FORTINET

WHITE PAPER

Fortinet Delivers the Most Flexible SASE Solution

Executive Summary

Digital transformation, multi-cloud adoption, and the widespread transition to remote work have fundamentally transformed enterprise networks and how they are secured. Organizations today are comprised of an increasingly distributed workforce that rely on cloud-based resources, such as Software-as-a-Service (SaaS) applications to communicate with each other and operationalize their business. This shift has moved the focus of security-driven networking beyond the datacenter toward a decentralized infrastructure comprised of multiple networks, applications and cloud environments. With this shift, organizations now must deliver high-performance, uninterrupted secure access to network and cloud-based resources in order to remain competitive and productive. The challenge is that many of the issues resulting from digital transformation efforts, such as dynamically changing network configurations and the rapid expansion of remote, off-network users means that traditional security solutions may not provide the flexibility and scalability that organizations require.

"Customer demands for simplicity, scalability, flexibility, low latency and pervasive security force convergence of the WAN edge and network security markets."[1]

Network security strategies must include a multi-layer approach that incorporates high-performance cloud-delivered solutions, in addition to more traditional thick edge solutions such as SD-WAN, and physical next-generation firewall (NGFW). Sometimes referred to as a a light-weight network edge strategy, cloud-delivered security provides essential network access in a way that allows infrastructure leaders to scale network protection for off-network users, protect network edges and enable better user access control across their distributed enterprise. This is the goal of secure access service edge, or SASE.

Accurately Defining SASE

Secure access service edge (SASE) is an emerging approach to network security that converges networking and cloud-delivered security services to enable flexible, anytime, and anywhere access for network edges and remote users. It enables digital innovation by ensuring business continuity in constantly evolving and expanding environments. SASE can also help establish and maintain a better user experience by delivering consistent and easy to use security for a dispersed workforce. SASE's goal of supporting the dynamic security and access needs of today's distributed enterprise is right in line with the security-driven networking strategy that Fortinet has been actively developing and promoting for years.

SASE was designed to help organizations control capital expenditures and reduce security infrastructure complexity resulting from digital transformation and the challenges that come with an expanding network. SD-WAN connectivity and cloud-delivered security are a good start, but have also created serious concerns about degraded performance, uptime, and service-level agreements (SLAs) of cloud-delivered services.

SASE fills gaps in connectivity and cloud security by enabling enhanced flexibility, consistent availability, and proven advanced security for the WAN and cloud edge. It is designed to support cloud-first initiatives for business applications, especially for employees who are increasingly working off-network. SASE is designed to improve business continuity, ensure secure access to cloud applications, and enhance user experience. To achieve this across a distributed network and mobile workforce, SASE leverages a purpose-built cloud architecture to protect remote workers, secure the edge of the network, and provide cloud-delivered access control.

SASE fills gaps in connectivity and cloud security by enabling enhanced flexibility, consistent availability, and proven advanced security for the WAN and cloud edge. It is designed to support cloud-first initiatives for business applications, especially for employees who are increasingly working off-network. SASE is designed to improve business continuity, ensure secure access to cloud applications, and enhance user experience. To achieve this across a distributed network and mobile workforce, SASE leverages a purpose-built cloud architecture to protect remote workers, secure the edge of the network, and provide cloud-delivered access control.

So, in addition to its essential cloud-based protections, a robust SASE solution also needs to support such things as zero trust (ZTNA) network segmentation and compliance requirements that cloud-based security can't address without shuttling traffic out to the cloud for inspection. Fortunately, Fortinet provides the most comprehensive and flexible solutions for SASE deployment, covering both cloud and physical device integration and deployment.

Key Elements of a SASE Solution

Conceptually, SASE was designed to address the security challenges created by SD-WAN vendors who may have delivered an innovative networking solution but failed to provide comprehensive and integrated security as part of their offering. Fortinet addressed this challenge head-on with a fully integrated Secure SD-WAN solution that provides a robust suite of both integrated networking and security features and functions that no other vendor has been able to achieve. And we have augmented on-demand, scalable security inspection and access controls delivered through our purpose-built cloud architecture.

Fortinet supports a fully integrated SASE solution with the broadest range of physical and cloud-based security solutions on the market. It starts with these essential elements:

- **Fortinet Secure SD-WAN** includes such things as dynamic path selection, self-healing WAN capabilities, and consistent application and user experience for business applications.
- The **FortiGate next-generation firewall** (NGFW) and FortiSASE cloud-delivered firewall provide a full stack of integrated security that spans both physical and cloud-based environments. Their physical, processor-enhanced hardware and optimized cloud-native software deliver high-security performance at scale, enabling maximum flexibility and security for any network configuration, including multi-cloud deployments.
- **Fortinet secure web gateway (SWG)**, deployed physically or on the cloud edge enforces internal internet access policies and filter unwanted software, especially malware, from user-initiated Internet connections. SWGs are critical for maintaining business and security policy continuity as enterprises continue to expand their WAN edge.
- **FortiCASB** is a cloud-based service that enables organizations to take control of their SaaS applications, secure application access, and eliminate shadow IT challenges. It can also be combined with on-premises DLP to ensure comprehensive data loss prevention.

Figure 1: SASE diagram.

Enhancing SASE with Additional Technologies

In addition to providing the core elements any robust SASE solution requires, Fortinet also offers optional tools designed to extend and enhance the security of the users and devices utilizing the SASE solution. And because they are integrated into the larger Security Fabric, they ensure that the entire solution can be seamlessly managed and controlled.

Endpoint security solutions, such as the FortiClient endpoint protection (EPP) and **FortiEDR** endpoint detection and response (EDR) technologies, ensure that the devices leveraging SASE are also secure. Advanced virtual private network (VPN) services provide secure data transmission and transactions while managing the complexities that can quickly arise when hundreds or thousands of remote offices and users need to interconnect. And the addition of Fortinet secure Wi-Fi and LAN controllers ensures that traffic leaving or entering the network receives an additional layer of inspection.

While every organization's needs are different, it's illogical for organizations to only embrace those technologies considered "core" to SASE—especially when a more comprehensive network and security strategy provides a richer set of business outcomes.

Lots of Potential and Too Few Qualified Vendors

While SASE is designed to address the access control and security challenges of today's WAN and remote user environments, the problem is that very few vendors are qualified to provide a complete SASE solution. For example, few if any of their tools—especially the security components—have been tested or certified. This means that consumers have no real way of knowing whether the security services they are purchasing will protect them in a real-world environment.

This is already a serious concern even within the highly specialized cybersecurity space, where vendors sometimes opt out of third-party testing and validation when their solutions cannot perform up to industry expectations. This problem is amplified when vendors provide SASE solutions with minimal or narrow security experience, but rush to take advantage of "SASE" as a buzzed-about marketing term.

The Fortinet Advantage

For SASE to work well, all of its components need to interoperate as a single integrated system—connectivity, networking, and security elements alike. The reason this might sound familiar is because Fortinet has been delivering the core SASE requirements—plus much more—for years as part of our integrated Security Platform and Security Fabric architecture. This unified approach supports true convergence of networking and security functions, enabling a security-driven networking approach that further enables the rapid acceleration of digital innovation—without ever compromising protection.

Many SASE vendors rely on public cloud providers (and their security) to provide connectivity and protection rather than investing in their own global network. We chose a different path. The Fortinet SASE cloud architecture is multitenant, scalable, and application-specific integrated circuit (ASIC)-powered—and our cloud architecture is among the top 8% most interconnected backbones in the world, enabling us to deliver ultralow latency and high performance.

Thanks to over 20 years of security innovation at Fortinet:

- We were the first major security vendor to fully integrate security into SD-WAN because we were able to combine years of security and networking experience into a single, unified solution.
- We then went a step further by developing the world's first SD-WAN processor designed to accelerate networking and security functionalities to provide the level of performance today's most demanding network environments require.
- We earned a designation in the Leader's quadrant in the Gartner 2020 Magic Quadrant for WAN Edge Infrastructure.
- Our security solutions are the most tested and validated in the industry. They have received six consecutive NSS Labs NGFW "Recommended" ratings.

Delivering the kind of comprehensive SASE solution your organization needs is already part of our approach to networking and security. Unlike other vendors, we can customize that solution with the widest range of advanced connectivity and security technologies in the industry—ensuring that your SASE solution is designed to adapt as your requirements evolve. And because it is part of the Fortinet Security Fabric, your SASE solution can be integrated and connected with other solutions you deploy, whether on-premises or in the cloud. What's more, all of this is covered by our single-pane-of-glass management system to ensure broad visibility and granular control across your entire network, including your SASE environment.

We're excited by the recent market momentum around SASE because it further validates our Security Fabric approach and underscores what we've been saying for years. In the era of cloud connectivity and digital innovation, networking and security must converge. There's no going back to outmoded and siloed architectures. Fortinet is engineered for the SASE era and so much more.

October 8, 2020 12:50 AM

742476-A-0-EN

D:\Fortinet\White Paper\Red White Paper\SASE\[UPDATE - 1032020]\wp-FA-fortinet-delivers-the-most-flexible-sase-solution-1082020