www.pipelinepub.com
Volume 20, Issue 1

Busting the Misconceptions that Surround SASE

By: Richard Kitney

SASE (Secure Access Service Edge, pronounced 'Sassy') is a term coined around four years ago. If you haven't come across it yet, you probably will, because Gartner forecasts that the SASE market will reach nearly $15 billion by 2025. SASE came about as a response to the rise in hybrid working and a dispersed workforce. It enables a corporate network to be deployed over the internet and addresses the security issues that come with more applications sitting in the cloud, data stored in multiple cloud services, and users connecting from anywhere on any device.

Four years is a short amount of time to fully come to grips with a new combination of a set of technologies, especially when there has been rapid take-up. It may therefore be useful to identify, and then bust, certain current misconceptions relating to SASE to help get a clear picture.

SASE is not a quick fix

SASE is a network security framework that combines networking and networking security into a cloud-delivered service. It is not a single product with a relatively short deployment window. Indeed, there is no one-size-fits-all route to solving all security issues. SASE is a transformation project, and because each organization is different, each requires a different SASE roadmap specific to its operations.

It is important to understand that not all the SASE offerings on the market are the same. Enterprises should look for a SASE framework that can be seamlessly integrated into their networking infrastructure and security architecture to ensure secure and robust connectivity alongside an enhanced user experience.

SASE does not come with zero trust as standard

From a business perspective, SASE delivers a boost to productivity by enabling employees and devices to securely access the right data regardless of location or device. It is already highly focused on security, but partnering SASE with a zero trust strategy further enhances security. However, like SASE itself, zero trust is not a single off-the-shelf product. A zero trust framework is a set of security principles designed to ensure that all users and devices, both within and external to an organization, are continuously validated when accessing applications and data. It fundamentally relies on these validations being kept up-to-date and accurate for the model to work.

Zero trust as an integral part of SASE and can help enterprises centralize their security tools, close visibility gaps, and streamline operations, leading to a stronger security posture. At the same time, zero trust network access (ZTNA) can be attained by utilizing a single solution to apply security policies across the network.

Enterprises must understand that zero trust is evolving. It requires continuous monitoring to control what each user can do in each application using its principles. In addition, the technologies must be configured to ensure users get the right level of access while adhering to the enterprise security strategy and policy.

SASE does not need a full cloud deployment from day one

Too often, enterprises are told that everything must sit in the cloud for SASE to work and provide security across the entire enterprise. However, this is only half the story.

A hybrid cloud approach, one combining private cloud with public cloud services and often on-premises infrastructure, allowing data and applications to be shared between them, is appealing to many enterprises. Hybrid can help enterprises ease into cloud migration, optimize workload resources, and protect data according to its sensitivity and regulatory requirements.

SASE should not be rushed

The final misconception is that an enterprise's transition to SASE is urgent and must go full speed ahead. The reality is that SASE should be prioritized but not rushed. SASE architecture will require careful planning as part of a migration strategy that will likely take several years to implement. Enterprises should be wary of any SASE sales pitch that pushes them to abandon existing IT investments or offers a vendor solution that is not fully mature.

What SASE is

SASE enables resilient and secure distributed networking for the way we work now – where employees and end users work remotely, and intelligent devices need to be "dangerously" connected to core applications and databases. It is all about balancing the end-user experience with security requirements as organizations address the challenge of securing their data everywhere. And regulations are getting tighter.

Distributed networking means that the end user is the new perimeter to defend and protect on three levels: identity, data, and access. This level of protection must be implemented with the sole purpose of enhancing the end-user experience in utilizingapplications that are increasingly delivered from the cloud (public, hybrid, private) and less from legacy data centers. The public internet is rapidly becoming the next enterprise and corporate network.

SASE is the response to the restrictions of traditional networking and security architectures. It comprises wide-area networking (WAN) and network security services, such as zero-trust network access (ZTNA), secure web gateway (SWG), and firewall as a service (FWaaS), all delivered from the cloud.

SASE at Stolt-Nielsen

Stolt-Nielsen, a global expert in bulk liquid logistics and sustainable land-based aquaculture, is an example of an enterprise benefitting from a SASE implementation combining SD-WAN connectivity with global Security Service Edge (SSE) to securely support its global, hybrid workforce and drive business growth.

The multinational enterprise has a diverse business portfolio, including the world's largest fleet of chemical tankers, terminals for the safe storage and handling of bulk liquids, and bulk door-to-door chemical delivery logistics. In moving to integrate the next generation of advanced solutions, the company sought to replace a diverse set-up of Internet Service Providers and network solutions with one integrated service to optimize performance and security for its 2,500 hybrid users globally.

In accordance with the points made above, Stolt-Nielsen did not want to rush its SASE deployment. Instead, the company chose to do so in stages with the help of a trusted partner to migrate from its former infrastructure and develop a phased SASE strategy.

The fully managed Orange SASE Advanced offering, created for Stolt-Nielsen by Orange Business in partnership with Netskope, provides enhanced global connectivity and consistent internet security on and off the network. With Netskope's SSE infrastructure located across more than 70 regions globally, plugging it into the Orange network, secured by Orange Cyberdefense, ensures data security can be managed centrally without affecting business productivity.

"As part of our transformation, we needed to define a secure, centralized, future-proofed digital infrastructure to support our business growth and innovation. We chose Orange because of its ability to provide seamless, reliable global connectivity with the highest security standards delivered via SASE," explains Peter Koenders, CIO at Stolt-Nielsen.

Considerations before SASE adoption

There is no cookie-cutter methodology to follow when it comes to adopting SASE. A transformation to SASE takes time. As a starting point, every enterprise that thinks it is ready to move forward on SASE needs to draw up its own customized strategy based on an audit of what they already have in place. Each enterprise should consider where it stands in relation to these seven components:

- A software-defined wide-area network (SD-WAN) solution is already fully or partially adopted, or at least under consideration, as SD-WAN is part of the strategy.
- Zero trust security strategies are already being pursued, recognizing their critical importance in hybrid work environments.
- Vendor consolidation is happening as contracts come up for renewal, to move away from a patchwork approach.

- Cloud-based security is being deployed instead of perimeter-based hardware and VPNs.
- Security policy is being streamlined and consistent enforcement regardless of location is being applied.
- User experience is being considered through improving the visibility of traffic and applications – within and beyond the network.
- Integration by embedding edge security into network designs and improving networking and security team collaboration.

An assessment of the above should help to establish a baseline for an enterprise's SASE journey, which then progresses following a well-considered plan to adopt each of the solution components, one by one, in whatever order makes the most sense for the organization.

Deploying SASE does not have to be complex, but enterprises shouldn't go it alone. Visibility of the above points will significantly increase with the right partner and milestones in place. However, with so many vendors offering SASE right now, it is crucial to understand that they do not all offer the same SASE capabilities. Partnering with a network and digital integrator who can identify the true baseline for a SASE journey and propose the best solution tailored to the organization's needs, combined with proven capabilities in cloud, connectivity, security, and digital integration, is a good place to start.