Developing REST APIs

Cloud Computing

Brenden west

Contents

Learning Outcomes

- Overview of REST APIs
- Amazon API Gateway
- Securing & monitoring APIs

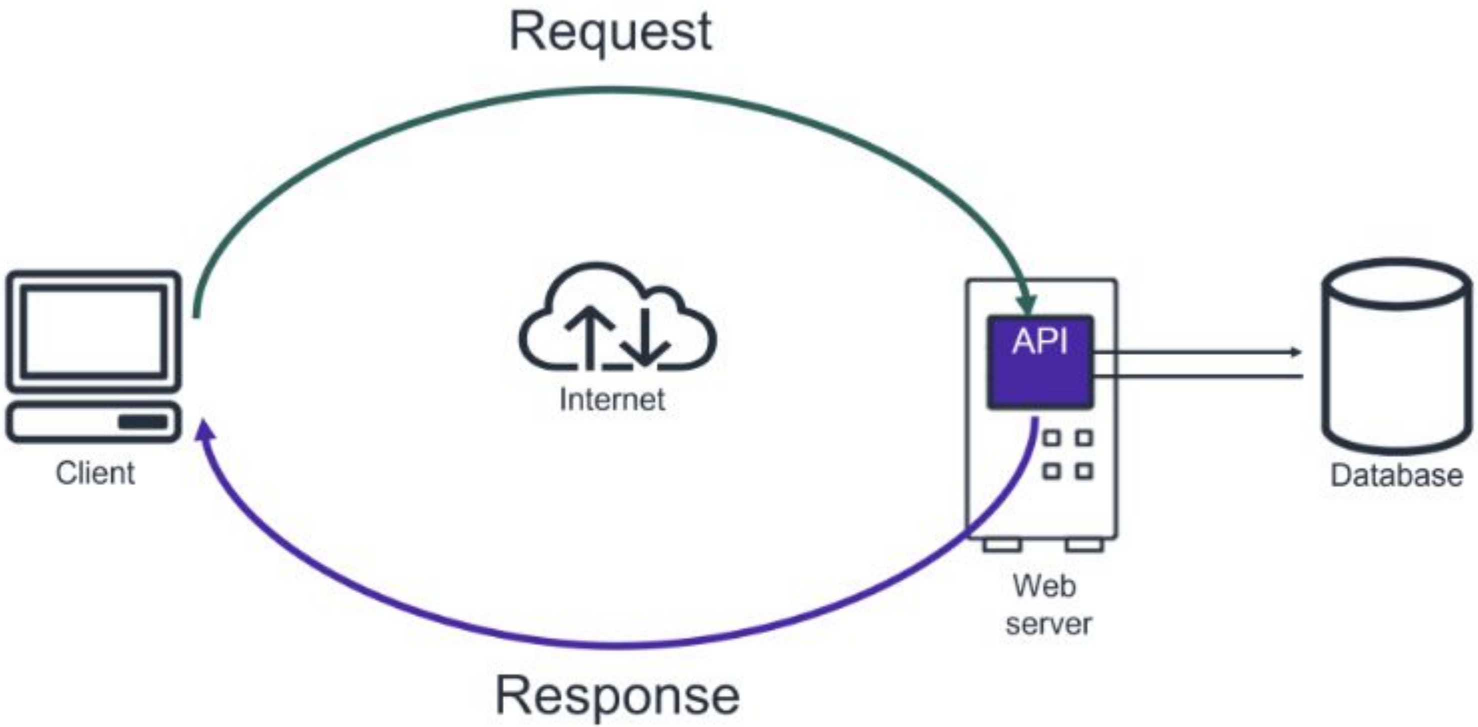
Reading

- AWS Cloud Developing - Module 6

REST APIs Overview

- **API (Application Programming Interface)** - hides app implementation details and exposes only allowed methods & data
- API requests can use a variety of protocols (e.g. SOAP, WebSockets, HTTP)
- **REST (Representational State Transfer)** - Architectural style that defines client request structure
    - **Uniform interface** - all requests for the same resource look the same
    - **Client-server decoupling** - client can only interact with the server via URI
    - **Stateless** - request contains all info needed for processing
    - **Cacheability** - resources should be cacheable on client or server. Server response must specify whether response can be cached.
    - **Layered system** - neither client nor server can tell whether it communicates with the end application or an intermediary.

A typical application



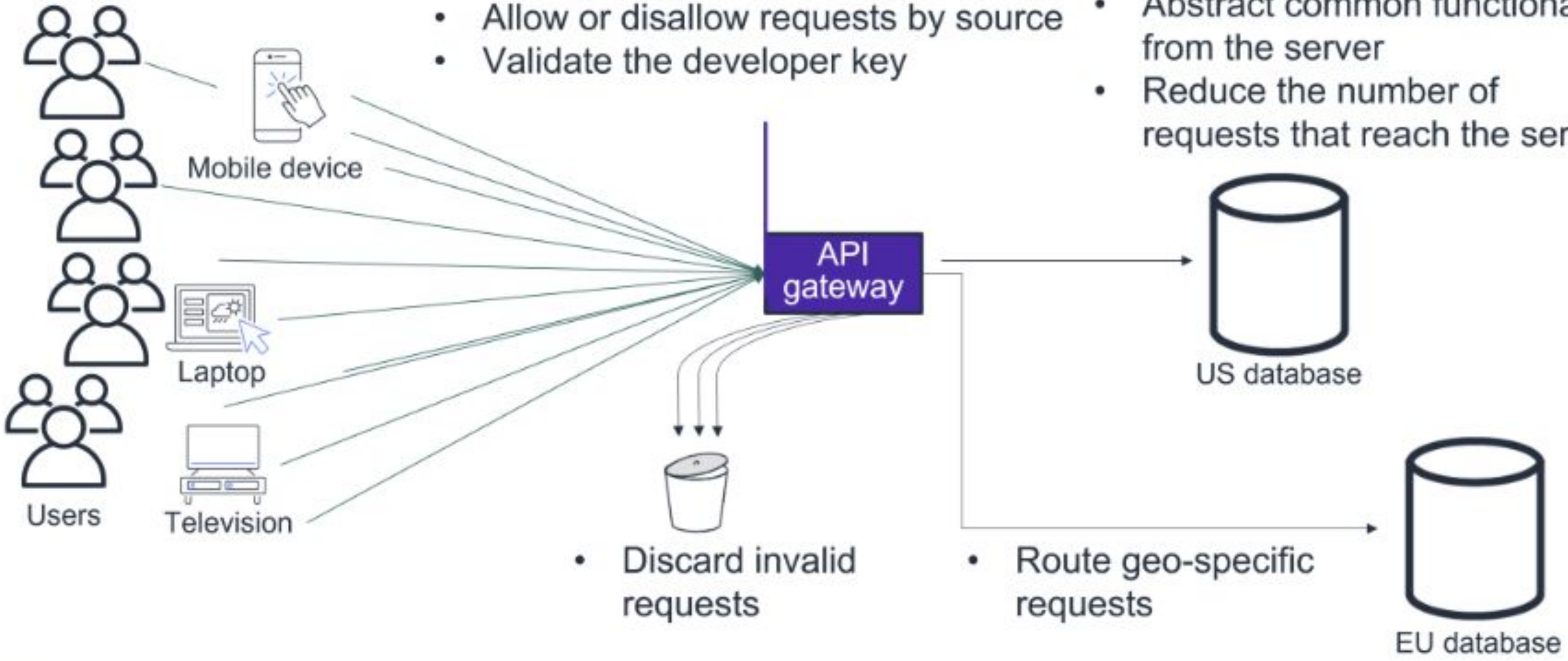
Amazon API Gateway

- Fully managed service to create, publish, maintain, monitor, and secure APIs
- Proxy that handles common request tasks to offload server:
  - Rate limit requests
  - Ensure request has required credentials
  - Limit access based on language or geographical region
  - Modify request data as needed by destination application
  - Allow client interface w/ AWS services not directly accessible by HTTP request
- Can support RESTful and WebSockets APIs
- Can be used for mock endpoints to enable prototyping

An API gateway is a proxy

- Limit the request rate
- Allow or disallow requests by source
- Validate the developer key

- Abstract common functionality from the server
- Reduce the number of requests that reach the server



- Discard invalid requests

- Route geo-specific requests

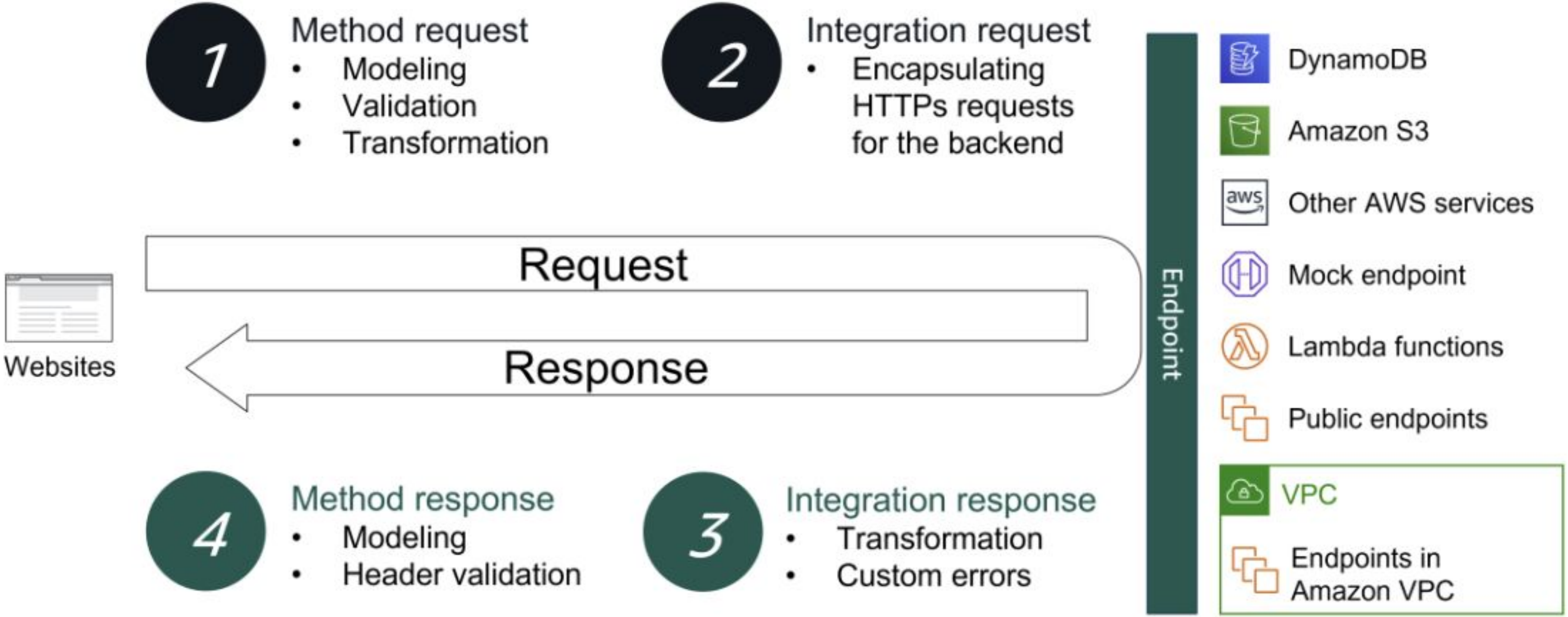
Types of APIs in API Gateway

- **REST API**
  - gives developer full control over request / response handling
  - Has option of an edge=optimized endpoint backed by CloudFront with built-in DDoS protection
- **HTTP API** - low cost, low latency option for simple proxy functionality
- **WebSockets** - real-time, two-way communication. Allows for small, efficient message payloads after initial setup

Creating an API

- APIs can be created & invoked via API Gateway console or AWS CLI
- Must specify **name**, **protocol**, & **target** service (for REST API)
- Can create specific routes with placeholder for dynamic values
- For WebSocket API, must specify **route-select-expression**
- Can import an OpenAPI or Swagger definition file
- Can export SDK for a custom-defined REST API for use with client code

Example integration flow



1 Method request
- Modeling
- Validation
- Transformation

2 Integration request
- Encapsulating HTTPs requests for the backend

3 Integration response
- Transformation
- Custom errors

4 Method response
- Modeling
- Header validation

Integrating with an API

- API Gateway receives a client request and:
  - may transform request before passing **integration request** to target service
  - Wraps **Lambda** requests with necessary metadata
  - May transform **integration response** from server before sending to client
- Response from target service must be in format supported by API Gateway
- First-class integrations connect an HTTP APU route to an AWS service API (e.g. SQS, SNS, Step Functions, etc.)

Deploying an API

- Create an api deployment
- Associate with a **stage** to manage & optimize a deployment
    - different stages can connect to different versions of a backend (e.g. dev, prod)
    - Each stage can use different stage variables
    - Can use stages for **canary** deployments
-

Controlling API access

API Gateway

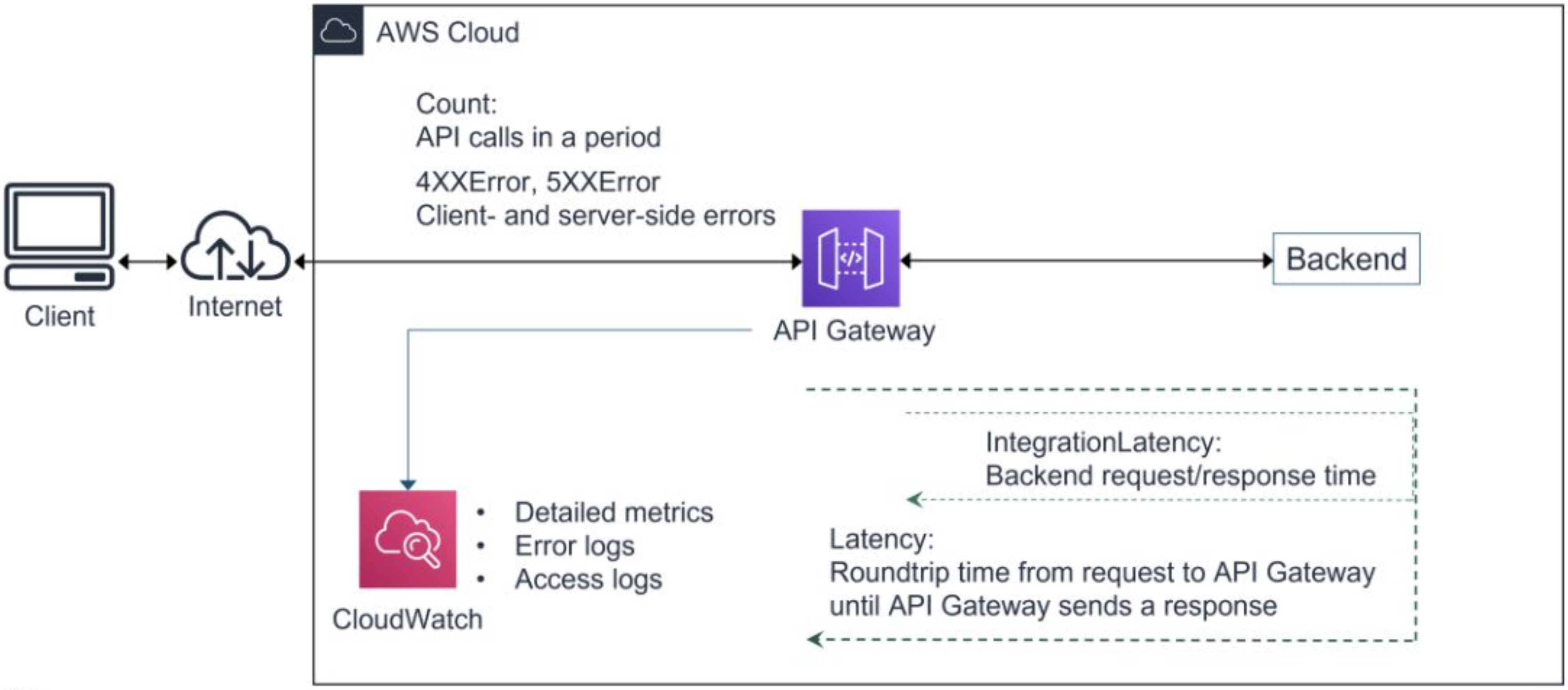
- can apply IAM resource policies on REST APIs to control endpoint access
- can generate SSL certificates for custom domains to validate client requests
- can act as a proxy to handle CORS preflight options requests
- Can enforce rate limiting with region-wide and per-API, per-method, or per-client limits
- Can authorize requesters via IAM, JSON Web Token (JWT), Lambda

AWS WAF (Web Application Firewall) - service to protect APIs against common web exploits using managed rules

Monitoring an API

- **AWS CloudWatch** can collect & process raw data from API Gateway for near real-time metrics:
  - Count - total number of API calls
  - Integration Latency - responsiveness of backend
  - Latency - Time between request and response
  - HTTP 400 & 500 errors

API Gateway default metrics and logging options for REST APIs



Count:
API calls in a period

4XXError, 5XXError
Client- and server-side errors

- Detailed metrics
- Error logs
- Access logs

IntegrationLatency:
Backend request/response time

Latency:
Roundtrip time from request to API Gateway until API Gateway sends a response