ONE PAGE SUMMARY

IT & Software › API Development › API Gateway

Introduction to API Gateway

API Gateways: The Control Center for Your APIs

DEFINITION

> An API Gateway is a server that acts as an intermediary for requests from clients seeking resources from backend services. It simplifies API management by handling requests, routing, and security.

KEY CONCEPTS

Request Routing

API Gateways direct incoming requests to the appropriate backend service based on the request path.

Load Balancing

They distribute incoming traffic evenly across multiple servers to optimize resource use and prevent overload.

Security Features

API Gateways provide authentication, authorization, and encryption to protect data and services.

Rate Limiting

They control the number of requests a client can make in a given time to prevent abuse.

Response Transformation

API Gateways can modify responses before sending them back to clients, ensuring compatibility.

EXAMPLES

→ A mobile app uses an API Gateway to access user data from multiple microservices.

→ An e-commerce site employs an API Gateway to manage payment processing and inventory services.

→ A weather application routes requests through an API Gateway to fetch data from various weather APIs.

MEMORY TIPS

★ Think of the API Gateway as a traffic cop directing data flow.

★ Remember 'RSLR' for Routing, Security, Load balancing, and Rate limiting.

★ Visualize an airport terminal where the gateway directs passengers to their flights (services).

COMMON MISTAKES

✗ Overlooking security configurations can lead to vulnerabilities.

✗ Failing to implement proper rate limiting can cause service outages.

✗ Neglecting to document API Gateway routes and services can confuse developers.

QUICK RECAP

API Gateways streamline communication between clients and services by managing requests and security. They enhance performance through load balancing and protect services with security features. Understanding their functions is crucial for effective API management.