Prepared for

JUNIPER
NETWORKS

SASE Transitions are Hard, but There are Ways to Make Them Less Painful

August 2021 EMA White Paper
By Paula Musich

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Executive Summary

In early 2020 many organizations were already well along in their digital transformation initiatives, but the rush to support users now working from home put those projects into overdrive. It also spurred greater interest in the emerging set of solutions described as Secure Access Service Edge, or SASE (pronounced sassy). When it comes to SASE adoption, the most difficult part of the journey in moving from separate, on-premises-based networking and security stacks to a largely cloud-based service is in the transition. The convergence of networking and security that forms the centerpiece of a SASE service has a number of implications that, when planned well, can make that transition significantly less painful.

Like a mantra, nearly all SASE providers murmur the phrase single policy engine when discussing the advantages of their SASE solution. That single policy engine may apply to all of the functions covered by their service, but it doesn't take into account the fact that there are still legacy security (and networking) technologies in use within new SASE customer environments—and those are governed by separate policy management systems. Inherent in any architectural shift is the need to manage new services or applications in parallel with legacy systems. This increases complexity, which was already an ongoing issue for security operations teams trying to manage a large number of best-of-breed security tools that offer little in the way of integration.

Introduction

Although the market for converged networking and security services for remote users (better known as SASE) is relatively nascent, the need to better support changing network traffic patterns has been building over several years. As enterprises engaged more cloud services and as users more frequently needed to access the services and applications necessary to do their jobs from any location, the legacy architectures that required sending traffic through a centralized data center for inspection and policy enforcement before it reached its destination no longer fit the bill. This evolution only accelerated in 2020 as IT teams scrambled to quickly support work-from-home initiatives. In research conducted on SASE interest and usage in the second half of 2020, Enterprise Management Associates found that among respondents whose organizations were in the midst of adopting a SASE solution, at least half indicated that the COVID-19 global pandemic had accelerated their SASE engagement.

As enterprises engaged more cloud services and as users more frequently needed to access the services and applications necessary to do their jobs from any location, the legacy architectures that required sending traffic through a centralized data center for inspection and policy enforcement before it reached its destination no longer fit the bill.

What constitutes a SASE service varies from one SASE provider to another. Most higher-layer networking and security functions are typically executed in the cloud. At minimum, a SASE service should provide SD-WAN, SWG, CASB, ZTNA, FWaaS, the ability to identify sensitive data (including encrypted data) and malware, and consistency in line-rate operations at the network's edge and from the cloud. Beyond those core capabilities, some enterprises looking to adopt a SASE service may also seek to incorporate web application and API protection, remote browser isolation, recursive DNS, network sandbox, API-based access to SaaS for data context, and support for managed and unmanaged devices. Still others may look for Wi-Fi hotspot protection, network obfuscation, legacy VPN, edge compute protection, and UEBA. Given the complex mix of capabilities that can make up a SASE service, and given the different approaches each SASE provider takes in creating their service, embarking on a SASE engagement can be daunting. Following are seven tips to help make transitioning to SASE less risky and ensure engagements are more successful.

01. Starting Down the SASE Path

Where and how organizations begin their SASE journey will vary from one enterprise to the next, depending on each's unique business requirements. Like any new technology adoption process, it's best to start with smaller projects and specific use cases as an enterprise looks to deploy elements of a SASE solution. Early SASE adopters often urge those starting a SASE deployment to gradually transition by replacing existing on-premises equipment, such as firewalls or secure web gateways (SWG), as their contracts near expiration. Starting with a small site can be a good place to gain experience in crafting policies. These can be geared toward specific use cases that represent the organization's business priorities. Some organizations will start with use cases, such as an MPLS replacement project, while others will start with an initiative to replace edge firewalls or VPN infrastructure with cloud-based security. Still others may start with transitioning SWG functionality from legacy gateway appliances located in branch offices and other remote locations to cloud-based web filtering.

The types of organizations that will find it easier to engage SASE service providers include newer technology companies born in the cloud and smaller companies that don't have as much legacy baggage as larger organizations. For the latter type of organization, overcoming inertia will be a bigger barrier to adoption, involving a longer education period.

For existing security and networking software or appliances that won't be replaced or that don't have near-term contract expirations, it's also important to consider where and how those can be redeployed. Are there some locations within the organization that require more in-depth, best-of-breed functionality than what a chosen SASE provider offers? Or are there locations that require greater performance than is available from the SASE provider's nearest point of presence? At the same time, does a prospective SASE provider offer integration with any of the existing security tools that will be redeployed to other locations?

In getting started with a SASE project, there is one other key consideration in planning for converged networking and security services: what will the workflows look like for team members responsible for managing a SASE deployment? Which existing security and networking processes should remain in place, and what has to change to ensure efficient and secure operation?

02. SASE Migration: It Takes Two to Tango

Converging networking and security functions into a single service requires close collaboration between networking and security teams. Although EMA research suggests that networking teams predominantly represent early SASE adopters, input and guidance from the CISO's team should be incorporated from the get-go. Large organizations looking to adopt SASE services should consider creating a dedicated team that draws on both networking and security practitioners, and that team should be assigned common objectives and goals to ensure a successful deployment. Given the borderless nature of SASE architectures and changing network traffic patterns as they move toward a range of cloud services, including security team members with more expertise in cloud security will bring vital insights to a SASE engagement. Their thinking has already moved beyond outdated notions of perimeter security and protecting a private, centralized data center where all enterprise traffic is aimed. At the same time, security practitioners involved in SASE migrations will need to elevate their focus from low-level security tool configuration and deployment to a higher-level business risk focus that takes into account the identity of users, devices, and applications.

SASE will ultimately require a change in culture, and IT executives can help to foster greater collaboration and trust by creating common incentives for SASE deployment teams that help to break down different IT silos. IT executives should lead by example to change culture from the top down.

One other thought about organizational challenges in adopting a new SASE service: any service under consideration should support multi-tenancy and role-based access control to enable more technical operations team members to perform their work without stepping on each other's toes.

03. Don't Let Policies Get Lost in Translation

One of the potential benefits of SASE is having centralized, role-based policies that can streamline operations, but the security industry in general has never taken into account what it takes to get there. SASE is no different, and many SASE providers—especially in the early days of the market—are typically not focused on playing nice with established policies, processes, and workflows. Centralized policy management is a misnomer if it does not combine the management of SASE services with remaining, on-premises networking and security functions. As networking and security teams assess potential SASE providers, it's important to look under the hood to determine how easily existing policies can be migrated to the new service while minimizing the opportunity for errors in the process.

As they transition to SASE services, larger organizations will want to use on-premises policy management tools and leverage an instance in the cloud. What's key to reducing operational complexity is to be able to synchronize both on-premises versions and cloud instances rather than requiring administrators to establish policies and manage them separately. Synchronization should be multi-directional so that any configuration or policy changes made within individual network security devices (such as firewalls or web proxies) that affect other devices in the network are propagated across the network, rather than having to be redone in the cloud instance or on-premises policy engine.

At the same time, prospects should also peer into the provider's architecture to gauge whether the provider started with a clean slate or whether they created their service via multiple acquisitions and/or through OEM relationships. The latter enables a best-of-breed collection of network and security services, but it requires solid integration among technology partners to ensure good orchestration across different service-chained policy engines and effective data sharing to reduce operational friction. The former can increase operational complexity, which can slow the migration and obviate any capex savings.

In planning a SASE transition, it's also important to keep in mind how policies need to change as enterprises move from heavy branch architectures, in which more security and networking functions are processed locally, to thin branch architectures, in which more functions are executed from the cloud. It will be critical to plan how access policies need to change to reflect the new architecture without changing the intent of existing policies as a result of human error. At the same time, policy decisions should be informed by greater context, such as the sensitivity of data users wish to access, the location and device from which they wish to access data, and whether a payload appears to be potentially malicious based on correlated threat intelligence.

04. Follow the App

One of the top benefits of a SASE architecture is that it frees applications from the confines of private data centers, enabling them to reside where it works best for the business. This is because with SASE, the perimeter where policies are applied becomes the identity of entities, whether those are devices, users, or applications, rather than the traditional DMZ. As applications migrate from private data centers to the cloud as part of organizations' digital transformation initiatives, and as cloud applications or workloads move, it's important to consider how adaptable the SASE provider's policy engine is. How much effort is required to ensure that the correct policies are applied to applications as they move from private data centers to a cloud provider's facilities? Do administrators have to manually reconfigure policies to move with those applications, or can those policies automatically be applied to the application in its new location? Is it possible to tag applications based on their identity and other contextual information so that policies automatically move with those applications? SASE services that deliver that level of integration and automation can help to reduce the time it takes to successfully deploy a SASE service by reducing the complexity surrounding its deployment. It also reduces day-to-day operational overhead as organizations move applications to meet changing business requirements.

Synchronization should be multi-directional so that any configuration or policy changes made within individual network security devices (such as firewalls or web proxies) that affect other devices in the network are propagated across the network, rather than having to be redone in the cloud instance or on-premises policy engine.

05. Identity Needs Context

With SASE identity, the new perimeter becomes a multi-dimensional construct. No longer just a MAC and IP address, identities include richer context to enable the enforcement of more fine-grained policies. As IT teams tackling SASE projects look at identity, they need to think beyond basic usernames and passwords stored in an Active Directory vault. For human users, identity information should go deeper to include the user's role, department, main geographic location, and the primary devices they use to access enterprise digital resources. This greater level of identity information, coupled with real-time contextual data, allows security practitioners to create policies that better match the changing network traffic patterns SASE is intended to serve. Policies can be tailored to better address changes in location, types of network connections being used, applications that users want to access, and more. The application of security controls and higher-layer network services, such as quality of service, can vary depending on whether the user is requesting access from a coffee shop or an airport Wi-Fi network, versus a branch office or headquarters' enterprise network. Policy decisions will also vary based on whether the application to which the user is requesting access is an enterprise CRM system, enterprise email, or financial application.

The application of security controls and higher-layer network services, such as quality of service, can vary depending on whether the user is requesting access from a coffee shop or an airport Wi-Fi network, versus a branch office or headquarters' enterprise network. Policy decisions will also vary based on whether the application to which the user is requesting access is an enterprise CRM system, enterprise email, or financial application.

The concept of identity also applies to different device types and applications. Beyond just servers and laptops, devices can include an increasingly broad array of OT and IoT devices, such as industrial control systems or smart refrigerators. SASE services should be able to gather details on devices to create a profile that governs policy decisions regarding the types of activities and levels of access they are allowed. The more granular the identity information, the more effectively the entity can be secured and compliance mandates met.

Understanding context is especially critical for applications and workloads located in the cloud, whether it is a SaaS, PaaS, or IaaS service. As IT teams evaluate SASE providers, they should ensure that the provider leverages the APIs of the cloud providers most important to their organization to be able to inspect out-of-band activity associated with their cloud usage.

06. You Can't Secure What You Can't See

SASE service providers are no different than many legacy network and application security providers. They all promise some form of single-pane-of-glass management. That may be true for all of the SASE functions that they directly support, but more often than not, it does not extend to legacy security appliances still in use within the organization. For multi-vendor SASE providers that work with a range of different partners to deliver a service-chained series of SASE functions, the ability to provide a single policy engine and management interface is limited by how well they integrate with those partners. This can increase operational complexity and greatly limit visibility into the customer's network traffic handled by products and services from the different partners, which makes it more difficult for security teams to spot malicious traffic or investigate an incident.

Observability into changing network traffic patterns from a centralized management interface is another key capability that can affect the successful rollout of a SASE service. The ability to detect and block malicious traffic does not end at the boundary between SASE-provided network and security services and services that internal security controls still support.

With users in a constant state of motion, connecting at different times from different locations, and cloud-based workloads and applications being spun up and down on a continual basis, with new locations coming online, maintaining visibility to determine what activity is legitimate and what is malicious is a big challenge. This raises the questions: is a prospective SASE provider's security monitoring capability up to the challenge? Can it correlate threat intelligence generated by not only its own monitoring capability, but from intelligence gathered by other security tools in use within the organization? Can it fill in the blanks between seemingly unrelated but anomalous activity to show the timeline of an attack as it progressed along the kill chain?

07. SASE Partner, not Product Pusher

As IT networking and security teams prepare for a SASE deployment, many will likely look to their SASE provider for advice and help in making the transition to a new architecture. What educational tools do they offer to help architects and operations professionals wrap their arms around how to deploy and manage their new SASE services? Are strategic planning services and deployment services options available? Does the provider have a customer success team to help ensure the deployment meets its objectives? What does the provider offer in the way of migration services? If there is no customer success team, is there an option of having a dedicated support engineer to assist with onboarding of the SASE service? Once onboarded, what type of support does the provider offer if or when problems arise that require help to determine the root cause? This is especially critical for SASE solutions that draw on best-of-breed services from different vendors so customers are not subjected to finger-pointing between technology integration partners. The selected SASE services provider should have a stake in the customer's success, given the relative immaturity of the market.

About Juniper Networks

Juniper Networks is dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security, and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability, and equality. Additional information can be found at Juniper Networks (www.juniper.net) or connect with Juniper on Twitter, LinkedIn, and Facebook.

Juniper Networks, the Juniper Networks logo, Juniper, Junos, and other trademarks listed here are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com** You can also follow EMA on **Twitter** or **LinkedIn**

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com** 4099.082021

PN: 2000781