

The Salesforce logo, consisting of the word "salesforce" in white lowercase letters inside a blue cloud-like shape.

salesforce

SASE for Akraino

Chris Donley

Sr. Director, Network Security



Network Expectations are changing

Corporate Networks were built on the expectation that people worked in an office

Over the past several years, the environment has changed

- COVID
- Rise of the cloud
- Faster broadband at home

These changes in the way we work put pressure on corporate networks

- VPN capacity
- Security
- User experience (latency, throughput, etc.)



The Office



The New "Office"

Enter SASE

Secure Access Service Edge

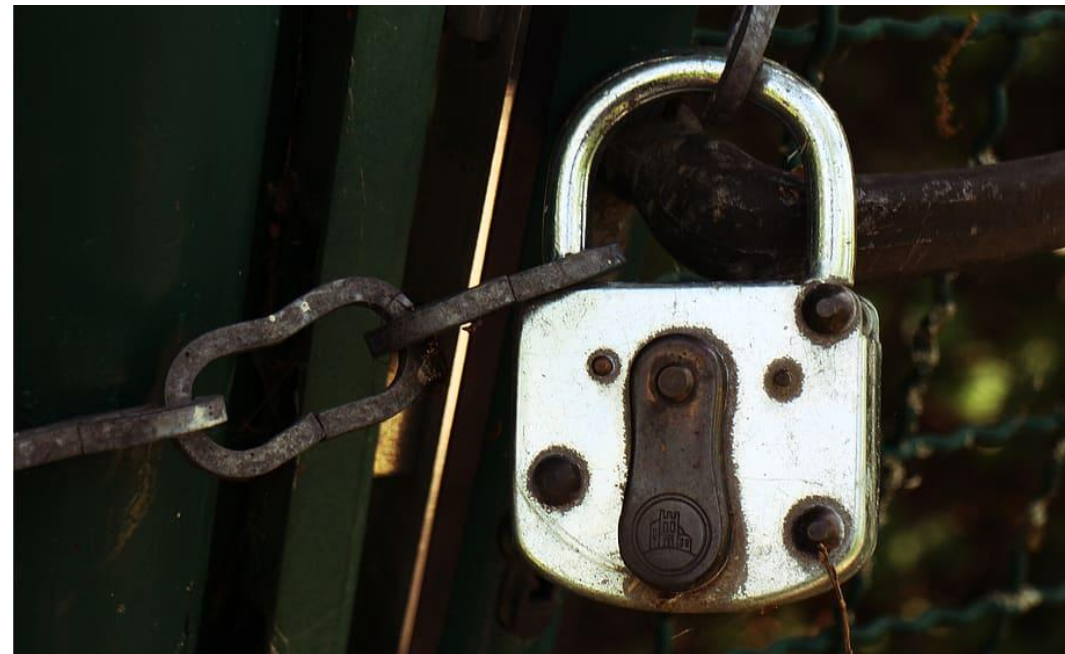
Emerging cybersecurity paradigm for remote connectivity


Combines multiple technologies for a holistic secure tunnel solution

- Firewall as a Service (FWaaS)
- Zero Trust Network Access (ZTNA)
- Cloud Access Security Broker (CASB)
- Digital Loss Prevention (DLP)
- SD-WAN

Key Use Cases (for this presentation)

- Work-from-Anywhere
- Multi-Cloud Access





“SASE capabilities are delivered as a service based upon the identity of the entity, real-time context, enterprise security/compliance policies and continuous assessment of risk/trust throughout the sessions. Identities of entities can be associated with people, groups of people (branch offices), devices, applications, services, IoT systems or edge computing locations.”

- Gartner

Use Case: Work From Anywhere



We've all learned to work remotely during COVID

- Even after re-opening, expect significantly more remote work

Who is securing the home network? or coffee shop?

- How does that affect enterprise risk?

How does remote work affect the user experience?

- Latency/throughput
- interaction with other applications
- printing

What about VPN capacity?



Use Case: Multi-Cloud Access

Companies used to have compute workloads in datacenters

- And then we added the cloud
- And then we added multi-clouds

Challenge: enforce consistent security policies across all clouds

Challenge: consistent user experience accessing all clouds

Challenge: shadow IT / users accessing the cloud through non-approved methods



SASE Deployment Types



Philosophy

Build-your-own

- Higher initial cost & complexity (stitching together multiple services)
- Higher step functions as you add users
- More control, Higher trust
- User experience location-dependent

Managed Service

- Easier to get started
- Lower step functions to add users/use cases
- How trustworthy is your partner? How complete & secure is the offering?
- Integration
- User experience - partner proximity?

Methodology

Topology-aware (e.g. managed VPN)

- Access specific hosts based on DNS
- Good for DevOps engineers who need to access specific servers
- Challenging for users accessing XaaS resources (HR, expense reporting, project tracking, etc.)

Topology-unaware

- Services are exposed, not hosts
- Easier for corporate services, but harder for operations

User Requirements

“Why would I switch from my VPN client?”

Improved user experience

- Latency/Throughput
- Bufferbloat

Ease of use

Compatibility with my other IT apps

Home network compatibility

- Can I print?



Operational Considerations

What will it take for SASE to work with my network?

Security Posture

- 2 Factor Authentication
- Don't trust the end user environment

Ecosystem - technology & service provider partners

Ease of Integration with my existing solution

- Compatibility
- APIs
- Automation

Global reach

- Proximity to my users and my workloads
 - First-party and Public Cloud





Takeaways for Akraino

Edge can have a prominent role in SASE due to your proximity to the users

An Akraino edge blueprint should address the following:

- Trust & security offering
- Federation model for global reach
- Centralized management
- APIs / Integration with customer tools & processes
- Monitoring/Alerting



Thank You

