FORTINET

Concept Guide

FortiSASE

DEFINE / DESIGN / DEPLOY / DEMO

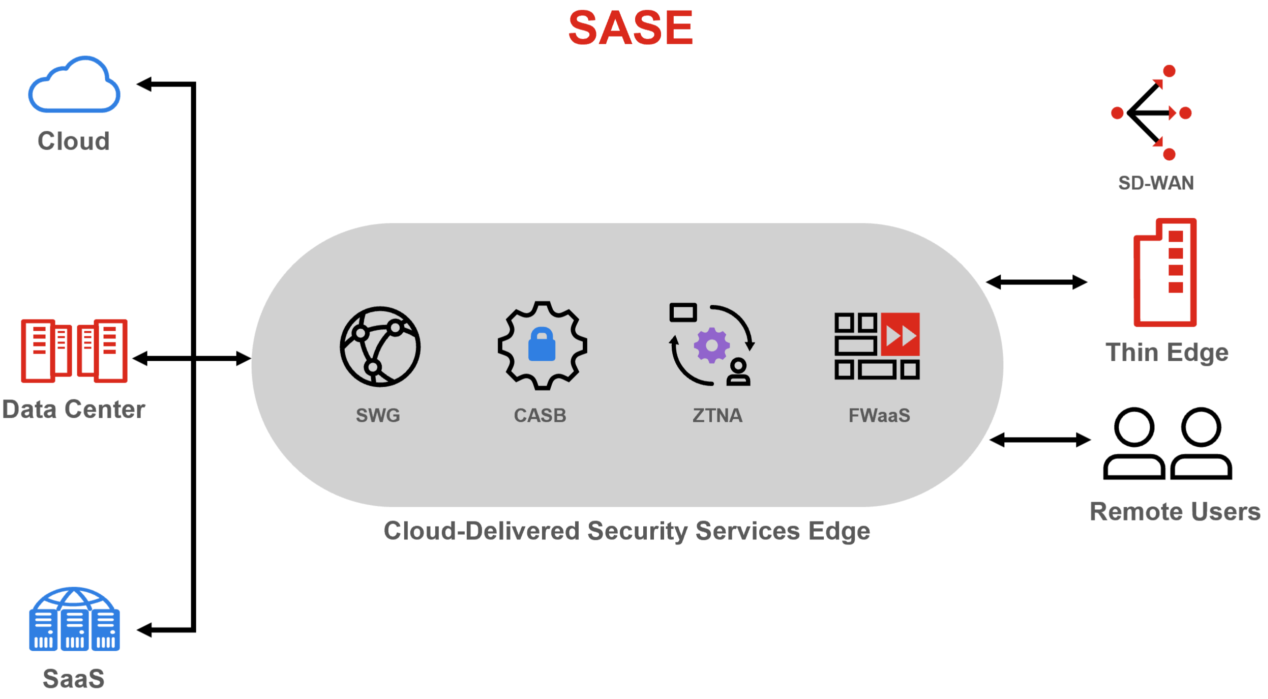
Table of Contents

Introduction

This document presents information about the secure access service edge (SASE) networking and security architecture and provides a broad overview of Fortinet's SASE solution, a cloud-delivered service called FortiSASE.

Executive summary

SASE is an architecture that combines network, security, and WAN capabilities delivered as a service to provide endpoints (remote users, devices, and branches) with secure Internet, cloud, and data center network access. The SASE architecture achieves secure network access using network security technologies including firewall-as-a-service (FWaaS), secure web gateway (SWG), zero trust network access (ZTNA), and cloud access security broker (CASB), and relying on WAN technologies including software-defined wide-area network (SD-WAN).



Today's work from anywhere environment makes it difficult for IT administrators to keep up with securing users' devices. These users' devices, also known as endpoints, are off-net, that is, located outside the corporate network. SASE extends network security functions beyond where they have been typically available in the past, namely, beyond an organization's internal network. SASE aims to provide remote users and branches located anywhere with secure network access.

Typically, an organization has a remote user use a virtual private network (VPN) connection to redirect their Internet traffic to a next generation firewall (NGFW) located at its data center. After performing its security functions, the NGFW sends the user's web traffic out the NGFW's WAN link. Remote users with VPN connections established also experience high latency when accessing the Internet over this backhauled WAN connection because the firewall's WAN link becomes congested with Internet traffic that other remote users generate. SASE reduces this latency by allowing remote users to connect directly to the closest geographical point-of-presence (PoP) for a cloud-delivered FWaaS. Also, each PoP can scale to meet user demand and reduce the possibility that a single WAN link becomes a congestion point for these remote users.

FortiSASE is Fortinet's cloud-delivered security service that implements the SASE architecture (FWaaS, SWG, ZTNA) to provide secure access to remote users through the following use cases:

- Secure Internet access (SIA) when users access Internet and web-based applications
- Secure private access (SPA) when users access private company-hosted applications protected by a FortiGate NGFW
- Secure SaaS access (SSA) when users access SaaS applications

This document explores SASE concepts, components, and architecture, and describes how Fortinet delivers its SASE solution.

Intended audience

This concept guide is intended for a technical audience, including system and network architects, design engineers, network engineers, and security engineers who want to understand the SASE architecture and the FortiSASE service offering to secure their remote workers and branch offices.

This guide is targeted at small and medium organizations and enterprises. It assumes that the reader is familiar with basic concepts of applications, networking, routing, security, and proxies, and has a basic understanding of network and data center architectures.

About this guide

This guide provides a broad overview of SASE concepts and introduces the FortiSASE cloud-delivered service and related Fortinet products used to deploy a SASE solution. It uses industry standard terminology with introductions to Fortinet-specific terms, concepts, and technologies.

Once readers are familiar with FortiSASE concepts and terminology and ready to explore different architectures in their environment, they can proceed to the FortiSASE Architecture Guide.

SASE overview

This chapter provides an overview of secure access service edge (SASE) and covers the following topics using a top-down approach:

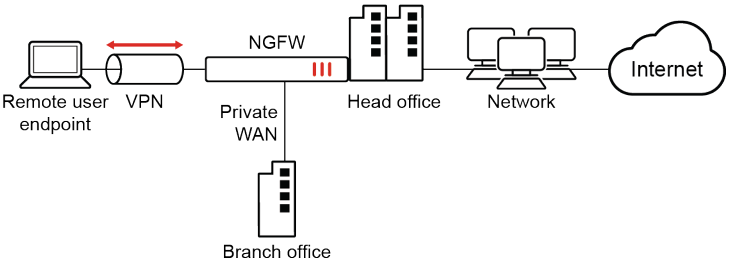
SASE concepts

This section describes the context and challenges behind the need for the secure access service edge (SASE) architecture:

- Standard firewall architecture on page 5
- Work from anywhere on page 6
- Challenges on page 6

Standard firewall architecture

Typically, an organization has a next generation firewall (NGFW) that protects its network or data center from the Internet and acts a default gateway to the Internet through one or more WAN links, as the diagram shows:



The NGFW is usually a physical or virtual appliance situated at the organization's network edge.

A virtual private network (VPN) is the industry-standard solution that provides remote access, authentication, and encryption capabilities using a software client or agent to secure traffic between a user on the Internet and the VPN gateway protecting an organization's network. Remote access VPNs rely on IPsec or SSL-based VPN implementations.

Typically, an organization provides its remote users with protected access to its network via VPN connections or provides its branch users with protected access via other WAN technologies, such as multiprotocol label switching.

Organizations have extended this scenario to ensure its remote users have secure Internet access by enforcing VPN connections with full tunneling enabled. With full tunneling VPNs, the following traffic goes through the VPN:

- Traffic destined for the organization's internal network
- Traffic destined for the Internet is sent to the Internet through the VPN to the NGFW for threat detection and mitigation

Therefore, a remote user's Internet traffic not only goes through its own local ISP to establish a VPN connection with the NGFW, but also goes through the NGFW's WAN link. This operation is known as WAN backhauling.

Work from anywhere

When users are located behind the organization's next generation firewall (NGFW) and reside on the local network, they are said to be on-net and are subject to the security policies and security features that are configured on the NGFW.

With the practice of working from anywhere, users are often located outside the organization's NGFW and are said to be off-net. Off-net users are also typically unmanaged, that is, the organization's IT team does not manage them, and they typically access the Internet directly via the local Internet service provider, which bypasses all security policies and security features.

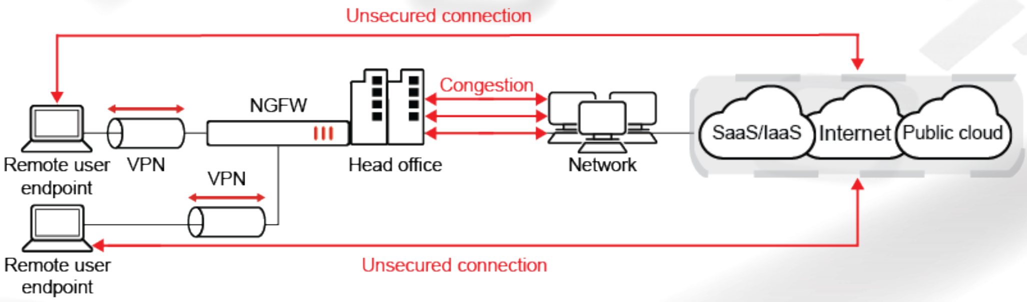
Challenges

The practice of work from anywhere and the standard firewall architecture present distinct yet significant challenges for organizations.

When working from anywhere, off-net endpoints, by default, use direct Internet access for most of their traffic without any network security protection, thus becoming susceptible to malware and other network security threats, as the diagram shows. Therefore, to combat this challenge, organizations rely on the standard firewall architecture and full tunneling VPNs to backhaul their WAN traffic through the next generation firewall (NGFW).

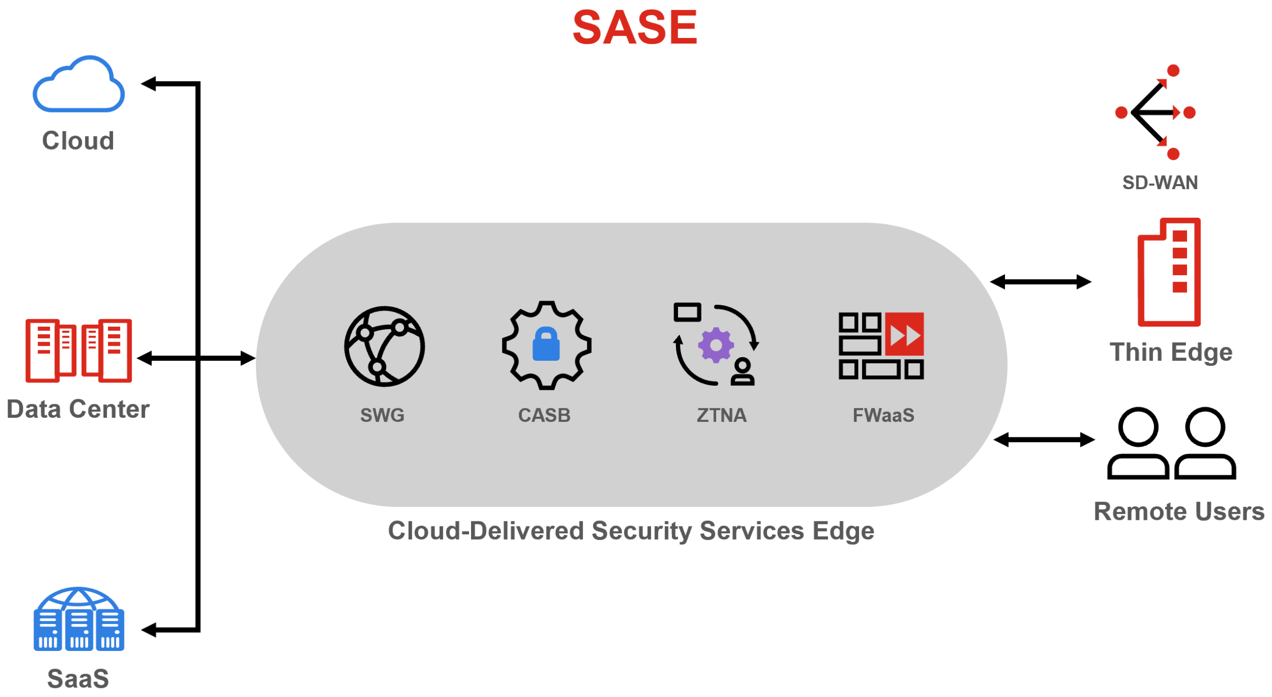
Using the standard firewall architecture for WAN backhauling introduces extra load on the NGFW and its WAN links, which can lead to network congestion at a firewall's WAN links, especially at peak working hours, as the diagram shows. Also, this load slows down the NGFW as it must use more CPU resources for VPN encryption and decryption. Therefore, performance degrades at both the NGFW and WAN link, which leads to remote users experiencing latency when accessing networks through full tunneling VPNs, ultimately degrading their overall user experience.

In addition, when working from anywhere, off-net endpoints are typically unmanaged, meaning that the devices' security posture may be vulnerable due to lack of software and vulnerability updates, and therefore cannot be considered trusted devices.



SASE architecture

This section describes the overall secure access service edge (SASE) architecture and goals. The following diagram illustrates the SASE architecture as Gartner describes:



As the previous section describes, the standard firewall architecture and practice of working from anywhere introduces network security challenges. Organizations can overcome these challenges using the SASE architecture.

The SASE architecture focuses on using a cloud-delivered security service that enforces secure access at the farthest network edge, namely, at the service edge or at the user endpoints. This architecture has the following goals:

- Achieve secure Internet access for off-net endpoints that connect to a cloud-delivered security service that comes between a user and the Internet
- Reduce latency by having off-net endpoints connect to a cloud-delivered security service's closest point of presence (PoP)
- Meet off-net endpoints' traffic demand by providing a cloud-delivered security service that can scale dynamically
- Reduce congestion by distributing endpoint traffic to different PoPs with sufficient geographical spread

and avoiding a single point required for traffic flow

- Enforce a zero trust model to provide protected network access for off-net endpoints

An endpoint or branch redirects its traffic to the cloud, data center, or software-as-a-service (SaaS) to pass through a firewall-as-a-service or a secure web gateway where the traffic is subject to security policies and advanced threat protection measures. For traffic redirection, remote users' endpoints rely on a software agent, while devices and branches rely on a thin edge device.

You can use cloud access security broker and zero trust network access services within the SASE architecture to restrict access to cloud/SaaS and data centers, respectively. In the SASE architecture, WAN capabilities from the branch to a cloud-delivered security service or from within the cloud-delivered service itself can use a variety of WAN technologies, with SD-WAN currently being at the forefront of those technologies.

The cloud-delivered security service is located between the remote endpoints and any networks those endpoints access, regardless of the location of the remote endpoints: essentially, moving the security to the cloud and delivering secure access from anywhere.

SASE components

Secure access service edge (SASE) relies on a variety of network security technologies as SASE architecture components. This section explores these components:

Firewall-as-a-service

Firewall-as-a-service (FWaaS) is a firewall solution delivered as a cloud-based service that can scale and have new services provisioned to it to meet expanding and changing needs. Essentially, a FWaaS is a location-independent perimeter firewall for secure access. It provides next-generation firewall (NGFW) capabilities like web filtering, advanced threat protection, intrusion prevention system, and domain name system (DNS) security.

SWG

Secure web gateway (SWG) is a web gateway or proxy solution that forwards or proxies a user's web-based traffic to a web gateway or proxy server that applies web filtering, DNS security, antivirus, antimalware, antibotnet, SSL inspection, and data loss prevention functions to the traffic before sending it to the Internet.

ZTNA

Zero trust network access (ZTNA) is a solution that protects applications by allowing only trusted entities access to the application. Therefore, you can use ZTNA as an alternative to VPN for accessing protected resources on an organization's network.

For explanation of ZTNA concepts, see the ZTNA Concept Guide.

CASB

Cloud access security broker (CASB) is a software or hardware solution that is located between users and a cloud service to enforce security policies around cloud-based resources. You can consider CASB a subset of ZTNA.

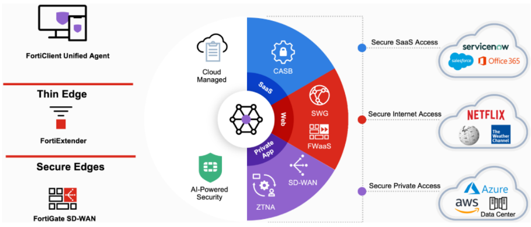
SD-WAN

Software defined wide-area network (SD-WAN) is a software-defined approach to managing WANs, providing link redundancy and load balancing, and using intelligence to route traffic based on defined performance and business priorities. You typically deploy SD-WAN at the branch or remote office level by using a router or NGFW device to optimize on-net users' access to the Internet. You can also implement SD-WAN from within the cloud-delivered service and offered as a service. This is analogous to private networks that WAN service providers provide using multiprotocol label switching, providing optimized connectivity to other cloud services or as-a-service applications.

For information on SD-WAN concepts, see the SD-WAN / SD-Branch Concept Guide.

Fortinet's SASE solution: FortiSASE

Fortinet’s secure access service edge (SASE) solution, FortiSASE, is a cloud-delivered security service that implements the SASE architecture that SASE architecture on page 7 describes. The following depicts the FortiSASE architecture:



SaaS: FWaaS, SWG, and FortiGuard threat intelligence

FortiSASE supports firewall-as-a-service (FWaaS) and secure web gateway (SWG) functionality, both of which rely on threat intelligence that FortiGuard labs provides. Powered by FortiOS, the FortiSASE FWaaS has all the same features, security, and reliability that customers depend on from Fortinet’s FortiGate next generation firewall physical and virtual appliances. Likewise, FortiSASE SWG relies on FortiOS explicit web proxy, captive portal, and authentication features to secure customers’ web traffic.

Common FortiSASE use cases

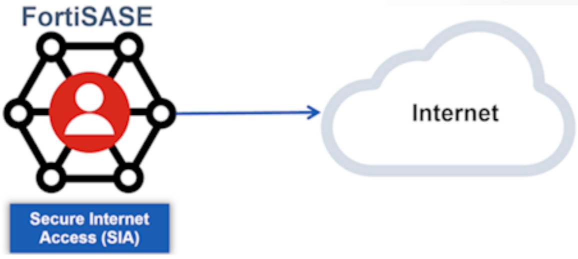
FortiSASE offers remote connectivity to its users. The following use cases describe the security that FortiSASE offers:

- SIA on page 11
- SPA on page 11
- SSA on page 12

SIA

Secure Internet access (SIA) extends an organization's security perimeter that a next generation firewall typically achieves to remote users by enforcing common security policy for the following:

- Intrusion Prevention Systems
- Application Control
- Web and DNS filtering
- Antimalware
- Sandboxing
- Antibotnet/Command and Control



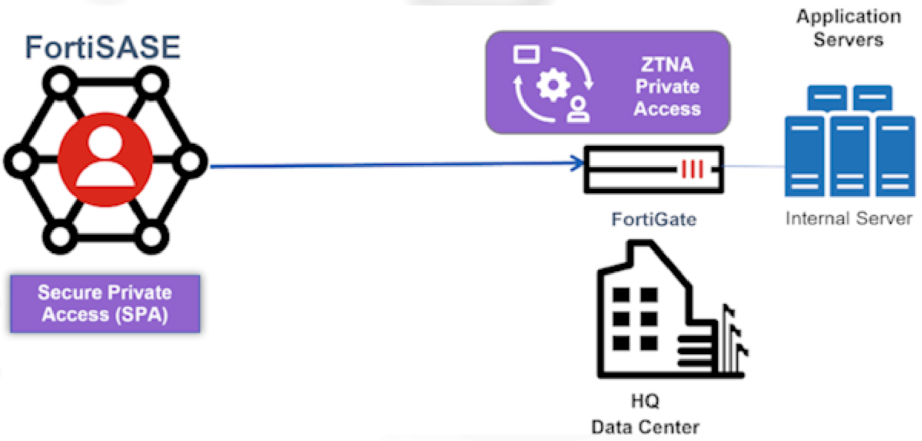
The most common SIA use cases for FortiSASE are:

Use case	Description
Agent-based remote user Internet access	Remote users on supported endpoint devices can use FortiClient software to establish secure connections via SSL VPN to the FortiSASE firewall as a service. Since this use case requires FortiClient software to be installed on the endpoint, it is described as agent-based, which is also known as endpoint mode.
Agentless remote user Internet access	Low-end devices, operational technology devices, or browser-only solutions such as Chromebooks use a proxy autoconfiguration file or proxy settings to securely proxy Internet traffic through FortiSASE secure web gateway (SWG). Since FortiSASE can achieve this connectivity without agent-based software, this use case is described as agentless, which is also known as SWG mode or explicit proxy.
Site-based remote user Internet access	Branch offices can use a thin-edge device such as FortiExtender or a secure edge device such as a FortiGate SD-WAN device to establish secure connections to the FortiSASE platform where these Fortinet devices act as FortiSASE LAN extension devices. Since all user devices and endpoints configured for Internet access through the FortiExtender or the FortiGate redirect its Internet traffic to FortiSASE, these use cases are described as site-based.

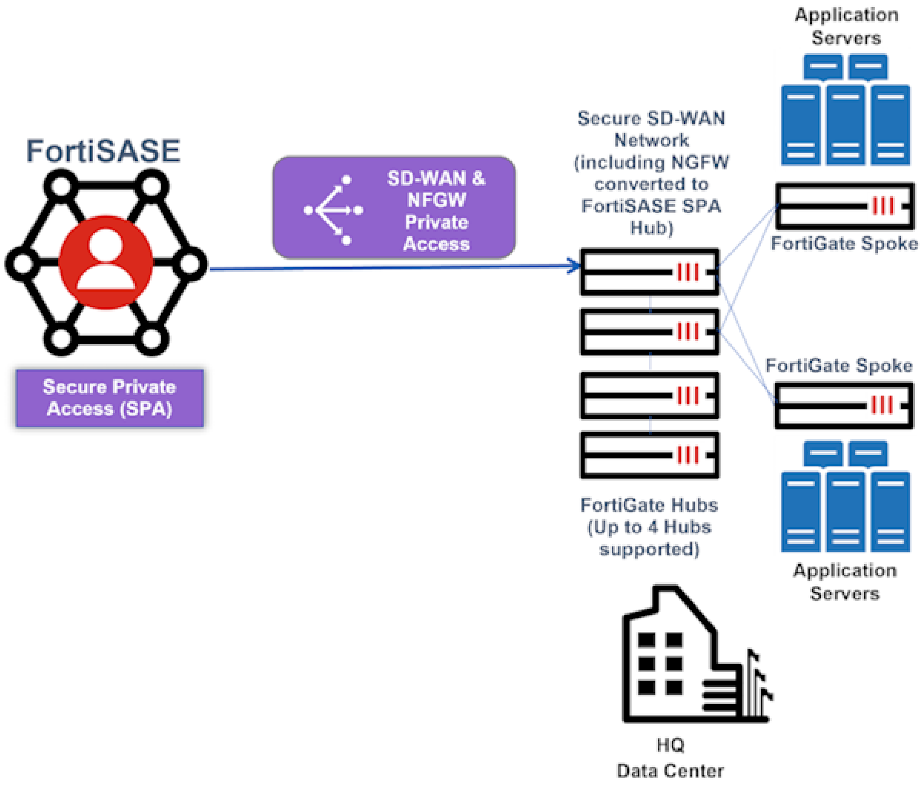
SPA

Secure private access (SPA) secures FortiSASE remote user access to private company-hosted applications that a FortiGate next-generation firewall (NGFW) protects.

SPA using zero trust network access (ZTNA) secures private TCP-based applications, namely, leveraging FortiSASE integration with the FortiGate ZTNA access proxy. This use case offers a direct (shortest) path to private resources and per-session user authentication thus offering greater performance and security.



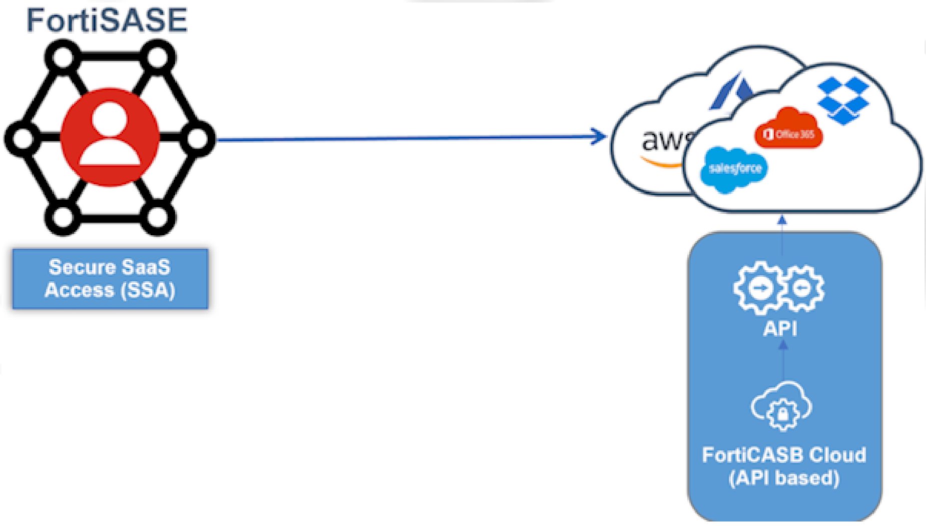
For securing private TCP-based and UDP-based applications, FortiSASE supports SPA using SD-WAN or SPA using an NGFW converted to a standalone FortiSASE SPA hub.


FortiSASE
Secure Private Access (SPA)
SD-WAN & NFGW Private Access
Secure SD-WAN Network (including NGFW converted to FortiSASE SPA Hub)
Application Servers
FortiGate Spoke
FortiGate Spoke
FortiGate Hubs (Up to 4 Hubs supported)
Application Servers
HQ Data Center

FortiSASE security points of presence and the organization's FortiGate hubs form a traditional hub-and-spoke topology that supports the Fortinet autodiscovery VPN (ADVPN) configuration. ADVPN is an IPsec technology that allows a traditional hub-and-spoke VPN's spokes to establish dynamic, on-demand, direct tunnels, known as shortcut tunnels, between each other to avoid routing through the topology's hub device.

SSA

Secure SaaS access (SSA) uses FortiCASB for advanced API-based deep inspection of cloud activity to provide monitoring, analysis, and reporting features that alert network administrators of any suspicious user activity, threats, or security policy violations. Network administrators can then act upon insights that FortiCASB determined to enhance FortiSASE security features and settings to block and mitigate such detected activity.


FortiSASE
Secure SaaS Access (SSA)
aws
Office 365
salesforce
API
FortiCASB Cloud (API based)

Conclusion

A secure access service edge (SASE) architecture's main goal is to secure off-net remote users and endpoints from anywhere while optimizing the remote user’s experience and still making it possible for remote users to access internal network resources securely and conveniently. Fortinet’s FortiSASE service, FortiClient software, and FortiGate next-generation firewall devices integrate seamlessly to provide solutions for securing Internet access and access to protected resources using firewall-as-a-service, secure web gateway, and zero trust network access functionality. FortiSASE covers common remote user use cases including secure Internet access, secure private access, and secure SaaS access.

Appendix: Documentation references

FortiSASE feature documentation

- FortiSASE Administration Guide

Fortinet resource centers

- Fortinet FortiSASE overview
- Fortinet Cyberglossary: SASE
- Fortinet Cyberglossary: SASE Architecture

FortiSASE 4-D documents

- FortiSASE Architecture Guide
- FortiSASE Secure Internet Access (SIA) Agent-based Deployment Guide
- FortiSASE Secure Private Access (SPA) using ZTNA Deployment Guide
- FortiSASE Secure Private Access (SPA) with a FortiGate SD-WAN Deployment Guide
- FortiGate NGFW to FortiSASE Secure Private Access (SPA) Hub Conversion Deployment Guide

FortiOS 4-D documents

- ZTNA Concept Guide
- SD-WAN / SD-Branch Concept Guide

www.fortinet.com

72-241-997800-20240212