Secure Access Service Edge

The ultimate networking architecture

timus

ZERO TRUST NETWORK PROTECTION

Introduction

In the new way of working, workforces are increasingly becoming distributed, and most business applications reside in the cloud. Increased globalization has compelled businesses to open branches on distant continents. The coronavirus pandemic has also forced forward-looking companies to embrace remote working policies. These changes demand technologies that can facilitate data access from anywhere and at any time using any device.

Traditional networking architectures are not designed to meet these needs. The need for an advanced network architecture has risen due to the inefficiencies of traditional networking architectures to handle complexities introduced by cloud services and distributed workforces. The advent of SASE promises to address these needs by providing a network architecture that is secure and tailored for cloud services.

© Timus Networks, Inc. 2025. All Rights Reserved.

Contents

What is SASE? 3
Need for Better Remote Access

Need for Better Remote Access 3

Purpose of SASE 4

Main Components of SASE 5
Zero Trust Network Access (ZTNA)
Software-defined WAN (SD-WAN)
Firewall as a Service
Secure Web Gateway
Threat Protection

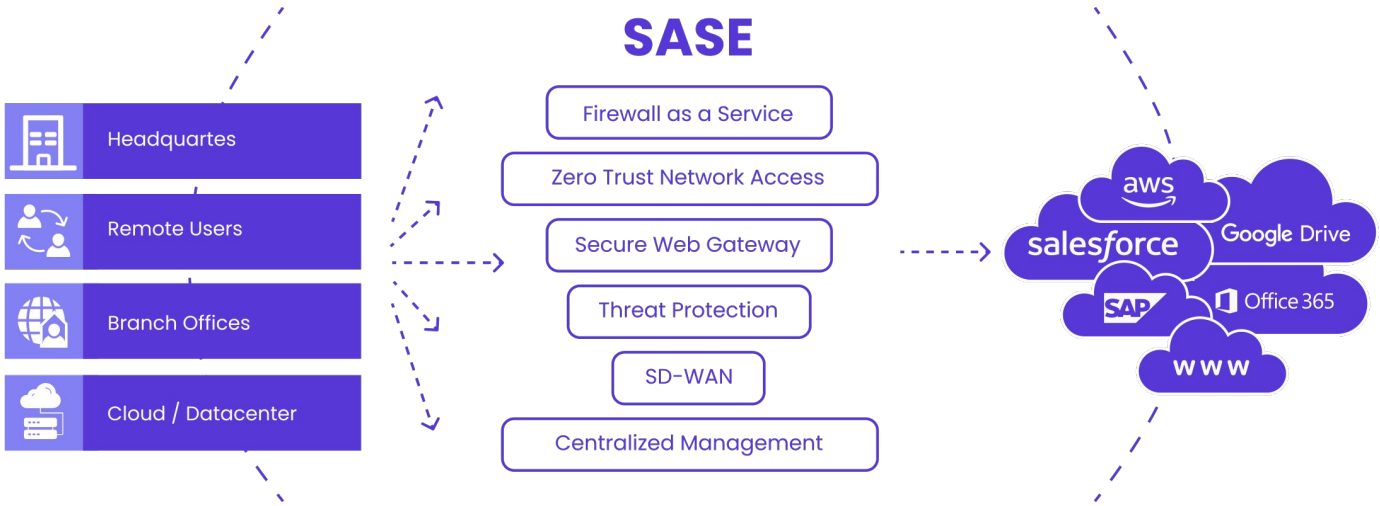
Use Cases 6
Companies With Remote Workers
50+ Branch Company

Conclusion 7

© Timus Networks, Inc. 2025. All Rights Reserved.

What is SASE?

Secure Access Service Edge (SASE) is a cloud-based architecture that combines networking and security. This model is designed to handle the secure Access needs of modern organizations. The main components of SASE are Zero Trust Network Access (ZTNA), Firewall as a Service, Secure Web Gateway, Threat Protection and Software-Defined WAN (SD-WAN). In other terms, SASE is a federation of technologies that address the challenges of digital business transformation and distributed workforces.



Need for Better Remote Access

Poor network performance is one of the greatest challenges companies with remote offices or work sites are forced to endure. Most of these companies are forced to leverage VPNs to enable offsite workers to connect to the company's networks. Remote workers connecting to the network via VPNs are often treated to chokepoints created by traffic backhauls, causing latency issues and saturation of internet connection. Implementing redundancy on traditional networks can also be quite expensive. Consequently, most companies use a single connectivity line for remote workers.

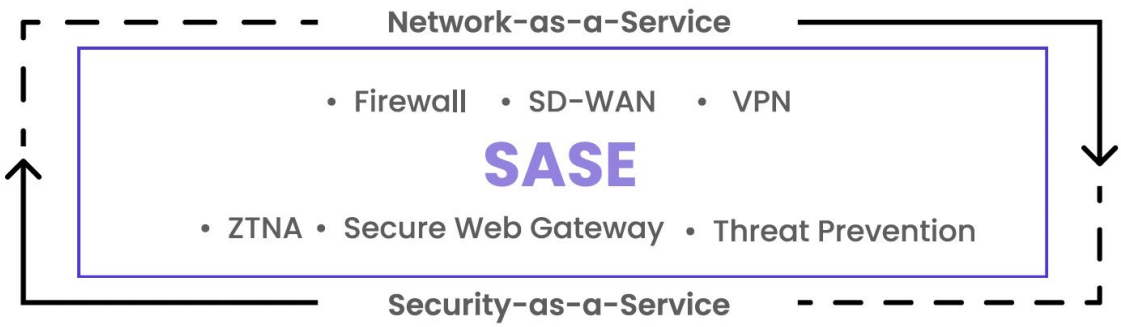
When these lines are broken, all remote workers are unable to work. Managing user-owned devices can also be a significant challenge. To onboard new workers, the IT teams must send VPN configurations to new employees. The process is excruciating. The use of VPNs also creates security concerns. Implementing access control for workers connecting to the network via VPNs is challenging. SASE addresses these challenges by allowing remote users to connect to company resources conveniently and safely.

© Timus Networks, Inc. 2025. All Rights Reserved.

Purpose of SASE

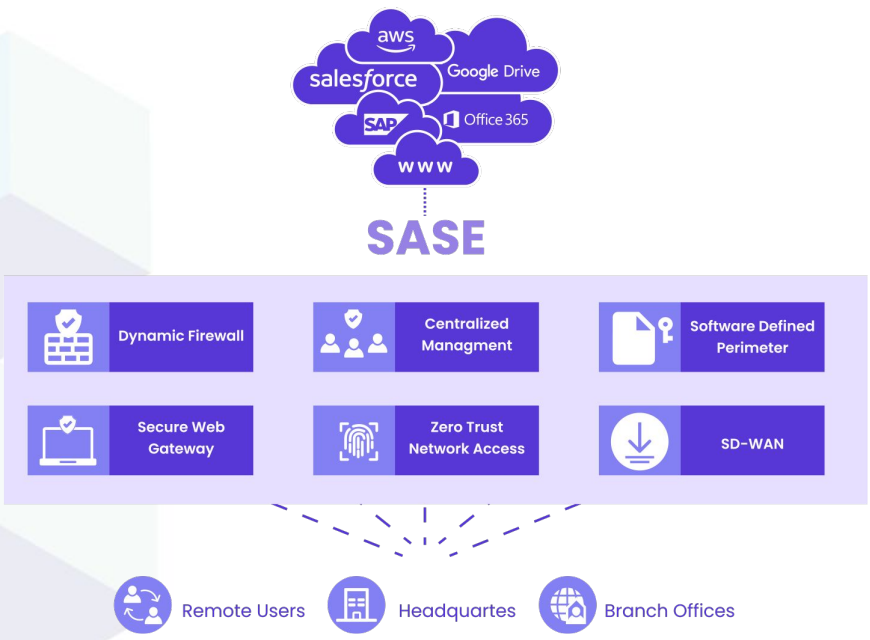
The three core purposes of SASE are driving productivity, facilitating network security, and reducing the cost of internet connectivity.

For businesses using SaaS applications, rerouting SaaS traffic back to a data center HQ creates congestion which adversely impacts user experience and reduces productivity. SASE augments performance by providing a fast, reliable, and secure connection to cloud-based applications and data.



SASE leverages multiple approaches to guarantee network security. One of these methods is zero-trust network access. Zero trust network access (ZTNA) is an advanced identity check and access control mechanism that continuously verifies the identity of users. Users can only access resources they are entitled to. This paradigm is vital for limiting the extent of breach in case of an attack. Secure web gateway and threat protection are the other security building blocks of a SASE network.

Channeling internet traffic back to the data centers via MPLS circuits is expensive. Changing transport from traditional MPLS to SASE SD-WAN is a majör driver for cost efficiencies. SD-WAN may reduce the cost of internet connectivity by more than 65 percent.



© Timus Networks, Inc. 2025. All Rights Reserved.

Main Components of SASE

SASE is composed of various technologies that serve different functions to support all facets of modern networks. Some of the key technologies that constitute SASE include Zero Trust Network Access (ZTNA), Firewall-as-a-Service (FWaaS), Secure Web Gateway (SWG), Threat Protection and Software-Defined WAN (SD-WAN).



Zero Trust Network Access (ZTNA)

ZTNA is a set of technologies that work together based on the premise that everything accessing the network is untrustworthy. The primary function of ZTNA is to verify users and grant access only to accepted resources.



Software-Defined WAN (SD-WAN)

SD-WAN facilitates the optimal performance of wide-area networks cost effectively. Some of the fundamental functions of SD-WAN include secure branch connectivity, latency optimization, and bandwidth aggregation.



Threat Prevention

With the Threat Protection System, outside and inside cyberattacks on the business network are instantly detected and prevented.



Secure Web Gateway (SWG)

SWG is designed to protect work-from anywhere users from internet-sourced threats. The technology detects and blocks threats such as malware and unwanted software. Some of the standard functions of SWG are enforcement of internet security and compliance policies, application identification and control, and filtering malicious internet traffic.



Firewall as a Service

Firewall as a Service (FWaaS) is a cloud based firewall service that enables businesses to overcome the security and scalability challenges of on-premises UTM and firewall systems.

© Timus Networks, Inc. 2025. All Rights Reserved.



Use Cases

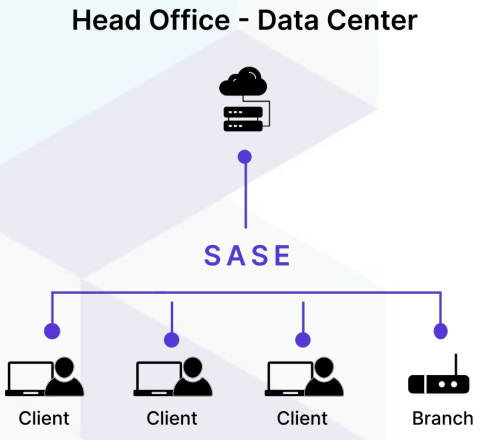
Secure Access Service Edge (SASE) is taking the IT world by storm. Though some experts attribute this rapid adoption to the Covid-19 pandemic, the reality remains that the use of SASE technology is increasing in the IT sector because of its many use cases in the modern world. Some of the notable use cases for SASE are:

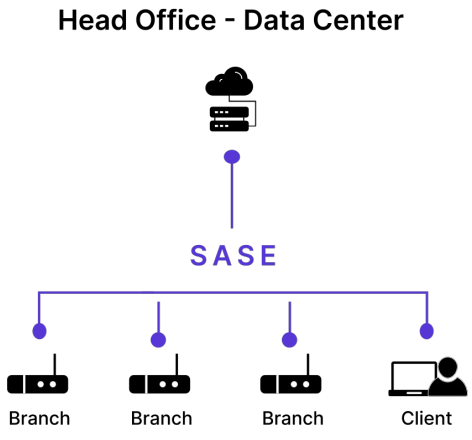
Companies With Remote Workers

One of the leading reasons SASE became popular is the surge in remote workers. IT departments realized that traditional VPN systems could not keep up with the demands of remote workers and the company's security needs. This compelled them to adopt SASE and ZTNA technologies. The ability to serve remote workers in scale makes SASE one of the best technologies for companies that have remote workers.

50+ Branch Company

Before the inauguration of SASE technologies, some companies were using SD-WAN solutions. Though these technologies were beneficial in various ways, they presented IT teams with new challenges. For example, IT teams were obligated to provide services such as firewalls, intrusion prevention, and URL filtering at every branch office. This made running the technology labor intensive and risked bottlenecks in network performance. SASE technology alleviates all these challenges. The technology allows branch offices to connect to the nearest cloud gateways. It also enables security teams to deploy policies from a central management application in the cloud.





© Timus Networks, Inc. 2025. All Rights Reserved.

Conclusion

SASE is a revolutionary network architecture. However, its implementation should not start with architectural requirements. Instead, it is prudent for companies wishing to adopt the technology to start assessing use cases that make the most sense for their businesses. Timus is one of the leading brands providing SASE solutions. Contact us today, and let's transform your business network.

timus

timusnetworks.com

About Timus

Timus Networks simplifies network security and access for SMBs and mid-market enterprises helping to significantly reduce business risks and bolster compliance. Our premier product, Timus SASE, transforms complex setups involving multiple tools into a single, unified solution that secures networks and safeguards users, regardless of their location or device.

Developed by firewall experts with decades of cybersecurity experience, Timus SASE is purpose-built for the MSP/MSSP Channel. It offers simplicity and rapid deployment, with installation in under 30 minutes.