FORTINET

WHITE PAPER

# Fortinet Delivers the Most Flexible SASE Solution

## Executive Summary

**Digital innovation, cloud adoption, and the recent widespread shift to remote work have fundamentally transformed the network. And with the increased reliance on cloud-based resources, such as Software-as-a-Service (SaaS) applications and data moving from the data center to multi-cloud environments, the need for a new approach to secure network access—especially the challenges of implicit trust inherent in legacy network architectures—has become clear.**

**Today's organizations require immediate, uninterrupted access to network and cloud-based resources and data, including business-critical applications, from any location, on any device, at any time. The challenge is that many of the issues resulting from digital innovation efforts, such as dynamically changing network configurations and the rapid expansion of the attack surface, mean that many traditional security solutions no longer provide the level of security and access control that organizations and users require.**

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

**Secure access service edge (SASE) is an emerging enterprise strategy that combines network security functions with WAN capabilities. SASE's goal is to support the dynamic, secure access needs of today's organizations—right in line with the security-driven networking strategy that Fortinet has been actively developing and promoting for years. SASE plays a critical role in ensuring that security can be delivered anywhere, including at the WAN edge, cloud edge, data-center (DC) edge, core edge, and endpoint devices used by today's heavily mobile remote workforce.**

## Start by Accurately Defining SASE

As with any emerging technology category, there is still some uncertainty about a precise definition of a SASE solution. Is it strictly a cloud-based offering? Or does it include physical solutions as well? And what technologies are involved in a SASE solution?

While SASE is generally classified as a cloud-delivered service, there are common circumstances that may require a combination of physical and cloud-based solutions for SASE to be effectively integrated into the network. This may include combining SASE connectivity with network access controls and edge security devices for remote workers, supporting a physical software-defined wide-area networking (SD-WAN) device—especially one that contains a full stack of security—or even needing to integrate with technologies such as wireless local-area network (LAN) controllers or Wi-Fi access points at branch offices.

So, in addition to its essential cloud-based protections, a robust SASE solution also needs to support such things as network segmentation and compliance requirements that cloud-based security can't address without shuttling traffic out to the cloud for inspection. Because of this, Fortinet provides the most comprehensive and flexible solutions for SASE deployment, spanning both cloud and physical device integrations and deployments.

## SASE Is All About Secure Access

Conceptually, SASE is an attempt 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. These are all part of the security-driven networking and Security Fabric platform strategy we have been providing to customers for years.

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 security elements:

- **A fully functional SD-WAN solution.** As the heart of the SASE solution, SD-WAN needs to include such things as dynamic path selection, self-healing wide-area networking (WAN) capabilities, and consistent application and user experience for business applications.

- **A next-generation firewall (NGFW) (physical) or Firewall-as-a-Service (FWaaS) (cloud-based) firewall.** SASE also needs to include a full stack of security that spans both physical and cloud-based scenarios. For example, organizations with a remote worker strategy will require a combination of edge security and internal segmentation to prevent guest or Internet-of-Things (IoT) threats from crossing over to restricted corporate network resources, combined with cloud-based security for accessing resources located online or in the cloud. Physical, processor-enhanced hardware and scalable cloud-native security can deliver the same high performance at scale, enabling maximum flexibility and security for the organization.
- **Zero-Trust Network Access (ZTNA)** is used to identify users and devices and authenticate them to applications. Because ZTNA is more of a strategy than a product, it includes several technologies working together. Multi-factor authentication (MFA) identifies all users. On the physical side, ZTNA includes secure network access control (NAC), access policy enforcement, and integration with dynamic network segmentation to limit access to networked resources. And on the cloud side, ZTNA supports things like microsegmentation with traffic inspection for secure east-west communications between users, and always-on security for devices both on- and off-network. By combining physical and cloud-based ZTNA services, organizations can ensure secure access and the enforcement of policy, whether devices and users are on- or off-premises.
- **A Secure Web Gateway** is used to protect users and devices from online security threats by enforcing internet security and compliance policies and filtering out malicious internet traffic. It can also enforce acceptable use policies for web access, ensure compliance with regulations, and prevent data leakage.
- **A CASB** cloud-based service enables organizations to take control of their SaaS applications, including securing application access and eliminating Shadow IT challenges. This needs to be combined with on-premises DLP to ensure comprehensive data loss prevention.


Figure 1: SASE diagram.

## Enhancing SASE with Additional Technologies

SASE is designed to enhance and support digital innovation, but without looking at a SASE approach holistically, organizations may also end up creating yet another isolated security solution that needs to be managed separately from the rest of the security architecture. This can severely limit both visibility and control across the network. So, 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 they also ensure that the entire solution can be seamlessly integrated into the larger Security Fabric.

For example, endpoint security, such as endpoint protection (EPP) and endpoint detection and response (EDR) technologies, ensures that devices leveraging SASE are themselves secure. An advanced virtual private network (VPN) provides 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 secure Wi-Fi and LAN controllers ensures that traffic leaving or entering the network receives an additional layer of inspection.

Every organization's needs are different, but it's illogical for organizations only to embrace those technologies considered "core" to SASE when a more comprehensive network and security solution 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 secure WAN challenges today's organizations face, 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

At Fortinet, we are often asked, "What is your SASE strategy?" For SASE to work well, all of its components need to interoperate as a single integrated system—connectivity, networking, and security elements alike. Part of the reason that sounds so familiar to us at Fortinet is that we have been delivering the core SASE requirements—plus much more—for years as part of our integrated Security Platform and Security Fabric architecture. This creates true convergence of networking and security functions as part of a security-driven networking approach that further enables the rapid acceleration of digital innovation—without ever compromising protection. A number of our customers looking to implement SASE have found that, with minor adjustments, they already had a SASE solution in place thanks to the power of the Security Fabric.

SASE endeavors to solve a real problem. But it's the same sort of problem Fortinet has addressed before.

- 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 are proud that Fortinet security tools are the most tested, validated, and certified solutions in the industry today.

What this means is that delivering the kind of SASE solution your organization needs is already part of our approach to networking and security. And we can customize that solution with a range of advanced connectivity and security technologies, ensuring that your SASE solution is designed to adapt as your requirements evolve. The Fortinet Security Fabric can also integrate and connect with other solutions you deploy, whether on-premises or in the cloud. And all of these elements are covered by our single-pane-of-glass management system to ensure broad visibility and granular control across your entire network, including your SASE environment.

Fortinet is uniquely positioned to offer a complete SASE solution that ensures security is delivered consistently anywhere across the network—not just at the WAN and cloud edges, but at the DC edge, core network edge, and endpoint edge as well, to enable seamless connectivity, visibility, and control.

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.

[1] Frank Marsala, "The Future of Network Security Is in the Cloud," Gartner, September 13, 2019.





August 10, 2020 1:05 PM

Macintosh HD:Users:bhoulihan:Downloads:wp-FA-fortinet-delivers-the-most-flexible-sase-solution-7312020:wp-FA-fortinet-delivers-the-most-flexible-sase-solution-7312020

742476-0-0-EN