SASE
The Optimal Architecture to Secure and Connect the New Enterprise Perimeters
Introduction

The enterprise Perimeter has been the focus of networking and security leaders for decades. The basic planning assumption, and associated best practices, was that the Perimeter was drawn around the corporate datacenter that hosted all sensitive data and applications. IT has invested significant resources to secure all traffic coming into and going out of the Perimeter with network security technologies like firewalls, intrusion prevention systems, secure web gateways, and more.

Beyond security, the Perimeter was a clear physical boundary that requires optimal connectivity to the outside world: employees, partners, suppliers, and later distributed applications across regions and the cloud.

The single enterprise Perimeter paradigm came under pressure over the past decade. The datacenter Perimeter was stretched with the migration of many applications to cloud datacenters and public cloud services. The combination of cloud applications and the expanding mobile workforce created new traffic patterns that completely bypassed the traditional datacenter Perimeter.

This change in the way modern enterprises conduct business, and use cloud and mobile technology, requires a new architecture that is not based on a single Perimeter design. This architecture, the Secure Access Service Edge (SASE), was defined by Gartner, as a way to secure the new enterprise multi-Perimeters. In this document, we will explore SASE and how it can address a range of common use cases with optimal user experience and without compromising security.
What is SASE and How it Effortlessly Secures All Enterprise Perimeters

The Secure Access Service Edge (SASE) is a new enterprise networking technology category introduced by Gartner in 2019. SASE converges the functions of network and security point solutions into a unified, global cloud service. These include SD-WAN, Global Private Backbone, Secure Web Gateway, Firewall as a Service, and more. SASE architecture is marked by four main attributes. It is identity-driven, cloud-native, supports all edges, and is distributed globally.

SASE Architectural Attributes

Identity-driven
User and resource identity, not simply an IP address, drives SASE networking and security policies. This approach reduces operational overhead by letting companies develop one set of networking and security policies for users regardless of device or location.

Cloud-native
SASE is a cloud-first and cloud-native architecture. All networking and security functions are implemented in the cloud. Only capabilities that must be deployed at the edge, are delivered as simple edge clients. SASE architecture leverages key cloud capabilities including elasticity, adaptability, self-healing, and self-maintenance to uniformly deliver security and networking capabilities across the enterprise.

Supports All Edges
SASE creates one secure network for all company entities — datacenters, branch offices, cloud resources, and mobile users. For example, SD-WAN appliances support physical edges while mobile clients and clientless browser access connect users on the go, and while working from home.

Globally Distributed
To ensure the full networking and security capabilities are available everywhere and deliver the best possible experience to all edges, the SASE cloud is globally distributed across dozens of Point of Presence (PoPs). Enterprise edges connect to the nearest PoP so all traffic is secured and optimized at the PoP and across the global backbone of PoPs to its destination.
SASE is Optimized for Total Visibility and Control

SASE's cloud-first architecture is uniquely positioned to support the change to the enterprise Perimeters. How? The primary problem presented by the changes to the Perimeters is restricted traffic visibility and inspection blind spots. Traditional appliance-based security is optimized to secure a single traffic path. To ensure visibility and control of all traffic paths such as mobile-to-cloud or branch-to-cloud, enterprises had to force all traffic through their datacenter Perimeter — or go without security at all. This is a sub-optimal design that adds latency and pressures the datacenter security engines.

SASE architecture is built for full visibility to all traffic from all edges - physical, cloud, and mobile - including traffic between the edges (WAN), and from the edges to the Internet. SASE applies a rich set security and networking engines on that traffic, for full inspection for threat prevention and access control. This is why SASE has been touted, by Gartner, as the future of networking and security.

SASE Components

**SASE Cloud**
A globally distributed cloud service that delivers the networking and security capabilities to all edges. The SASE cloud operates as a single entity and its internal structure is transparent to the end users.

**SASE Edge**
Designed to connect a specific edge to the SASE cloud. SASE clients include SD-WAN appliances for branches, IPSec-enabled firewalls and routers, and device agents for Windows, Mac, iOS, Android, and Linux.

**SASE PoP**
A specific instance within the SASE Cloud that hosts the resources needed to deliver the SASE capabilities including servers, network connectivity, and software. SASE PoPs are symmetrical, interchangeable, multi-tenant, and mostly stateless. They are built to serve any enterprise edge connected through them as an integral part of that particular enterprise network.

**SASE Management**
A cloud-based management application to configure all policies and view network and security analytics and real-time status.
SASE Connects and Secures the Modern Enterprise

Use Cases

1. **Securely Connect ACME Branches to Any Application**
   - **Transform Effort and a Security Chokepoint**
   - Optimal and Secure Branch-to-Application Access
   - With Converged Traffic Optimization, Access Control, Threat Prevention

2. **Securely Connect ACME Remote Users to Any Application**
   - **Transform Effort and a Security Chokepoint**
   - Optimal and Secure User-to-Application Access
   - With Converged Traffic Optimization, Access Control, Threat Prevention

3. **Optimally Connect ACME Branches Globally to a New Cloud ERP System**
   - Edge-to-Cloud MPLS network into a Physical Datacenter
   - Optimal and Secure Cloud ERP Access for All Locations and Users

4. **Securely Connect ACME Multi-Cloud and On-Premise Datacenters (Future)**
   - Converge Multiple Clouds and On-Premise Environments
   - Optimal and Secure Any-to-Any DC Connectivity

Conclusion

SASE: The Optimal Architecture to Secure and Connect the New Enterprise Perimeter
About Cato Networks

Cato is the world’s first SASE platform, converging SD-WAN and network security into a global, cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize global connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into the network with a zero trust architecture. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into the network with a zero-trust architecture. With Cato, the network, and your business, are ready for whatever’s next.

Cato Cloud
Global Private Backbone
Edge SD-WAN
Security as a Service
Cloud Datacenter Integration
Cloud Application Acceleration
Secure Remote Access
Cato Management Application

Managed Services
Managed Threat Detection and Response (MDR)
Intelligent Last-Mile Management
Hands-Free Management
Site Deployment

Cato. The Network for Whatever’s Next.