JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

API Gateway Security and Management with Kong Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

API Gateway Security and Management with Kong Training Course

API Gateway Security and Management with Kong is a 1-week training course for platform engineers, API developers and integration architects who run Kong Gateway in front of production APIs, and it ends with a secured Kong gateway configuration for a set of real services. APIs now carry payments, patient records and partner orders, so the gateway has become the first line of control for both traffic and attackers. Jupiter Prime Training runs this course for engineers who own that layer.

Why API Gateway Security and Management with Kong Matters Now

Three forces push the gateway to the centre of platform work: the growth of microservices that multiplies the number of exposed endpoints, partners and mobile apps that expect stable, documented APIs with predictable limits, and attackers who now target business logic and broken authentication rather than network ports. A well-run gateway enforces identity, throttles abuse and gives clear visibility into every call; a poorly configured one leaks data through forgotten routes and lets a single client exhaust capacity. The course maps gateway controls to the Protect and Detect functions of the NIST Cybersecurity Framework 2.0 NIST CSF 2.0.

Who Gains Most from API Gateway Security and Management with Kong

- Platform engineers who deploy and upgrade Kong clusters and their data planes
- API developers who publish services and need consistent authentication and limits
- Integration architects who connect partners, mobile apps and internal systems through APIs
- Site reliability staff who monitor latency, errors and capacity at the edge

A platform team that sends its gateway operators with the developers who publish APIs gains most, because route, plugin and policy choices then follow one shared pattern.

API Gateway Security and Management with Kong Capabilities

Participants leave able to stand up, secure and observe a Kong gateway that their organisation can run with confidence.

- Design services, routes and upstreams for clean traffic separation — API owners and architects
- Apply authentication plugins such as key, JWT and OAuth 2.0 flows — security engineering
- Specify rate limiting and request size policies per consumer — product owners and partners
- Build declarative configuration managed through version control and pipelines — platform operations
- Test gateway behaviour against common API attacks and misconfigurations — application security

Key API Gateway Security and Management with Kong Terms

- API gateway — A proxy that sits in front of APIs to route requests and enforce security, limits and logging in one place.
- Route — A Kong rule that matches incoming requests by path, host or method and sends them to a defined service.
- Plugin — A Kong module that adds behaviour, such as authentication, rate limiting or logging, to a service, route or consumer.
- Consumer — A Kong entity representing an application or user of an API, used to attach credentials and per-client policies.
- Rate limiting — Capping how many requests a client may send in a period to protect capacity and slow abuse.
- Declarative configuration — Describing the whole gateway set-up in files that tools apply, so changes are reviewed and repeatable.

API Gateway Security and Management with Kong Day by Day

Day 1: Gateway Architecture and Traffic Design

- Kong Gateway Control and Data Planes — Deployment Topology Choices
- Services, Routes and Upstreams — Clean Separation of API Traffic
- Load Balancing and Health Checks — Resilient Upstream Targets
- Hybrid and Kubernetes Ingress Modes — Fit With Platform Strategy
- NIST CSF 2.0 Protect Function — Where the Gateway Enforces Controls

Day 2: Authentication and Access Control

- Key Authentication and Consumer Credentials — Simple Client Identity
- JWT Validation Plugin — Token Trust and Claim Checks
- OAuth 2.0 and OpenID Connect Flows — Delegated Access for Partners
- Access Control Lists by Consumer Group — Fine-Grained Route Permissions
- Mutual TLS Between Gateway and Upstreams — Internal Service Trust

Day 3: Traffic Control and API Threat Protection

- Rate Limiting and Quotas — Fair Use Across Consumers
- Request Size and Validation Plugins — Blocking Malformed Payloads
- Bot Detection and IP Restriction — Filtering Abusive Clients
- CORS and Header Hardening — Browser-Facing API Exposure
- Broken Object-Level Authorisation Cases — Banking and Retail Lessons

Day 4: Declarative Operations and Observability

- decK Declarative Configuration Files — Gateway State in Version Control
- CI/CD Pipelines for Gateway Changes — Reviewed and Repeatable Releases
- Secrets Management for Credentials — Vault References Instead of Plain Text
- Prometheus Metrics and Logging Plugins — Latency, Errors and Usage
- Distributed Tracing Across Services — Pinpointing Slow or Failing Calls

Day 5: Practising the Secured Kong Gateway Configuration

- Service and Route Build for a Sample API Set — Structured Traffic Design
- Authentication and Rate Limit Policies Applied — Consumer-Specific Controls
- Attack Simulation Against the Gateway — Gaps Found and Closed
- Dashboard and Alert Set-Up — Operational Readiness Check
- Secured Kong Gateway Configuration Completion — Declarative Files, Policies and Runbook

Applying API Gateway Security and Management with Kong After the Course

- Export the current gateway into declarative configuration files and place them under version control with peer review for every change
- Audit all routes for missing authentication or rate limiting plugins and close the gaps on externally exposed APIs first

API Gateway Security and Management with Kong Questions FAQ

What is API gateway security and management with Kong and why does it matter now?

API gateway security and management with Kong is the practice of routing, protecting and observing API traffic through Kong Gateway. It matters now because microservices and partner integrations expose more endpoints, and the gateway is where identity, limits and logging are enforced consistently.

Which roles gain most from API gateway security and management with Kong training?

Platform engineers, API developers, integration architects and site reliability staff gain most. You benefit if you deploy Kong, publish APIs behind it or must keep partner and mobile traffic secure and stable.

How does API gateway security and management with Kong training differ from a general API design course?

It concentrates on running and securing the gateway layer rather than designing API contracts. You configure routes, plugins, authentication and observability in Kong, while API design courses cover resource modelling and documentation.

What do you bring back from API gateway security and management with Kong training?

You bring back a secured gateway configuration in declarative files for a set of sample APIs. It includes routes, authentication and rate limit policies, monitoring settings and a short runbook you can adapt to production.

API Gateway Security and Management with Kong: The Way Forward

The secured Kong gateway configuration first informs which authentication and rate limit policies become the default for new APIs. Platform engineers maintain it, developers inherit its patterns and security staff review its changes. After the first production release, revisit consumer limits, because real traffic usually shows which partners need different quotas.