**API Gateway Setup Documentation**

**Project:** Telco Cloud Migration Project  
**Component:** API Gateway Configuration and Deployment  
**Prepared by:** [Your Name / DevOps Lead]  
**Date:** [DD-MM-YYYY]  
**Confidentiality:** Internal Use / Public (if in GitHub)

**1. Purpose**

To document the setup, configuration, and deployment of the API Gateway within the Telco cloud environment, enabling secure and scalable API access across OSS/BSS, CRM, mobile money (M-PESA), and third-party integrations.

**2. Objectives**

* Secure API traffic using authentication and throttling policies
* Enable seamless routing to microservices (via Kubernetes or service mesh)
* Expose APIs for internal teams and external partners (with RBAC)
* Log, monitor, and audit API usage for SLA and compliance tracking

**3. Tools & Technologies**

| **Tool/Tech** | **Description** |
| --- | --- |
| **Kong / Apigee / AWS API Gateway** | API Gateway Platform (based on architecture) |
| **Kubernetes Ingress** | For routing and gateway deployment |
| **OAuth 2.0 / JWT** | Authentication standards |
| **Terraform / Helm** | Infrastructure-as-Code deployment |
| **Prometheus + Grafana** | Monitoring & alerting |
| **ELK Stack** | Logging and analytics |

**4. Architecture Overview**

lua

CopyEdit

Client / Device

|

v

+--------------+

| API Gateway |

+--------------+

|

+---> Auth Plugin (OAuth/JWT)

+---> Rate Limiting / Throttling

+---> Routing Rules

|

v

+--------------------+

| Backend Microservices|

| (via K8s Ingress) |

+--------------------+

**5. Deployment Steps**

**5.1 Pre-requisites**

* Cloud cluster (EKS/GKE/AKS or private K8s)
* DNS and TLS certificate (via ACM/Let's Encrypt)
* IAM roles for API Gateway access
* OAuth provider integration (e.g., Keycloak, Okta)

**5.2 Infrastructure Provisioning**

Using Terraform or Helm:

bash

CopyEdit

terraform init

terraform plan -out gateway.plan

terraform apply "gateway.plan"

Helm (example for Kong):

bash

CopyEdit

helm repo add kong https://charts.konghq.com

helm install kong kong/kong --set ingressController.installCRDs=false

**5.3 Gateway Configuration**

**Define Routes & Services**

yaml

CopyEdit

apiVersion: configuration.konghq.com/v1

kind: KongIngress

metadata:

name: user-service

proxy:

path: /users

**Enable Authentication Plugin**

bash

CopyEdit

curl -i -X POST http://<gateway-url>/services/user-service/plugins \

--data "name=oauth2" \

--data "config.enable\_password\_grant=true"

**Enable Rate Limiting**

bash

CopyEdit

curl -i -X POST http://<gateway-url>/plugins \

--data "name=rate-limiting" \

--data "config.minute=100" \

--data "config.policy=local"

**6. Security Setup**

| **Control** | **Method** |
| --- | --- |
| AuthN/AuthZ | OAuth 2.0 + JWT Tokens |
| TLS Encryption | Terminate SSL at API Gateway (Cert Manager) |
| IP Whitelisting | CIDR restrictions on endpoint access |
| RBAC | Role-based API scopes via Identity Provider |

**7. Monitoring & Logging**

* **Metrics**: Expose Prometheus metrics (requests/sec, latency, errors)
* **Dashboards**: Pre-built Grafana dashboards for APIs
* **Alerts**: Trigger alerts on 5xx spikes, auth failures, or rate-limit breaches
* **Logs**: Forward gateway logs to ELK or cloud-native log service (e.g., CloudWatch)

**8. Testing**

| **Test Type** | **Description** | **Tools Used** |
| --- | --- | --- |
| Functional | Test routing, auth, and response mapping | Postman, curl |
| Load & Throttle | Validate rate limits and API scaling | JMeter, k6 |
| Security | Token validation, CORS, injection testing | OWASP ZAP, Burp |

**9. Risks & Mitigations**

| **Risk** | **Mitigation** |
| --- | --- |
| Token replay or theft | Short TTL, refresh token cycle, rotate secrets |
| Misconfigured routing | Use automated config testing in CI/CD |
| Denial-of-service | Rate limits, WAF rules, IP filtering |

**10. Maintenance Guidelines**

* Rotate secrets and TLS certs quarterly
* Audit API usage monthly for anomalies
* Review rate limits per partner quarterly
* Update gateway plugins and patches regularly

**11. Appendices**

* Appendix A: API Inventory List
* Appendix B: CI/CD Pipeline for Gateway Configs
* Appendix C: Monitoring Dashboard Screenshots
* Appendix D: Swagger/OpenAPI specs
* Appendix E: Change History & Config Backups