

Akamai AI and API Manager

API Gateway Throttling vs. WAF DDoS Protection

SOLUTION OVERVIEW FOR AKAMAI CONNECTED CLOUD

When disaster strikes — API traffic surges

The most common reason an outage is caused by a traffic surge is **not** malicious attacks, but accidental misuse—typically a customer or partner with an accidental for-loop. There are two types of tools that help protect your APIs from surges: Web Application Firewalls (WAF) with DDoS protection, and fine-grained rate limits from your API Gateway. Both are necessary for a strong posture to prevent outages of your API.

WAF DDoS rate limits vs. API Gateway throttling

> Granularity & context

WAFs aggregate requests by network-level properties like IP address. These rules drop high-volume malicious traffic but would easily overlook the clumsy partner or customer scenario. Fine-grained rate limiting in an API gateway can stop a rogue partner or organization by looking at data inside the token or request.

> Short-term vs. long-term

Akamai DDoS protection operates on small time frames (e.g. a burst-mode threshold with a range of 1–5 seconds, and a fixed regular threshold of 2 minutes), great at preventing attacks. API gateways enforce both short- and long-term limits, sometimes called quotas.

> Observability & analytics

WAF metrics show aggregate 'allowed' and 'blocked' counts per rule but rarely identify which API operation or developer caused the flood. API gateways provide dashboards that break down calls by client, endpoint, response code, even geographic region.

Implementing rate limiting & quotas with AAM

Akamai AI and API Manager (AAM) is the market leader in rate-limiting flexibility, with a global rate-limiter that synchronizes counts at the speed of light.

> Programmable rate limiting

Rate limiting on any property accessible to the gateway (e.g. per user or team).

> Powerful quota enforcement

Store and enforce long-term quotas to manage resources used over time.

> Analytics at your fingertips

Combine with monitoring tools to unlock insights (e.g. alerts when a customer reaches 80% of quota for an upsell opportunity).

> Revenue-driven API strategy

Customized per-customer, enabling different limits per pricing tier to upsell API customers.

Akamai AI and API Manager

API Gateway Throttling + WAF DDoS Protection

DEFENSE IN DEPTH ON AKAMAI CONNECTED CLOUD

Defense in depth: AAM x Akamai Connected Cloud architecture overview

The Akamai WAF stops malicious requests and higher-scale distributed attacks, but they're only part of the solution you need to deploy. You're more likely to be impacted by rogue code with a valid key. Akamai AI and API Manager complements the Akamai WAF with its fine-grained controls, programmability, and reporting.

