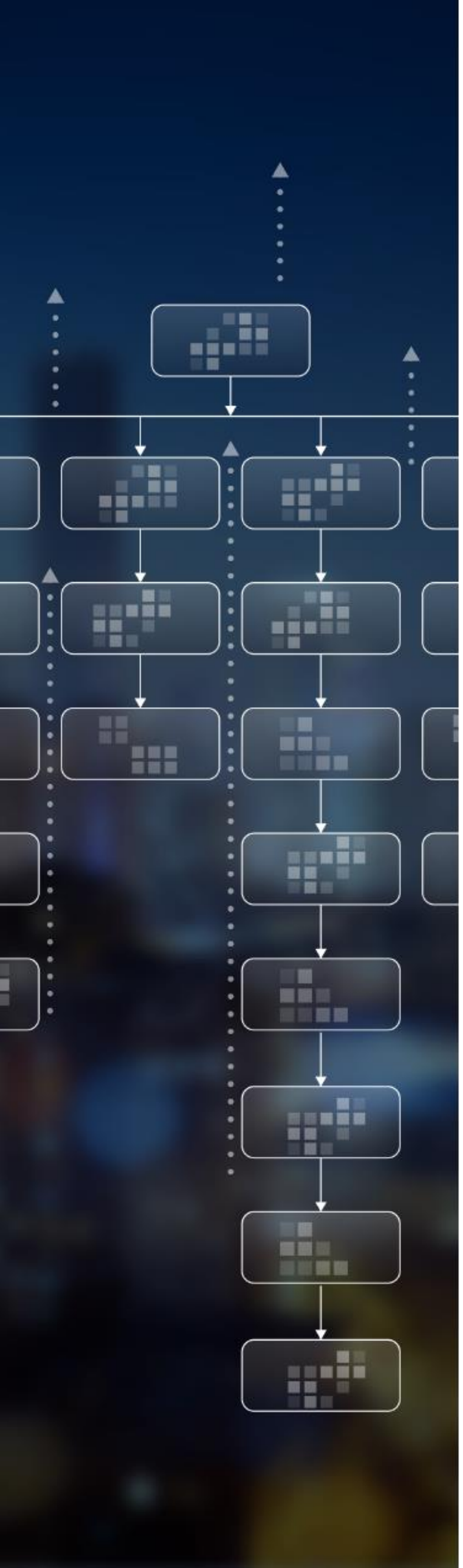


The complete secure access service edge (SASE) guide

July 2024

In this guide:

Secure access service edge, or SASE, is a cloud architecture model that combines network and security functions into a single cloud-based service. It aims to connect and secure users and devices across the data center, WAN, public and private clouds, remote locations, branch offices and IoT environments. This guide explores how SASE works, the benefits and challenges of SASE and tips to evaluate provider offerings. It also explores how SASE differs from other technologies, such as SD-WAN, SSE and zero trust.

In this guide:

The complete secure access service edge (SASE) guide

JENNIFER ENGLISH, EXECUTIVE EDITOR

Secure access service edge, or SASE, is a cloud architecture model that combines network and security functions into a single cloud-based service. It aims to connect and secure users and devices across the data center, WAN, public and private clouds, remote locations, branch offices and IoT environments.

With the rise of cloud workloads and remote work, enterprise networks must handle more external traffic that originates outside the corporate network. Instead of routing this traffic back to the data center, SASE directs traffic to a nearby point of presence (PoP), where it is subject to specified network and security policies.

This guide explores how SASE works, the benefits and challenges of SASE and tips to evaluate provider offerings. It also explores how SASE differs from other technologies, such as software-defined WAN (SD-WAN), security service edge (SSE) and zero trust.

In this guide:

WHAT IS SASE?

SASE is a cloud-native framework that integrates multiple networking and security functions to handle the demands of external traffic. It distributes these critical functions from the cloud, close to the user and applications, which helps alleviate the burden on the data center, improves scalability and speeds network response times.

The SASE model helps ensure secure access to corporate resources regardless of where the users and devices are located. It does this by using zero-trust security elements -- such as identity and access management, policy enforcement, data loss prevention (DLP) and automation -- and adheres to the principle of least privilege. It verifies and monitors every user and device using granular access controls and authentication.

SASE also integrates SD-WAN capabilities to enhance network performance and reliability. For example, it uses dynamic path selection to find the best path for traffic based on real-time conditions, sensitive data and business-critical requirements. It also relies on centralized management to distribute and enforce policies.

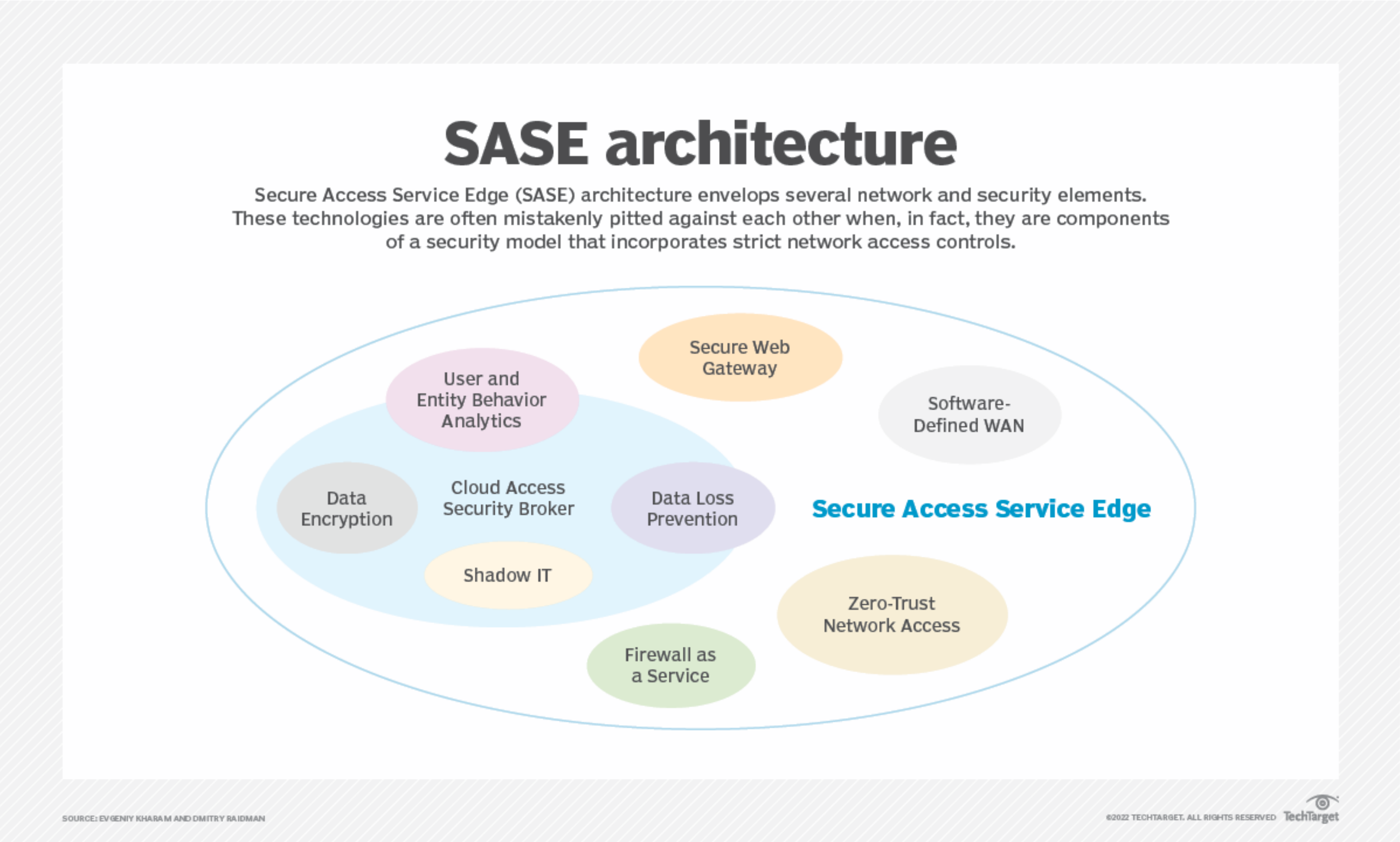
SASE ARCHITECTURE

SASE architecture incorporates both SD-WAN and zero-trust security. But the specific features included in SASE architecture vary depending on the vendor's technology stack.

Typically, SASE architecture includes a combination of the following network and security functions:

- Cloud access security brokers (CASBs).
- DLP.
- Firewall as a service (FWaaS).
- Intrusion detection and intrusion prevention.
- Malware protection.
- SD-WAN.
- Secure web gateway (SWG).
- Software as a service.
- VPNs.
- WAN optimization.
- Zero-trust network access (ZTNA).

In this guide:



SASE architecture

Secure Access Service Edge (SASE) architecture envelops several network and security elements. These technologies are often mistakenly pitted against each other when, in fact, they are components of a security model that incorporates strict network access controls.

Secure Web Gateway
User and Entity Behavior Analytics
Software-Defined WAN
Data Encryption
Cloud Access Security Broker
Data Loss Prevention
Secure Access Service Edge
Shadow IT
Zero-Trust Network Access
Firewall as a Service

SOURCE: EVGENIY KHARAM AND DMITRY RAIDMAN

©2022 TECHTARGET. ALL RIGHTS RESERVED TechTarget

Ideally, SASE architecture pulls together all network and security services into a single platform with centralized policy management, converging these different functions into one universal customer premises equipment (CPE) device. SASE relies on a global network of PoPs, similar to network as a service. These PoPs enable more scalable cloud-based services and help reduce latency. SASE vendors might have their own PoPs or partner with public cloud providers to use their PoP networks. When evaluating SASE offerings, enterprises should consider how many PoPs are available and how close they are to users, as the distance affects latency, performance and user experience.

Other factors to consider about SASE architecture include the following:

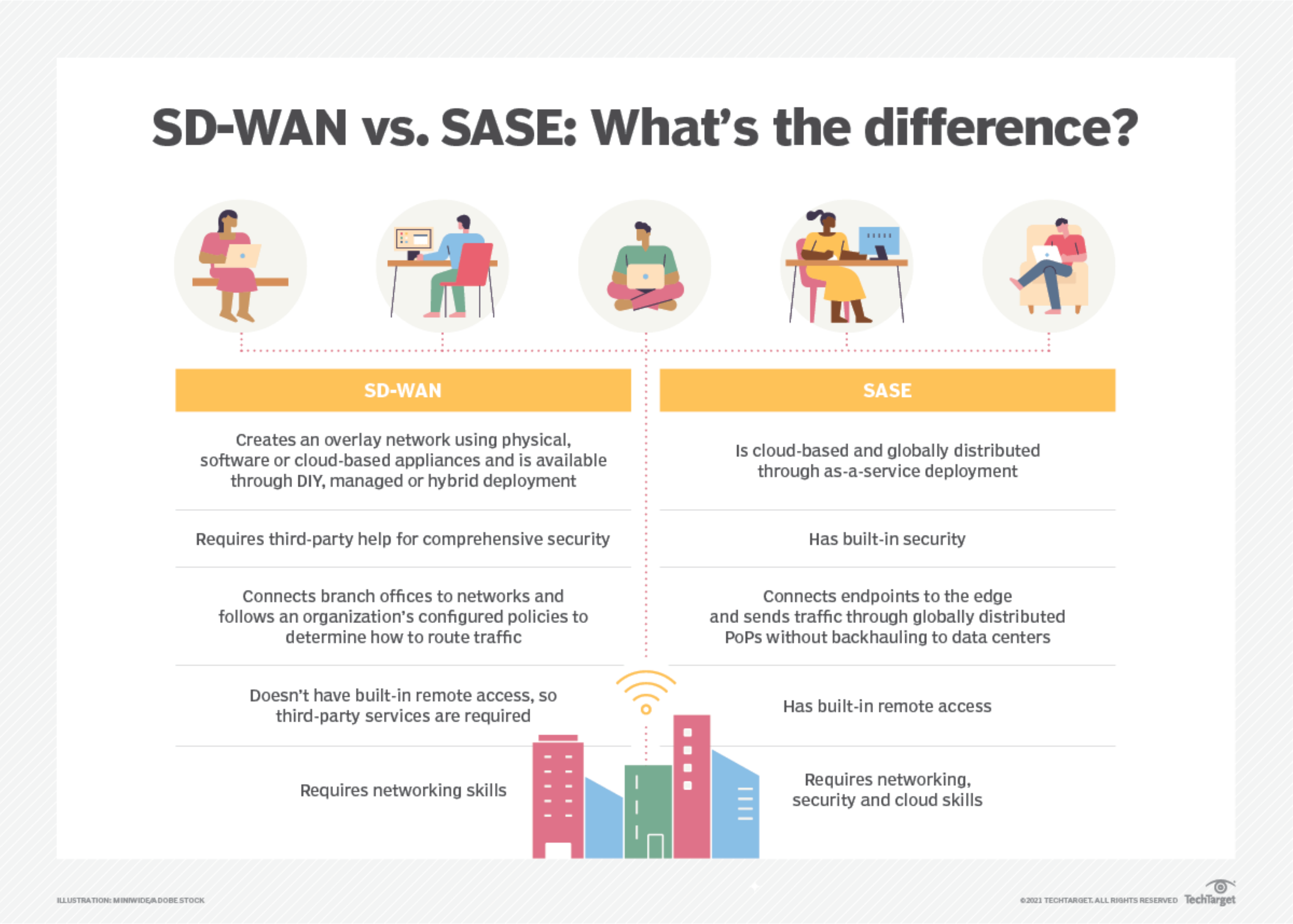
- How end-user devices connect to the SASE architecture, such as through IPsec tunnels or proxy chaining.
- How to onboard the SASE agents, which are the software components installed on user and network devices.
- Whether the vendor has dedicated hardware or allows customers to choose their own hardware.

SASE VS. SD-WAN

Although SASE and SD-WAN are related, they have different objectives. SASE focuses on providing secure access to endpoints and end-user devices from any location. Meanwhile, SD-WAN's primary goal is to connect and optimize WAN and branch connections.

SASE is deployed using a cloud-based platform with PoPs, while SD-WAN can be deployed on premises or in the cloud and creates an overlay network. Security is another differentiator between the two technologies, as SASE includes a full portfolio of security functions in the architecture, while SD-WAN has only basic network security features.

In this guide:



SD-WAN vs. SASE: What's the difference?

SD-WAN	SASE
Creates an overlay network using physical, software or cloud-based appliances and is available through DIY, managed or hybrid deployment	Is cloud-based and globally distributed through as-a-service deployment
Requires third-party help for comprehensive security	Has built-in security
Connects branch offices to networks and follows an organization's configured policies to determine how to route traffic	Connects endpoints to the edge and sends traffic through globally distributed PoPs without backhauling to data centers
Doesn't have built-in remote access, so third-party services are required	Has built-in remote access
Requires networking skills	Requires networking, security and cloud skills

ILLUSTRATION: MINIWIDE/ADOBE STOCK

SASE and SD-WAN differ in the following key areas:

- Deployment and architecture.
- Security integration.
- Traffic handling and connectivity.
- Remote access.
- Required expertise for deployment and management.

Despite the differences between SASE and SD-WAN, most SASE offerings include SD-WAN capabilities as part of their core capabilities.

SASE VS. SSE

Security service edge is another framework closely related to SASE. While SASE includes both networking and security functions, SSE focuses primarily on security. Essentially, it's SASE without the WAN components. The core elements of SSE include CASB, FWaaS, SWG and ZTNA.

Many enterprises start with SSE deployment first, aiming to minimize their attack surface to mitigate potential vulnerabilities, bolster their security posture management and enhance overall threat protection. Depending on business requirements, an organization might use SSE as a bridge to SASE deployment.

WHAT ARE THE BENEFITS OF SASE?

One of SASE's greatest benefits over on-premises security is its support of cloud-based enterprise security. A cloud model enables organizations to cost-effectively apply the latest network and security features without disrupting application performance or the end-user experience. For IT teams, it also helps reduce the burden of conducting intense refresh cycles.

With SASE, organizations can scale their networking and security capabilities to properly protect enterprise users and sensitive data. Network and security teams can create security policies based on specific roles and manage those policies centrally. Additionally, the convergence of networking and security functions, especially in a single-vendor SASE offering, helps simplify deployment and maintenance.

The following are five key benefits of SASE:

- Applications can live anywhere.
- Centralized, dynamic and role-based policies help streamline operations.
- Integrated security and routing.
- Reduced WAN costs.
- More resilient distributed architecture.

WHAT ARE THE CHALLENGES OF SASE?

SASE presents some issues for organizations entrenched in their IT team structure. For instance, enterprises might find it difficult to move out of network and security team silos and manage competing interests and change controls.

A switch to SASE might require a change in IT culture to facilitate integrated networking and security teams. IT should also ensure the SASE platform supports integrated universal CPE devices and role-based access control because most larger firms have distinct architecture, engineering, implementation and operations teams.

SASE can seem complex because it takes what were once individual services and moves them into a framework, yet it isn't a single product. IT teams can partner with their providers to determine which architectural components they require and deploy them in a simpler manner.

SINGLE-VENDOR SASE VS. MULTIVENDOR SASE

The SASE market is largely divided into two categories: single-vendor SASE and multivendor SASE. A single-vendor SASE offering includes all elements of the SASE architecture from one provider. A multivendor SASE model stitches together network and security functions from an array of providers.

Multivendor SASE provides flexibility, but it introduces complexity. Single-vendor SASE streamlines the number of devices, contracts and analytics tools enterprises need to manage.

Many customers initially gravitate toward multivendor SASE because they have incumbent providers or want comprehensive functionality. The simplicity and integration of single-vendor SASE make it a compelling option, however.

Many SASE providers shifted from a networking- or security-focused portfolio to add the functionality they lacked.

SASE USE CASES

Cloud applications, IoT sensor traffic and an expanded remote workforce have helped drive SASE adoption. For example, SASE helps connect and secure connectivity to cloud and SaaS resources. It can also monitor IoT devices and ensure edge devices adhere to specified policies.

SASE can help with the following use cases:

- Consistent security across all users and devices.
- Improved network performance.
- Improved management for cloud-heavy environments.

- Optimized and accelerated application performance.
- Enforced data security and protection policies.

As SASE continues to gain momentum, organizations should assess the value of this cloud-based network security architecture for their own business requirements.

Editor's note: *This article was originally written by Sandra Gittlen and updated by Jennifer English to reflect industry changes and improve the reader experience.*

Jennifer English is executive editor for TechTarget's Networking and Cloud sites.

Sandra Gittlen is former editor at large for TechTarget's Networking and Security Media Group.

CONTINUE READING

- **SASE vs. SD-WAN: What's the difference?**
- **Why it's SASE and zero trust, not SASE vs. zero trust**
- **Top SASE use cases balance network connectivity, security**