www.pipelinepub.com
Volume 18, Issue 10

Security Where Needed with Cloud-Managed SASE

By: Renuka Nadkarni

With digital transformation, users and applications are anywhere, and the traditional network and location-based design architecture is obsolete. Users require flexibility with hybrid workforce and applications delivered as-a-service or across multiple clouds. The technology around access control, threat protection, and authorization must evolve to this new paradigm. At the same time, enterprises are looking for agility—fast provisioning of applications along with the corresponding network, security, and observability. While IaaS allows instantiating a workload in just a few minutes, the end-to-end provisioning may take days or even months.

As an example, one of our enterprise customers shared the fact that the service-level agreement to provision applications was 24 hours, whereas the networking and security team required two weeks. These disconnects in deploying network and security services slow down the business and its ability to operate at the speed of change.

As a lifeline, about three years ago, Gartner proposed the secure access service edge, or SASE, with the promise of integrated cloud-first networking and security capabilities that can be easily orchestrated along with application provisioning. The underlying concept of SASE is the twin pillars of network-as-a-service and network security-as-a-service. The former includes SD-WAN, optimization, CDNs, and other connectivity features. The latter includes a mix of security functions that include a secure web gateway (SWG), firewalling, cloud access security broker (CASB), and zero trust network access (ZTNA). More recently, Gartner has defined this security pillar as the security service edge, or SSE to include SWG, CASB, and ZTNA. But what is key is SASE's as-a-service aspect, aligned with the movement to the cloud.

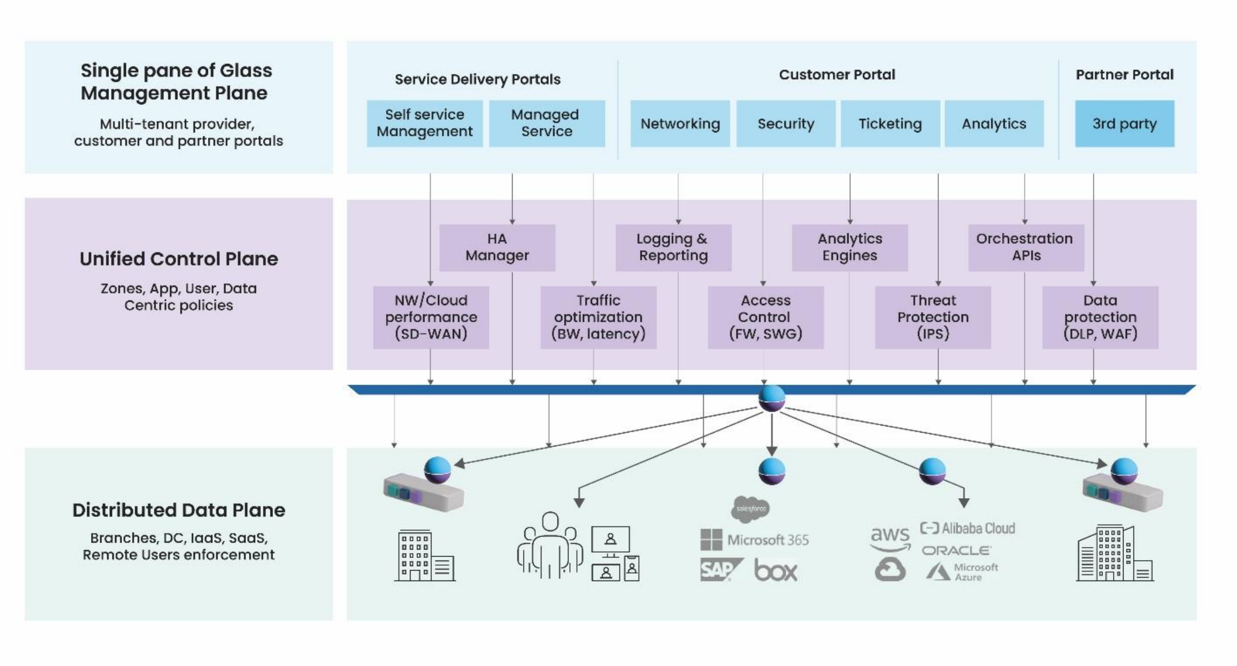

Figure 1: A look at the architecture
click to enlarge

Within the market, most of the focus is on the technology underpinnings for SASE—the various networking and security capabilities, and who offers what. Ultimately, to guarantee SASE success, we need to take a step back and look at the bigger picture. To offer the true flexibility that SASE promises and to deliver choice when required requires an underlying architecture equipped for this evolution. There are a few different important dimensions to this requirement, including technology, operations, sustainability, and cost.

Technological needs

Distributed data plane

With users and applications anywhere, security enforcement must happen closer to the source. Security controls should be easily enforceable at multiple places and wherever needed. This approach requires a combination of security applied at the customer premise closer to where the users are, in the cloud, and closer to the destination where the applications are. It must be truly distributed, a cloud-native data plane where the various security functions may be deployed at any edge and in support of any resources. To address the entire spectrum of the attacks, appropriate security functions need to be able to be applied at any location. This is something lacking in many current implementations, an oversight that can lead to future enforcement issues.

For instance, traffic bound to the Internet will need secure web gateway capabilities such as URL filtering, malware scanning, and data exfiltration detection. For user traffic going to the public cloud, one may want to scan assets for sensitive data for compliance and will need features like CASB for SaaS applications. It is critical to apply security controls based on the context while ensuring a good user experience. While inline technologies work best for access control, low and slow advanced threats can only be detected with more sophisticated analysis of data patterns over prolonged periods of time. Observability to the traffic pattern variations can ensure detection of anomalous behavior.

This distributed data plane architecture is based on a combination of intelligent 'services PoPs' as well as cloud-managed edge devices, with both hosting security functions. A service PoP goes beyond conventional connectivity services in supporting scale-out compute and storage required for SASE functions. Paired with the distributed data plane is effective control.

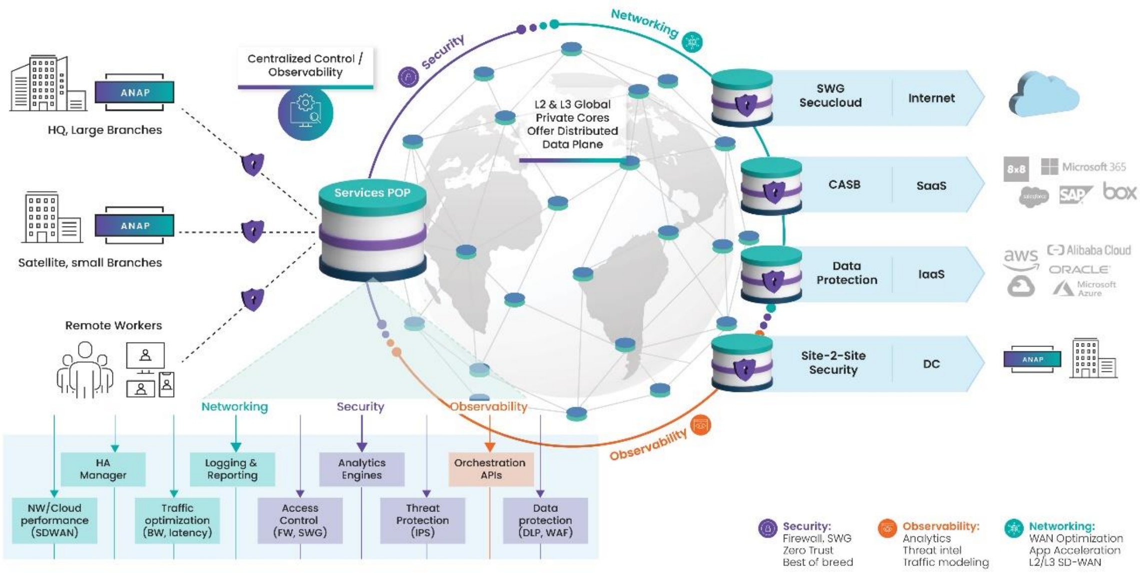

Figure 2: Going beyond conventional connectivity
click to enlarge

Unified control plane

SASE must be centrally orchestrated, a unified control plane that ties these capabilities together in a coherent way to apply policies consistently across hundreds of locations and ensure they get applied properly. As is common knowledge, the main reason for security breaches is misconfiguration due to complexity, lack of knowledge, and lack of oversight. Without a unified control plane, it is hard or even impossible to apply security ubiquitously and consistently. Given the as-a-service aspect of SASE, a managed services provider may effectively offer this control, removing the burden and chance of misconfiguration from the IT department.

'Single pane' management

The third technology underpinning is single pane management and observability in support of both network and security services. This is the ability to provide visibility into performance characteristics and security aspects of the traffic, and there are multiple locations across the network where this capability resides. As part of the managed services, the NOC/SOC will have visibility across the deployment, with the ability to leverage AI/ML and data analytics for proactive issue identification and resolution. The enterprise also requires a role-based portal into its slice of the network, and any management tools must interface with one or more logging applications.

Operational aspects

Organization structure

One of the main challenges cited as a cause that gets in the way of the SASE dream is the current structure of the organization. Typically, network decisions are made by network teams, and security decisions are made by security teams. But this traditional organization structure is soon fading as customers move away from rigid, network-centric thinking to modern application-centric thinking. This phenomenon started more than a decade ago when enterprises started adopting virtualization and cloud IaaS. The ’cloud’ team, sometimes referred to as a cloud ‘center of excellence’ with cross representation from different organizations, made the decisions. We think this blurring of lines between the network and security will accelerate as customers want to adopt digital transformation and protect against security threats. Going forward, the discussion will shift from network-focused thinking to more of an emphasis on application delivery.

Labor shortage

Another phenomenon is the shortage of skilled labor, and many newer companies or ‘born-in-the cloud’ enterprises do not even have network or security teams on their staff. They outsource almost all infrastructure with cloud for compute, network, and storage as well as security. The problem is that larger, older enterprises suffer the same skills shortages, leading to higher costs, lack of efficiency, and potential for breach. One alarming statistic is that almost 45 percent of cybersecurity professionals are considering resigning due to stress and workloads, a trend that will result in many fewer individuals entering the field than are required. A managed approach may help close this gap.

Audit and compliance

Most organizations still need to meet regulatory compliance standards and keep up other aspects for audits and change management. Requirements are becoming even more onerous over time as personal information protection and data residency become leading considerations.

Sustainability and cost considerations

Architecting sustainable solutions

It is tempting to adopt the newest technology or best-of-breed offering, only to find out later the implementation constraints that come with the need to stitch disparate solutions. As an example, one of our enterprise customers had all the global traffic routed to a single data center that did malware scrubbing. This turned out to be unsustainable as the business grew and became more distributed. As introduced earlier, a distributed data plane architecture offers the enterprise flexibility and scalability in where to implement the required functionality.

Alert fatigue and manageability of disparate solutions

Another customer shared how they needed a six-person team to process the alerts from many of the security devices and yet they were unable to effectively tie them together in a meaningful way. This leads back to the single pane of glass, and with a scale-out services PoP architecture, the different functions are more effectively 'chained' in a way that makes it easier to correlate alerts.

Cost savings

Lastly, it's essential to consider the cost of operations, maintenance and personnel needed to manage the fragmented solutions. This again leads back to the promise of SASE as a managed service with proven lower total cost of ownership. Analogous to the cloud consumption model with demonstrated advantages, the network and security consumption model delivers the same business outcomes.

The future

The combination of these three SASE attributes will deliver enterprise agility via integrated provisioning, configuration, orchestration, and management of both networking and security. Instead of convoluted traffic paths with service chaining, the new approach is to have 'single pass' architecture to provide relevant network and security services where needed.