DEFINE • DESIGN • DEPLOY

FortiSASE

Concept Guide

Version 23.1.17

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 01, 2023
FortiSASE 23.1.17 Concept Guide
72-23117-877767-20230301

TABLE OF CONTENTS

Change log

Date	Change Description
2023-03-01	Initial release.

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 using the FortiClient software agent or the web browser's proxy settings and to branch offices using thin edge devices such as FortiExtender. FortiSASE is a security solution that FortiOS powers, delivered as a cloud service, which remote users and branch offices access using global PoPs.

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-sized 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 terminologies, 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 these guides:

- FortiSASE Cloud Deployment Guide
- FortiSASE SWG with VPN Deployment Guide
- FortiSASE ZTNA Deployment Guide

SASE overview

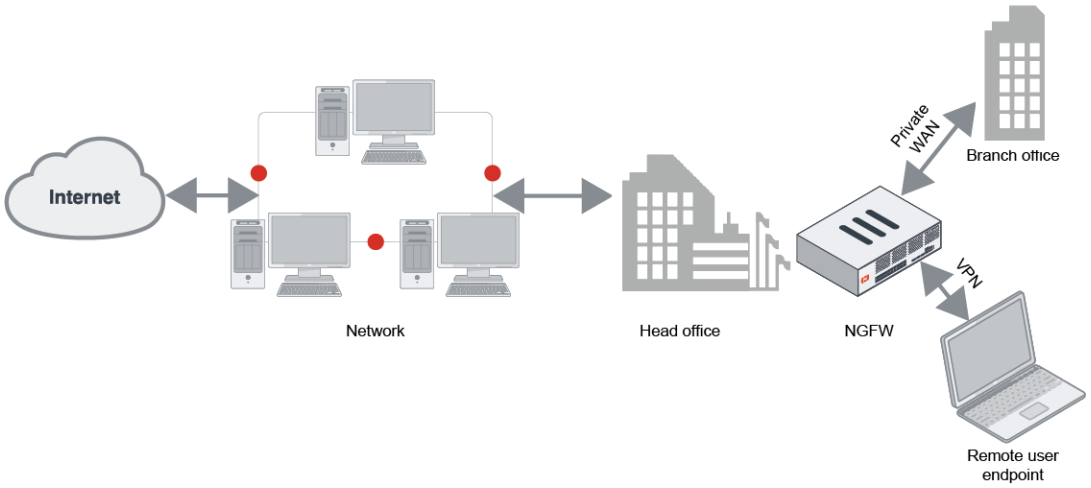
This chapter provides an overview of Secure Access Service Edge and covers the following topics using a top-down approach:

SASE concepts

This section describes the context and challenges behind the need for the Secure Access Service Edge architecture:

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, not managed by the organization's IT team and typically access the Internet directly via the local ISP, which bypasses all security policies and security features.

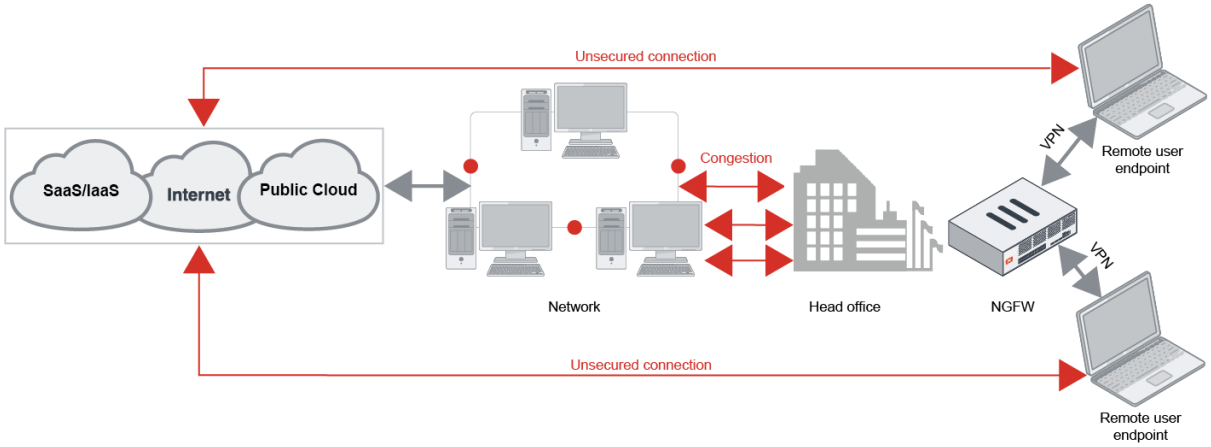
Challenges

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 (DIA) 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 diagrams 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 edge of the network, 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 that can 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.

Secure web gateway

Secure web gateway is a web gateway or proxy solution where a user's web-based traffic is forwarded or proxied to a web gateway or proxy server that applies web filtering, DNS security, antivirus, antimalware, antibbotnet, SSL inspection, and data loss prevention functions to the traffic before sending it to the Internet.

Zero trust network access

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

Cloud access security broker

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.

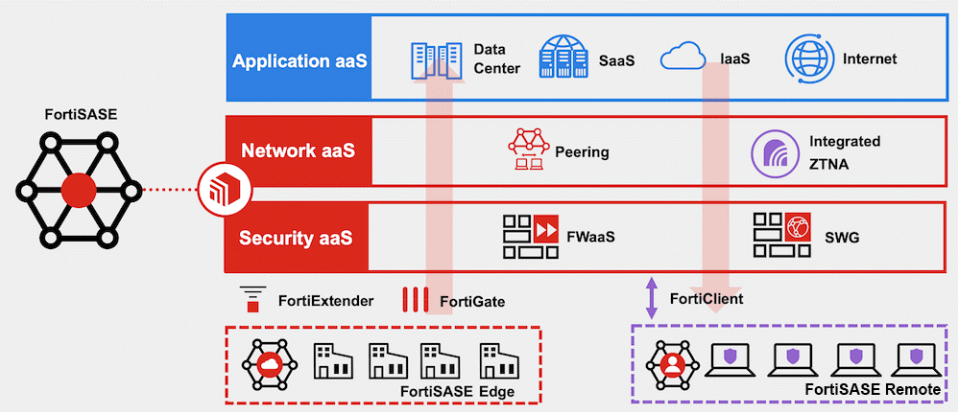
Software-defined wide-area network

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 more 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 9 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.

Accessing the FortiSASE platform

You can access the FortiSASE platform using FortiSASE Remote or FortiSASE Edge methods:

FortiSASE Remote

Remote users on endpoint devices use FortiClient software to establish secure connections via SSL VPN to the FortiSASE firewall-as-a-service via endpoint mode. For details on configuring FortiClient end users via endpoint mode, see the FortiSASE Cloud Deployment Guide.

Low-end devices, operational technology devices, or browser-only solutions use a proxy autoconfiguration file or proxy settings to connect to the FortiSASE secure web gateway (SWG) via SWG mode. SWG mode provides an agentless way to connect while still securely proxying traffic to the FortiSASE gateway.

For endpoints using FortiClient, FortiSASE can also leverage FortiClient features to perform endpoint management, vulnerability scanning and autopatching, and security posture determination for managed endpoints which can be used to implement a zero trust network access solution with existing FortiGate next generation firewall devices already being used to protect an organization's network.

FortiSASE Edge

Branch offices can use thin-edge devices such as FortiExtender to establish secure connections to the FortiSASE platform. All devices directly connected to the thin-edge device redirect their Internet traffic to FortiSASE.

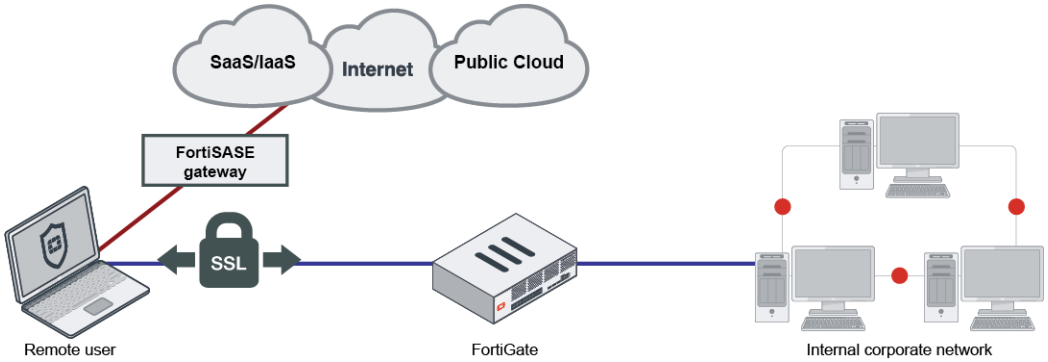
Remote access to FortiGate-protected networks

FortiSASE integrates with a FortiGate next generation firewall (NGFW) device that is already protecting an organization's network. This integration allows remote users to access these protected networks by deploying secure web gateway (SWG) with SSL VPN or FortiClient with FortiGate zero trust network access (ZTNA).

FortiSASE SWG mode with SSL VPN

For organizations that already use VPN for remote access and want to secure their remote clients from malware and malicious attacks, endpoints can use SWG mode to secure Internet access through the FortiSASE SWG while using VPN connections to an NGFW to remotely access protected networks.

For networks already using FortiGate NGFW devices, you can implement this solution by configuring proxy settings on the endpoint's system settings or web browser settings, and by using FortiClient software and SSL VPN configured on the FortiGate. The diagram depicts this architecture:

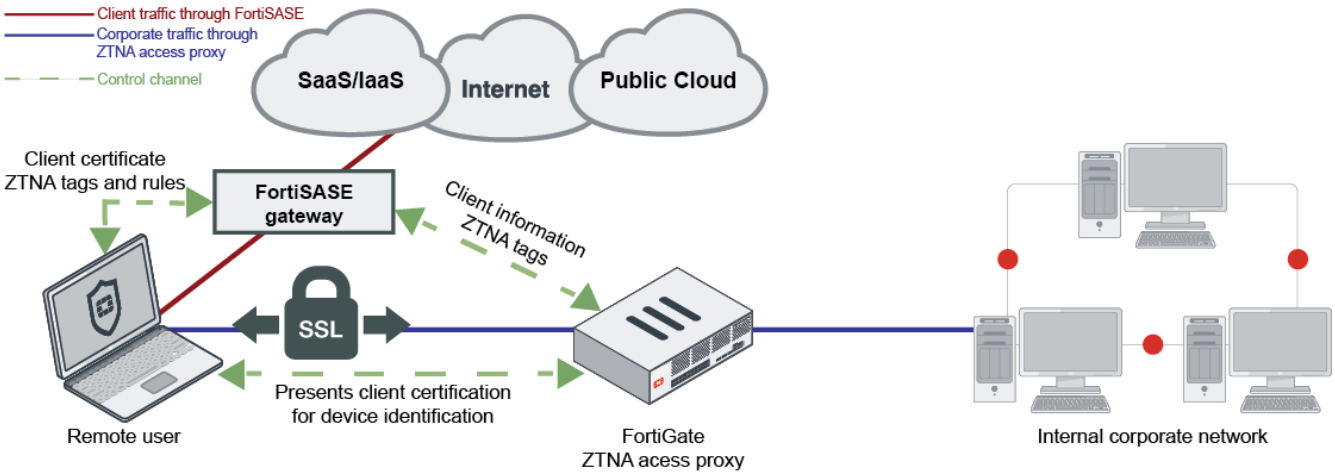


FortiSASE exempts traffic destined for corporate networks using the SSL VPN from being proxied by the FortiSASE SWG. FortiClient only tunnels traffic for the corporate network by using SSL VPN split tunneling. Therefore, with this solution, remote users establish distinct yet secure connections for all their traffic.

For complete deployment details, see the FortiSASE SWG with VPN Deployment Guide.

FortiSASE endpoint mode with FortiGate ZTNA

For organizations that are ready to deploy ZTNA for remote access and still want to protect their remote endpoints' Internet access, endpoints can use endpoint mode for secure Internet access through the FortiSASE firewall-as-a-service while relying on the integration between FortiSASE, FortiGate, and the FortiClient endpoint to securely access resources behind a FortiGate acting as a ZTNA access proxy. The diagram depicts this architecture:



Unlike traditional IPsec and SSL VPN, ZTNA offers direct connections to protected resources without requiring establishment of a persistent tunnel.

The key to ZTNA is verifying the connecting device's and user's identities and ensuring the device's security posture before admitting it to the protected network. These security checks happen instantly and transparently thanks to the integration between FortiSASE, FortiGate, and the FortiClient endpoint. If a device cannot pass these security checks, it is considered untrusted and the connection is rejected.

For complete deployment details, see the FortiSASE and ZTNA Deployment Guide.

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 for securing access to protected resources using firewall-as-a-service, secure web gateway, and zero trust network access functionality.

Appendix: Documentation references

FortiSASE 4-D documents

- FortiSASE SWG with VPN Deployment Guide
- FortiSASE and ZTNA Deployment Guide

Other FortiSASE documentation

- FortiSASE Administration Guide
- FortiSASE Cloud Deployment Guide

Fortinet resource centers

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

FortiOS 4-D documents

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

www.fortinet.com