cloudpro™

CLOUDFLARE | PARTNER NETWORK

6 Considerations for Your SASE Setup

Today, enterprises need flexibility at every layer of the network and application stack. Users need secure, authenticated access no matter where they are: at the office, on a mobile device, or working from home.

SASE, or secure access service edge, is a cloud-based security model that simplifies network security by combining software-defined wide area networking (SD-WAN) with core network security services and delivering both from the cloud edge.

For enterprises that have invested serious time and resources in elaborate on-premise setups, manage complex webs of cloud-based security services, or are still adjusting to the future of remote work, SASE adoption may seem intimidating — but it doesn't have to be.

What does a SASE strategy involve?

Building and managing networks

SD-WAN enables organizations to establish private corporate networks without the assistance of hardware routers or multiprotocol label switching (MPLS) circuits.

Connecting users to applications

SASE protects against external and internal threats with a zero trust security model, in which user identity and access is granted based on a combination of factors.

Filtering traffic

A secure web gateway (SWG) prevents cyber threats and data breaches by filtering unwanted content from web traffic, blocking unauthorized user behavior, and enforcing company security policies.

Protecting applications and infrastructure

Cloud-based firewalls protect cloud infrastructure and applications from cyber attacks through a set of security features that includes URL filtering, intrusion prevention, and uniform policy management.

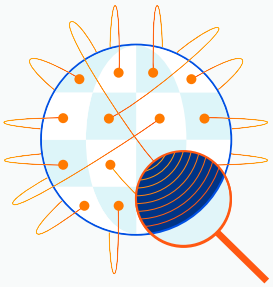
Securing data

A cloud access security broker, or CASB, secures confidential data through access control and data loss prevention, reveals shadow IT, and ensures compliance with data privacy regulations.

Here are six steps that will guide you through the first stage of your SASE journey:

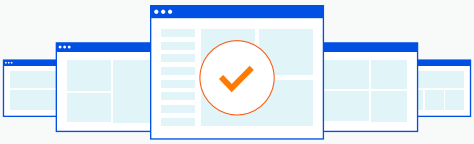
1. Evaluate your network traffic.

Before you implement any SASE solution, conduct a full assessment of where your users work, what applications they access, and which network and security resources they interface with most frequently. Then, you can start to determine the level of privilege and access that should be applied to your workforce on a role-by-role basis.



2. Assess your total application landscape.

Once you know where your users are and what degree of network access they require, it's time to decide which applications to bring into a SASE framework first. Evaluate these on the axes of total data sensitivity and breadth of employee impact. Consider prioritizing access control for applications with broader adoption and usage, as well as more stringent security requirements.



3. Prioritize your remote workers.

A network is only as strong as its weakest endpoint — in this case, employees who access your network from remote locations and unsecured devices. Equip your remote workforce with cloud-based firewalls and zero trust access control so they can safely access your network from any location and device.

4. Reimagine your branch offices.

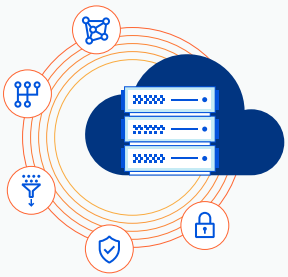
After you secure your remote workforce with a SASE framework, find ways to strengthen the security of your smaller branch offices. This may be as simple as replicating the model used for remote workers and allowing local offices to function as an Internet café. By routing network traffic to a SASE solution, you can ensure firewalls and logging remain consistent for all employee devices connecting to the Internet.

5. Extend SASE to high-density locations.

Unlike smaller branch offices, high-density offices will likely have SD-WAN solutions, cloud firewalls, and other network protections in place. However, this is still the most complicated phase of SASE adoption, since legacy on-premise security tools will need to be carefully migrated to the cloud, while the volume and diversity of employee access requirements must be thoughtfully considered and managed.

6. Identify areas for improvement.

Although many cloud providers are on their way to offering the five core components of a true SASE solution, some may have gaps in their product suites. Evaluate vendors on the breadth of their current SASE offering, while keeping an eye out for any critical additions and security integrations that may be included in the future.



No matter where applications are hosted, or employees reside, enterprise connectivity needs to be secure and fast. Cloudflare is uniquely architected to deliver integrated network and security services across 200+ locations worldwide, so enterprises don't need to run traffic through a centralized data center or manage multiple point solutions in the cloud.

Cloudflare One™ is a comprehensive network-as-a-service (NaaS) solution that simplifies and secures corporate networking for teams of all sizes. It enables your corporate network to match the state of your enterprise: global, distributed, and consistently connected.

To learn more about Cloudflare One, contact us today.