What is SASE?

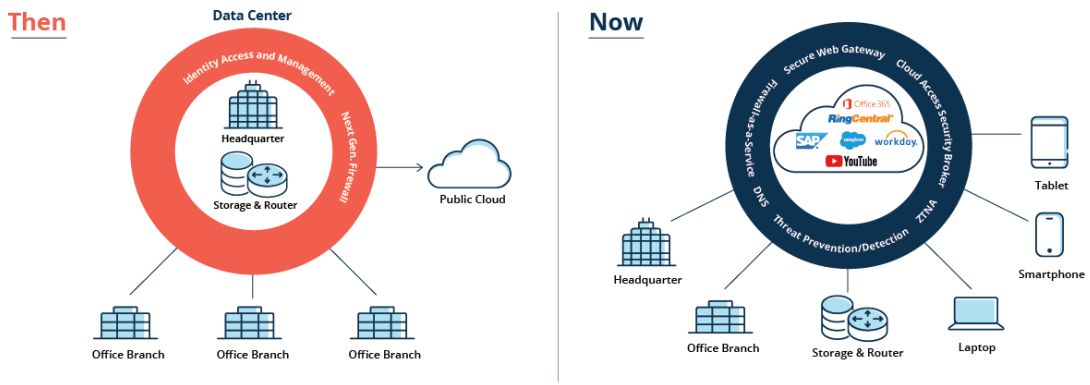
SASE (Secure Access Service Edge) technology for cable link architecture, WAN capabilities, including SD-WAN (Software Defined Wide Area Network), WAN routing and optimization, with cloud-delivered services, applications such as SWG, CASB and ZTNA. With user access anywhere and access to sensitive data in the cloud, SASE provides a secure way to connect without redirecting application traffic to the data center. Instead, SASE intelligently controls traffic to the clouds and provides advanced security controls directly in the cloud. SASE applies to application performance and covers network security as the number of end users grows and the enterprise continues to move applications to the cloud.

How does our SASE solution work?

SASE for advanced SD-WAN edge deployed in branch offices and end-to-end cloud security services.

Traditionally, all branch location application traffic went through private MPLS (Multiprotocol Label Switching) services to the corporate data center for security inspection and verification. This architecture was available when applications were hosted solely in a corporate data center. Now that applications and services have moved to the cloud, traditional network architecture is no longer sufficient. Since internet traffic must first pass through the data center and corporate firewall before reaching its destination, there will be a decline in applications and user experience.

Thanks to access to mobile devices, it is directly from the application using traditional security technology available on a wireless basis. By transforming WAN architecture and security with SASE, enterprises can have direct, secure access to applications and services in multi-cloud environments, location-based devices and access devices to access them.



The main components of SASE are advanced SD-WAN and comprehensive cloud-delivered security (Security Service Edge or SSE).

There are key advanced SD-WAN capabilities that allow you to fully enable SASE:

• Tight integration with multiple cloud-delivered security services to avoid vendor lock-in
• Application identification with first packet to enable granular traffic control
• SaaS acceleration and WAN optimization
• Best path selection based on business needs and quality of service (QoS)
• Tunnel bonding to connect multiple links and support automatic failover
• Zero-touch provisioning for automatic deployment of remote locations and seamless rollout of changes

To fully enable SASE, there are key SSE features:

• ZTNA or Zero-Trust Network Access: Assumes that no user can be trusted by default and supports least privileged access. Provides secure access to remote users.
• CASB or Cloud Access Security Broker: Protects sensitive data in cloud applications by enforcing security policies
• SWG or Secure Web Gateway: Protects organizations from online threats using several techniques such as URL filtering and malicious code detection.
• FWaaS or Firewall as a Service provides cloud firewall functionality to analyze traffic from multiple sources.
• Other security services such as data loss prevention (DLP), remote browser isolation (RBI), and sandboxing.

If you have any questions or would like a presentation regarding our SASE offer, please contact your Partner Manager or Distributor