LEARNING MADE EASY

Secure Access Service Edge (SASE) Checklist

The enterprise network has seen a huge transformation over the past decade. As a result, security products are evolving, too. The market is moving from single-purpose point products to multi-function security solutions tightly integrated in a cloud service offering. The goal is simple: to deploy security services how and where you choose, with the capability to control and secure direct-to-Internet access, cloud applications, and protection for central, remote, and roaming users alike, without the need for additional hardware.

Use this checklist to help you select the right secure access service edge (SASE) solution for your organization.

What Is SASE?

In 2019, Gartner published a report called *The Future of Network Security is in the Cloud*. In this report, Gartner introduced the SASE (pronounced "sassy") concept which it defines as "an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS and ZTNA) to support the dynamic secure access needs of digital enterprises."

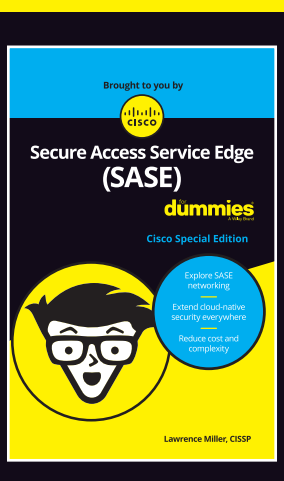
Key SASE Components

Key networking and security components to look for in a SASE solution include:

- ☐ **Software-defined wide area network (SD-WAN)** is a virtual wide area network (WAN) that allows companies to use any combination of transport services – including multiprotocol label switching (MPLS), cellular Long-Term Evolution (LTE) and 5G, and broadband – to securely connect users to network locations. It can select the most efficient communication method while reducing costs and simplifying management.
- ☐ **Zero Trust network access (ZTNA)** is based on the Forrester Zero Trust security framework which takes a "never trust, always verify" approach to security. ZTNA verifies user identities and establishes device trust before granting access to authorized applications, helping organizations prevent unauthorized access, contain breaches, and limit an attacker's lateral movement on your network.
- ☐ **Domain Name System (DNS) layer security** is the first line of defense against threats and a great way to stop attacks before users connect to risky destinations.
- ☐ **Firewall as a Service (FWaaS)** provides consistent policy enforcement across all locations and users through a single, centralized cloud-delivered firewall.
- ☐ **Secure web gateway (SWG)** is a web-based proxy that provides security functions such as malware detection, file sandboxing and dynamic threat intelligence, Secure Sockets Layer (SSL) decryption, app and content filtering, and data loss prevention (DLP).
- ☐ **Cloud access security broker (CASB)** works by ensuring that network traffic between end-user devices and the cloud provider, primarily software-as-a-service (SaaS) solutions, complies with the organization's security policies. CASB uses auto-discovery to identify cloud applications in use and identify high-risk applications, high-risk users, and other key risk factors.

TIP

There are a lot of networking and security components in this checklist. That's why a SASE solution can make everything easier for your organization – it eliminates the cost and complexity of multiple standalone point solutions at all your locations and consolidates these networking and security capabilities in a cloud-delivered, fully integrated solution.



Discover how to:

- **Address networking and security challenges**
- **Extend cloud-native security anywhere**
- **Reduce cost and complexity**

Ready to get started? Download your free copy of *Secure Access Service Edge (SASE) For Dummies, Cisco Special Edition*.

READ THE EBOOK

cisco

for dummies® A Wiley Brand

Wiley part no.: 978-1-119-68243-1