GTI Operator Secure Access Service Edge White Paper

Version:	v1.0.4
Deliverable Type	□ **Procedural Document** ☑ **Working Document**
Confidential Level	□ **Open to GTI Operator Members** □ **Open to GTI Partners** ☑ **Open to Public**
Working Group	**5G ENS**
Task	**Task-T-PM3-PJ5-6: 5G Endogenous Security**
Source members	CMCC
Support members	CT
Editor	Jia Chen(CMCC), Li Su(CMCC), Kai Yang(CMCC), Peng Ran(CMCC), Cancan Chen(CMCC), Yuhang Zhao(CMCC), Haiyang Su(CMCC), Haiyan Zhao(CMCC), Xinmiao Yang(CMCC), Dongjie Lu(CMCC), Yi Jiang(CMCC), MingXia Bo(CT), Bangling Li(CMCC)
Last Edit Date	（06-08-2023）
Approval Date	

Document History

Date	Meeting #	Version #	Revision Contents

Table of Contents

1	SASE Overview	4
2	Scenario Requirements Analysis	6
3	Operator SASE Framework	8
4	Telecom Operators SASE Application Cases	12
5	Outlook	16
6	Summary	17

1 SASE Overview

1.1 Background

With the widespread adoption of mobile networks and cloud computing, enterprise digital transformation is accelerating. The core business and critical data of enterprises are being transferred from traditional data centers to the cloud. At the same time, the operation mode and work styles of enterprises are being changed significantly, with the popularization of multi-point office and remote/mobile office.

Traditional network security architecture is no longer suitable for the trend of business digitization and cloudization. For example, traditional security strategies are primarily based on boundary protection, which sets up security devices at the network boundary of the enterprise to protect its network and data. However business digitization and cloudization have blurred traditional network boundaries, and stacking multiple security technologies may increase the complexity of enterprise security systems, leading to operational difficulties and decreased efficiency.

In the process of business digital transformation, enterprises need to flexibly configure their network and security services to cater to various network access scenarios, and provide security that meets experience and policy requirements. In 2019, Gartner introduced SASE(Secure Access Service Edge) in their report "Hype Cycle for Enterprise Networking 2019", which they believed was the solution to this problem.

1.2 Definition

According to the Gartner report ‘The Future of Network Security Is in the Cloud’, the secure access service edge is an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS and ZTNA) to support the dynamic secure access needs of digital enterprises. SASE supports branch office, remote worker and on-premises secure access use cases. SASE is primarily delivered as a service and enables zero trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies.

1.3 Benefits

With SASE, enterprises can eliminate the effort and costs required to maintain complex and fragmented infrastructure made of point solutions. SASE also obtains more flexible, efficient, and secure network and security services to better cope with the growing challenges of modern networks:

1. Simplicity

SASE integrates network security services into cloud platforms, providing identity-centered security protection. It determines routing selection and access level based on comprehensive trust evaluation of roles, device information, user behavior, location, and other

features, and formulates a unified security policy for the entire network, protecting enterprise networks and achieving network security and data security in a blurred network boundary environment without any device or location restrictions.

2. Efficiency

The SASE security framework can sink security and network capabilities to PoP, CPEs, or controlled terminals. Branches and users can access nearby according to their needs, reducing the middle link of data transmission, thereby reducing network latency and packet loss, and improving network performance and efficiency.

3. Security

SASE integrates multiple security functions on one platform with abundant services. By using intelligent proxy technology, all data flows through unified security control and detection, thereby improving security and reliability and reducing the risk of data leakage and attacks.

4. Flexibility

With SASE, enterprises can flexibly expand and customize cloud or edge-side security functions according to their business scenarios to meet the network security needs of different businesses.

1.4 Advantages for Telecom Operators

As providers of network infrastructure, telecom operators have significant advantages in building SASE compared to other industries, specifically in terms of the comprehensive network infrastructure, the strong standard promotion capability, and the high brand influence:

1. Network advantage

Operators already have a network infrastructure that covers the world, providing high-reliability and high-performance network services globally, saving other industries' investment costs in constructing and maintaining the network infrastructure. In addition, operators have years of experience and resources in the security field and can provide comprehensive security solutions for enterprises to ensure their network security. Also, SASE PoPs can reuse network access points and cloud resource pools deployed by operators in various locations, and SASE edge devices can reuse network CPEs of operators, thereby reducing the implementation cost of SASE.

2. Standard advantage

By promoting the development of enterprise and industry standards, operators can integrate the network and security capabilities of various manufacturers, and provide enterprise customers with a full-stack, optimal network and security capability.

3. Brand advantage

Operators have a wide range of industry customer base and strong brand effect. SASE services promoted by operators are more easily accepted by enterprise customers. In addition, adding security capabilities to existing network services makes it easier for users to accept.

2 Scenario Requirements Analysis

2.1 Scenario 1: Wide Area Network Interconnect

The traditional enterprise network is centered around the headquarter, with communication between branches and access to the internet generally passing through the headquarter where unified security measures are deployed. In a wide area network scenario, it is necessary to achieve flexible interconnection among multiple entities across the network, and there is a greater need for interconnection between branches and the cloud. Direct branch access to the internet is also becoming more common.

Enterprises should strengthen network security protection, perform security detection on endpoints, and ensure data security in servers. Enterprises need to dedicate encrypted transmission channels to prevent data theft and tampering. Boundary security devices need to be deployed to protect against DDoS attacks and network intrusions from the internet. In addition, to prevent unauthorized access to branches, clouds, and headquarters, an identity authentication mechanism should be deployed among branches, clouds, and headquarters.

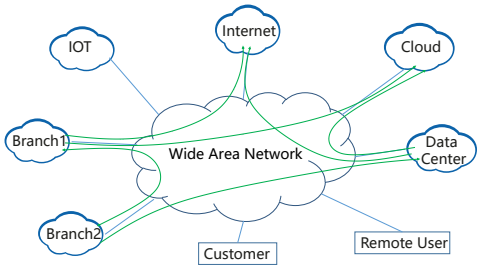

Figure 2-1 wide area network interconnect

2.2 Scenario 2: Mobile/Remote Access

When employees work remotely, and when customers or third parties (contractors, partners, etc.) access enterprise services, they need seamless access to enterprise applications located in the cloud and data centers, while also being able to access the internet. Enterprises need to provide security protection strategies at the endpoints, in the cloud, and at the enterprise headquarters.

Enterprises should strengthen security protection from the terminal, network, and server. To prevent the access terminal from being used as a springboard to attack the internal network and applications, enterprises should protect the security of employees' office terminals, such as preventing viruses and intrusions. Access from client endpoints and third-party endpoints should be restricted to preventing network threats, such as deploying web protection facilities and antivirus facilities. After a terminal accesses the network, it is essential for enterprises to authorize the identity of the users and monitor their behavior to ensure security. Moreover, enterprises also need to monitor encrypted/non-encrypted data streams to prevent enterprise data from being leaked or tampered, and detect enterprise data downloaded by access terminals to prevent data from downloading or obtaining unauthorized.

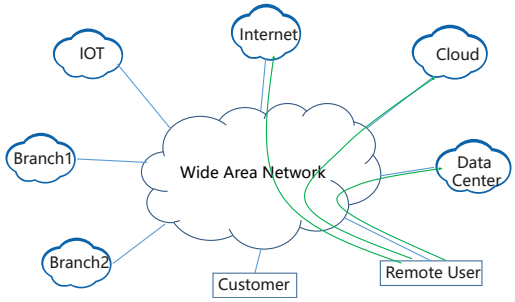

Figure 2-2 Mobile/remote access

2.3 Scenario 3: Business Migrate to the Cloud

In certain 5G and IoT use cases, low latency and high reliability are essential. To achieve this, traffic must be forwarded to local edge computing nodes for rapid computation and processing. Besides, once the data is processed by the edge computing nodes, the results can be uploaded to the cloud or data center.

Enterprises need to strengthen endpoint security and protect data security. When the private network is connected to the public network, access devices need to be authenticated to prevent spoofed device access; DDoS attacks and network intrusion from massive private network devices need to be prevented; address obfuscation for private network devices is needed to prevent sensitive information leakage. Edge computing nodes need to implement secure storage of data to prevent user data leakage; to ensure edge devices from different industries can access to the independent network, computing, and storage resources, resource isolation should be implemented; encryption secure channels need to be established between private network devices and edge computing nodes, and between edge computing nodes and cloud/data centers, to protect data security.

In actual commercial operating environments, single access scenario is generally unable to meet enterprise needs. Enterprise networks often operate in mixed scenarios composed of multiple basic access scenarios, for example, a multinational catering company has branches around the world that access the central data center, and employees or third parties need to access it remotely.

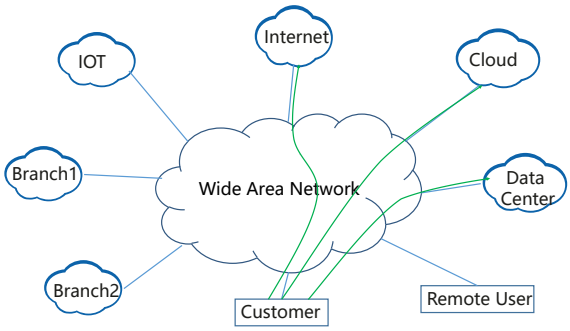

Figure 2-3 business migrate to the cloud

2.4 Summary

Based on the above application scenarios, the corresponding security requirements and capabilities of the scenarios under new business are summarized in Figure 2-4.

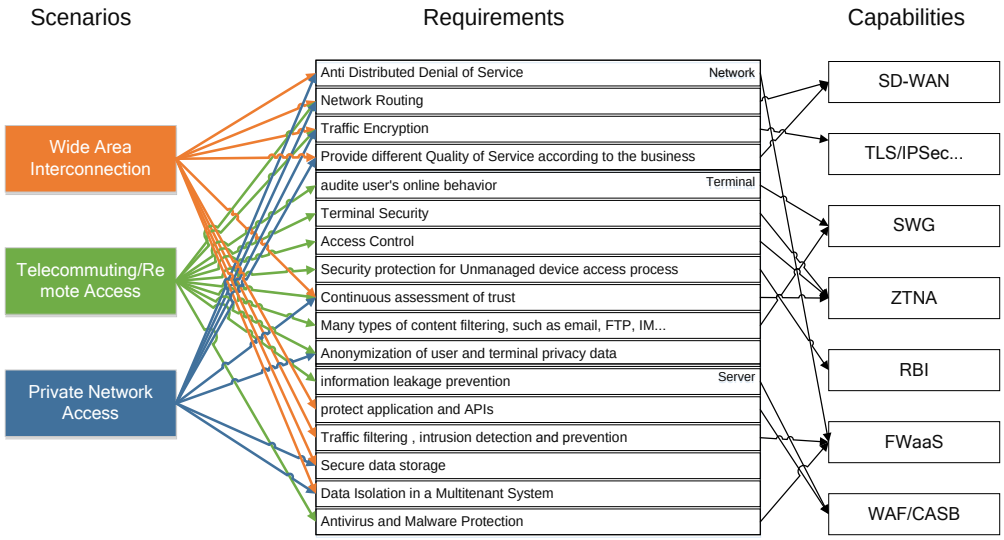

Figure 2-4 requirements and capabilities of the scenarios

3 Operator SASE Framework

3.1 SASE Key Capabilities

SASE involves five key capabilities including SD-WAN, ZTNA, SWG, CASB, and FWaas, as well as other security capabilities such as WAAP, SDP, and RBI.

- SD-WAN is the foundation of the entire SASE architecture, providing traffic orchestration, unified network management, on-demand network service activation, and the ability to integrate network and security to achieve dynamic routing and secure access control, to meet network connectivity and security requirements.
- ZTNA is the most critical security technology in SASE, which, based on user identity, user behavior, device information, network packets, and application information, uses dynamic permission mechanisms to meet the demand for secure access.
- SWG is usually deployed on the gateway that provides external access for internal users in a company, to achieve traffic inspection, filtering, and behavior control for internal employees, avoid sensitive data leakage, to provide protection for users.
- CASB is usually deployed on the cloud service side to monitor cloud resources, ensure data security, detect and respond to malicious access, and prevent sensitive data leakage, to meet the protection requirements of cloud services.
- FWaaS (including IPS/IDS) is usually deployed near the critical nodes that store data resources in data centers and branch offices. Based on user protection policies, it filters network packets and application data, to meet the protection requirements of critical positions.

- Other security capabilities, such as WAAP, SDP, RBI and Network sandbox, are used to meet the demands for web application protection, network invisibility, browser security, and other requirements.

3.2 SASE Functional Framework

To manage the above network and security capabilities, a complete SASE architecture must include network and security capability management, orchestration and configuration management functions, capability configuration, data visualization, and tenant management, as well as infrastructure to deploy all functions. Therefore, the basic functional framework of SASE is as follows:

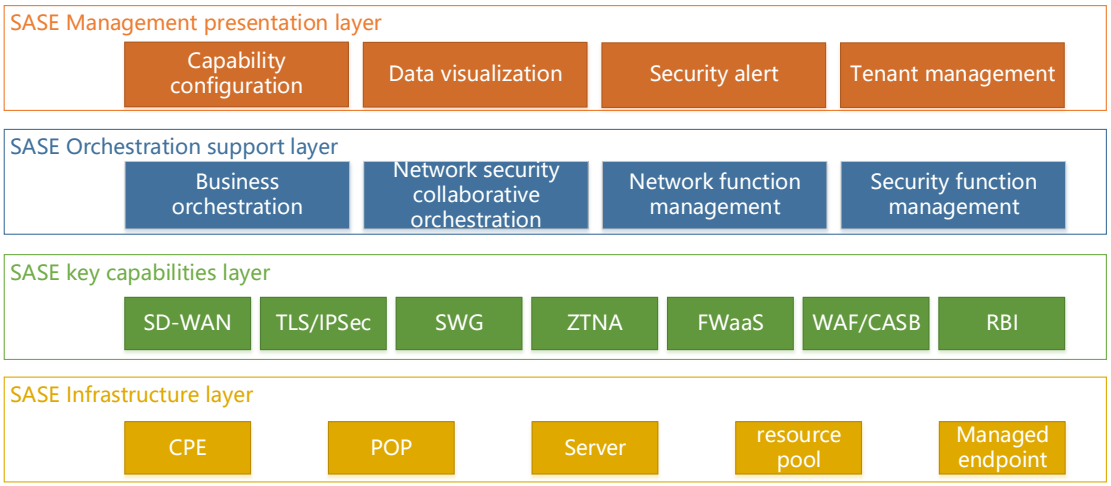

Figure 3-1 SASE Functional Framework

- The SASE management presentation layer is the interface that SASE presents to users, providing functions such as capability configuration and data visualization to users;
- The SASE orchestration support layer is responsible for the orchestration and management of network and security capabilities. It analyzes user business requirements, collaboratively orchestrates and manages network and security functions;
- The SASE key capability layer provides network and security capabilities for various scenario demands in the SASE framework;
- The SASE infrastructure layer is the software and hardware infrastructure for deployment, operation and maintenance management, key technologies, and basic support, including but not limited to CPEs, PoPs, resource pools, controlled terminals, servers, and other devices.

3.3 Operator SASE Deployment Architecture

Operators can use their existing networks to build an operator SASE. The deployment architecture of operator SASE is as follows:

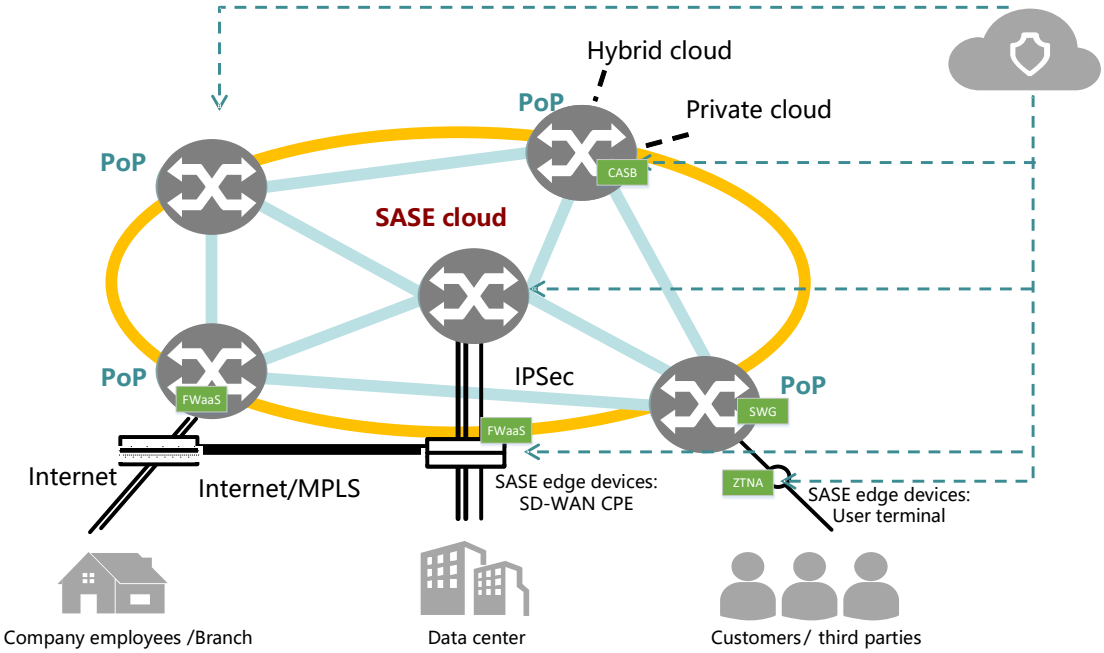

Figure 3-2 SASE Deployment Reference Framework

SASE PoPs are part of the SASE infrastructure layer, controlled by the SASE orchestration support layer, and carry the SASE key capability layer. SASE PoPs can deploy various network and security capabilities on demand and are the main implementation points for SASE network and security functions. SASE PoPs can reuse network access points and cloud resource pools deployed by operators in various locations, thereby saving the construction cost of SASE.

SASE cloud is a multi-tenant cloud composed of SASE PoPs, which integrates various network and security functions of operators and provides them to access users under the coordination and management of the SASE management platform.

SASE edge devices, including controlled terminals and CPEs, are part of the SASE infrastructure layer, controlled by the SASE orchestration support layer, and carry the SASE key capability layer. SASE edge devices can introduce user traffic into the SASE cloud through encrypted channels, and can also deploy various network and security capabilities with lower resource requirements on demand, thus ensuring the flexibility of the SASE framework. SASE edge devices can reuse network CPEs of operators to save the cost of SASE construction.

The SASE management platform is a unified visual and manageable control platform that carries the main functions of the SASE orchestration support layer and the management presentation layer. It is responsible for the unified management of network and security capabilities, the configuration of network and security policies, visualization, and operation and maintenance functions. Customers can subscribe to network and security services as needed and selectively enable configuration services. The SASE management platform can be integrated as a part of the operator's network management platform, reducing the cost of SASE construction and usage.

When carriers build the SASE framework, they usually use the following two modes:

1. SASE mode based on public network tunnel

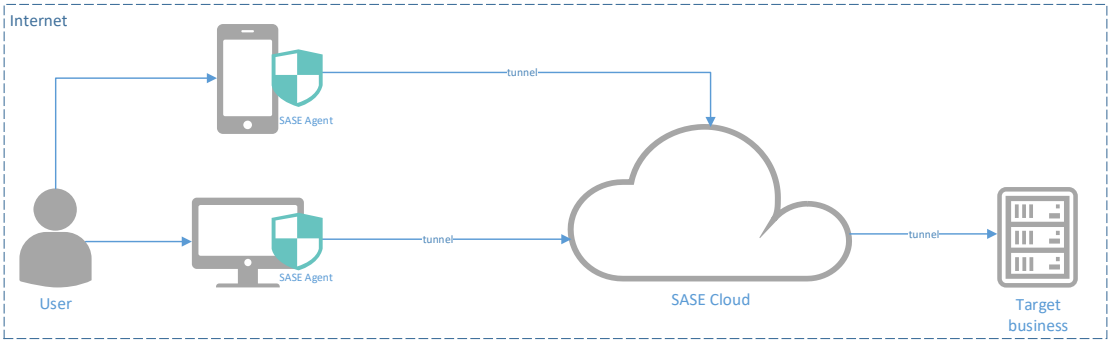

Figure 3-3 SASE model based on public Internet

The operator establishes a tunnel on the public network to divert user traffic to SASE Cloud for network and security processing and then diverts it to the target business.

The common implementation method is that the operator deploys security and network capabilities in public clouds, network clouds, and other locations to establish multiple SASE PoPs throughout the network to form SASE Cloud. Then, through the SASE multi-tenant management platform, the operator can call and manage these capabilities. Users install SASE Agent on their PCs and mobile devices to establish a public network tunnel with the nearest SASE PoP to access SASE Cloud. When users access the target business, the access traffic is diverted to SASE Cloud through the public network tunnel for network and security processing, and finally diverted to the target business to complete the secure access process.

This model targets small and medium-sized enterprises and individual users, focusing on providing cost-effective security and network services, achieving flexible mobile/remote access, and accessing target businesses across operators. The SASE service under this model does not require association with leased lines or SD-WAN and other network services.

2. SASE model based on leased line/SD-WAN

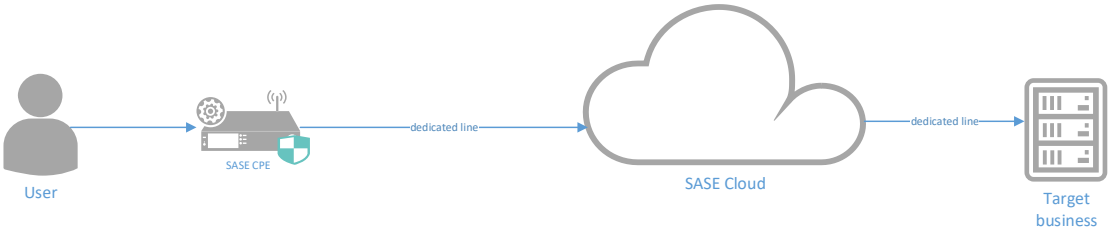

Figure 3-4 SASE model based on leased lines/SD-WAN

The operator diverts user traffic to SASE Cloud for network and security processing through leased lines/SD-WAN and then diverts it to the target business.

The common implementation method is that the operator customizes the deployment location of network and security capabilities and the SASE management platform based on user needs. The security capabilities and management platform can be deployed in edge clouds, user intranet servers, private clouds, network clouds, and other locations close to the user. Users access the leased lines through CPE devices and connect to SASE Cloud. When users access the target business, the access traffic is diverted to SASE Cloud through the leased line for network and security processing, and finally diverted to the target business to complete the secure access process.

This model targets large enterprises or government agencies with multiple branches, focusing on providing high-quality and efficient network and security services. The SASE service under this model is associated with leased lines or SD-WAN and other network services. Therefore, this model can deploy network and security capabilities and SASE management platforms locally, in edge clouds, private clouds, etc., and customize user traffic topology to meet user needs in security, privacy, and network quality of service.

In specific implementations, operators can mix the above two models. For example, they can use model 1 when users work remotely or move, and use model 2 when they work within the enterprise or access core businesses to meet the differentiated needs of users in multiple scenarios.

4 Telecom Operators SASE Application Cases

4.1 Case 1: WAN Interconnection of Multinational Corporation

Background: Due to national policies, multinational corporation need to converge their exposure. And they need to filter and monitor the traffic on the data sink node to ensure online behavior compliance.

Requirement: Constrict access to the Internet. Traffic is aggregated to unified Internet exports in the regional center through a leased WAN line in a large branch or headquarters to meet the traffic collection requirements. Protect the communication between branches and the headquarter. Protect and regulate the access of branches and the headquarter to the Internet. Prevent malware, malicious connections ,and data leakage, and unauthorized access to resources. And implement online behavior compliance.

SASE Solution:

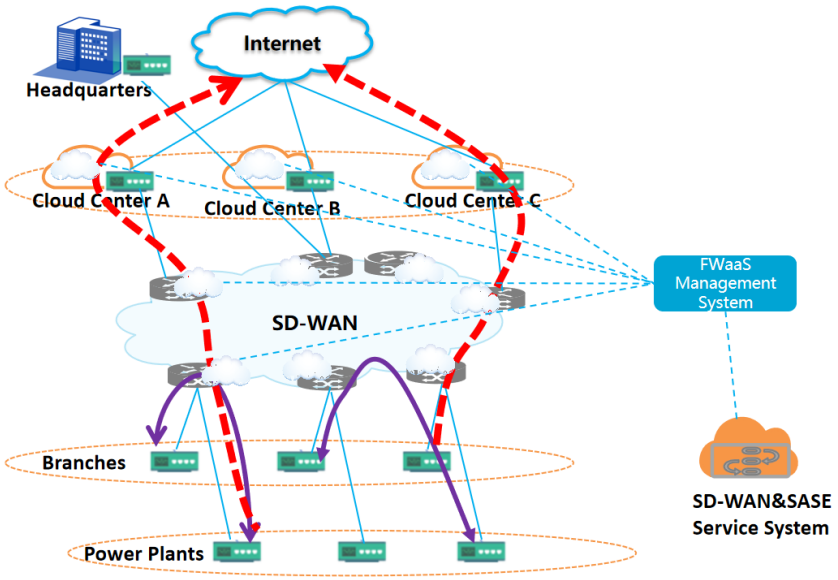

Figure 4-1 SASE Solution for WAN Interconnection of Multinational Corporation

This solution is based on SD-WAN traffic diversion. The user traffic is diverted to the SASE service system through the routing devices on the Internet exports and PoPs in SD-WAN for the network security processing.

Deploy enough FWaaSs that match the performance of the Internet exports. Routing devices on the Internet exports provide traffic diversion to the FWaaSs by tenants. Use security capabilities, such as application firewall, intrusion prevention, virus filtering, URL filtering, and bandwidth management, to ensure the southbound and northbound security of the FWaaSs.

Deploy enough FWaaSs that match the performance on PoPs. Routing devices on PoPs provide traffic diversion to the FWaaSs by tenants. Use security capabilities, such as application firewall and intrusion prevention, to ensure the eastbound and westbound security of the FWaaSs.

Ensure that all FWaaSs are managed by tenants in a centralized manner.

Operators' Advantages: For one thing, operators have a nationwide wide area network. And they have the infrastructure needed for a complete SASE system and the inherent advantages of working with various security vendors. They can deploy FWaaSs and various security capabilities at the Internet exports and PoPs. For another thing, operators have a wider customer base and are more trusted by government and enterprise customers to provide SASE services more efficiently, conveniently, and securely.

4.2 Case 2: Mobile Office and Remote Office of Insurance industry

Background: The mobile/remote access terminals of the employee may become the entry point for attackers and the channel for enterprise information leakage.

Requirement: Enterprises need to deploy unified management and security protection capabilities, such as malicious website filtering, mail security detection, and anti-virus, for employees' terminals. Enterprises also need to identify employees, monitor their behaviors and continuously conduct real-time trust evaluations based on their behaviors. Enterprises need to encrypt transmitted data to prevent data leakage and tampering.

SASE Solution:

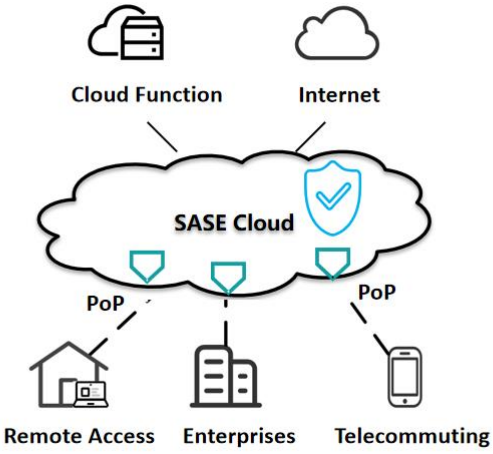

Figure 4-2 SASE Solution for Mobile/Remote Office of Insurance industry

This solution is based on public network tunnel traffic diversion. The user traffic is diverted to the SASE cloud through a secure tunnel on the public network for network security processing,

The control center of SASE is set in the cloud, and the user edge deploys multiple PoPs on demand. Office terminals deploy SASE client with drainage function, which is responsible for establishing a secure tunnel on the public network and diverting employees' Internet traffic to PoPs.

SASE PoPs deploy multiple security capabilities to ensure the security throughout the mobile/remote access process. PoPs protect against unknown threats through advanced threat detection and protection module, load EDR module to realize fast event response, load zero-trust online behavior management module and DLP module to ensure enterprise security.

The traffic of employees' mobile/remote access terminals is diverted to the edge PoPs through the SASE client. The identity management module on PoPs verifies the real-time identity information to maintain the minimum employees' access rights and prevent them to access any unauthorized resources.

Operators' Advantages: Operators have the necessary infrastructure for a complete SASE system, and can provide enterprises with SASE equipment leasing services on the enterprise side. Users can rent equipment from operators, and do not need to purchase enterprise-side hardware equipment, which reduces user costs.

4.3 Case 3: Multi-Cloud Deployed Business Accessing

Background: The enterprise cloud gradually moves to the hybrid multi-cloud mode, and the environment deployment is more and more diversified. Network boundary blurring leads to the failure of security policy, which brings new challenges to enterprise information security.

Requirement: Realize networking, cloud and multi-cloud interworking of access users, and independent network planning. Realize the network integration involving multiple devices and multiple operators. Establish effective security protection measures for the business systems.

SASE Solution:

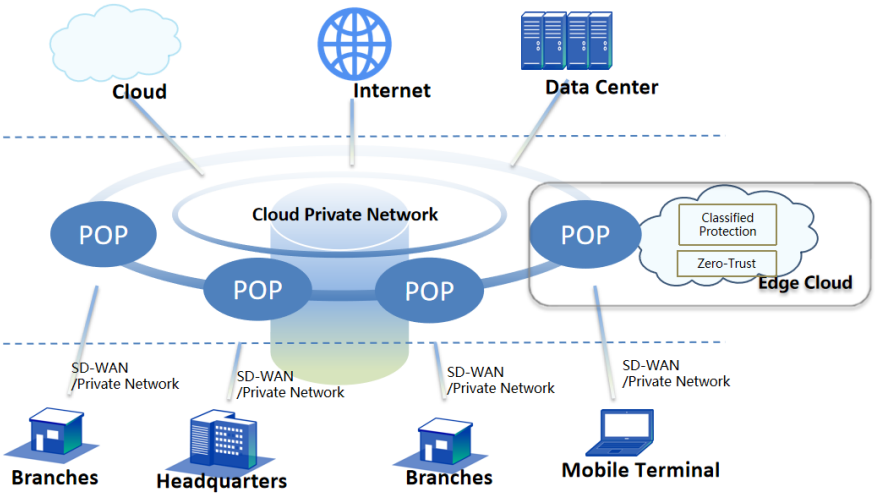

Figure 4-3 SASE Solution for Multi-Cloud Deployed Business Accessing

This solution is based on operators leased line/SD-WAN traffic diversion. The user traffic is diverted to the SASE cloud through the leased line or SD-WAN for network security processing.

Operators aggregate zero-trust access and service system security protection capabilities at the PoPs of the intelligent cloud network and provide external security services through SAAS products.

Operator cloud private network, based on the SRv6 standard, realizes end-to-end ultra-low latency through FullMesh networking. Enterprises can access it through local PoPs nearby, convenient to enter the cloud. And it builds edge clouds to complement the central cloud. Edge cloud hosts the business system and security, providing customers with near-field and low-latency cloud services. Operators build security resource pools in edge clouds to provide detection, protection, and audit security services. Zero-trust security services can provide functions such as application permission control, terminal management, watermarking, and application protection for remote access.

Operators' Advantages: Operators have complete cloud network infrastructure and operation and maintenance services, which can enhance traffic forwarding efficiency through operator cloud private network connecting edge clouds and central clouds. Users access the PoPs nearby to realize fast networking between the headquarter and branches. Operators can provide classified protection of cybersecurity capabilities and zero-trust security capabilities on edge clouds to protect customs' service systems.

5 Outlook

5.1 Challenges

Since the SASE framework was introduced, vendors from different levels have invested heavily in it to meet so many new security requirements of the network. Operators have many natural advantages in constructing the SASE framework, but they also face some technical challenges that must be overcome to manage and schedule networks and security capabilities provided by multiple vendors and deployed in multiple locations. The following challenges must be addressed:

1. **Lack of standardization**: The functional division of network and security products from different vendors is not clear enough, resulting in the functional overlap. Furthermore, the security capabilities provided by different vendors do not cover the same range of functions. The standardization of interfaces for common security capabilities has not yet been fully implemented.
2. **Lack of industry ecosystem**: The technologies involved in SASE services are diverse, and it is difficult for a single vendor to provide high-quality, full-stack network and security capabilities. Multiple vendors need to collaborate to achieve SASE services and jointly build the SASE ecosystem.However, the lack of a unified platform results in low collaborate efficiency and high costs, requiring a large amount of adaptation work.

To address the challenges mentioned above, operators can promote the development of the SASE industry in two aspects: standardization and industrial ecosystem, and further expand application scenarios.

5.2 Industry promotion for Operator SASE

5.2.1 Advancing research and standardization

The development of SASE technology requires the development of standards. These standards can help vendors to create SASE solutions with interoperability and connectivity, and promote the healthy development of the industrial ecology.

International organizations such as MEF and ITU are developing a series of SASE-related technical standards. In China, CCSA(China Communications Standards Association)、CIC(Chinese Institute of Communications) and CSA GCR(Cloud Security Alliance Greater China Region) have initiated multiple SASE-related projects, covering the overall technical requirements, key technical indicators, upper-level service-oriented capability requirements, and SASE capability requirements for cloud computing based security trust systems.

Operators have also increased their investment in the standardization of SASE technology, leading to the standardization of some directions. In the field of SASE technology's key area: orchestration management, China Mobile has led multiple standards domestically and internationally, promoting the standardization development of the SASE

industry. Among them, in ITU, 'Security Guidelines for Enterprise Networking Scenarios' led by China Mobile provides guidelines for orchestrating security capabilities and secure networks to protect the service access process. In CCSA, Orchestration for Secure Access Service Edge (SASE) series standards led by China Mobile and CAICT(China Academy of Information and Communications Technology) standardize the unified framework for network and security capabilities, providing users with open SASE services across vendors and operators. In addition, China Telecom has also led the development of the "Technical Guidelines for Secure Access Service Edge" series of standards in CCSA, aiming to standardize and promote the development of secure access service edge technology.

5.2.2 Building a industrial ecosystem

As a new model for network security and access, SASE requires cooperation among different companies. Operators need to build close cooperation with suppliers of network capabilities, cloud services, security capabilities, and so on, to provide more comprehensive and complete services. In addition, good relationships need to be established among operators to achieve the overall integrity and reliability of network security and promote the development of SASE together.

Operators has been advocating for the industry to develop the SASE industry through cooperation, promoting technical exchanges and cooperation among manufacturers, and establishing a healthy and open SASE ecology to provide users with better services.

5.2.3 Expanding the service scenarios of operator SASE

SASE has a wide range of applications in Operators, such as mobile office, remote access and wide area intranet access.

Operators can apply SASE to IoT access, providing network security, access control, data encryption, traffic optimization, and other functions for the large and complex heterogeneous IoT.

Operators can also apply SASE to accelerate office applications, providing bandwidth management, global network acceleration, load optimization, and other functions based on identity, device, or application.

In the future, Operators can help the development of the global computing power network through continuous optimization and innovation, expanding the use cases of SASE to emerging scenarios such as large-scale artificial intelligence, connected cars, and the Internet of Things.

6 Summary

In this white paper, we mainly introduce the background, definitions and requirements of SASE, and analyze the benefits and advantages of establishing a SASE framework for operators. Using SASE, enterprises can eliminate the effort and cost required to maintain a complex and decentralized infrastructure consisting of point solutions. SASE also gains more

flexible, efficient and secure network and security services to better cope with the growing challenges of modern networks. We also detail the key capabilities, functional frameworks, and deployment architectures required by operators when building SASE infrastructure, and present use cases of the SASE framework. Finally, the technical challenges, ecological cooperation and scenario expansion of SASE framework, as well as the future work are discussed.