BYTES

AN ESSENTIAL GUIDE TO SASE

CONTENTS

DEFINING SASE

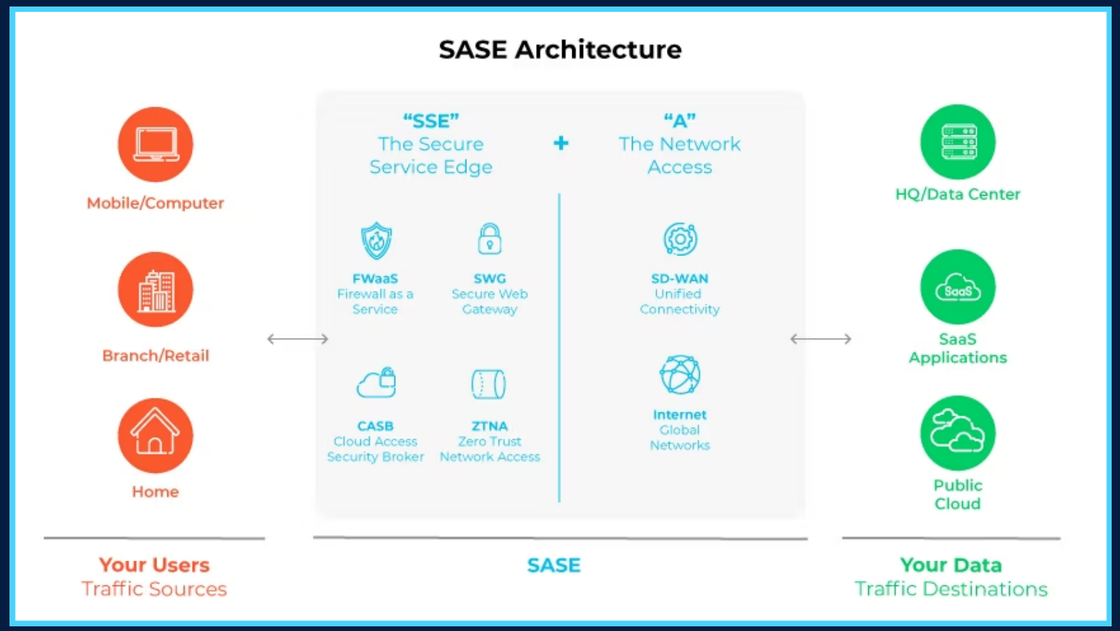
Service Access Service Edge (SASE) is a cloud-native architecture that unifies SD-WAN with security functions such as SWG, CASB, FWaaS, and ZTNA into one secure cloud service.

GARTNER STATES THAT 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’.

SASE ARCHITECTURE & HOW IT WORKS

A SASE (secure access service edge) architecture combines networking and security into a single cloud-delivered service at the network edge. This enables an organisation to support dispersed remote and hybrid users automatically by connecting them to nearby cloud gateways as opposed to backhauling traffic to corporate data centers. It also provides consistent secure access to all applications while maintaining full visibility and inspection of traffic across all ports and protocols.

The model radically simplifies management, reduces complexity and improves security, which are three of the main goals of SASE.



The above artwork is copyrighted by Palo Alto Networks.

It transforms the perimeter into a consistent set of cloud-based capabilities that can be deployed where and when they're needed. This is a more streamlined alternative to establishing a perimeter around the data center using a collection of disparate, point-product security appliances.

SASE provides a cloud-based solution which enables a more dynamic and high-performing network that adapts to changing business requirements, an evolving threat landscape, and the new innovations that will shape the future of your network.

UNPACKING THE KEY COMPONENTS OF SASE

SASE can be broken down into six essential elements in terms of its capabilities and technologies:

- **Software-Defined Wide Area Network (SD-WAN)** Seamlessly interconnect your resources, regardless of their location
- **Secure Web Gateway (SWG)** Protect web browsing against threats
- **Cloud Access Security Broker (CASB)** Secure and control cloud apps
- **Firewall as a Service (FWaaS)** Secure and traffic of any type
- **Zero Trust Network Access (ZTNA)** Secure remote access for users
- **Centralised Management** Manage all connectivity and security from a single point

KEY BENEFITS

- Easy scalability
- Cost savings
- Ease of use
- Unified security approach
- Network-wide data protection
- Secure cloud access
- Enhanced network visibility

USE CASES

- Migration from MPLS or legacy SD-WAN
- Multi-branch connectivity
- Network edge security services
- Secure remote access

Click here to learn more about our latest SASE Transformation Customer Case Study.

KEY CONSIDERATIONS: UNDERSTANDING YOUR ENVIRONMENT

CLOUD ADOPTION

Cloud and SaaS adoption is a key driver behind most SASE projects. New environments are being spun up and the traditional network is expanding out of the traditional boundaries. Ensuring secure and granular access to these new environments is key to any adoption program.

HYBRID WORKING

Historically we've been able to secure users by placing them behind a firewall or on a VPN which puts them behind that firewall. However with hybrid and remote working becoming the norm backhauling traffic to the DC can be an unsecure, costly, and painful process; especially when the data and apps users are trying to access are no longer hosted in the DC.

OFFICE-TO-OFFICE CONNECTIVITY

Legacy solutions utilised traditional hub and spoke designs, connecting branch offices and on premise data centres, which housed their corporate applications. However, the move to complex and distributed modern application networks renders these solutions inadequate in providing exceptional user experience, and security to all users and applications.

MIGRATION AND IMPLEMENTATION BEST PRACTICES

ASSESS

- Update existing document and diagrams
- Analyse existing security policies
- Define use cases and desired outcomes

DESIGN

- Define implementation timeline
- Map SASE components to sites and resources

IMPLEMENT

- Collaborate with vendor and implementation partner
- Start with a pilot program
- Migrate by phased approach

SUMMARY

SASE radically simplifies both the security architecture and policy management of the tools by providing a unified security architecture, which sits over the entire network (not just the physical network).

Whilst simple in architecture, it is crucial that your organisation understands the SASE market - and works with the most appropriate vendor(s) in order to meet your businesses unique needs.

SASE VIRTUAL EVENT

Are you ready to unlock the future of networking and security?

It’s time to embrace SASE – a unified platform that consolidates your security stack and simplifies your network infrastructure, all while ensuring secure access to your resources from any location.

Join Bytes & Palo Alto Networks* on Wednesday 21st February for our virtual event where a selection of Leading Experts will unpack & discuss how SASE can transform your Cyber strategy.

- **Time + Date:** Wednesday 21st February @ 10 – 11am
- **Location:** Virtual
- **Registration Link:** Click Here

USEFUL RESOURCES

- Gartner Market Guide
- Secure Remote Access Simplified
- ZTNA Guidebook

HOW BYTES CAN HELP

Book in a consultation with one of our in-house Network & Cloud Security experts to discover how best Bytes can support your SASE journey and **transform your IT security to deliver maximum protection against today's threats**.

Reach out to your dedicated Bytes Account Manager, or email our friendly team via tellmemore@bytes.co.uk