanisms previously used in conventional networking cannot protect the massive data generated by MEC nodes. New approaches to data security governance are required, such as lightweight data encryption, secure data storage, and sensitive data processing and monitoring. These technical capabilities will ensure the security of data throughout its lifecycle (data generation, collection, transfer, storage, processing, use, sharing, and destruction), covering data integrity, confidentiality, and availability.

It is essential to ensure the security of data stored on MEC nodes and transmitted in complex and heterogeneous MEC networks in WAN and LAN MEC scenarios. Important data that ensures service running should be identified among the large amount of data stored, ensuring its secure

backup and restoration to prevent service interruption due to data destruction. In addition, remote data backup should be provided, backing up important data to a remote site through the communication network. Functions such as backup data consistency check and backup location query should be supported.

Another security risk is privacy data leakage of MEC users. To address it, privacy protection technologies such as lightweight encryption, data aggregation, differential privacy-based data protection, and federated learning are required. In addition, data can be classified and managed based on data types during data routing. Data related to user privacy should be tagged and isolated at the data ingress of each MEC node by firewalls. At the same time, all unnecessary services and ports should be disabled based on the minimization principle. Then, the important tagged data should be provided with integrity, confidentiality, and anti-copy protection. In addition, to prevent privacy data leakage of open APIs, the intrusion detection technologies of the cloud computing service center can be applied to MEC nodes to detect API users, preventing attackers from obtaining users' privacy data. To address distributed MEC deployment, a distributed intrusion detection technology can be used, allowing multiple MEC nodes to collaborate with each other to detect malicious attacks in a self-organizing manner [3].

Data desensitization protects user data related to privacy (for example, data that can identify an individual, including identity information, location information, and privacy data) and identity (including data known to, owned (e.g. smart cards), and possessed (e.g. biometric features) by users), using mainstream data security technologies, such as encryption (including symmetric and asymmetric encryption) or desensitization (including anonymization and pseudonymization). In addition, data storage is enhanced to prevent data loss and ensure the confidentiality and integrity of user data. MEC should support user admission control, VPN secure access tunnels, and user data encryption, ensuring that devices have secure access. When it comes to enterprise campus networks in particular, user access authorization can be implemented by connecting the user access authorization server to the enterprise's authorization server.

5 Case Studies for 5G MEC Security

5.1 Smart Grid

5.1.1 Overview

WAN MEC is not limited to specific geographical areas. Generally, it is possible to securely carry services from different industries over E2E public networks of operators through network slicing. The main industries to apply WAN MEC are transportation, power grid, Internet of

Vehicles (IoV), and ultra-large enterprises with cross-regional business.

For example, MEC deployed for smart grids needs to match the traffic direction of power services to avoid traffic detours, in addition to satisfying service latency and isolation requirements. Specifically, MEC is deployed at the province, city, and district/country levels (aggregation and upper layers) based on the characteristics of power grid services, with large-scale implementation at the province and city levels. This makes smart grid a typical WAN MEC security scenario.

Province-level: centralized provincial services with the main site at branches and subsidiaries. The UPF is deployed at the provincial branch to offload centralized provincial service traffic, such as metering and bus monitoring.

City-level: municipal termination services with the main site at municipal bureaus. The UPF is centrally deployed at the city level to offload local traffic, such as automated telemetry, remote signaling, and remote control for power distribution networks, differential protection for power distribution networks, precise load control, phasor measurement unit (PMU), distribution transformer monitoring, intelligent power distribution room, online monitoring of transmission lines, and charging piles.

District/County-level (not for large-scale implementation): ultra-large

cities, substations/converter stations, and large-scale closed areas such as pumped storage power plants. In scenarios where substations have high requirements for both security and level-by-level offloading and monitoring, the UPF and MEC can be deployed in substations or districts/counties. For example, it is possible to deploy substation inspection robots, status detection, and video surveillance.

5.1.2 Smart Grid Security

Power grid security is critical to the national economy and people's everyday life. Therefore, as a typical WAN MEC scenario, smart grid has strict security requirements. Power grid security isolation requirements are based on the Provisions on the Security Protection of the Electric Power Monitoring Systems (Order No. 14 of the National Development and Reform Commission) and Notice of the National Energy Administration on Issuing the Overall Solution on Power Monitoring System Security Protection and Other Security Protection Solutions and Evaluation Specifications (No. 36 [2015] of the National Energy Administration). According to the latter, power grid services should comply with general security principles: security zoning, dedicated networks, horizontal isolation, and vertical authentication.

5.1.2.1 Security Zoning

Power grid business is mainly divided into the production control area

and management information area.

1. The production control area contains two types of services: production control and production non-control.

(1) Production control services include automated differential protection, wide area synchronous phasor measurement, and automated telemetry, remote signaling, and remote control for power distribution networks. Production non-control services are mainly metering services, such as power and voltage quality monitoring and smart power consumption in factories, campuses, and buildings.

(2) For production control area services, a massive number of network nodes are scattered and full network coverage is required through the whole phases, which is a WAN scenario. In this case, the 5G network needs to provide high security isolation, low latency, high-frequency forwarding, high-precision timing, and other capabilities. The user-plane UPF is connected to the dedicated MEC in the power production control area.

2. The management information area contains video services in the management zone and dedicated LAN services.

(1) Video services in the management zone include the inspection of substations and lines using robots and drones, as well as camera

surveillance. These services belong to WAN scenarios and require the user-plane UPF to be connected to dedicate MEC in the power management information area.

(2) Dedicated LANs are used to implement power grid services in LAN scenarios such as smart campuses and smart substations, with limited coverage in specific areas. These services require the 5G network to provide high uplink bandwidth and local data processing capabilities. The user-plane UPF is connected to the dedicated MEC in the power management information area. The user plane can be moved further downwards, and depending on the service requirements, it is possible to deploy a small-scale MEC at the power campus. This will ensure that data stays within relevant sites, complying with the security requirements of MEC for smart grids.

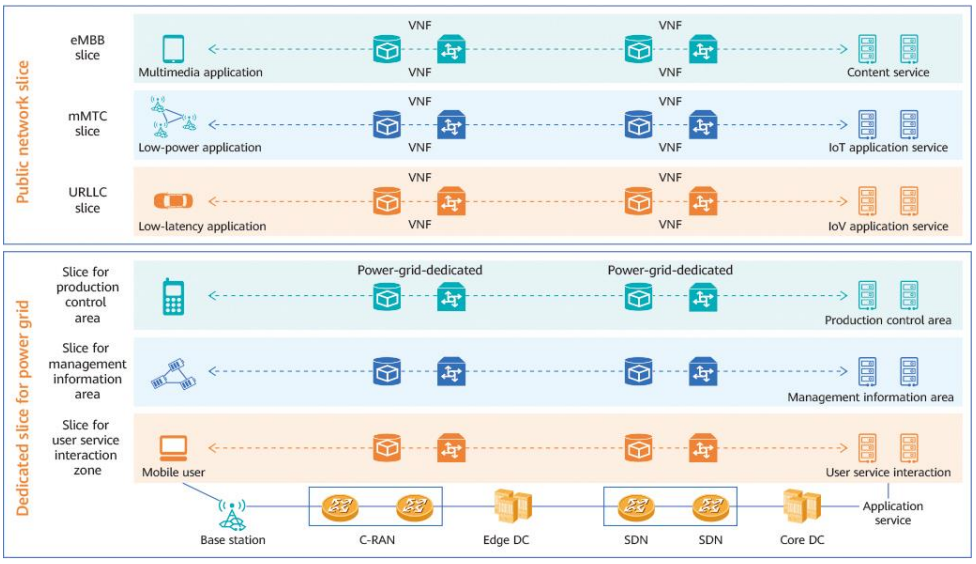

Figure 5-1 Overall framework of the 5G slices for power grid

5.1.2.2 Dedicated Networks

Dedicated networks are used for physical or logical isolation.

1. Physical isolation between production control area services and other services: If some production control area services use the wireless public network, wireless communication network, and network devices and terminals in the uncontrollable state for communication, and their security protection level is lower than that of other systems in the production control area, secure access zones should be set up, and security isolation, access control, authentication, and encryption measures should be taken. Typical services include distribution network automation, load control and management system, and distributed energy control system.

2. Logical isolation between different services in an area: MPLS VPN, security tunneling, permanent virtual circuit (PVC), and static routing technologies can be used to build subnets for logical isolation.

5.1.2.3 Horizontal Isolation

Horizontal isolation serves to isolate main sites in different areas.

1. Isolation between the production control area and management information area: A horizontal unidirectional security isolation device, one that is tested and certified by the designated national department,

must be deployed. The strength of isolation should be nearly or as strong as physical isolation.

2. Isolation inside the production control area: Network devices and firewalls that provide the access control function should be deployed to logically isolate different services.

3. When the production control area is connected to the secure access zone, a horizontal unidirectional security isolation device dedicated to the electric power industry should be deployed for centralized interconnection.

Legacy networks carrying electric power services can be dedicated power networks or public networks. For dedicated power networks, physical isolation is implemented using resources such as wavelengths, timeslots, and physical fiber cores, and logical isolation is implemented using VLANs and VPNs. For public networks, secure access zones should be used for production control services, and firewalls be used for management information services.

	Legacy network		5G	
	Production	Management	Production	Management
Physical layer of the dedicated network	Use different wavelengths, timeslots, and physical fiber cores		Slicing (time, frequency, and space domains on the air interface, time division on the transport network, and independent server on the core network)	
Logical layer of the dedicated network	Use VLAN, VPN, etc.		Slicing (VLAN, IP tunnel, and VM)	
Public network	Secure access zone	Firewall	Secure access zone	Firewall

Figure 5-2 Differences between 5G and legacy networks in carrying electric power services

Compared with legacy networks, 5G public networks have a brand-new E2E network slice isolation solution when carrying electric power services. With MEC and slicing, 5G can provide E2E physical and logical isolation for services. At the physical isolation layer, the air interface uses resource blocks (RBs) based on orthogonal dimensions of time, frequency, and space domains to transmit data. The transport network uses FlexE-based hard isolation to have exclusive timeslots similar to TDM; services can be carried over network slices based on time division, and services on different FlexE slices do not affect each other. The core network uses NFV to allocate independent physical server resources to the power grid. The E2E slicing technology from the wireless air interface, base station, transport network, to core network isolates a dedicated wireless network at the physical resource layer dedicated to the electric power industry, meeting the security and reliability requirements of power grid services. At the logical isolation layer, 5G network slices

still use VLANs, IP tunnels, and VPN VMs to logically isolate services.

5.1.2.4 Vertical Authentication

According to the 5G communication mechanism, attributes such as DNN (similar to the public network APN) and network slice identifier (NSSAI) are allocated in advance during account registration for power grid services. When a service goes online, the UE first initiates an attach request to the 5G network, and then completes the 5G AKA primary authentication during the attach process. The core network allocates the SMF and UPF based on the allocated subscription attributes such as DNN and NSSAI to establish a PDU session. The 5G communication mechanism requires user data to pass through the UPF before being forwarded. This ensures that data is transmitted over the transmission tunnel from the UE to the base station and then to the UPF. During this process, data is not exposed to the public network, thereby ensuring security of users' communication data.

However, there are some dispatching centers, power plants, and substations that require special protection because their data is highly sensitive. In this case, their data should pass through dedicated vertical encryption and authentication devices or encryption and authentication gateways and related facilities. This implements bidirectional identity authentication, data encryption, and access control. Vertical encryption

and authentication devices authenticate and encrypt WAN communication, protecting the confidentiality and integrity of the data in transmission, as well as ensuring secure filtering. In addition to all the functions provided by encryption and authentication devices, the encryption and authentication gateways should also be able to process power systems' data communication application-layer protocols and messages.

5.2 Smart Factory

5.2.1 Overview

A smart factory is a typical LAN MEC scenario. LAN MEC applies to situations where services are limited to specific geographical areas to implement closed-loop services on 5G networks in specific areas and ensure that core service data of the industry is not transmitted out of the campus. LAN MEC mainly applies to campus/plant-based enterprises, such as manufacturing, steel, petrochemical, port, education, and healthcare. Take the manufacturing industry as an example. Conventional manufacturing factories mainly use wired networks, Wi-Fi, 4G, and short-distance wireless technologies to connect to the Internet, and all of these networking technologies have their own shortcomings. Specifically, wired network deployment takes a long time and is difficult to implement; Wi-Fi is unstable and vulnerable to interference; 4G has insufficient bandwidth and high latency; short-distance wireless technologies such as

Bluetooth and radio frequency identification (RFID) can only transmit a small volume of data over a limited distance. Therefore, the industry urgently needs a network technology with comprehensive advantages.

5G networks feature high bandwidth and low latency. They are also stable and reliable, which makes them more suitable for production and manufacturing requirements of a smart factory. In this case, 5G service applications are implemented in a smart factory, including remote monitoring, visualization, remote guidance, and high-speed collaboration in physical and chemical inspection during equipment trial and manufacturing. The overall project covers component material inspection, AR-assisted component assembly, status monitoring and analysis during equipment trial, and AR-based remote guidance for the maintenance of any identified issues. The project preliminarily implements equipment trial and manufacturing throughout the process, achieves secure production, and improves the efficiency of research and production.

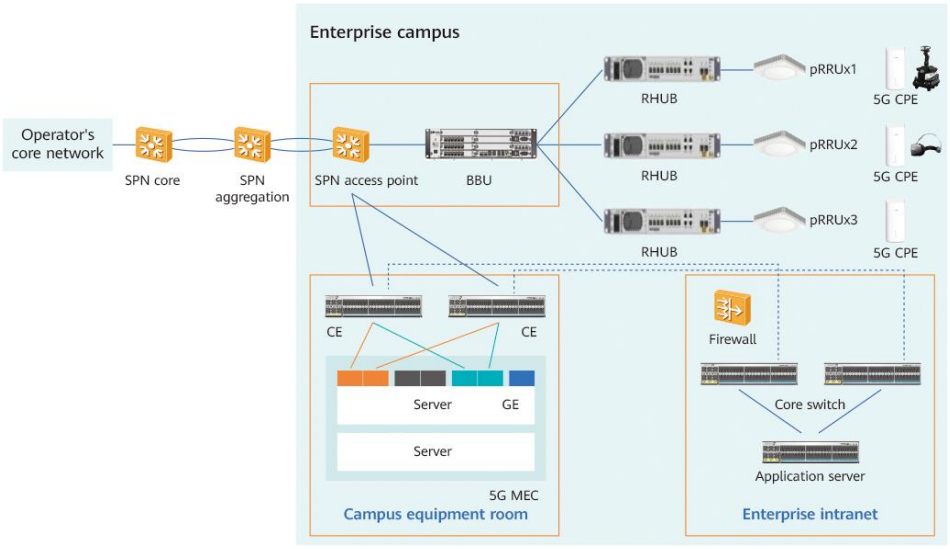

Figure 5-3 MEC network architecture for smart factory

To meet service requirements, the smart factory network architecture consists of 5G UEs, 5G base stations, 5G transport network, and 5G core network. In addition, the MEC LBO mode is deployed to implement low-latency and high-bandwidth access to local network resources and ensure that data is not transmitted out of the factory. In this case, the equipment complies with 3GPP specifications and meets the carrier-class reliability of 99.999% or higher.

5.2.2 Smart Factory Security

This case is designed based on the security requirements of level-3 classified protection. The 5G cyber security solution is provided for the smart factory, covering UE access security, confidentiality and integrity protection of the communication network, enterprise network border

isolation, and security management and audit, to meet the key requirement that factory data stays within the campus.

5.2.2.1 UE Access Security

A CPE equipped with a SIM card initiates a registration procedure to the 5G network, and then initiates a registration authentication procedure to the control plane of the 5G core network through the 5G base station and 5G transport network. During this process, the identity of the SIM card is authenticated (in compliance with the 5G AKA mutual authentication standard) to prevent unauthorized access to the 5G network.

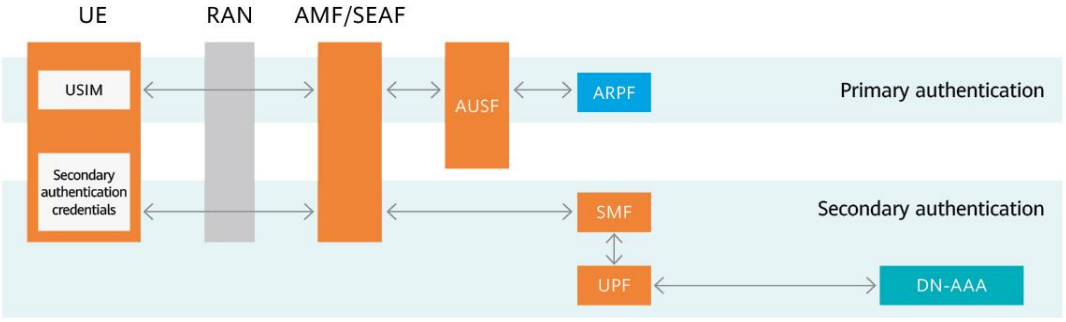

Figure 5-4 User authentication

Since operators provide the authentication capabilities of SIM cards, if enterprises need to independently authenticate and manage enterprise UEs, they can deploy AAA services to perform secondary authentication on enterprise UEs. This ensures that only authorized users and UEs are allowed to access the campus network.

For example, when employees enter their enterprise campus, they need to show their ID cards as primary authentication for their entry into the campus. They also need to show their employee ID cards as secondary authentication (where personal ID authentication is required) to demonstrate that they have permission to enter specific areas on campus.

5.2.2.2 Communication Network Confidentiality and Integrity Protection

1. The 5G air interface security and transmission security mechanisms are used to implement E2E segment-based confidentiality and integrity protection on 5G networks.

(1) 5G air interface security ensures confidentiality and integrity of radio interfaces (air interface) between 5G UEs and base stations.

- Confidentiality: On the 5G network, encryption protection is enabled for air interface signaling and user data (user authentication information is exchanged through signaling data) to convert user data into ciphertext, preventing data disclosure. In addition, the 5G network supports 128-bit encryption algorithms.

- Integrity: The 5G network supports integrity protection for signaling messages and user-plane data. 5G CPEs and base stations use integrity algorithms to ensure that signaling messages and user-plane

data are not tampered with.

(2) Transmission security ensures confidentiality and integrity from the base station to the UPF and from the UPF to the enterprise intranet. Operators and enterprises can deploy IPsec to ensure confidentiality and integrity of the transport network.

2. Enterprises deploy security capabilities of CPEs and border security gateways to ensure security of communication links at the application layer.

(1) Creating a dedicated tunnel for local transparent transmission: In addition to E2E segment-based confidentiality and integrity protection on 5G networks, 5G CPEs need to subscribe to DNNs. The core network control plane selects the UPF for a CPE based on its subscribed DNN. Then, the UPF and base station establish uplink and downlink dedicated tunnels for the CPE, ensuring that user data is transmitted only between the 5G base station, UPF on campus, and campus intranet. This establishes a dedicated pipe for local transparent transmission, ensuring that data is not transmitted out of the campus.

(2) Deploying E2E encryption and integrity at the application layer: The industrial-grade CPEs provided in this case support IPsec encryption. These CPEs can use IPsec-capable 5G modules, together with the

security gateway (built in the firewall) deployed at the enterprise intranet border to implement IPsec encryption and integrity protection between UEs and the security gateway. This E2E secure communication link is independent of security capabilities of operators' 5G networks.

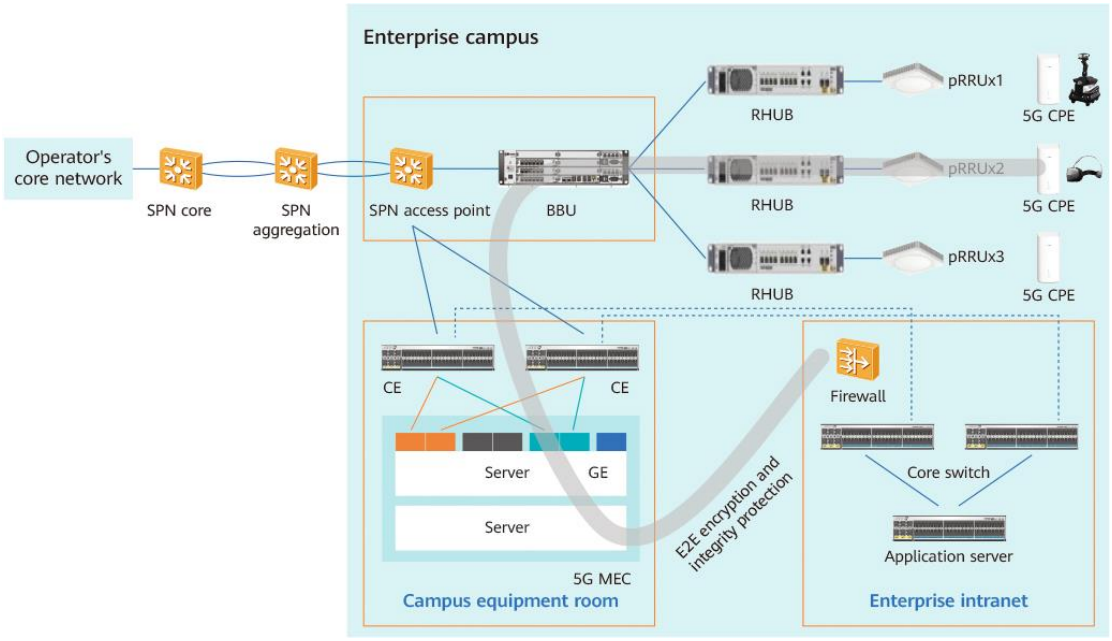

Figure 5-3 E2E encryption and integrity protection

5.2.2.3 Enterprise Network Border Isolation

To ensure the border security of the 5G and enterprise networks, a firewall can be deployed between the UPF and the core switch on the enterprise network. The firewall provides refined access control policies to reduce the attack surface, traffic and behavior analysis capabilities, and malware defection.

The firewall adopts a security policy of least privilege, so incoming

traffic enters the untrust zone. The security policy is configured based on protocols and allows only IKE and IPsec traffic to pass through. The firewall forwards outgoing traffic through the trust zone, with the destination being the IP address and port number of the server connected to the 5G CPE. This minimizes the attack surface and implements refined access control.

Logs (in syslog format) are generated if there are firewall configuration changes, traffic blocking by security policy, and abnormal traffic blocking. They are then sent to the security management center for compliance and audit purposes.

The firewall provides a UI with the read-only permission to read configurations, query historical packet loss records, and perform primary security troubleshooting.

5.2.2.4 Security Management and Audit

The log audit system deployed at the security management center collects system security events, user access records, system run logs, system operating status, and other information from the border firewall in a centralized manner. First, it standardizes, filters, and merges data, as well as analyzing alarms. Then, the system uniformly stores and manages the data in the form of logs. This facilitates the comprehensive auditing of information system logs, helps administrators troubleshoot faster, and

provides objective evidence for fault tracking and recovery.

6 Outlook

MEC is a new model to extend computing capabilities to the edge, with the support of networks. It involves the network, edge cloud, and edge applications, which together provide services in close proximity to users to reduce latency, save bandwidth through local computing, ensure security through data isolation, and reduce costs through computing offloading. 5G offers native support for MEC, which is ultimately an effective means to improve E2E user experience for new services.

As MEC continues to gain popularity, we shall ensure a secure 5G MEC environment, develop global unified 5G standards and certification systems, implement 5G security baseline requirements, promote E2E security by assessing the security of applications, and generally build upon the current level of cyber security by looking toward future implementation.

Appendix I: Acronyms and Abbreviations

Acronym or Abbreviation	Full Name
AI	Artificial Intelligence
AKA	Authentication and Key Agreement
API	Application Programming Interface
CAG	Closed Access Group
CAPIF	Common API Framework
DDoS	Distributed Denial of Service
EAS	Edge Application Server
EES	Edge Enabler Server
MEC	Multi-Access Edge Computing
MEP	MEC Platform
NID	Network Identifier
RAN	Radio Access Network
SMF	Session Management Function
TPM	Trusted Platform Module
UEBA	User and Entity Behavior Analytics
UPF	User Plane Function
VM	Virtual Machine

Appendix II: References

[1] MEC Security White Paper, Alliance of Industrial Internet, November 2019

[2] 3GPP TS 33.501. Security Architecture and Procedures for 5G System[S], 3GPP

[3] 5G-ENSURE_D2.7 Security Architecture[R], 5GPPP

[4] ETSI GS MEC-002. MEC Technical Requirements[S], ETSI

[5] 3GPP TS 23.222 Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs

[6] GTI 5G Network Security Consideration[R], GTI

[7] 5G empowering vertical industries, EU 5G PPP