Info Snapshot, sponsored by Tata Communications
DECEMBER 2023

Secure Access Service Edge: Next-Generation Approach to Secure Connectivity

Nikhil Batra
Research Director, Telecom and IoT
IDC Asia/Pacific

What Is All This Chatter SASE?

What is secure access service edge (SASE), and more importantly, how can it help your organisation?

In its most distilled form, SASE is the integration of networking and network security as a single unified, cloud-delivered service.

The core constructs of a SASE architecture typically encompass software-defined wide area network (SD-WAN) with integrated cloud-based security functions, such as a secure web gateway (SWG), cloud access security broker (CASB), firewalls, and zero-trust network access (ZTNA). The idea coined by SASE is to provide users with secure access to applications hosted anywhere in the world, including applications across multiple private and public cloud environments.

SASE Core Components

SASE challenges the traditional centralised security stack and instead promotes delivering integrated security and networking services via the cloud.

Historically, traffic flows have led to the age of the single, on-premises security stack. However, the rapid adoption of cloud platforms and services, as well as changes in the traffic types, has inverted the traffic model. As a result, organisations are faced with a new wave of hurdles consisting of security concerns, cost, performance, management of tools and vendors, integrations, and maintenance.

SASE is the convergence of two interrelated concepts — **network as a service (NaaS)** and **security as a service (SECaaS)** — into a single-service cloud-native model. Table 1 summarises the major technologies encapsulated in the definition of SASE.

Network and data security was highlighted **as the top connectivity-related challenge** (from an ICT and networks perspective) by organisations globally.

- IDC's 2022 Worldwide Future of Connectedness Survey

TABLE 1: Key technologies that defines SASE

NaaS Components	SECaaS Components
SD-WAN. A secure SD-WAN technology forms the building blocks of a SASE solution by enabling optimal performance and intelligent routing in a client-cloud network architecture.	**CASB.** A CASB offers products and services to address security deficits in an organisation's use of cloud services and applications.
Edge computing and equipment. A SASE solution should offer distributed points of presence (POPs) via a well-established network to be able to put resources as close to the users as possible. This component of SASE is often overlooked, but this is essential in reducing latency without compromising on security.	**Firewall as a service (FWaaS).** A cloud-based firewall is a scalable, application-aware software solution allowing enterprises to eliminate the challenges of legacy appliance-based solutions, offering a full set of unified threat management (UTM) features.
	ZTNA. This is a framework of technologies working together that is based on the premise that nothing is trusted: neither the users, devices, data, workloads, locations, nor the network.
	SWG. SWGs prevent unsecured internet traffic from entering an organisation's internal network.

"SASE is quickly becoming a network and security framework of choice for organisations because it combines network and security capabilities, and it can be delivered in a consumption-based model."

- IDC Research

Streamlined Architecture: The Power and Benefits of Convergence

SASE offers various benefits for organisations looking to streamline and enhance their network and security infrastructure. Here are some benefits as experienced by organisations that have adopted the SASE framework:

Simplified operations. A SASE approach simplifies network architecture by converging various network and security functions into a single cloud-based platform, reducing the complexity of managing multiple solutions. Moreover, it offers centralized management and visibility, making it easier for ICT teams to monitor and control network and security services.

Reduced hardware footprint and cost. Less reliance on physical hardware and appliances can lead to cost savings on procuring, maintaining, and upgrading multiple network and security hardware, and this optimizes costs by paying for services on a consumption-based model.

Enhanced user experience. SASE allows for easier implementation and management of consistent user experiences regardless of their location or device, addressing organisational challenges around hybrid work.

Improved compliance and governance. SASE helps organisations enforce compliance and governance policies consistently across network and cloud resources, as well as their enterprise ecosystem, resulting in a reduced risk of data breaches and regulatory noncompliance.

Scalability, flexibility, and agility. Software-defined fundamentals of the SASE framework can adapt to the evolving needs of the organisation, enabling near-real-time deployment of security features and network services across different sites, enabling organisations to quickly respond to changing business conditions.

Overall, SASE is a comprehensive framework that addresses the challenges of modern networking and security by offering an integrated, cloud-based solution that enhances performance, security, and flexibility for organisations.

Breaking Down Barriers: SASE Implementation and Management

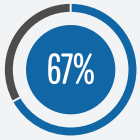
Although SASE is compelling, there are challenges to its implementation and management. SASE is a concept combining multiple cloud-native security technologies, together with WAN capabilities. SASE is not a single, one-stop shop, product or solution. The journey entails complexity in terms of purchase experience, choice of security services, deployment, and management.

Ensuring that these software-defined solutions are expertly designed, implemented, and managed will be more critical than ever as applications and workloads are increasingly residing across a broader IT landscape. Network consulting and integration and managed services by network SPs provide requisite services to enable enterprises to deliver on the connectedness strategies securely.

Organisations should keep the following pointers in mind as they get started or scale their SASE ambitions:

- **There is NO "one size fits all".** Instead of scrambling to achieve SASE nirvana by incorporating every single possible component in the market, tech buyers need to reassess the IT strategy and business needs of the organisation. Falling into the trap of a "checklist" mindset will leave organisations more confused and frustrated even before the commencement of the SASE journey.
- **Ensure a thorough migration strategy**. Migrating from traditional networking architecture to a software-defined paradigm or scaling SD-WAN/SASE implementations is highlighted as the top challenge by organisations on their network transformation journey. Network SPs often provide comprehensive frameworks to help with a robust network assessment and planning exercise, significantly reducing the risks along this transformation. The network SP must be able to demonstrate strong technology and professional/managed services expertise to stay in the running.
- **Align ALL stakeholders**. Historically, networking and security were decided on and deployed by separate teams within organisations. SASE frameworks' integrated networking and security capabilities can often raise some concerns internally between network and security teams, and it is crucial to engage both groups before getting started for a successful deployment journey.
- **Evaluate not only the technology**, but also ongoing operations and management strategy. Look for network SPs offering integrated, multivendor network management platforms to ensure ease of management and enhanced operational efficiencies. Assessing network SPs based on not only their networking and security capabilities but also advisory, integration, and service management capabilities will benefit the organisation in the long run.

Similar to any transformation, this road map to SASE is not an event but a journey, and organisations must understand that it is critical to find the right partner to ensure the success of your network, security, and the broader organisation's digital goals.



of organisations highlighted plans to increase their spend on SD-WAN/SASE framework solutions, in order to address security and operational challenges.

Source: IDC Asia/Pacific Communication and Collaboration Survey 2022-23, n = 1200

Message from the Sponsor

TATA COMMUNICATIONS

Tata Communications Managed SASE portfolio is composed of Hybrid and Hosted SASE. With the Hybrid SASE offering, customers can choose the best-fit SD-WAN and secure service edge (SSE) technology from among industry-leading technology solutions. Hosted SASE offers customer a unified SD-WAN and SSE solution delivered through a single technology stack.

For more information,

visit us

IDC Custom Solutions
Info Snapshot, sponsored by Tata Communications
DECEMBER 2023 | IDC #AP249569X