SECURE ACCESS SERVICE EDGE

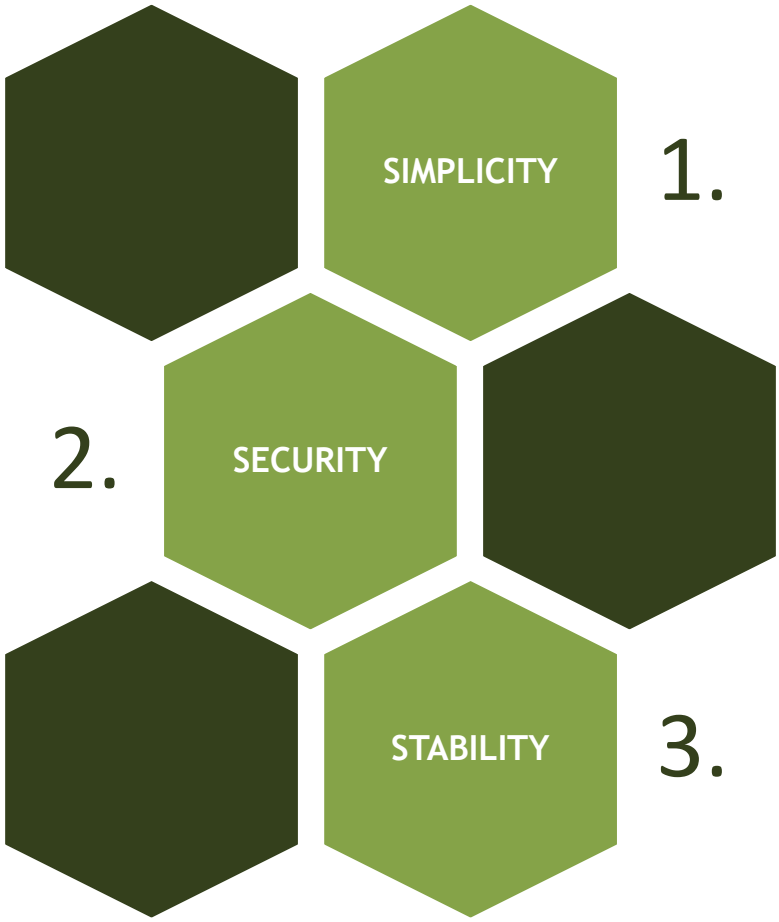
SASE WHITE PAPER 2021

WHAT IS SECURE ACCESS SERVICE EDGE?

Gartner first described secure access service edge, or SASE (pronounced "sassy"), in their August 2019 research The Future of Network Security in the Cloud and expanded on it in their 2021 Strategic Roadmap for SASE Convergence.

Before getting into the details of SASE, it's vital to have a basic understanding of the term. Traditional network methods and technology just can’t provide the kinds of identity and security management those digital businesses require. These companies expect that their users have quick, direct ties, no matter where they are. With more distant customers and applications, content flowing from the data center to operating systems, and much more data travelling to public cloud and service centers than returning to the data center, a new network security approach is necessary.

SASE is a cloud-delivered service model that combines wide area networking (WAN) and network security services such as CASB, FWaaS, and Zero Trust. “SASE functionalities are given as a service based on the entity's identification, relevant context, corporate security/compliance regulations, and continuous risk/trust assessment during the sessions,” according to Gartner. People, classes of people (branch offices), equipment, apps, services, IoT systems, and edge computing locations can all be associated with entity identities.”



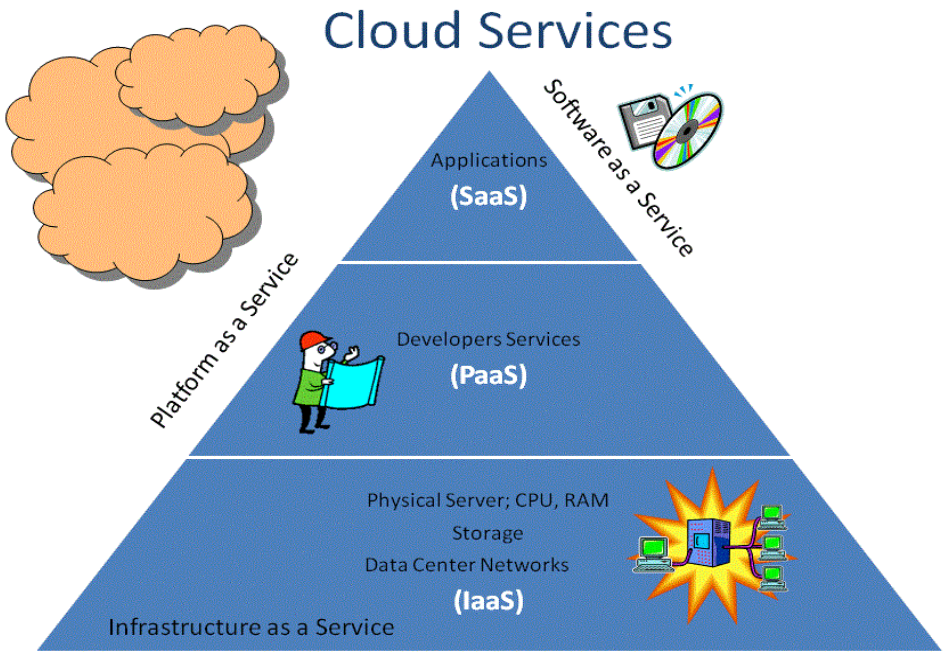
HOW IT WORKS?

As the number of remote employees grows, so does the dependency on SaaS services, resulting in new and bigger vulnerabilities. Simply put, protecting consumers at the edge is more difficult — maintaining seamless connections that increase productivity without causing performance concerns that reduce user pleasure.

The secure access service edge (SASE) is an architectural solution to data center-based security that offers an alternative. To ease cloud deployment and maintenance, SASE combines networking capabilities with cloud-native security features.

SASE combines network traffic and protection prioritization, pervasive risk and data security, and ultra-fast, explicit network-to-cloud communication. Whilst SASE was once a trade-off between performance and control, new

technology now allows organizations to have both. SASE is a concept that enables enterprise security experts to use identification and context to determine the exact amount of performance, dependability, security, and cost for each network session. Organizations that use the SASE framework can achieve higher scale and scope in the cloud while tackling the additional security issues that come with it.

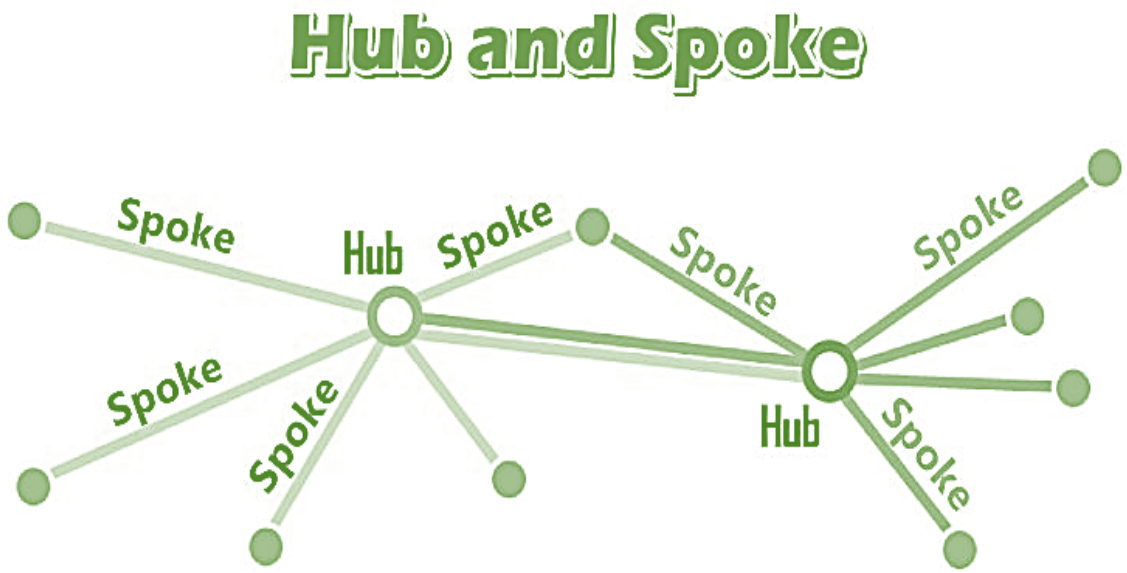


THE HUB AND SPOKE AND ITS PROBLEMS

The hub-and-spoke model is straightforward in theory. The paradigm, on the other hand, is incapable of dealing with the intricacies of cloud-based solutions such as software-as-a-service (SaaS) and growing remote employees. Organizations should re-evaluate where and how internet traffic is examined, as well as how protected user access restrictions are handled, as more workstations, applications, and sensitive customer data migrate to the cloud.

When multiple software and services are stored on the cloud, reconfiguring all traffic throughout a single data center isn't feasible. Remote users may experience latency when connecting to a business network using a VPN, which adds to the problem. It's not uncommon for disgruntled employees to exploit an

unprotected connection to access business resources, subjecting oneself to extra security concerns.

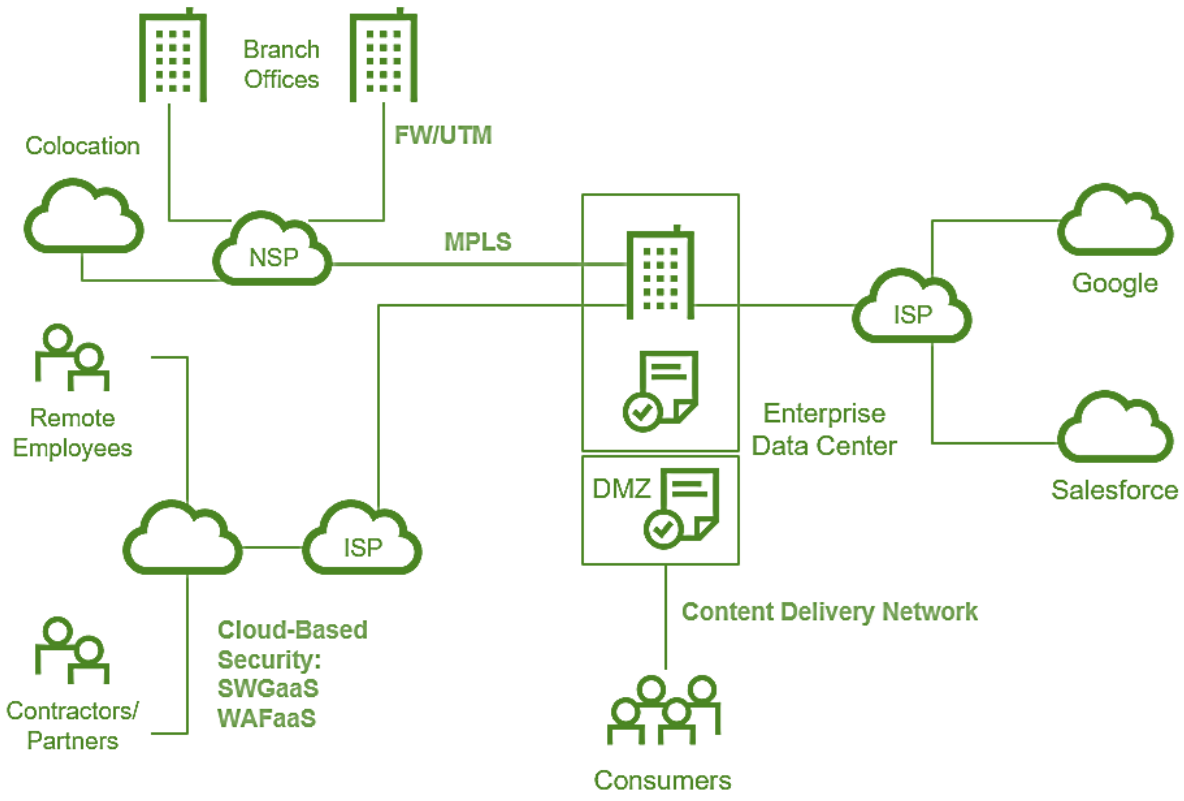


SASE TO SAVE THE DAY

SASE, for example, moves network controls from the corporate data center to the cloud edge, putting them closer to the service being used. SASE eliminates layered cloud services that require distinct implementation and management, allowing network and security services to be combined to provide a safe, cohesive network edge.

The implementation of identity-based, zero-trust access restrictions mostly on edge network is one of SASE's core characteristics. Enterprises can use it to grant users limited access to only the programs and data they need to perform their jobs, without requiring them to connect to a network through VPN. Network security regulations are more granularly controlled, and legacy hardware such as VPNs and firewalls can be eliminated.

Traditional Data Center-Centric, Hub and Spoke Network and Network Security Architecture
Data-Center-Centric Networking and Security Model



GOALS OF SASE

The SASE framework's major purpose is to assist in the modernization of networks and protection to meet the ever-changing business needs. SASE achieves this by providing consistent security among users, regardless as to where they conduct business, as well as knowledge and transparency over what may be accessible.

- Automated device control and comprehensive device transparency
- Network micro-segmentation to limit relative motion and prevent breaches
- Cyber and logistical risk are continuously monitored, assessed, and remedied.

- Multiple manufacturers' products and solutions, with unprecedented degrees of orchestration, automated, and response
- Manage endpoint IoT devices and related technologies in a secure and efficient manner (OT systems)
- Virtual and physical devices, as well as network infrastructure and workloads, are discovered, assessed, and remedied/controlled.

BENEFITS OF SASE

The SASE model combines many networking and security tasks, which were previously offered as separate point solutions, into a single, integrated cloud service. Businesses can benefit from SASE consolidation in the following ways:

- Costs and complexity are reduced.
- Help users gain smooth access by providing centralized orchestration and real-time application optimization.
- Increase the security of remote and mobile access.
- Access is restricted based on the identification of the person, device, and application.
- Increase security by enforcing policies that are consistent.
- Using centralized administration, you may improve the efficiency of your network and security workers.

COMPONENTS OF SASE

	Traditional networking models	SASE model
REMOTE ACCESS TO ON-PREMISES RESOURCES	Most traditional models largely rely on VPN technology through SSL/TLS browser access or a dedicated endpoint client.	SASE acts as a VPN replacement. Users connect to a SASE to access on-premises resources and cloud services. Policy is defined and applied through the SASE console.
ACCESS TO CLOUD RESOURCES	On-premises network access to cloud resources treats these like any other online properties, using traditional firewalls, proxies and routing controls.	SASE provides optimized, streamlined, cloud-aware network access for SaaS, PaaS and IaaS. These rely on API integration and request introspection for end-user requests.
NETWORK ACCESS CONTROLS	Most on-premises environments rely on switching, routing, firewalls and proxies for access control.	SASE services aggregate a number of network security and access controls—including firewalls as a service—into one unified fabric.
SD-WAN, WAN OPTIMIZATION, BANDWIDTH AGGREGATION	These controls and capabilities usually require several vendors and products to function, and they may lack in integration.	A SASE service integrates SD-WAN access and traffic optimization capabilities into a single brokering service for all access types.
WEB APPLICATION SECURITY	WAFs are usually separate appliances or platforms, or are achieved through brokering to a content delivery network or in-cloud service.	SASE platforms integrate WAF policies and services into the same brokered approach, although policies and capabilities may not be as mature yet.
NETWORK THREAT DETECTION	Network threat detection is accomplished using NGFWs, malware detection sandboxes or CASB brokering.	SASE services combine numerous network threat detection capabilities into one service fabric.

TOP 5 COMPANIES PROVIDING SASE:

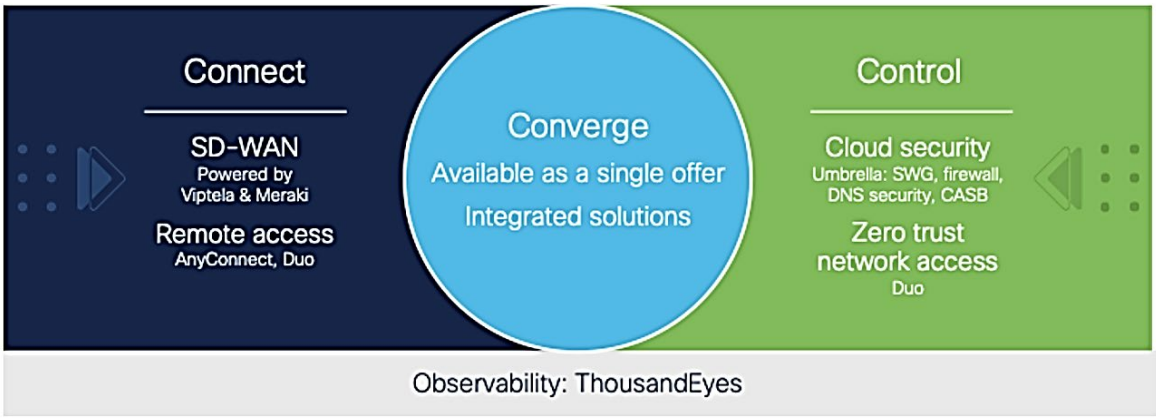
Akamai	Akamai Technologies, Inc. is a provider of digital and Online safety solutions, as well as a worldwide media distribution network, data security, and cloud service provider.
CATO NETWORKS	SD-WAN and security system are combined into a cloud storage solution in the organization 's primary offering.
CLOUDFLARE	Cloudflare, Inc. is an online infrastructural and computer safety business based in the United States that specializes in media distribution networks and DDoS mitigation.
Forcepoint	Forcepoint is a program firm based in Texas that specializes in cybersecurity technology and information security, as well as cloud accessible control brokers, firewalls, and cross-domain services.
McAfee	McAfee Corp. is a California-based worldwide cybersecurity program corporation.

WHY CISCO FOR SASE?

Many firms today encounter a significant dilemma: How can security and network personnel ensure accessibility to programs for an ever-dealing workforce without raising difficulty? This requires the standard network architecture to be revised, resulting in the conception of a secure access service edge (SASE). Just put, SASE corresponds connectivity and cloud security features. For Cisco, the SASE technology is not unique.

Cisco has been helping firms around the world construct a connection for their company for the past two and a half years. And the same corporations assisted defending themselves from increasing cyber dangers. It has evolved along the road, so that its expertise is simpler and more efficient. Cisco is again innovative in providing you with a secure cloud-friendly network.

Components of Cisco's SASE architecture



Cisco's SASE architecture secures and optimizes your connection, allowing you to provide the greatest user engagements possible. In this case, observability is seen as a crucial component in delivering that environment. More connections are beyond your management or complete control as your dependency on the internet and cloud services grows.

Even if they don't operate the infrastructures or have control over how network operators' direct traffic, organizations must ensure the efficiency and quality of the underlying transportation. Cisco provides complete view from the client to the software across any networking and cloud computing, as well as

meaningful information into performance problems, allowing you to swiftly detect, rectify, or report progress to keep your digital experience up to par.

Cisco isn't the first provider to offer a SASE system, but it does offer the most comprehensive set of services. Cisco SD-WAN 17.2 combines solutions from the company's connectivity and protection product lines. This contains connectivity, IDS/IPS, and URL filtration elements from Viptela and Meraki, as well as safe online portal, DNS safety, cloud access security broker (CASB), and firewall features from Umbrella.

Cisco is also combining safety features from its zero-trust solutions. Cisco certainly has several intriguing distinguishing features due to its scale. Cybersecurity features are to be available in the cloud, according. For delivering services, all of the present SASE suppliers depend on public cloud, datacenter, or third-party suppliers.

Although the SASE competitor environment is vast, most vendors offer safety and connectivity capabilities. Cisco is the leading company in networking and cybersecurity, and it can bring UC knowledge to the table while also providing a strategic advantage.

Cisco introduced a system that gives clients choices instead of constraining them to use a system that only addresses a portion of the business.