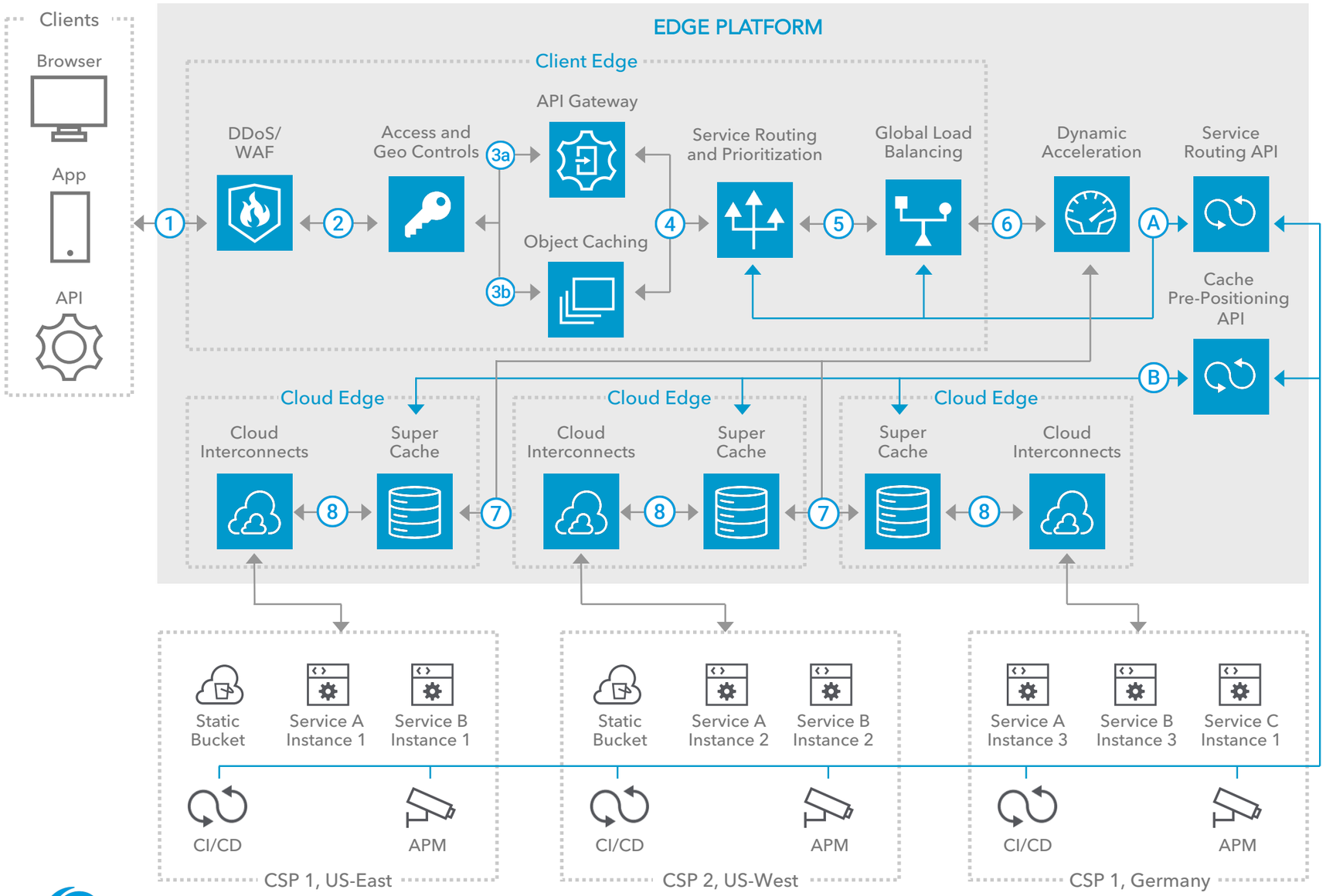
CLOUD-NATIVE TRAFFIC CONTROL

Reference Architecture



OVERVIEW

Modern applications require more than just computing. Load balancing, security, and other requirements force IT to deploy additional components in multiple regions. This duplication increases spending on cloud services and operations. A more scalable approach is to implement these components in a single platform — at the edge. Replacing multiple elements at the edge reduces cost, simplifies operations, and improves security posture.

1. Security controls are applied consistently regardless of the origin number, location, or tech stack.
2. Limit content to authorized users in valid geographies.
3a. Quota enforcement and requested authorization of API traffic ensures compute availability and minimizes cloud costs.
3b. Flexible caching for any content type, including APIs.
4. The edge applies routing rules per request host, path, session, and priority to determine candidate origins.
5. The edge selects the optimal target by applying performance, weighting, and health-check logic across regions and CSPs.
6. SureRoute and TCP optimizations ensure the fastest and most reliable path to and from any cloud region.
7. The super-cache tier serves static content, eliminating the request to the CSP and reducing egress costs.
8. Reduced cloud egress costs via Akamai Cloud Interconnects.
A. CI/CD integration into service routing enables blue/green and canary deployment strategies. APM integration allows dynamic traffic shifting.
B. CI/CD pipeline is used to "pre-position" static, eliminating cloud egress charges normally required to retrieve the content.

KEY PRODUCTS

DDoS/WAF, geo controls, and API discovery ▶ App & API Protector

Caching, routing, and acceleration ▶ Ion/API Acceleration

API authorization and throttling ▶ API Gateway

Global load balancing ▶ Application Load Balancer or Global Traffic Manager

Reserve cache ▶ Cloud Wrapper

Private cloud connectivity ▶ Cloud Interconnects

Published 02/22

Akamai