

Secure Access Service Edge (SASE) combines cloud computing and network security into a single solution. However, implementing SASE can be challenging, especially when testing and validating the network infrastructure.

This document provides an overview of SASE deployment and the importance of network emulation in its successful realization.

SASE Deployment

Validating Interoperability and Performance



Digital transformation is driving enterprises to reinvent their network security with SASE, a cloud-native model that converges capabilities like SD-WAN and CASB. By increasing visibility, agility, performance, resilience and security, SASE is seen as a driver for business transformation. It can enable operational change in areas such as workforce agility, deployment of edge computing and the utilization of cloud-delivered applications.

SASE's attractiveness also stems from its ability to simplify the delivery and operation of critical network and security services, resulting in significant cost savings for businesses. This can be achieved through vendor consolidation and faster IT deployment when setting up new users, locations, applications, or devices. However, realizing these benefits can be a complex task for some businesses.



SASE solutions – the implementation challenge

While single-vendor solutions would be a preferred option for end-user organizations to harness SASE benefits, the reality is that in the developing marketplace, finding a single vendor who can meet the unique needs for every organization is not always achievable.

The multi-vendor approach is, for many deployments, the only option. However, this can create implementation complexity for both the vendors delivering a solution and for the end-users seeking one:

- For vendors who can't offer an integrated SASE stack, the challenge quickly becomes how to prove interoperability and compete to become a preferred choice of supplier for their area of SASE specialization.
- For end users, adapting to vendor-specific limitations may necessitate adjustments to current or planned architecture. It's important to undertake these changes with confidence, ensuring that the vendor selection process validates both interoperability and full solution performance.

Regardless of position in the supply chain, whether among vendors or end users, the ultimate challenge remains validating interoperability to ensure successful deployment.

Validating interoperability: essential considerations

Gartner highlighted in their 2022 Strategic Roadmap for SASE Convergence that a migration plan is essential for those looking to adopt SASE. To deliver a successful migration they suggest identifying high, medium, and low priorities within a scheduled plan, with some key considerations including:

- A full SASE implementation requires a coordinated and cohesive approach across security and networking teams. This is challenging due to equipment refresh/renewal cycles, silo working and the level of available expertise with existing staff and incumbent suppliers.
- Mixing components like SD-WAN, firewalls, web gateways, CASB, and ZTNA is a complex task, and ensuring uniform policies, integrated workflows and a consistent user experience across disparate systems is difficult to achieve.
- Multi-cloud environments are the norm, routing traffic optimally between on-prem and cloud gateways requires coordinated orchestration.
- A lack of centralized monitoring and analytics makes troubleshooting any failures across the vendor stack challenging.
- A lack of unified end-to-end testing before vendor selection or rollout can leave blind spots for both vendors and end users.
- Solutions need to be future proof, delivering capacity, scalability, and compliance with security mandates.
- The introduction of security policies can affect overall network KPIs.
- Real-life network conditions are not stable; they fluctuate which may impact the performance of individual vendor solutions or the overall stack across different locations.
- Highly available, low-latency services are required for the end user and therefore needs to be contractually enforced through vendor SLAs.

Two common themes emerge from these considerations: readiness for change and risk mitigation. For a successful adoption of SASE, it's crucial that project teams collect comprehensive pre-deployment information and insights. This approach helps transform initial guesses and uncertainties into well-informed, fact-based decision making.

Performance and network insights

Each deployment has its own unique characteristics and therefore it also has different levels of resilience when it comes to performing under fluctuating network conditions. The key to achieving successful interoperability is to identify and understand the performance parameters, and then develop a deployment model against these.

This is done by carrying out a range of pre-deployment testing, gathering the intelligence this provides and then utilizing it to inform an optimal network design to meet the specific, and often unique, business needs.

Key considerations for effective SASE validation testing

The range of scenarios to be tested for obtaining key performance insights will be determined by the particular requirements of the project. However, some common SASE deployment factors to consider when thinking about validation testing are:

- Integration of multiple components like SD-WAN, firewalls, and ZTNA from different vendors
- End-user experience across multiple geographies
- Multi-edge global enterprise network models, including variable latency/network congestion
- Impact of security policies on network KPIs
- Capacity, scalability, and compliance with security mandates
- Visibility into third-party networks traversed
- Integration of non-standardized APIs and test tools

Creating a test-bed that addresses every scenario that a SASE deployment will need to be validated against is challenging in a conventional lab environment. SASE deployments will often be at scale, across multiple devices, geographies and network components. Therefore, validation testing must be carried out under the same set-up.

Network emulation provides flexibility in building and modeling complex real-life systems, enabling the simulation of networks and the emulation of the real-world conditions under which these SASE applications and platforms must perform. Vendor-neutral network emulation creates a scalable environment in which engineers can create repeatable and reproducible test cases to run under a specific set of performance characteristics. This provides a test-bed which generates the performance insights required for informed SASE project decision making.



Examples of using Network Emulation for SASE validation

SASE performance validation

A global enterprise achieved SASE deployment performance validation across 50,000 employees worldwide. By emulating their global network with 10 data centers, 150 branches and representative network impairments, they tested the integrated SASE stack under realistic conditions at scale. Latency and congestion issues were identified and resolved, improving performance by 35%.

Security Policy and Zero Trust validation

A SASE vendor validated their security policy implementation across multiple deployment scenarios during development. The environment modeled different network topologies and access levels representing real-world constraints. This allowed comprehensive policy testing without multiple physical test beds and accelerated release time by 30%.

SASE scalability testing

A Managed Security Provider tested the scalability of their SASE platform before rollout using an emulated environment. They modeled a 10x production workload with impairments, validating the platform's capacity for growth while ensuring reliable performance under peak load.

Optimizing SASE PoP placement

A service provider needed to model placement options for SASE Points of Presence (PoPs) across different geographic regions. Network latency, congestion and bandwidth limitations were modeled for each potential site, enabling optimized placement to ensure performance SLAs were consistently met for enterprise customers.

SASE validation solution

Calnex SNE Network Emulators enable comprehensive validation of complex multi-vendor SASE architectures at scale, ensuring security, performance and reliability goals are met before production, reducing deployment risk and accelerating ROI.

The advanced automation and network modeling capabilities of the SNE Network Emulators enable accelerated validation and actionable insights by:

- Emulating enterprise networks with 1000s of locations, data centers, internet links
- Introducing impairments like latency, jitter, loss, and congestion
- Assessing the performance of individual SASE components and integrated solution
- Identifying capacity bottlenecks, vendor compatibility issues
- Quantifying security policy impact on network KPIs like latency and throughput
- Creating realistic conditions to test and ensure security compliance and validate zero-trust access
- Accelerating testing through automation and an intuitive UI
- Scaling up concurrent sessions across a global topology

Acronyms

API Application Programming Interface

CASB Cloud Access Security Broker

KPI Key Performance Indicator

PoP Point of Presence

ROI Return on Investment

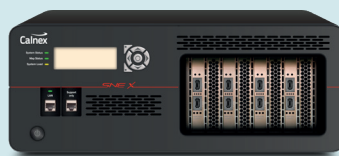
SASE Secure Access Service Edge

SD-WAN Software-Defined Wide Area Network

SLA Service Level Agreement

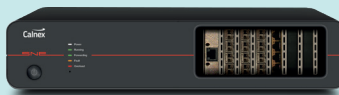
ZTNA Zero Trust Network Access

Related Products



Calnex SNE-X

- **Up to 28 ports** – enables multiple users and multiple links to simultaneously emulate different network conditions, facilitating interoperability testing between various components within the SASE ecosystem.
- **1 to 100GbE wire rate** – assess performance and scalability, validate QoS policies, and emulate realistic traffic scenarios in SASE deployments at any line rate and loading.



Calnex SNE

- 100GbE and 50GbE QSFP28 interfaces.
- RESTful API for easy automation.
- Jumbo packets for broadcast and video applications.
- Build and model complex real-life systems enabling you to simulate networks and emulate the real-world conditions under which applications and platforms need to perform.