THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

Why Closed Networks Need a New Approach

Traditional private WANs rely on static routing and perimeter firewalls, creating blind spots and high latency for modern cloud-first workloads. Enterprises struggle to apply consistent Zero Trust controls without exposing traffic to the public internet.

→ Static, point-to-point links limit agility

→ Perimeter-centric security cannot verify user or device context

→ Latency spikes affect SaaS and edge applications

CONTROL FRAMEWORK

KDDI SASE Gateway Overview

KDDI's Secure Access Service Edge (SASE) Gateway consolidates SD-WAN, firewall-as-a-service, secure web gateway, and CASB into a single cloud-native point of presence. It delivers policy enforcement at the edge, close to the user or device.

→ Unified networking and security stack

→ Policy engine runs in a distributed cloud fabric

→ Supports any-to-any traffic, including SaaS, IaaS, and on-prem

CONTROL FRAMEWORK

SP Interconnect: Private Backbone for SASE

KDDI's Service Provider (SP) Interconnect creates a dedicated, carrier-grade MPLS-like backbone that links enterprise sites directly to the SASE Gateway, bypassing the public internet.

- → End-to-end encrypted tunnels between sites and SASE edge
- → Predictable latency and SLA-backed performance
- → Seamless integration with existing MPLS or broadband circuits

CONTROL FRAMEWORK

Zero Trust Enforcement Over Closed Networks

With traffic routed through the SASE Gateway via SP Interconnect, every session is inspected, authenticated, and authorized based on identity, device posture, and application context—without ever leaving the private backbone.

→ Identity-driven policies applied at the edge

→ Continuous risk assessment for each flow

→ Micro-segmentation across sites as if they were a single cloud

CONTROL FRAMEWORK

Operational Simplification

The combined SASE-SP solution reduces the number of point-to-point circuits, centralizes policy management, and automates provisioning through APIs, freeing network teams to focus on business outcomes.

- → One-pane-of-glass console for networking and security
- → Zero-touch onboarding of new sites via SD-WAN orchestrator
- → Policy changes propagate instantly across the private backbone

CONTROL FRAMEWORK

Security Benefits at Scale

By keeping traffic off the public internet, the solution reduces exposure to DDoS, man-in-the-middle attacks, and data exfiltration while delivering consistent threat intelligence updates from KDDI's global security operations center.

→ Encrypted private path eliminates opportunistic eavesdropping

→ Integrated sandboxing and malware detection at the edge

→ Real-time threat feed applied uniformly across all sites

EXECUTIVE TAKEAWAY

Executive Takeaway

KDDI's SASE Gateway paired with SP Interconnect converts a fragmented, perimeter-based WAN into a unified, Zero Trust-enabled private fabric. The process delivers faster, more secure connectivity, reduces operational complexity, and aligns with modern compliance expectations.