Intelligent Connectivity Solution for Enterprise Networking Services

Junya Huang[a*], Jiaqi Sun[b], Xuejing Yuan[c], Zhongmin Zheng[d]

Institute of Basic Operational Technology, China Telecom Research Institute, Guangzhou, China

[a*]huangjy40@chinatelecom.cn, [b]sunjiaq@chinatelecom.cn, [c]yuanxj2@chinatelecom.cn, [d]zhengzm@chinatelecom.cn

Abstract. Business requirements of cloud transformation for enterprises have changed dramatically in recent years, and hybrid cloud has become the dominant enterprise IT architecture. In the hybrid multi-cloud era, the traditional Internet can no longer meet customer needs, in the meantime, the complexity of network operation and maintenance has been greatly enhanced. Facing rapid growth of the demand for cloud SD-WAN (software-defined networking in a wide area network) operation and maintenance services, an intelligent connectivity solution for enterprise is provided, offering leading services that integrate networking, cloud, security service and management. This solution has been put into practice in different industries and the feasibility as well as effectiveness has been verified.

Keywords: intelligent connectivity; SD-WAN; SASE; security

1 Introduction

The business requirements of cloud transformation for enterprises have changed dramatically in recent years. According to IBM's global survey on cloud transformation, only 3% of executives surveyed said their organizations will use a single private or public cloud in 2021, compared to 29% in 2019 [1]. This downward trend means that hybrid cloud has become the dominant IT architecture for enterprises. In report "Three Key Lessons from Hybrid Cloud Operations in China", Gartner mentioned that the penetration rate of hybrid cloud in China is expected to reach 70 percent by 2024, much higher than the global average rate of 50 percent [2]. The hybrid multi-cloud market in China will soon reach 100 billion.

In the hybrid multi-cloud era, demand of enterprises for networks has become more complex and urgent, and traditional Internet as well as dedicated line access can no longer meet customer needs. The deployment of SD-WAN that support remote working, provide high flexibility and scalability, and significantly reduce network costs, has shown a high growth [3]. It also shows an evolving trend toward cloud-

C. Chen et al. (eds.), *Proceedings of the 3rd International Conference on Digital Economy and Computer Application (DECA 2023)*, Atlantis Highlights in Computer Sciences 17,
https://doi.org/10.2991/978-94-6463-304-7_69

based SD-WAN. Cloud-based SD-WAN has become the mainstream of enterprise cloud network deployment in the hybrid multi-cloud era thanks to its characteristic of easy deployment, high security, high reliability and high quality [4]. Meanwhile, with the continuous strengthening of security requirements, enterprise networking has gradually changed from cloud SD-WAN to SASE (secure access service edge) [5].

In the hybrid multi-cloud scenario, the complexity of network operation and maintenance has been greatly enhanced, which brings challenges to enterprises and promotes the rapid growth of demand for cloud SD-WAN operation and maintenance services. Based on the advantages of network together with security, leading international operators build managed SD-WAN, managed security, and SASE service capabilities, aiming to improve customer service level and to enhance user experience. Based on SD-WAN and SASE, an intelligent connectivity solution for enterprise is provided, offering leading services that integrate networking, cloud, security service and management. This solution has been put into practice in different industries and the feasibility as well as effectiveness has been verified. This study could be used as an experience reference for industry promotion.

2 Intelligent connectivity solution for enterprise networking

2.1 Overview of the general scheme

The intelligent connectivity solution includes underlay network, overlay network and the control center. We transformed the existing network and its management system to adapt to the network construction requirements of intelligent connectivity, and reconstructed overlay network capability based on SASE system. The control center is the "intelligent brain" of the whole solution, which undertakes the core functions of management and policy definition, including network arrangement management and security policy management. The overall technical scheme is shown in Fig. 1.

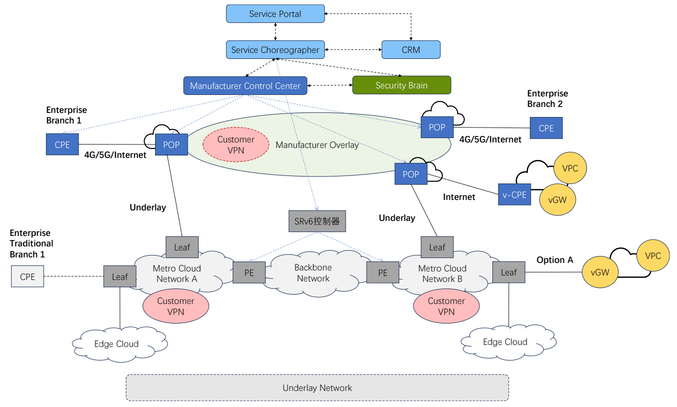

Fig. 1. Overall technical scheme of the intelligent connectivity solution

The core composition and key technology of the solution is stated as below.

2.2 Overlay network

An overlay network is a virtual logical network constructed on the same underlay network through network virtualization technology. Overlay network can shield the complexity of the underlying physical network. In this way, communications between nodes become simpler, more transparent and more flexible.

The integration of controller and overlay network via SDN brings useful functions and capabilities including:

- Traffic transmission does not depend on a specific line. Overlay network uses tunnel technology, which can flexibly select different underlying links and ensure the stable transmission of traffic in various ways.
- Overlay network can build different virtual topologies according to requirements without modifying the underly network.
- The encryption method can be used to protect the private traffic communication on the Internet.
- It supports network slicing and segmentation. Segmentation of different services can realize the optimal allocation of network resources.
- It supports multi-path forwarding. In an overlay network, traffic can be transmitted from the source to the destination through multiple paths to realize load balancing and maximize the bandwidth utilization of lines.

Overlay networks are widely used in SD-WAN solutions.

2.3 SD-WAN solution

SD-WAN develop on basis of software defined network (SDN) technology [6]. It is a service formed by applying SDN technology to the wide area network (WAN) scenario. This kind of service connects a wide geographical area of enterprise networks, data centers, Internet applications and cloud services, aiming to help enterprises to reduce WAN expenses and to improve flexibility of network connectivity.

SD-WAN provides more flexible configuration options through virtual link and tunnel technology. Users can choose to route all traffic through a central SD-WAN hub. It is also possible to route some specific traffic through an enterprise's private network and directly onto the Internet. The architecture of SD-WAN is also more flexible and can be deployed with physical or virtual devices and can be configured to be centrally managed or split. SD-WAN is also highly scalable. The SD-WAN manager can manage thousands of nodes. Since SD-WAN targets branch connections, as branches are added or changed, SD-WAN can simplify these operations by operating on the cloud without manually configure routers at individual branches as traditional VPN solutions usually do.

In addition, SD-WAN provides traffic encryption to ensure that the transmitted data cannot be seen by others. It can also provide VPN features to keep the data secure. When it comes to improving performance, SD-WAN can be employed in two ways. The first way is to improve network performance through mechanisms such as traffic optimization, dynamically adjusting load balancing, and selecting the best connections. These mechanisms can help to distribute traffic dynamically across multiple connections, thus, guaranteeing optimal network performance and availability. The second way is by providing the shortest path to the cloud service provider, thereby reducing latency and jitter. These techniques can improve the performance of the application. Therefore, SD-WAN can help enterprises to manage and maintain wide area networks better and to serve customers better.

China Telecom deploys SD-WAN POP (point-of-presence) v-CPE (virtual customer premise equipment) in each region into the Tianyi cloud resource pool and builds overlay interconnection according to demand based on the cloud backbone between the cloud private line and the Internet to POP. Edge is connected to the nearest POP point through the Internet, establishing an SD-WAN overlay tunnel with POP, and realizes cross-POP communication through the POP overlay backbone network. For the last hop to the cloud, deploy the v-CPE in a cloud user's VPC as a cloud site, and the cloud site establishes an overlay tunnel with the POP site over the Internet. Thus, the SD-WAN edge access network is built based on the cloud backbone to realize multi-network integration and multi-cloud interconnection. Fig. 2 is a schematic diagram.

2.4 SASE Scheme

In 2019, Gartner introduced the concept of SASE. The official definition of SASE by Gartner is that SASE provides enterprise customers with a new network security architecture by integrating the functions of network and network security into a unified service model, as shown in Fig. 3 [7].

SASE combines SD-WAN capabilities with large numbers of network security features, all delivered from a single cloud platform. In this way, SASE enables employees to authenticate and securely connect to internal resources from anywhere and gives organizations a better control over the traffic and data that flows in and out of their internal networks.

SASE is a solution for a suite of technologies that includes software-defined WAN (SD-WAN), Internet security gateway (SWG), cloud access security broker, zero trust network access, and firewall as a service [8].

SASE consists of four core security components.

- Secure web gateway (SWG): SWG prevents networking threats and data breaches by filtering unwanted content from Web traffic, blocking unauthorized user actions, and enforcing corporate security policies. SWGS can be deployed anywhere, making them ideal for protecting remote workforce.
- Cloud access security broker (CASB): CASB performs a variety of security functions for cloud hosted services, including uncovering shadow IT, protecting confidential data through access control and data loss protection, and ensuring compliance with data privacy regulations.
- Zero trust network access (ZTNA): ZTNA platform keeps internal resources from public view and helps to defend against potential data breaches by requiring real-time verification of every user and device in every protected application.
- Firewall as a service (FWaaS): FWaaS are firewalls that delivered from the cloud as a service. FWaaS protect cloud-based platforms, infrastructure, and applica-

tions from networking attacks. Unlike traditional firewalls, FWaaS are not physical devices but a set of security features including URL filtering, intrusion prevention, and unified policy management across all network traffic.

We have deployed several SASE schemes with flat networking and multi-plane parallel deployment. This architecture facilitates rapid service commissioning, fault location, and operation and maintenance.

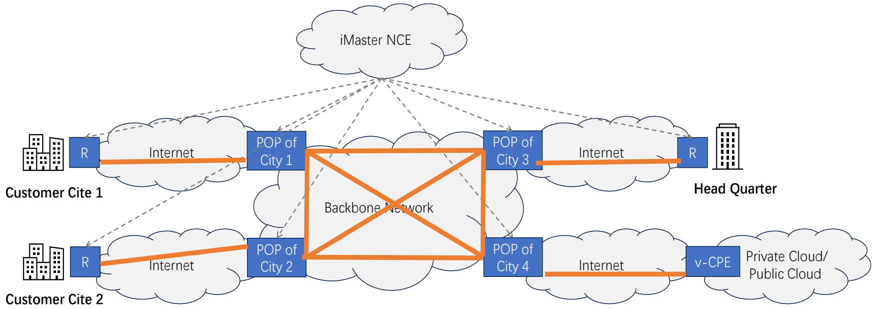

Fig. 2. Schematic diagram of SD-WAN

2.5 Service Choreographer

Service choreographer is the core of the control center. To support the fast loading and automatic commissioning of products, a cloud-based and micro-costume-based dynamic orchestration engine is built. The orchestration package is flexibly arranged and loaded and run based on the open API system to realize the fast loading and automatic commissioning of services. Fig. 4 shows the functional architecture of the service choreographer.

The key functions of the service choreographer are as follows.

- orchestration package preparation: to complete the orchestration package loading, presentation, testing, going online and other functions.
- Service order reception: to receive the order issued by CRM, complete the verification and analysis of order data and other functions.
- Service instance management: to generate service instance data according to policy.
- Orchestration engine: to decompose service object tree according to service invocation parameters and related policy, build service API tree, find API invocation parameters and related process templates based on dependencies and policy, and generate process instances, process collaborative control, object API invocation and other functions.
- Policy engine: to provide various service functions of business policy.

2.6 Security Brain

The security capability pool is integrated into the metro cloud network architecture. Adopting the unified IPv6+/SRv6 technology, SRv6 SFC service chain and security service integration technology is developed to realize security capability pool sharing, traffic diversion and security value-added services. Pulling through the security brain, cloud network service orchestration and network controller, we provide flexible and agile security protection, cloud network security integrated service capabilities. Through the deployment of BGP FlowSpec+SRv6 policy intelligent drainage technology in the backbone and metropolitan area network, it solves the problem of nearby traction and reinjection of a large range of traffic and provides a strong guarantee for government enterprises, ICP and differentiated international Internet services.

China Telecom provides differentiated Internet access services and security services for different customer groups such as government, enterprise, public and international. The Internet access needs to pass through various service nodes of cloud dike security providers according to business logic, namely firewall FW/WAF of cloud dike security center, intrusion detection and prevention system IDS/IPS, VPN and address translation NAT. SRv6 SFC service link add the SRv6 path information into the original data packet to guide the packets to pass through the application layer service device in sequence according to the specified path, thus realizing the combination of service link SFC and VAS application. According to the VAS service ordered by users, the SRv6 policy is enabled in combination with the situation of the live network, and the Internet/cloud line security products are provided.

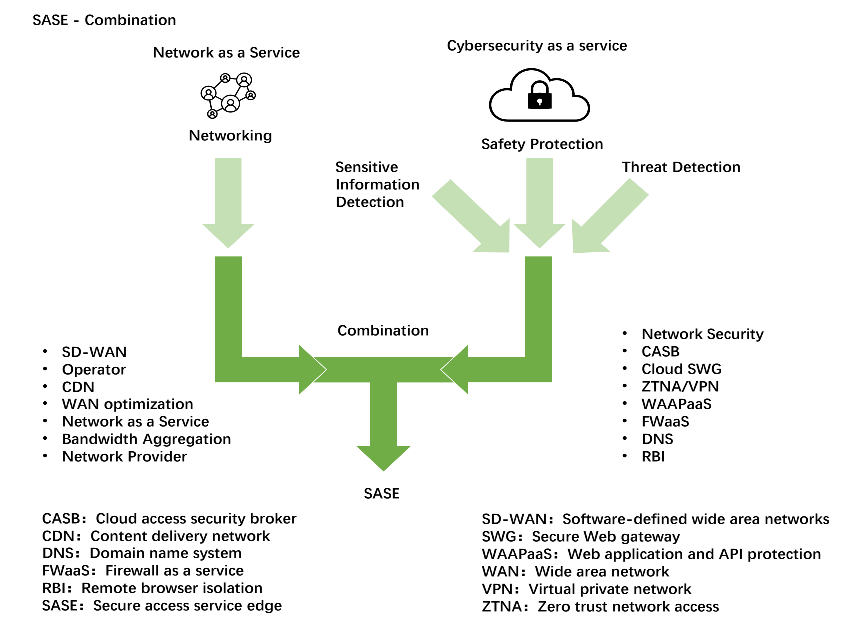
SASE - Combination
Network as a Service
Cybersecurity as a service
Networking
Safety Protection
Sensitive Information Detection
Threat Detection
Combination
• SD-WAN
• Operator
• CDN
• WAN optimization
• Network as a Service
• Bandwidth Aggregation
• Network Provider
• Network Security
• CASB
• Cloud SWG
• ZTNA/VPN
• WAAPaaS
• FWaaS
• DNS
• RBI
SASE
CASB：Cloud access security broker
CDN：Content delivery network
DNS：Domain name system
FWaaS：Firewall as a service
RBI：Remote browser isolation
SASE：Secure access service edge
SD-WAN：Software-defined wide area networks
SWG：Secure Web gateway
WAAPaaS：Web application and API protection
WAN：Wide area network
VPN：Virtual private network
ZTNA：Zero trust network access

Fig. 3. Technical concept chart of SASE

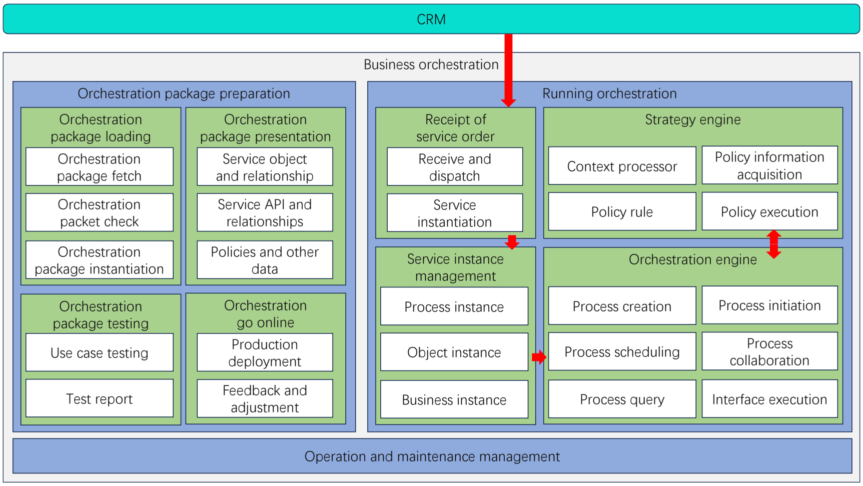

Fig. 4. Functional architecture of the service choreographer

3 Application and achievements

Intelligent connectivity service provides safe management services with quality assurance for the internal cloud network of government and enterprise customers, with the goal of becoming the network manager of the internal cloud network of government and enterprise customers. Compared with the traditional network special line, the service boundary of the intelligent connectivity has changed from PE to CPE of customers.

China Telecom has advantage of wide IDC location. We could do nearby deployment of POP, using the network to ensure the time delay, packet loss and jitter between CPEs. We can also provide customers with SLA quality assurance of internal cloud network. In addition, through the combination of CPE and SASE capabilities, the next generation firewall capabilities are deployed to give play to the security advantages of cloud dikes, which can provide security management services for government and enterprise customers. The intelligent connectivity solution has capabilities as below.

- Agile delivery: zero configuration of CPE and security services on demand, reaching a demote delivery rate of more than 90%.
- Managed operation and maintenance services: 7*24h support, monitoring and alarm, intelligent routing, fault self-healing, log analysis.
- Managed security services: 7*24h support, 13 categories of security capabilities on-demand subscription, real-time risk reporting, on-site support in high-risk period.
- Super high SLA: availability rate ≥99.9%, time delay between sites ≤ 45ms (except Xinjiang, Tibet), packet loss rate ≤1 ‰. Taking Shanghai as an example, up

to now, it has achieved thousands of new Ethernet/cloud private lines/cloud private networks and continues to provide high-quality services for large government and enterprise users and small and medium-sized enterprises.

4 Conclusions

In the hybrid multi-cloud scenario, facing rapid growth of the demand for cloud SD-WAN operation and maintenance services, an intelligent connectivity solution for enterprise is provided, aiming to offer leading services that integrate networking, cloud, security service and management. This solution which has been put into practice in different companies is supposed to provide some reference for the industry.

References

1. China Information Weekly (2021) "The cloud market has entered the Hybrid multi-cloud era".
2. Resource Operation _ Service _ Platform _ Capability of enterprise multi-cloud management (2022) _ Service _ Platform _ Capability. Available at: https://www.sohu.com/a/589007341_120201716 (Accessed: 15 September 2023).
3. Sarabjit Singh, “SD-WAN Service Analysis, Solution, and its Applications.” Available at: https://era.library.ualberta.ca/items/2613b784-8aa6-498c-accb-b8bb86462b58
4. Raghavan Kasturi Rangan, “Trends in SD-WAN and SDN.” Available at: https://link.springer.com/article/10.1007/s40012-020-00277-5.
5. Li Changlian, Ma Jichun, Lin Xuan, “The idea of constructing SASE model based on SD-WAN Analysis [J],” Post and Telecommunications Design Technology, 2021(06): 78-83.
6. Jiang Tong, “Research and implementation of the key technologies of SDWAN controller for dynamic overlay network.” Available at: https://kns.cnki.net/kcms2/article/abstract?v=4u_pwZ3OVlCTlu2ttlg9NFHpouDjF9CcFGOPnRpP2IhKdY0NTV8licdzuO-MkFjqsw2kA7PFbYwOUQqDz79ToLOHQ0IJpq0Ye2KTOSVHqKtgPpUUfjyESwLZmOlzGy6NlOwOsmB0I2DYG3lDC5joZQ==&uniplatform=NZKPT&language=CHS.
7. Xi Wang, Chen Chen, Junfeng Jing, Jiazhen Ji, “SASE Technology Solution and Implementation Practice for Large Enterprise.” Available at: https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTlOAiTRKibYlV5Vjs7ioT0BO4yQ4m_mOgeS2ml3UOgwnY6dSNCwdv8NFwXY7DzPS5yeGXN1GuPal74mTCwH&uniplatform=NZKPT.
8. Yong Zhi, “Build zero-trust network security based on SASE.” Available at: https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTlOAiTRKibYlV5Vjs7iJTKGjg9uTdeTsOI_ra5_XVAeH9RrhpJsYqpY03FLE3tKnoKhhGjcf1DSV5G-LF7b&uniplatform=NZKPT.