SOLUTION BRIEF

FortiSASE: Securing Internet Access for Remote Users

Executive Summary

The hybrid workforce has become a reality for most businesses, yet it creates new headaches by expanding the organization's attack surface. This challenges security and IT teams as they work to secure these remote users. One struggle is ensuring that security policies are being applied and enforced consistently for users on and off the corporate network. Secure access service edge (SASE) architecture helps extend secure access and high-performance connectivity to users regardless of their geographic location.

The Fortinet FortiSASE solution enables secure internet access and more while allowing organizations to shift from a CapEx to an OpEx business model. FortiSASE empowers organizations to enable secure access to the web, cloud, and applications anywhere while delivering enterprise-grade security and superior user experience.

"IT leaders need to balance priorities, protecting the user experience yet also satisfying security requirements. This makes SASE a compelling solution because it can achieve both at the same time."[1]

– Franz Chavez, VP, Solutions Engineering, Masergy (now part of Comcast Business)

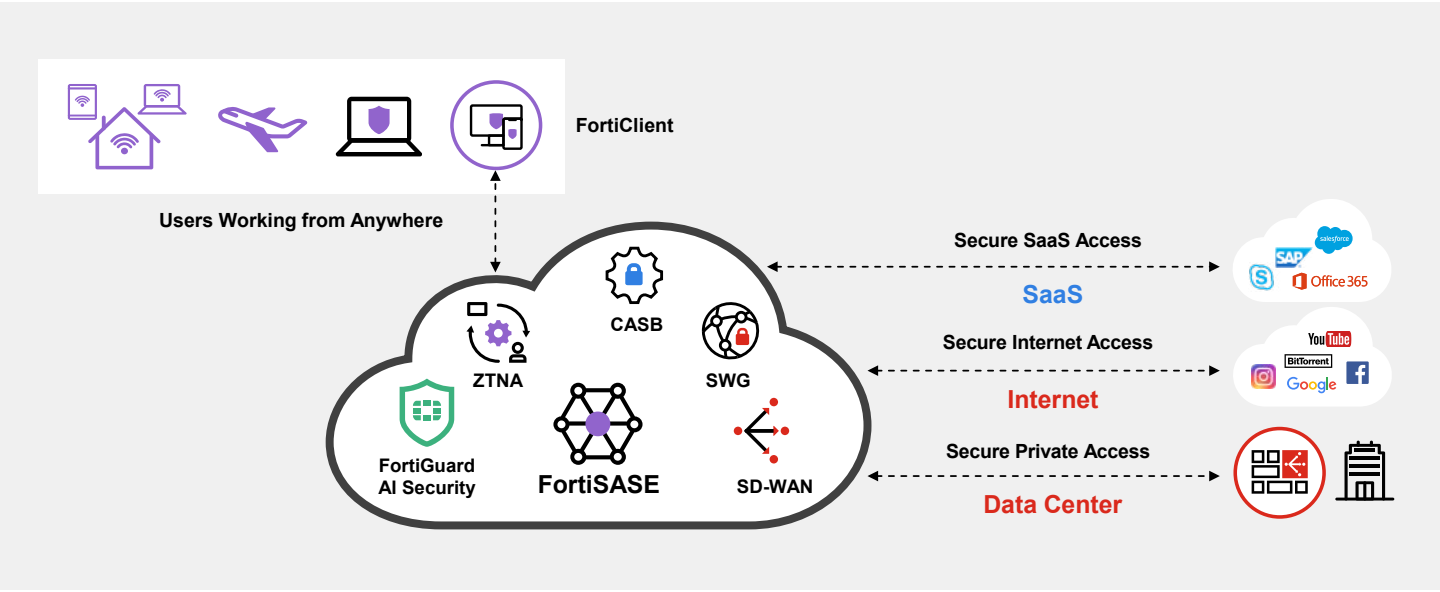

Figure 1: Consistent security at every edge, powered by FortiOS

FortiSASE: Simple, Seamless, and Scalable Cloud-Delivered Security

FortiSASE offers simple cloud-based management with self-service design, easy user onboarding, and a flexible, tiered, and user-based licensing model.

FortiSASE supports Firewall-as-a-Service (FWaaS) and secure web gateway (SWG) functionality, which relies on the threat intelligence that FortiGuard Labs provides. Powered by the FortiOS operating system, the FortiSASE FWaaS has all the same features, security, and reliability that customers depend on from FortiGate Next-Generation Firewalls (NGFWs). Additionally, FortiSASE SWG relies on the FortiOS explicit web proxy, captive portal, and authentication features to secure users' web traffic. Together, these threat protection capabilities enable secure internet access.

FortiSASE also includes Universal zero-trust network access (ZTNA), next-generation dual-mode cloud access security broker (CASB), and secure SD-WAN integration to enable other use cases such as secure Software-as-a-Service (SaaS) and private access.

Why Organizations Choose FortiSASE

Cybercriminals will continue trying to infiltrate an enterprise's always-expanding attack surface. That's why organizations need a solution capable of following, enabling, and protecting users no matter where they—or the applications they use—are located. FortiSASE provides more than an encrypted tunnel to address today's advanced threats. It includes a portfolio of enterprise-grade security solutions designed to inspect traffic and detect and respond to known and unknown threats.

FortiSASE also integrates endpoint and network security, providing seamless visibility and control across and between all endpoints, enforcing conditional access policies, and delivering an automated threat response. It provides end-to-end visibility for both hosts and endpoint devices to help organizations harden endpoints and enhance their security posture. Specifically, the Fortinet endpoint security agent FortiClient simplifies endpoint management by centralizing critical security tasks, identifying vulnerabilities, and correlating events to improve incident reporting.

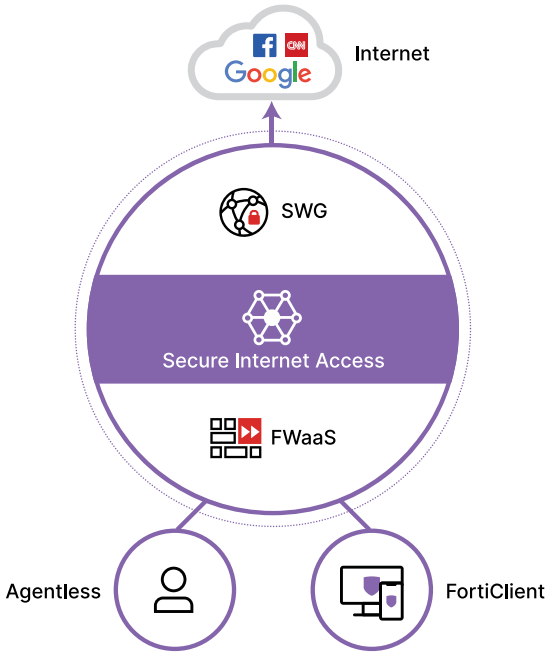

Figure 2: Secure internet access for work-from-anywhere (WFA)

FortiSASE secure internet access enables:

- **Simplicity:** With Fortinet best-in-class security deployed everywhere, FortiSASE allows for a consistent experience for on-premises and remote security to reduce security gaps, simplify operations, and significantly reduce overhead resources associated with setup and configuration.
- **Consistent security:** Overcome security gaps and minimize attack surfaces with a consistent security posture across physical offices and remote users. Simplify network and security policy management by using a unified networking approach and single agent for strong security everywhere.
- **Advanced detection:** Get advanced threat detection with high-performance secure sockets layer (SSL) inspection and threat detection techniques with Fortinet FWaaS and FortiGuard AI-powered security services. Easily implement identity control and protection with ZTNA everywhere for all users and devices.

FortiSASE Secure Internet Access Features

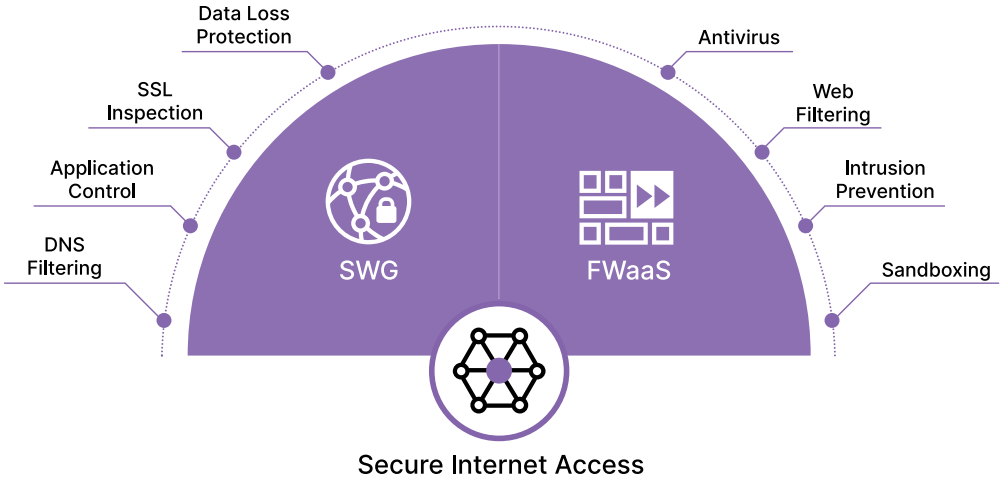

Figure 3: Comprehensive security services for safe browsing

Antivirus (AV)	FortiSASE AV delivers automated updates that protect against the latest polymorphic attacks, viruses, spyware, and other content-level threats. Based on patented content pattern recognition language (CPRL), the anti-malware engine is designed to prevent known and previously unknown malware variants.
Application Control	FortiSASE can recognize network traffic generated by many applications. Application control sensors specify what action to take with the application traffic. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic, even if the traffic uses non-standard ports or protocols.
Data Loss Prevention (DLP)	DLP allows businesses to identify sensitive information across multiple cloud-based systems, prevent the accidental sharing of data, and monitor and protect data.
DNS Filtering	DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, including malicious newly registered domains (NRDs) and parked domains. It protects against sophisticated DNS-based threats, such as DNS tunneling, DNS infiltration, C2 server identification, and DGAs (Domain Generation Algorithms).
Intrusion Prevention System (IPS)	IPS provides near-real-time intelligence with thousands of intrusion prevention rules to detect and block known and zero-day threats before they reach your devices. The service is augmented by our in-house research team, credited with more than 9 million network intrusion attempts blocked every minute.
Sandbox	The FortiSASE client (FortiClient) submits unknown or suspicious objects to the sandbox for detailed analysis. Once the sandbox identifies the threat, it notifies all FortiClient-protected endpoints and other security elements within the Fortinet suite of products. This proactive approach allows IT infrastructure leaders to pinpoint and block unknown and zero-day threats quickly and easily.
SSL Inspection	While Hypertext Transfer Protocol Secure (HTTPS) offers protection on the internet by applying SSL encryption to web traffic, encrypted traffic can be used to get around your network's normal defenses. When you use deep inspection, FortiSASE impersonates the recipient of the originating SSL session, then decrypts and inspects the content to find threats and block them. It then re-encrypts the content and sends it to the real recipient. Deep inspection not only protects you from attacks that use HTTPS, but it also protects you from other commonly used SSL-encrypted protocols, such as SMTPS, POP3S, IMAPS, and FTPS.
Web Filtering	Web filtering leverages a database of hundreds of millions of URLs classified into 90+ categories to enhance granular web controls and reporting. TLS 1.3 support extends analysis to encrypted traffic. It also blocks unknown malicious URLs almost immediately. Web filtering with keyword search and YouTube filters blocks web pages containing words or patterns that you specify, as well as limits users' access by blocking or only allowing specified YouTube channels. Web filtering also includes file filter capabilities, which allows the blocking of files passing through a FortiGate NGFW based on file type.

Achieve Better Business Outcomes with FortiSASE

FortiSASE meets the need for consistent networking and security from any location, ultimately delivering enhanced user experiences and better business outcomes. Wherever your organization is on its digital acceleration journey, Fortinet's goal is to help consolidate security under one vendor, with one client and one operating system to reduce complexity, increase security effectiveness, and ensure a reliable user experience across today's expanding networks. It enables hybrid workforce security and cloud-delivered security for WFA for any organization worldwide.

[1] "2022 SASE Market Trends Study: Benefits Exceed Expectations in Security and Remote Connectivity," Masergy, Fortinet, and CIO, June 28, 2022.

FORTINET

www.fortinet.com

December 28, 2022 11:43 AM
1880366-0-0-EN