AWS re:Invent

SVS212-R

I didn’t know Amazon API Gateway did that

Eric Johnson

Senior Developer Advocate – Serverless

Amazon Web Services

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Who am I?

- Eric Johnson, @edjgeek
- Sr. Developer Advocate – Serverless, AWS
- Serverless/tooling/automation geek
- Software architect/solutions architect
- Music lover
- Pizza/Diet Dr. Pepper fanatic



What is an API, anyway?

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

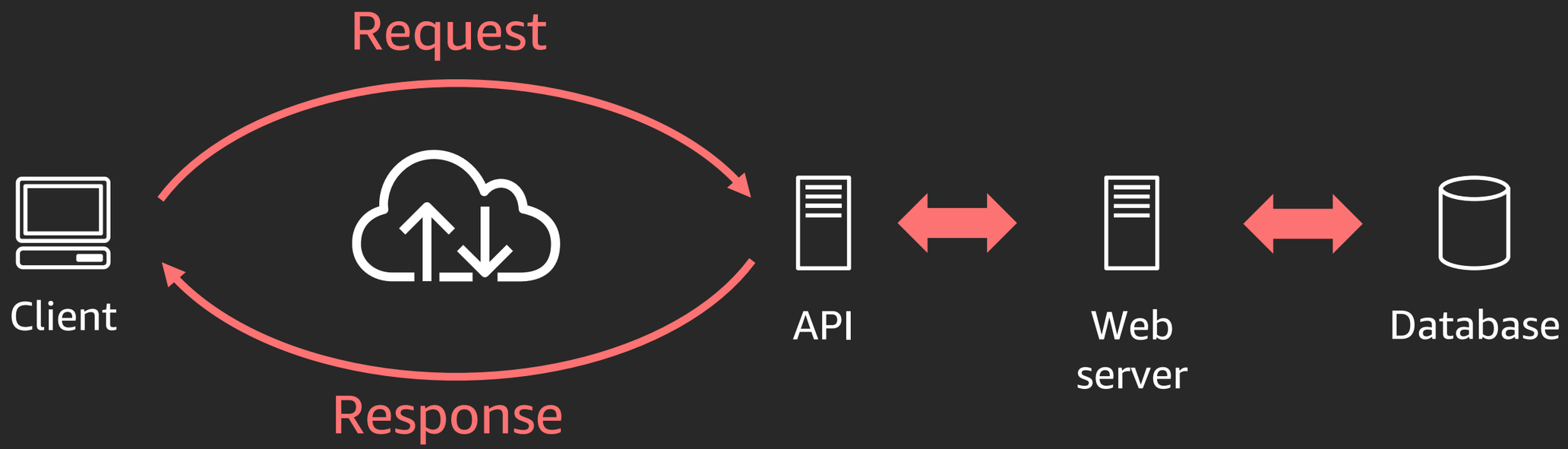
"In building applications, an API simplifies programming by abstracting the underlying implementation and only exposing objects or actions the developer needs."

"Application Programming Interface," Wikipedia

https://en.wikipedia.org/wiki/Application_programming_interface

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Application programming interface (API)

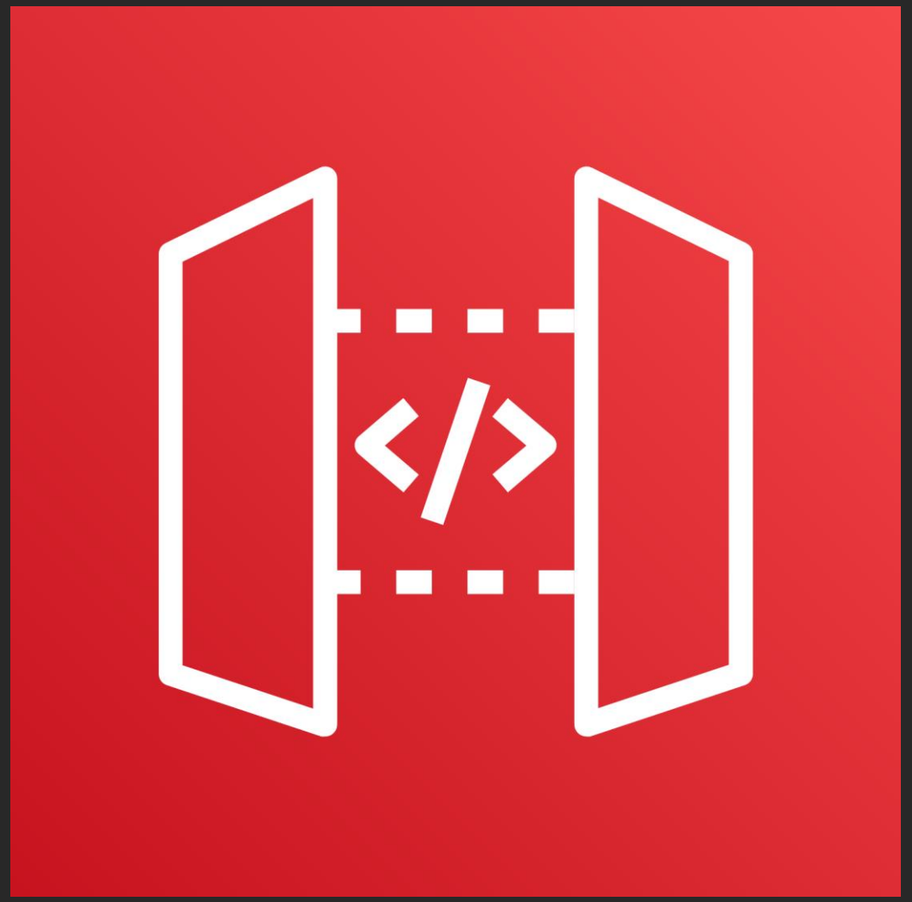


Web services offer APIs for developers to use, for example:

- Social networks: Facebook, Twitter, and so on
- Payment processing: Amazon Pay, PayPal, and so on

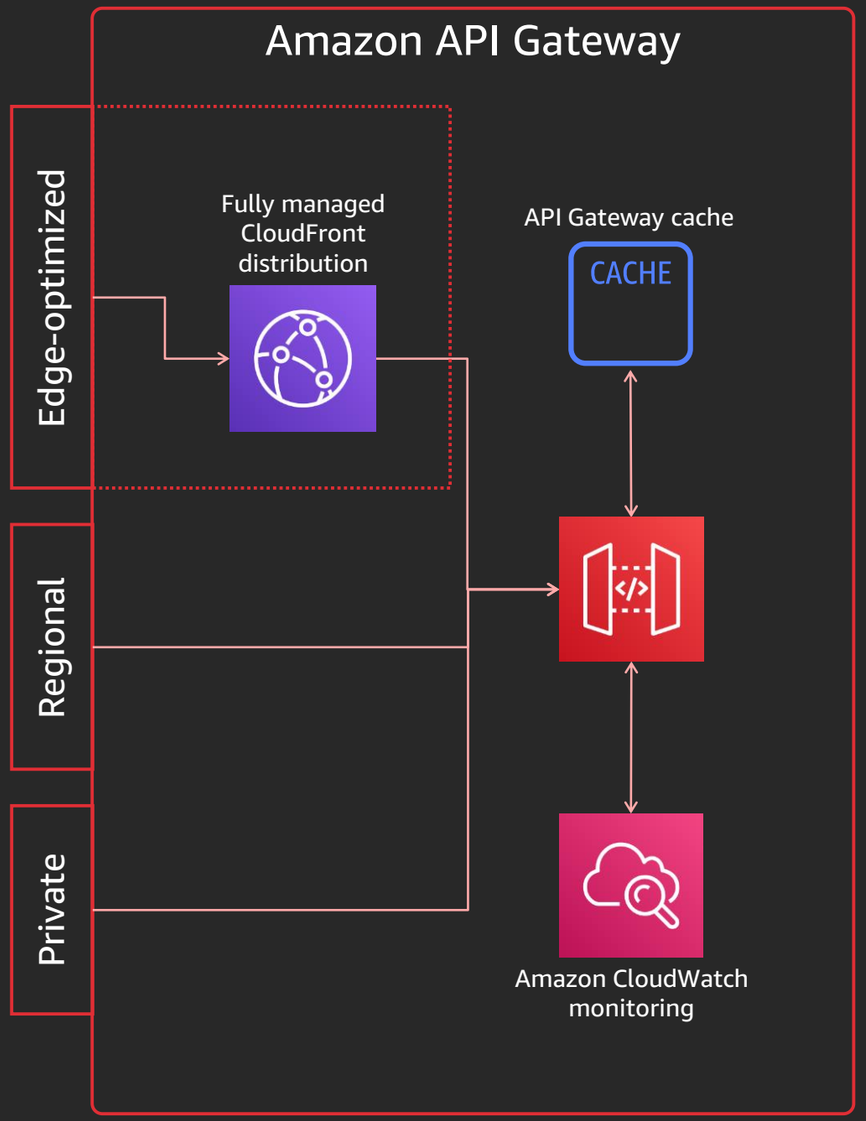
Amazon API Gateway

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale



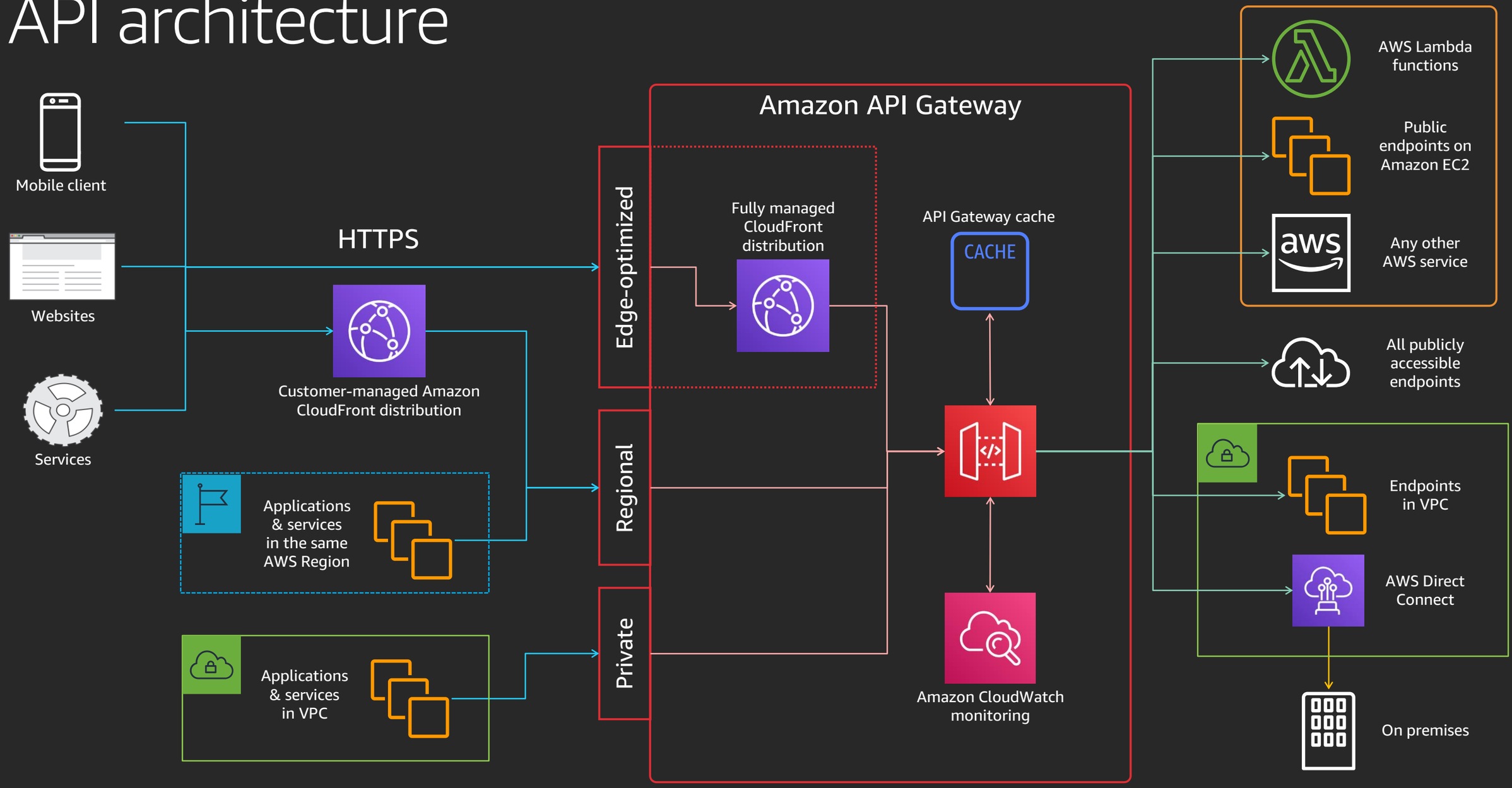
Types of APIs available

- **Edge-optimized**
  - Utilizes Amazon CloudFront to reduce TLS connection overhead (reduces roundtrip time)
  - Designed for a globally distributed set of clients
- **Private**
  - Only accessible from within a VPC (and networks connected to a VPC)
  - Designed for building APIs used internally or by private microservices

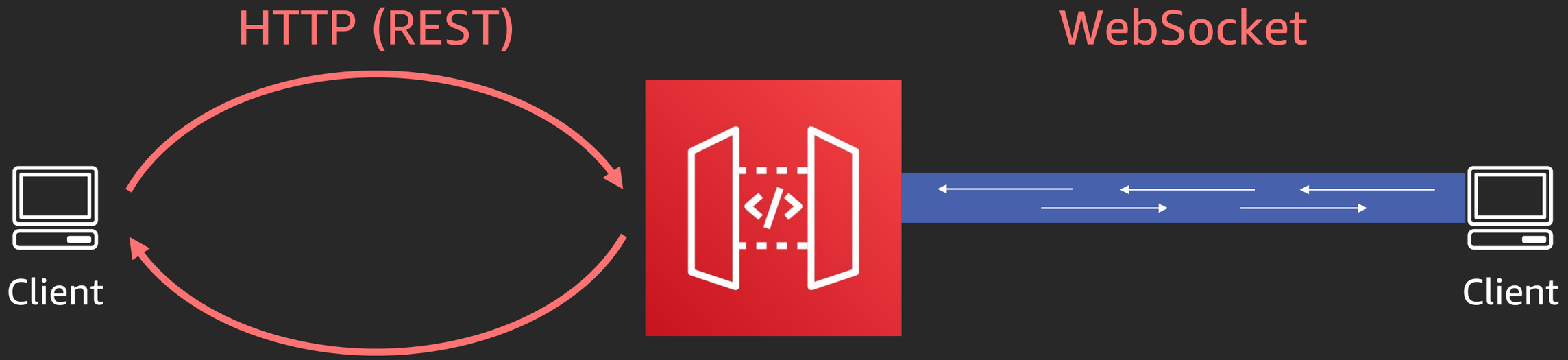


- **Regional**
  - Recommended API type for general use cases
  - Designed for building APIs for clients in the same region

API architecture



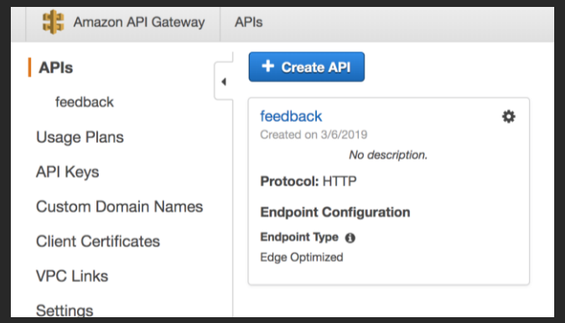
Supported protocols



- Request/response
- HTTP methods such as GET and POST
- Short-lived communication
- Stateless

- Serverless WebSocket
- 2-way communication channel
- Long-lived communication
- Stateful

API Gateway management



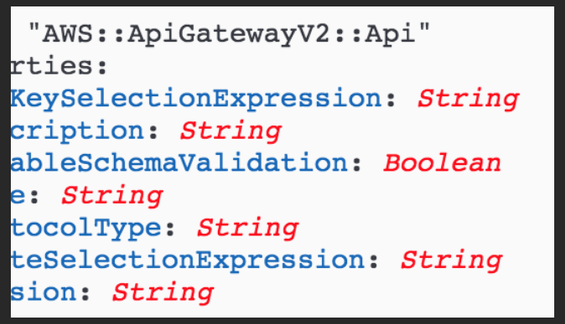
AWS Management Console



AWS Command Line Interface (AWS CLI)



AWS Serverless Application Model (AWS SAM)



AWS CloudFormation



Swagger/OpenAPI



AWS Cloud Development Kit (AWS CDK)

OpenAPI image source: https://swagger.io/blog/news/whats-new-in-openapi-3-0/

Integrating backend services

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Integration types

Lambda function

Connect via proxy or direct integration

HTTP

Connect to an HTTP(S) endpoint inside or outside of AWS

Mock

Respond to requests without a backend service (OPTIONS)

AWS Service

Connect to 100+ service endpoints inside of AWS, such as Amazon DynamoDB or Amazon Kinesis

VPC Link

Connect to a VPC link that allows access to resources in a VPC via Elastic Load Balancing (a Network Load Balancer)

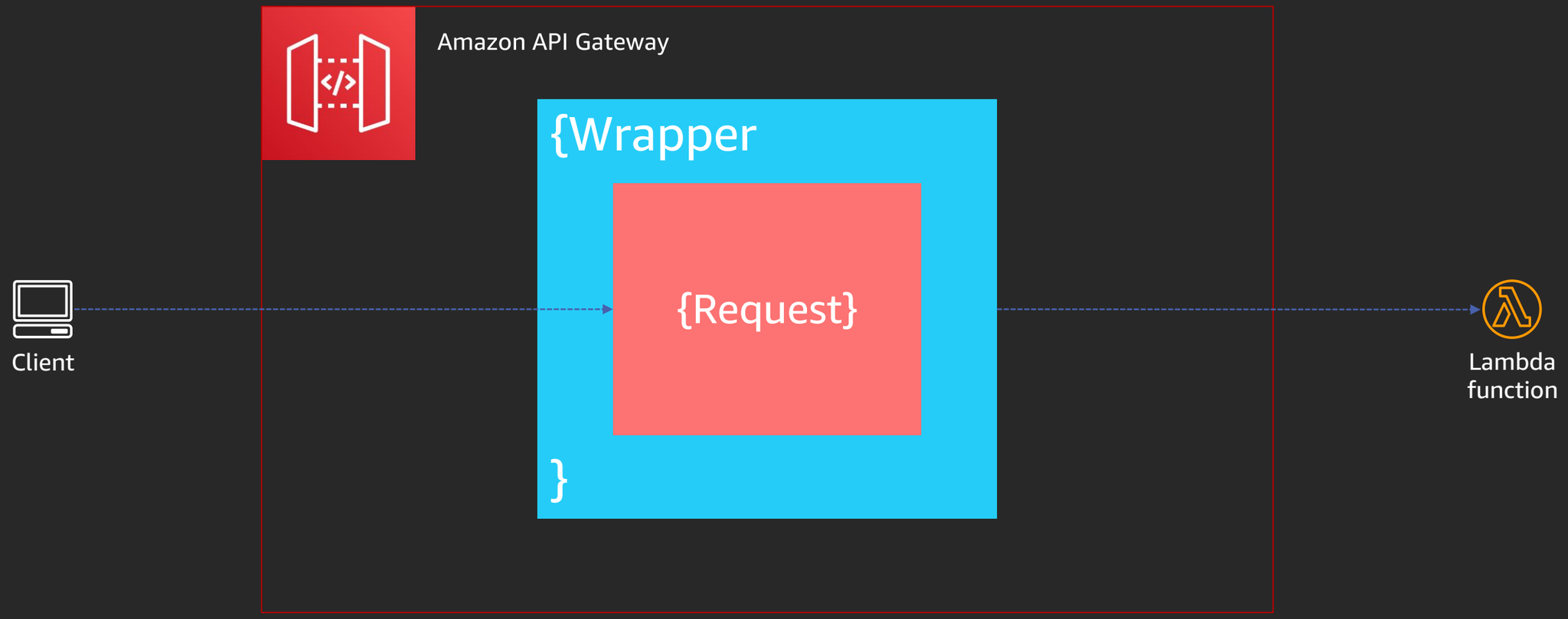
Lambda function integration

Proxy?

Integration?

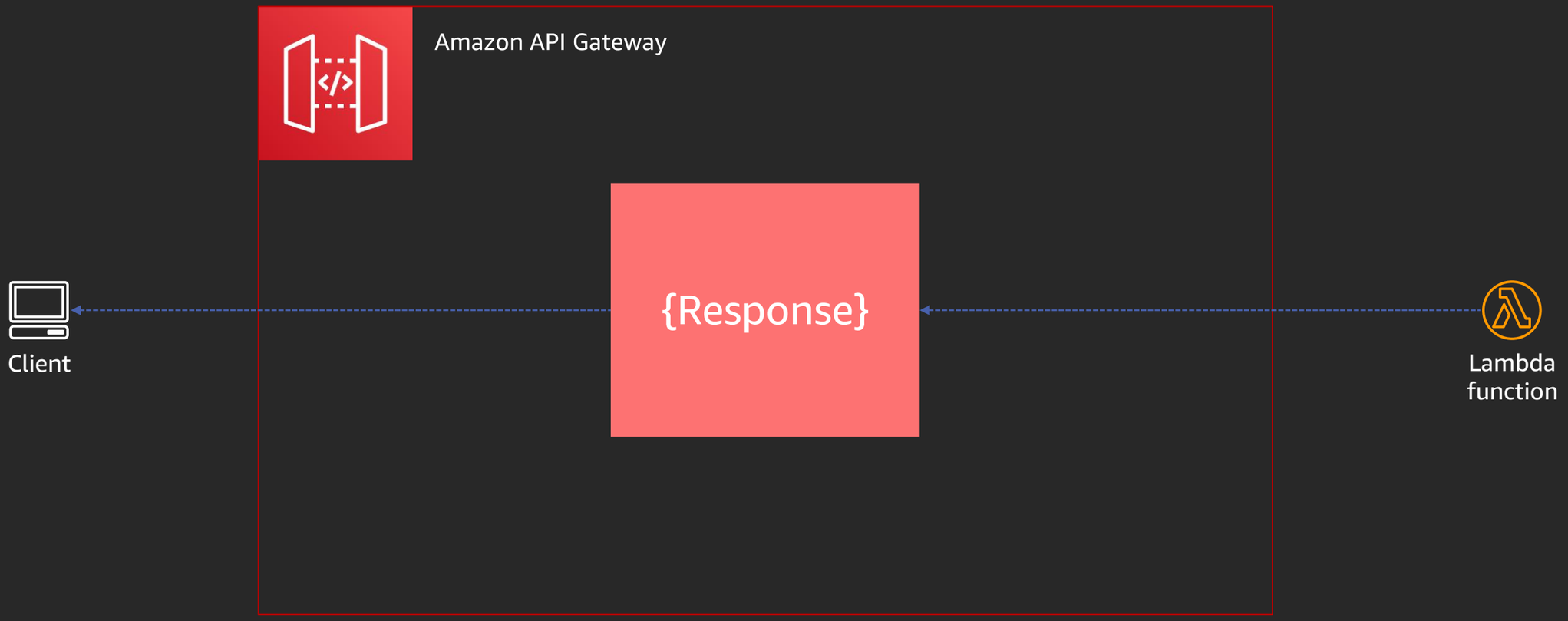
Huh?

Lambda function via proxy



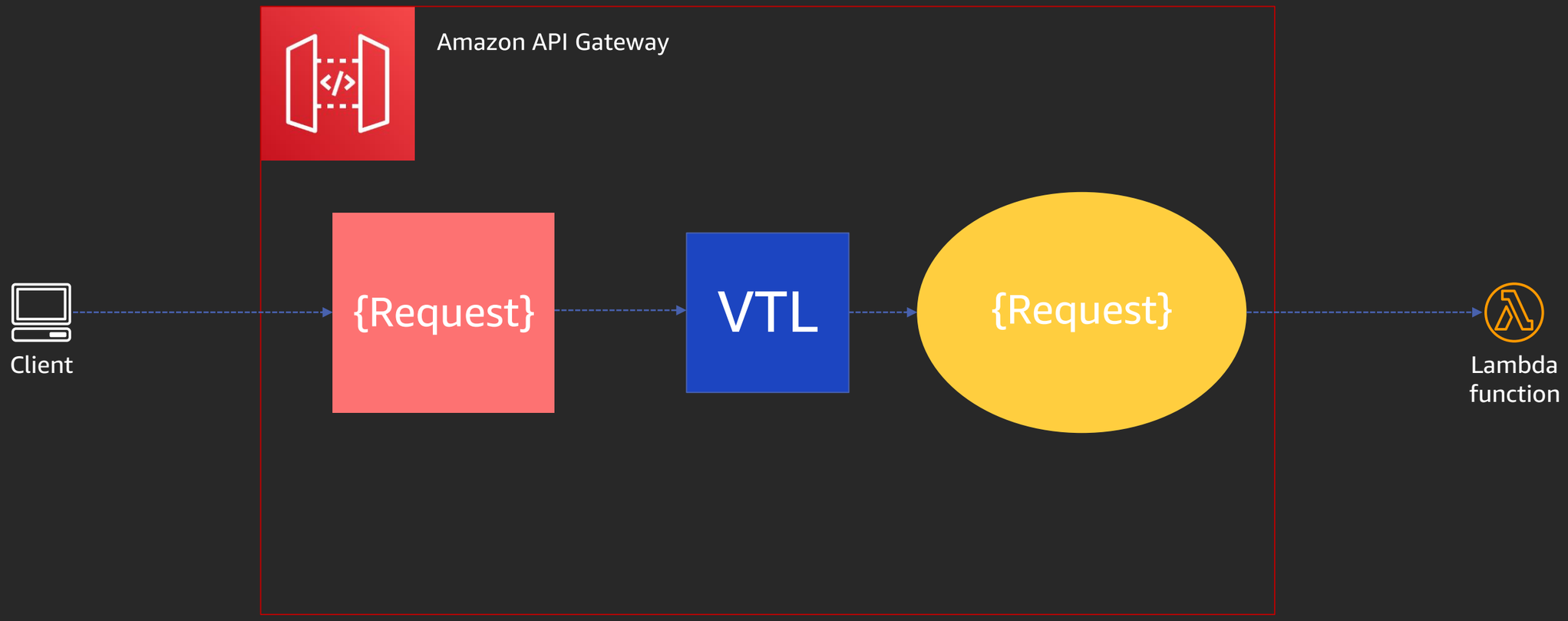
Requests are wrapped with metadata and passed to the backend

Lambda function via proxy



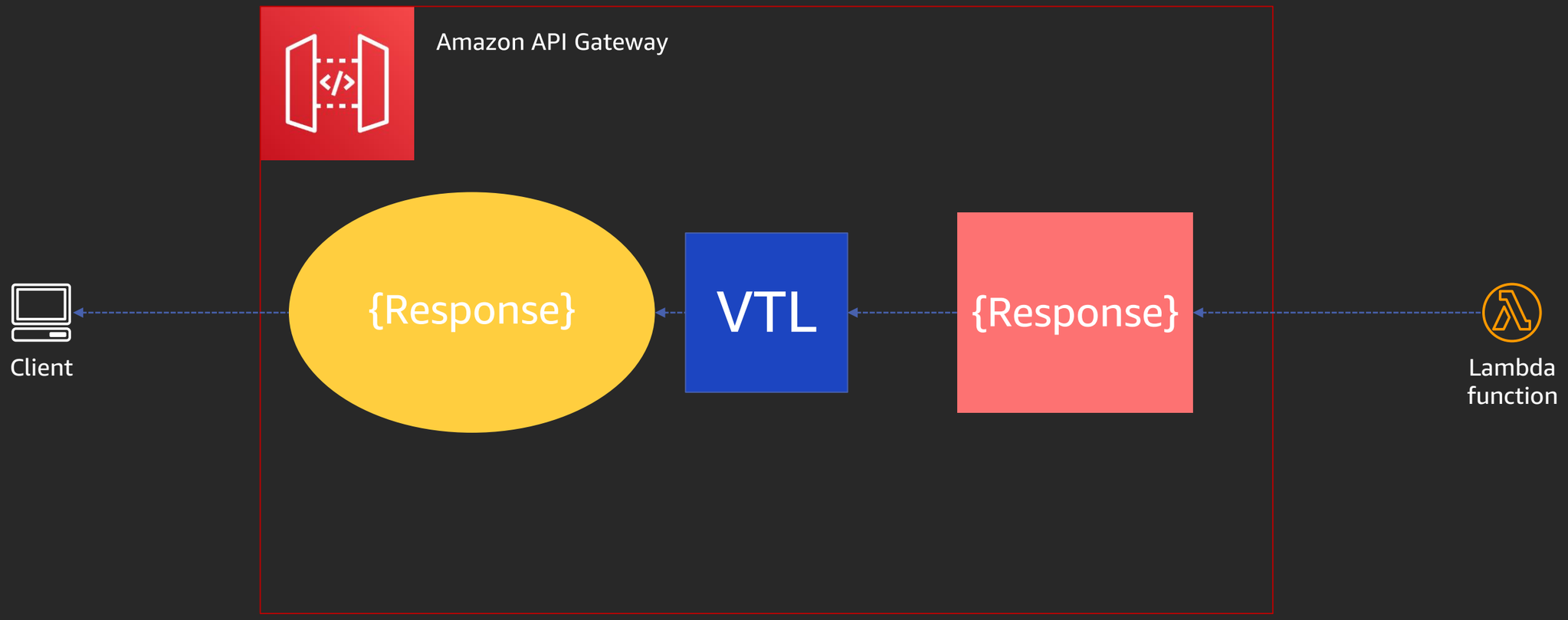
Responses pass, untouched, to client

Lambda function via direct integration



By using VTL, requests can be modified by API Gateway

Lambda function via direct integration



By using VTL, responses can be modified by API Gateway

VTL example

Before VTL

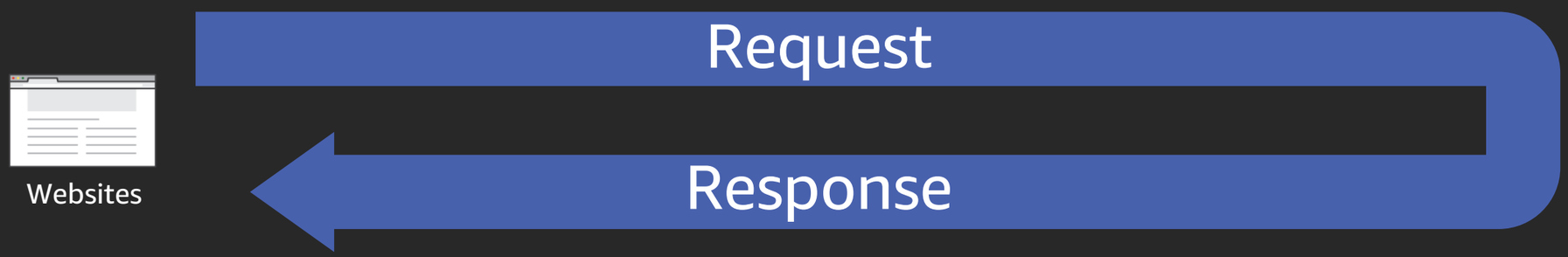
```
{
  “firstName”: “Fred”,
  “lastName”: “Jones”,
  “phone”: “555-555-5555”,
  “city”: “Miami”,
  “state”: “Florida”
  “favoritePizza”: “pineapple”
}
```



After VTL

```
{
  “name”: “Fred Jones”,
  “phone”: “555-555-5555”,
  “address”:{
    “city”: “Miami”,
    “state”: “Florida”
  }
  “favoritePizza”: “peperoni”
}
```

Integration flow



Integration flow

1

Method request

- Modeling
- Validation
- Transformation



Websites

Request

Response

Integration flow

1 **Method request**
- Modeling
- Validation
- Transformation

2 **Integration request**



Websites

Request

Response



Amazon S3



Amazon DynamoDB



AWS Lambda





Other AWS & on-premises services

Integration flow

1 Method request
- Modeling
- Validation
- Transformation

2 Integration request



Websites

Request

Response



Amazon S3



Amazon DynamoDB



AWS Lambda





Other AWS & on-premises services

4 Integration response

Integration flow

1 **Method request**
- Modeling
- Validation
- Transformation

2 **Integration request**


Websites

Request

Response


Amazon S3


Amazon DynamoDB


AWS Lambda




Other AWS & on-premises services

3 **Method response**
- Transformation
- Custom errors

4 **Integration response**

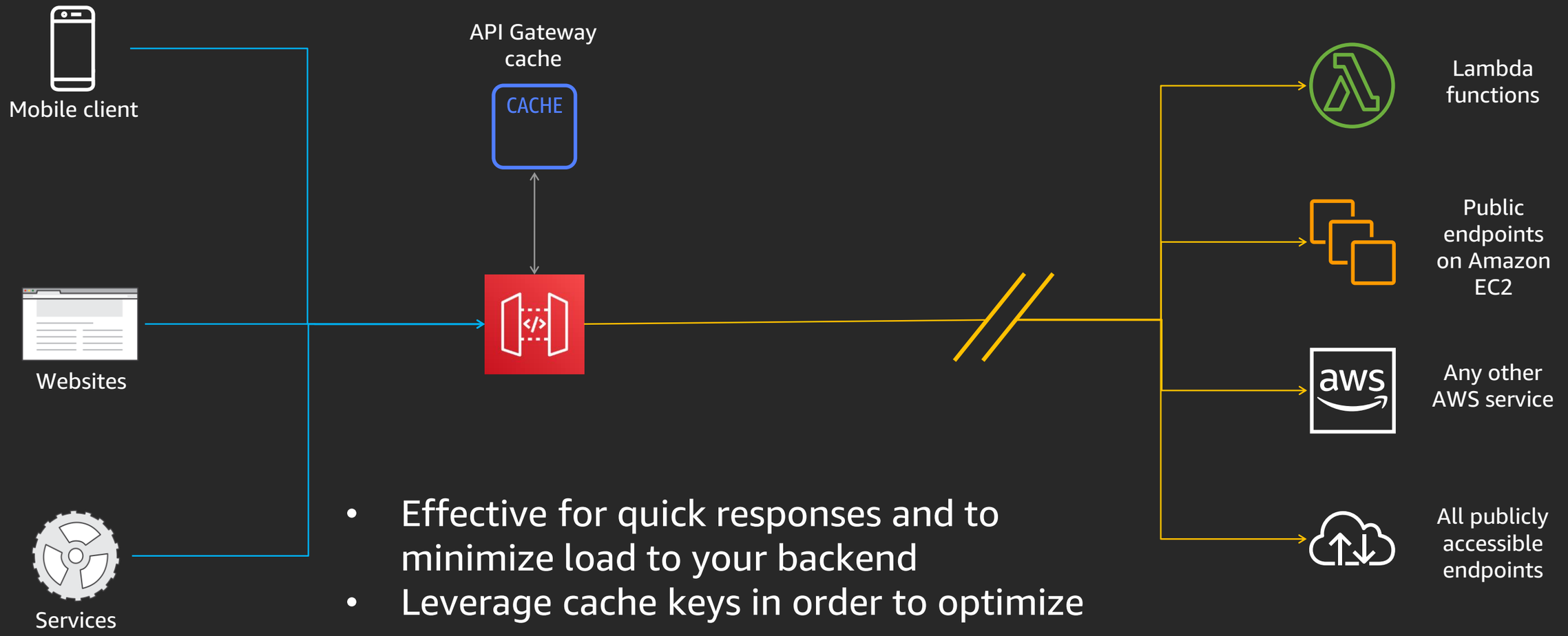
Amazon API Gateway features

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Authorization

- Open
  - No authentication or authorization
- IAM permissions
  - Use IAM policies and AWS credentials to grant access
- Amazon Cognito authorizer
  - Amazon Cognito is a managed user directory for authentication
  - Connect to the Amazon Cognito User Pool and, with OAuth, scope to enable authorization
- Lambda authorizers
  - Use Lambda to validate a bearer token (OAuth or SAML, for example), or request parameters and grant access

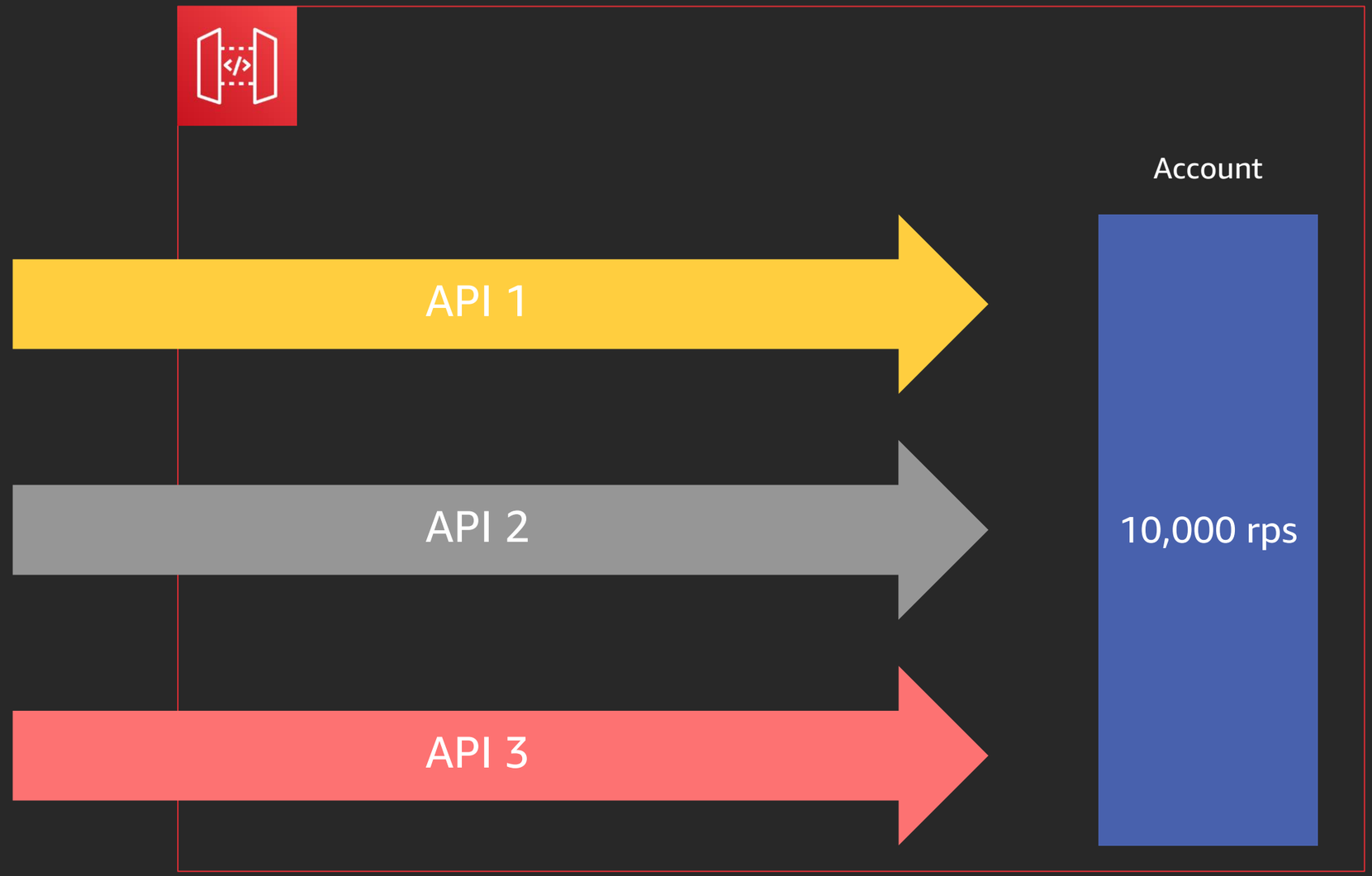
Caching



- Effective for quick responses and to minimize load to your backend
- Leverage cache keys in order to optimize response
  - Path, headers, query strings
- Can be set up by stage or method

Throttling

All APIs share a region-wide throttling of 10k requests per second*

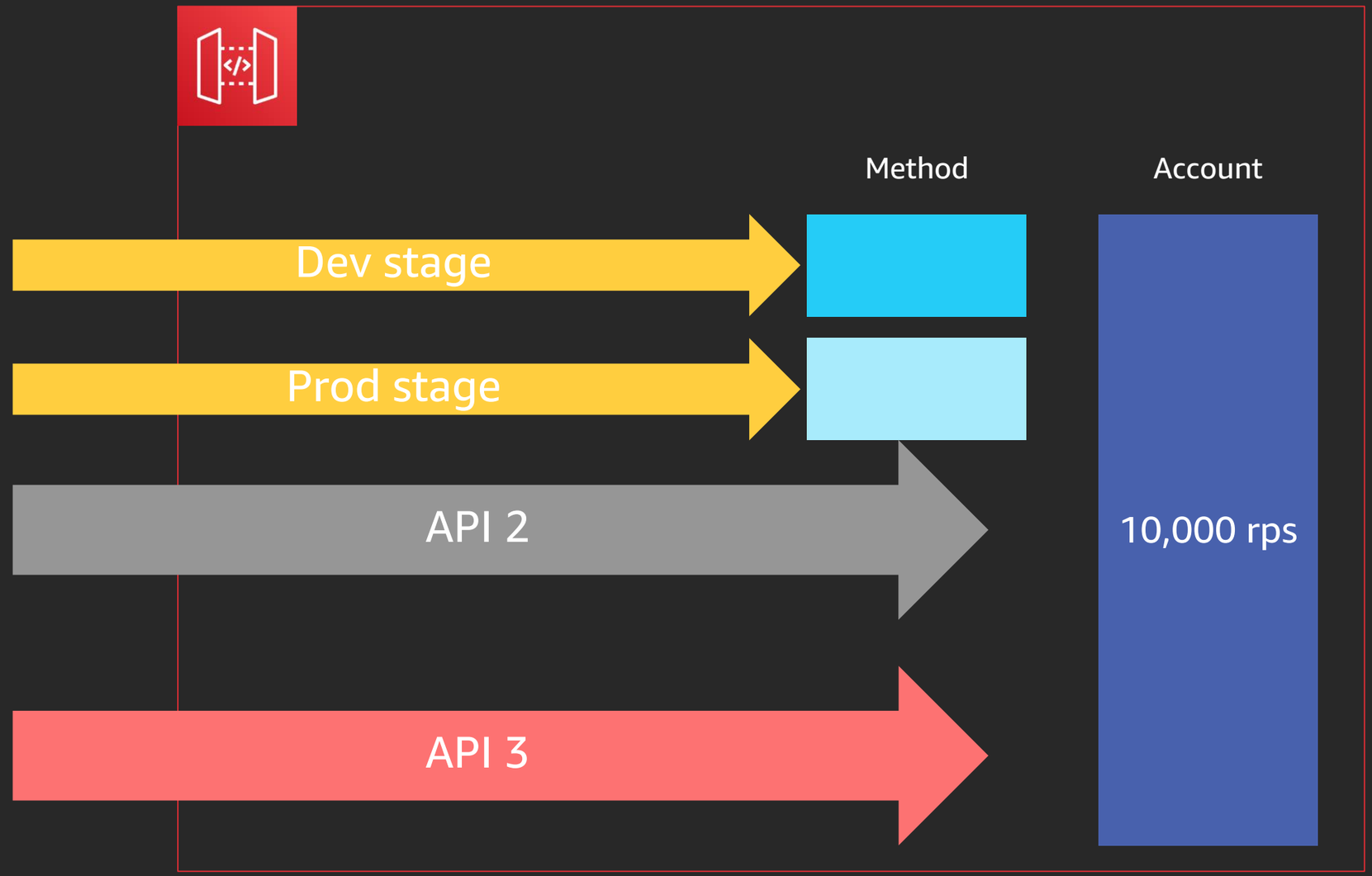


*A soft limit that can be raised upon request

Throttling

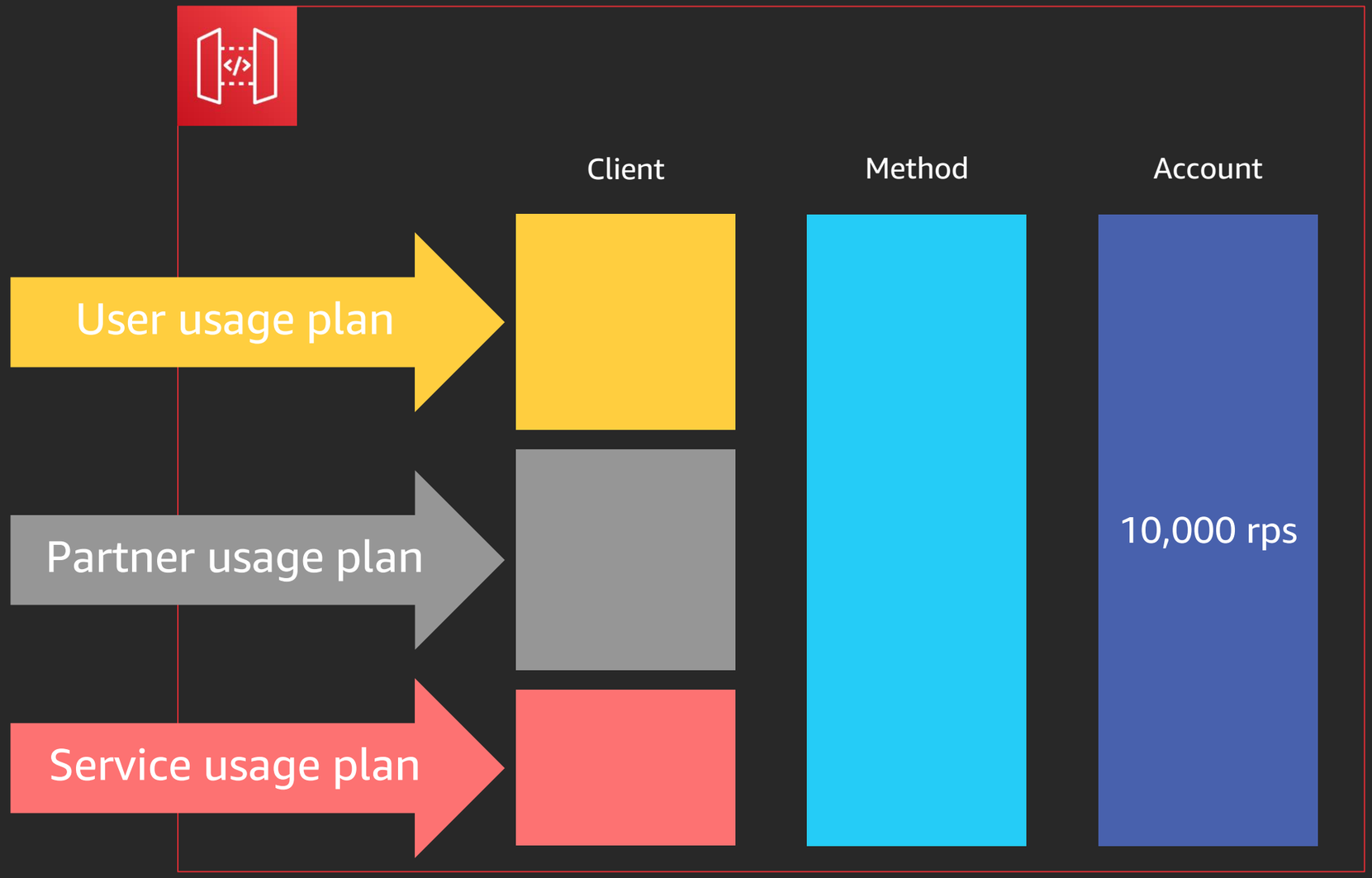
Method-level overrides can be added on API stages

Note: cannot override the account-level rates



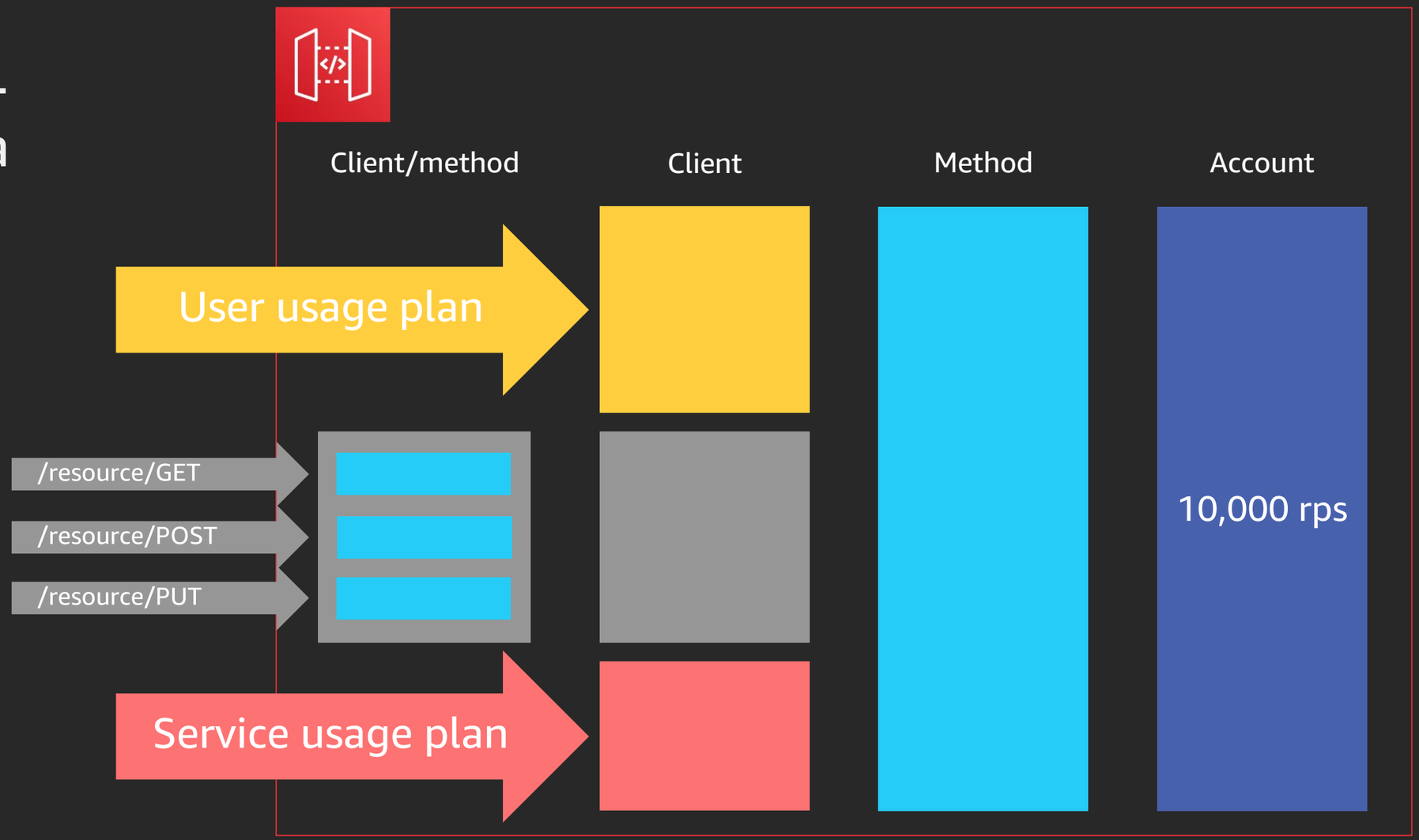
Throttling

Configure API-level or stage-level throttling through a usage plan



Throttling

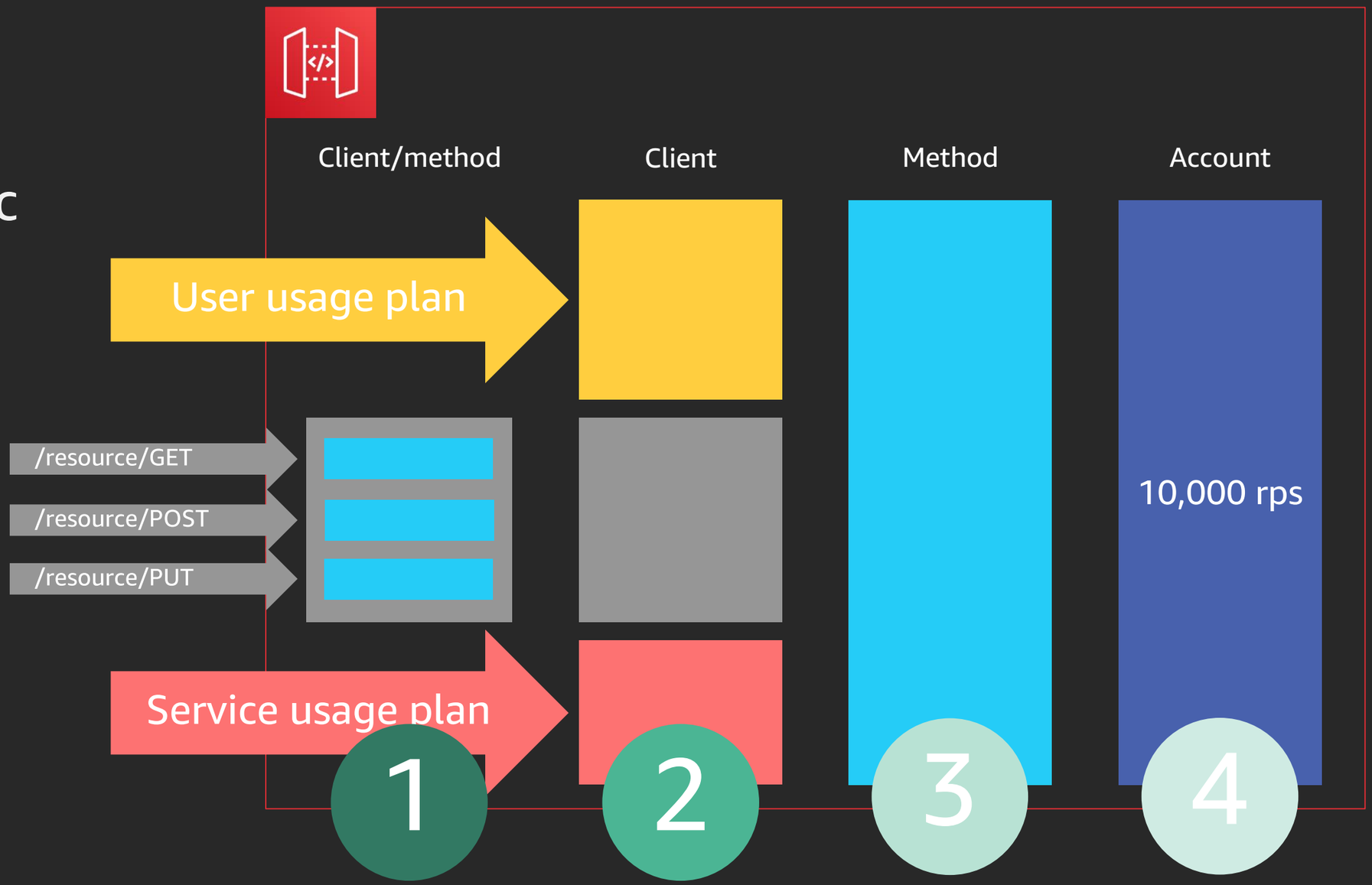
Configure method-level throttling in a usage plan



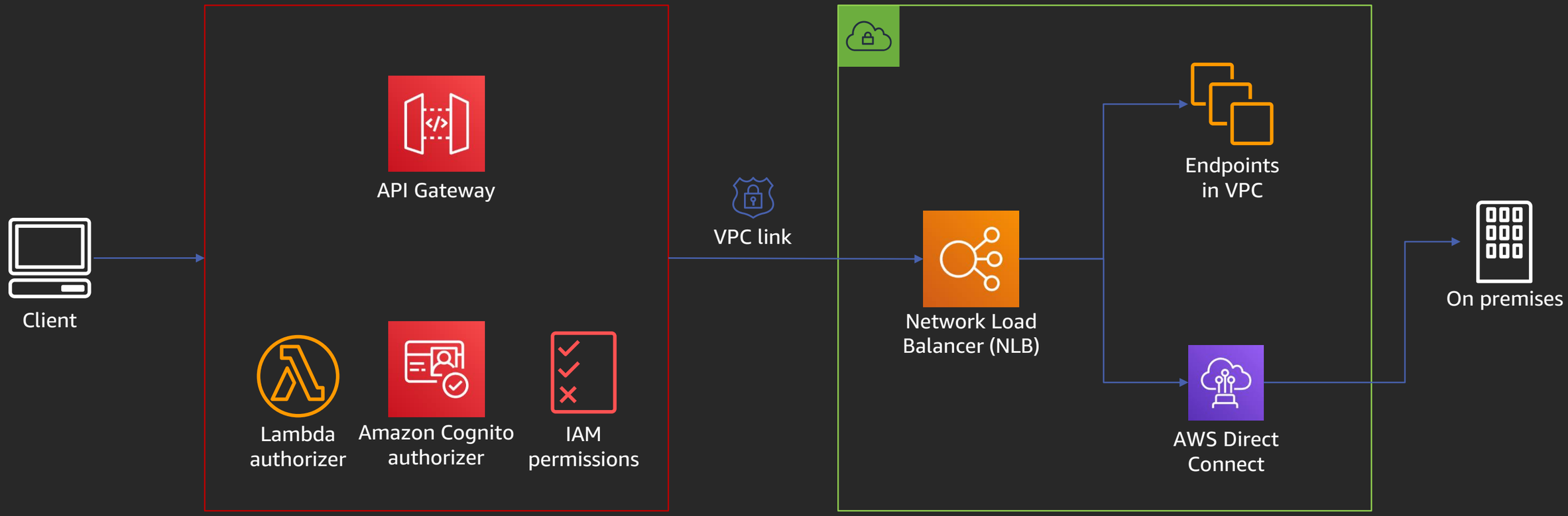
Throttling

Throttling-related settings are applied in a specific order

Note: Account RPS settings cannot be overridden in client or method settings but can be increased through a limit increase request

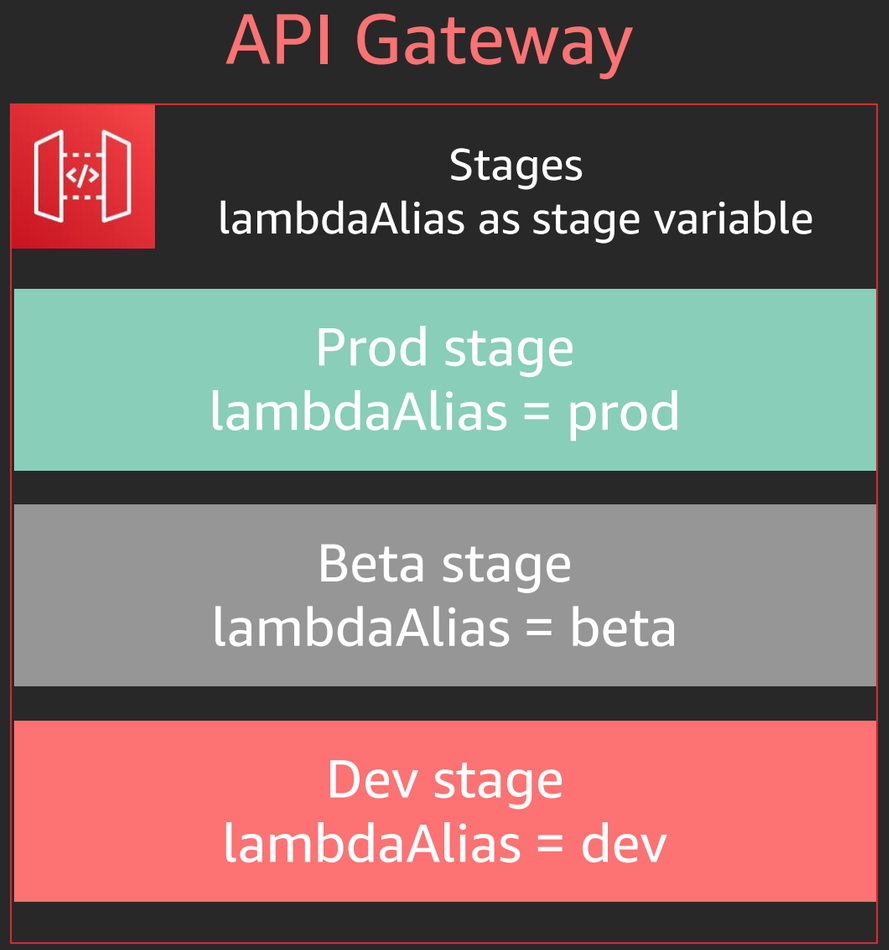


VPC links (private integrations)



Allows resources outside of a VPC to connect to resources inside a VPC

Stages



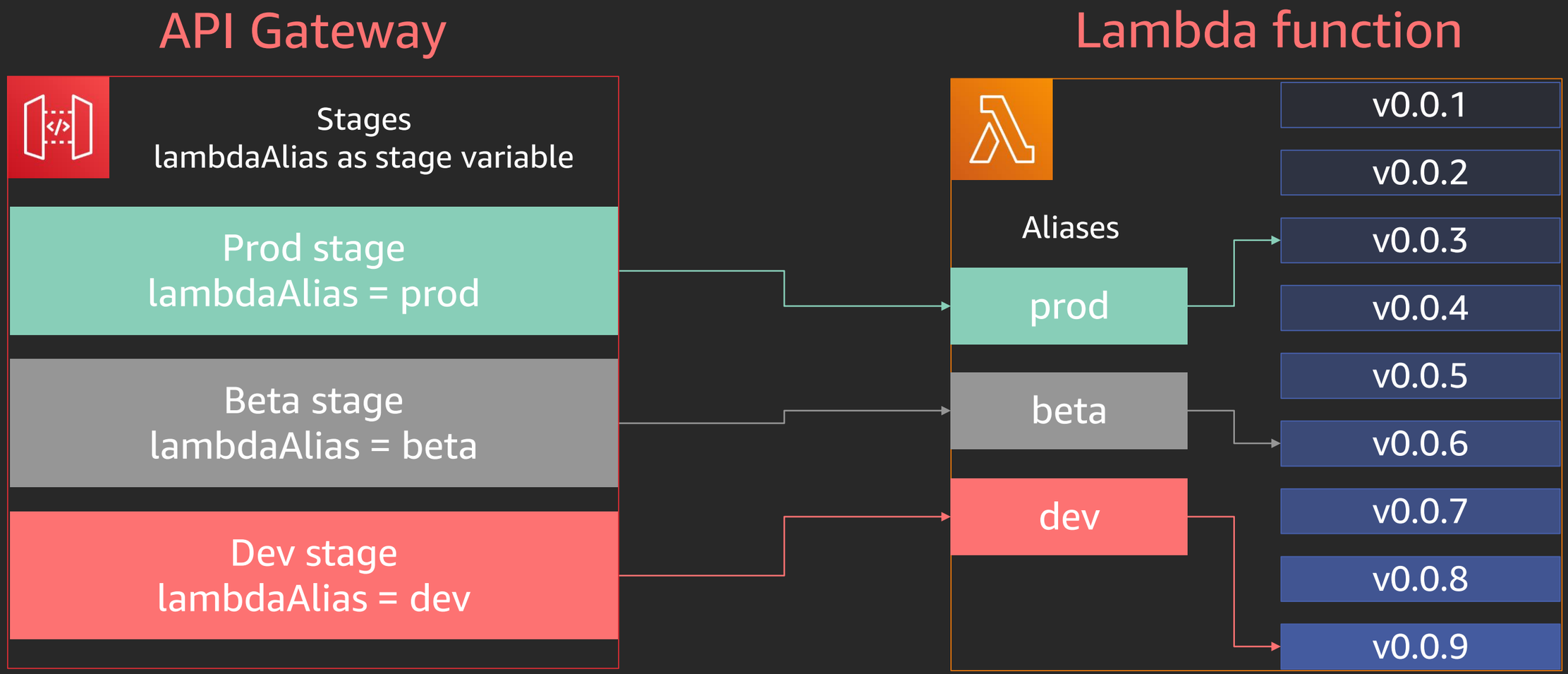
API endpoints can support multiple stages

= http://my.api-endpoint12345.com/prod/

= http://my.api-endpoint12345.com/beta/

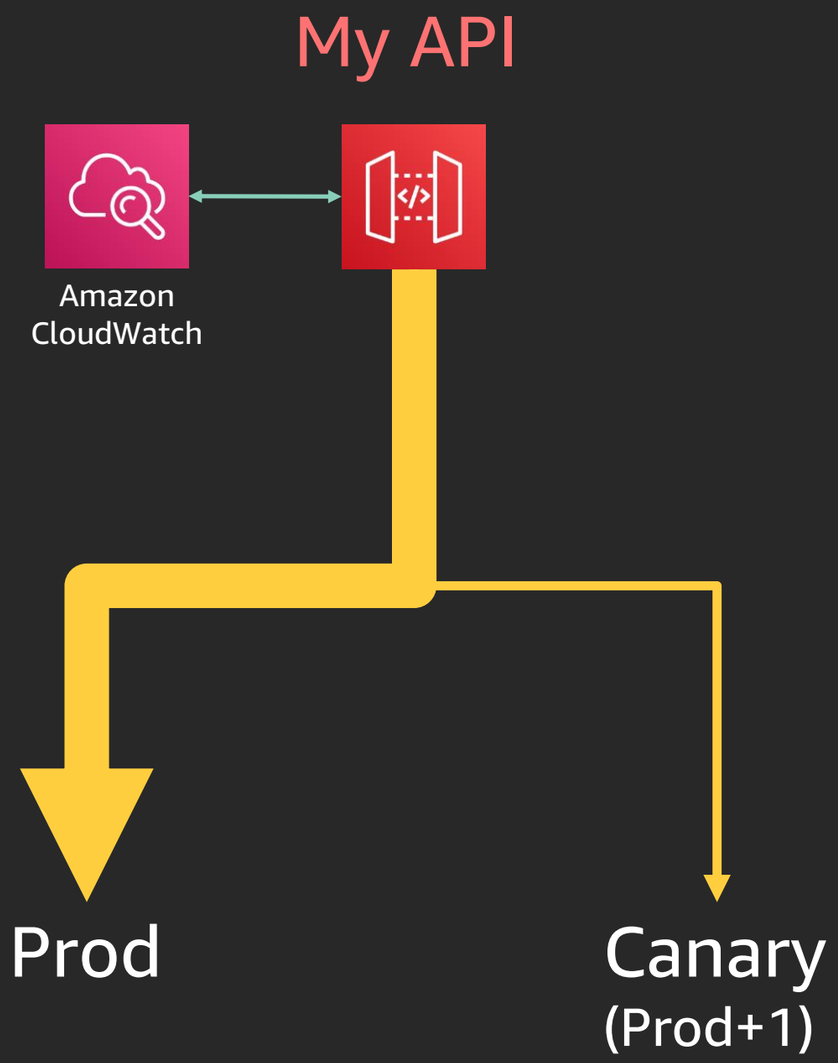
= http://my.api-endpoint12345.com/dev/

Stages



Stage variables can be used to dynamically select Lambda aliases

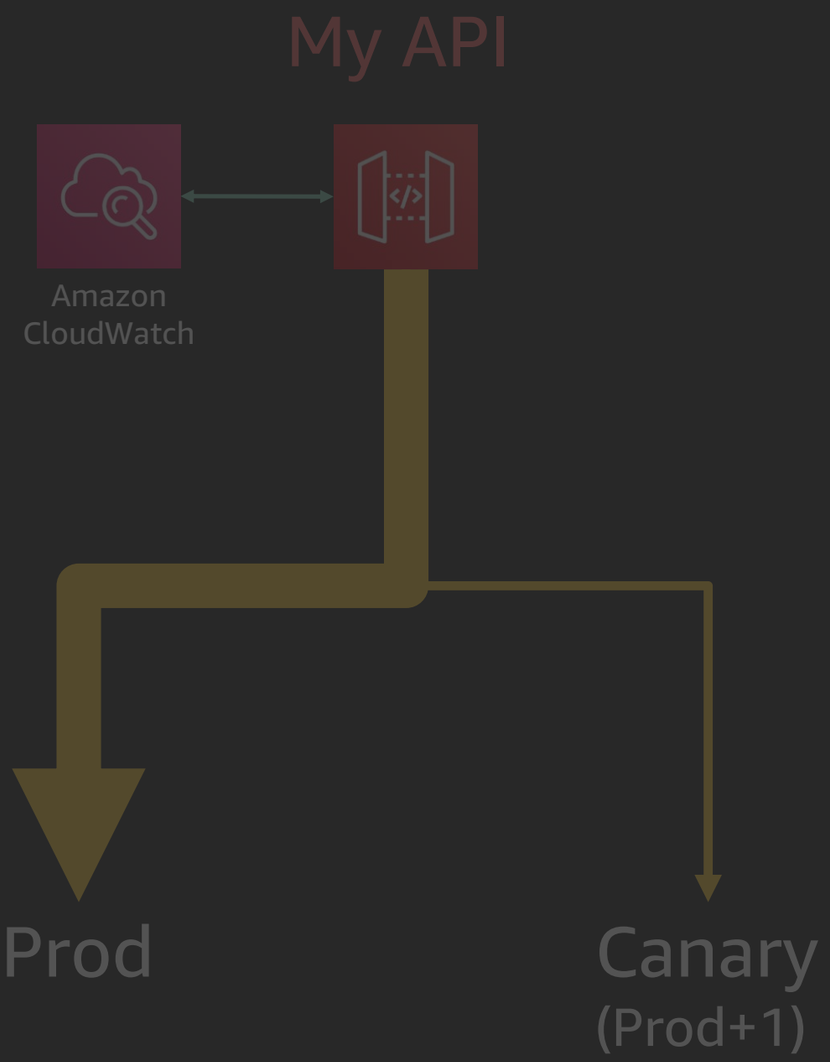
Canary releases

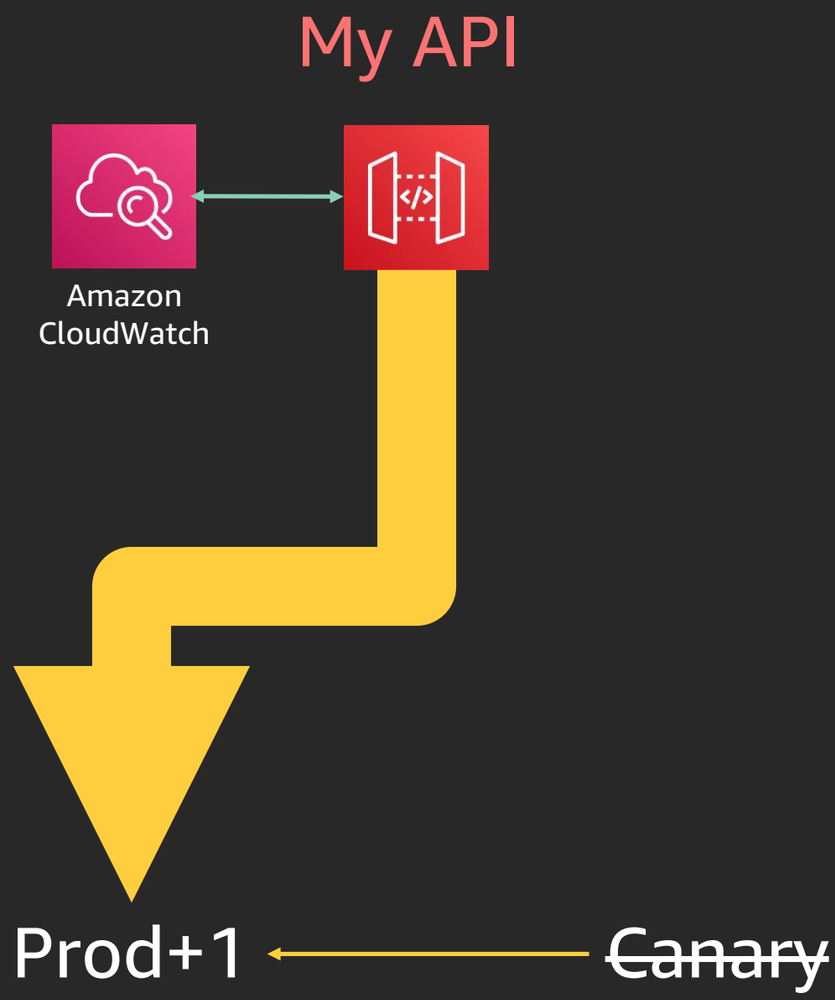


API deployments to limited traffic for a designated amount of time

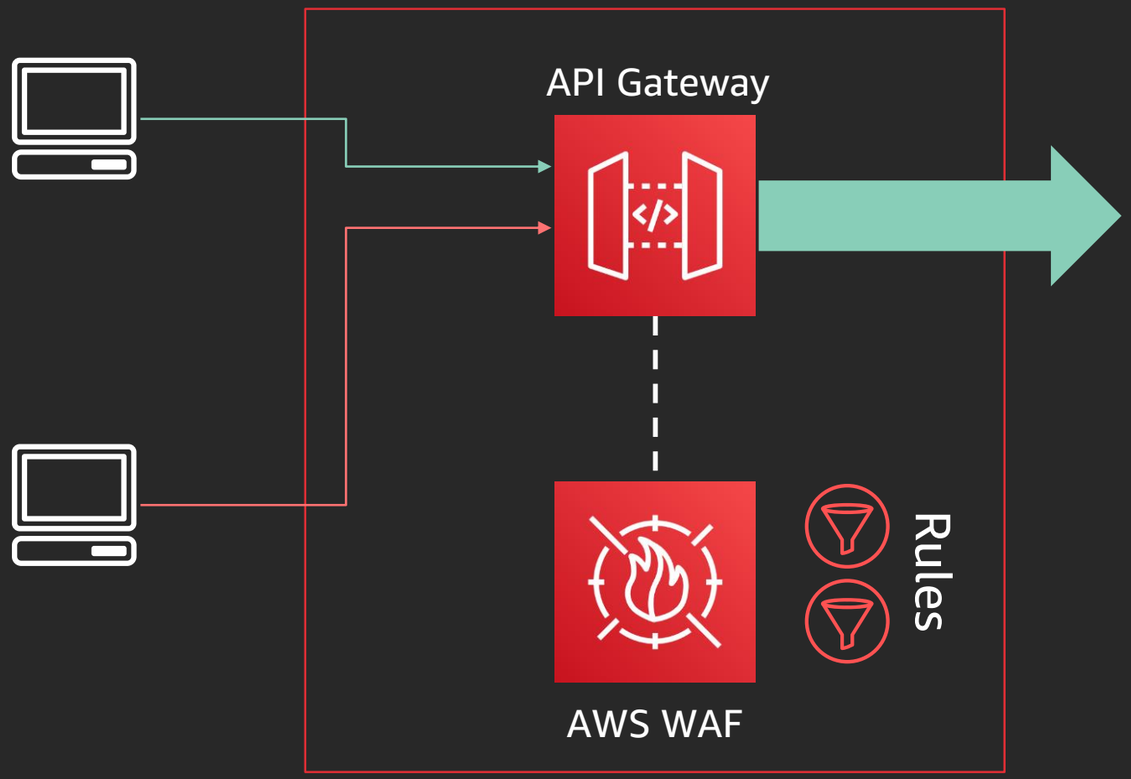
N% of traffic for *X* duration

Canary releases



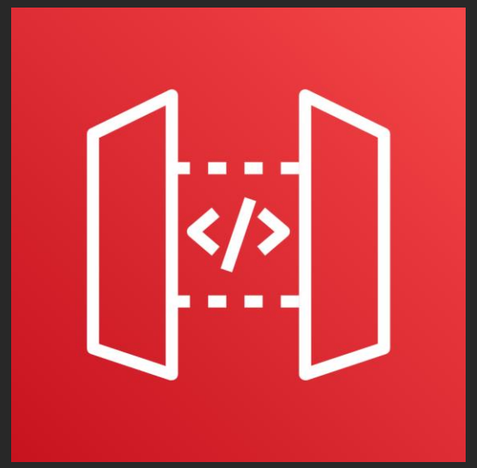


Web application firewall (WAF)



- Protect API Gateway APIs from common web exploits such as SQL injection and cross-site scripting (XSS) attacks
- Block requests from specified IP address ranges or CIDR blocks
- Block requests originating from a specific country or region
- Match a specified string or regular expression pattern in the HTTP header, method, query string, URI, and the request body
- Block attacks from specific user-agents, bad bots, and content scrapers

Monitoring & metrics



Amazon API Gateway



Amazon CloudWatch

API-, stage-, and method-level metrics

- 4XXError
- 5XXError
- Count
- IntegrationLatency
- Latency
- CacheHitCount*
- CacheMissCount*



AWS X-Ray

Trace and analyze requests end to end



AWS Config

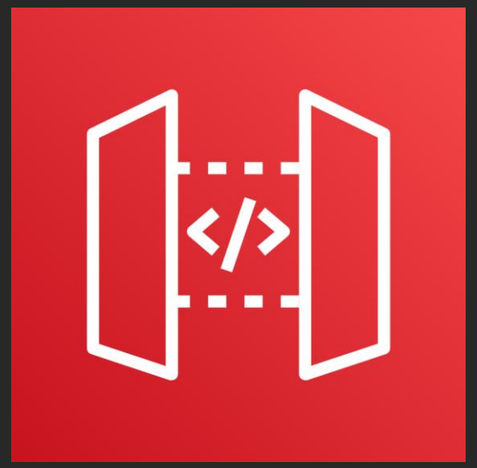
Assess, audit, evaluate configuration updates



AWS CloudTrail

Obtain a record of actions taken by a user, role, or an AWS service on API Gateway

Logging

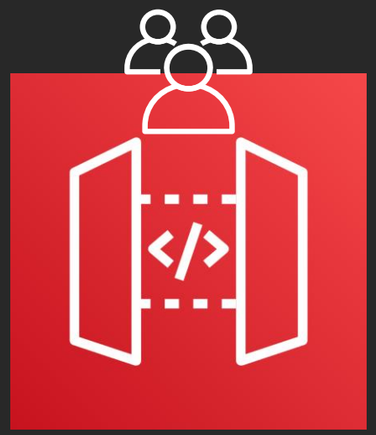


Amazon API Gateway

Log to CloudWatch Logs

- Execution logs
  - Great for debugging and troubleshooting issues
  - Error/info level
  - Log full requests/responses
- Access logs
  - Customize log format
  - CLF (common log format), JSON, XML, and CSV
- Export logs for custom analytics and reporting
- Log directly to Amazon Kinesis Data Firehose

Developer portal



Amazon API Gateway developer portal



API self-discovery



API registration & key generation



API monitoring and usage



API documentation



API testing

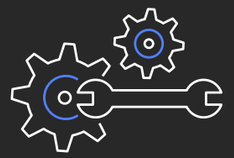


SDK generation

Developer portal



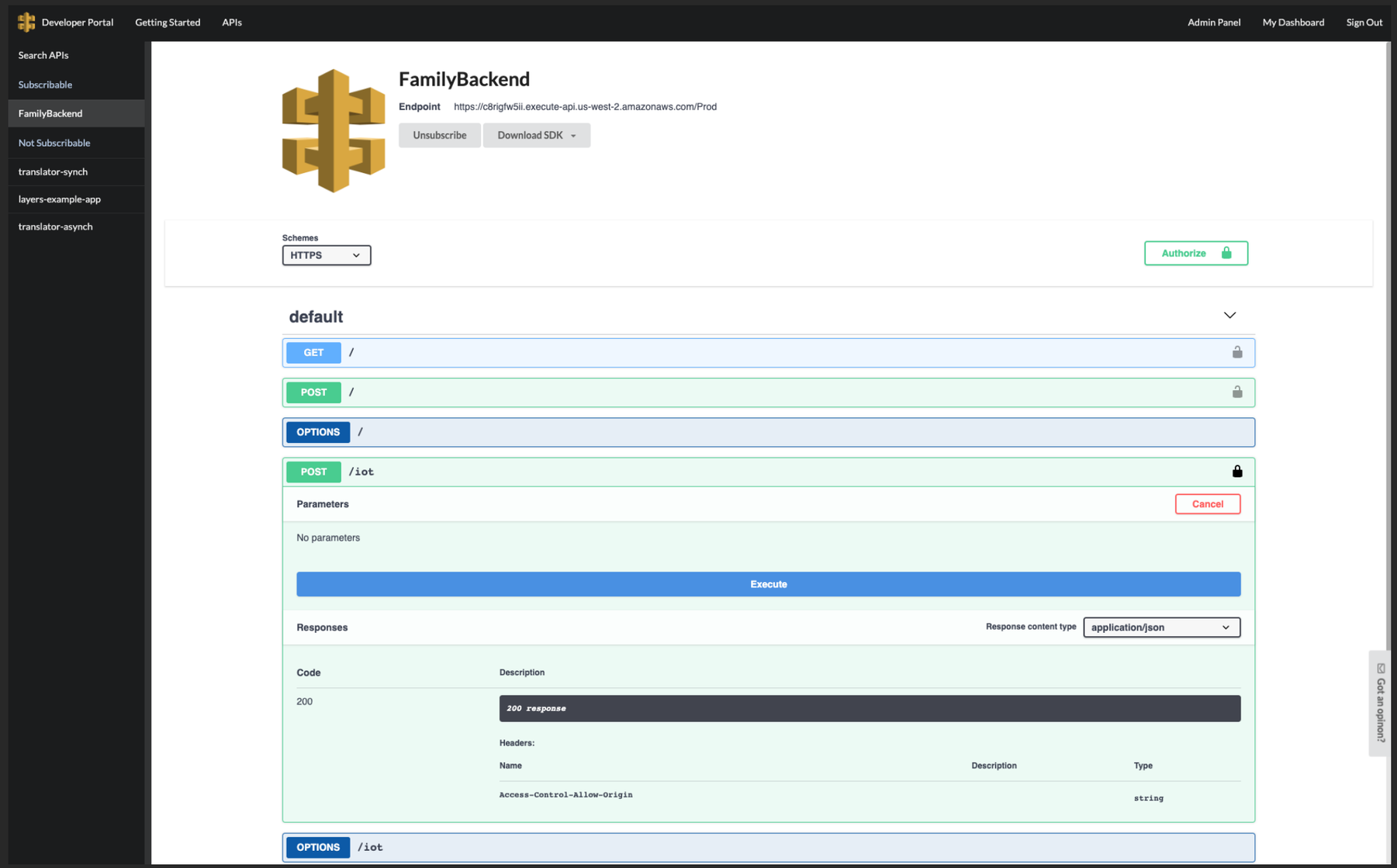
API self-discovery



API testing



API documentation



Developer portal

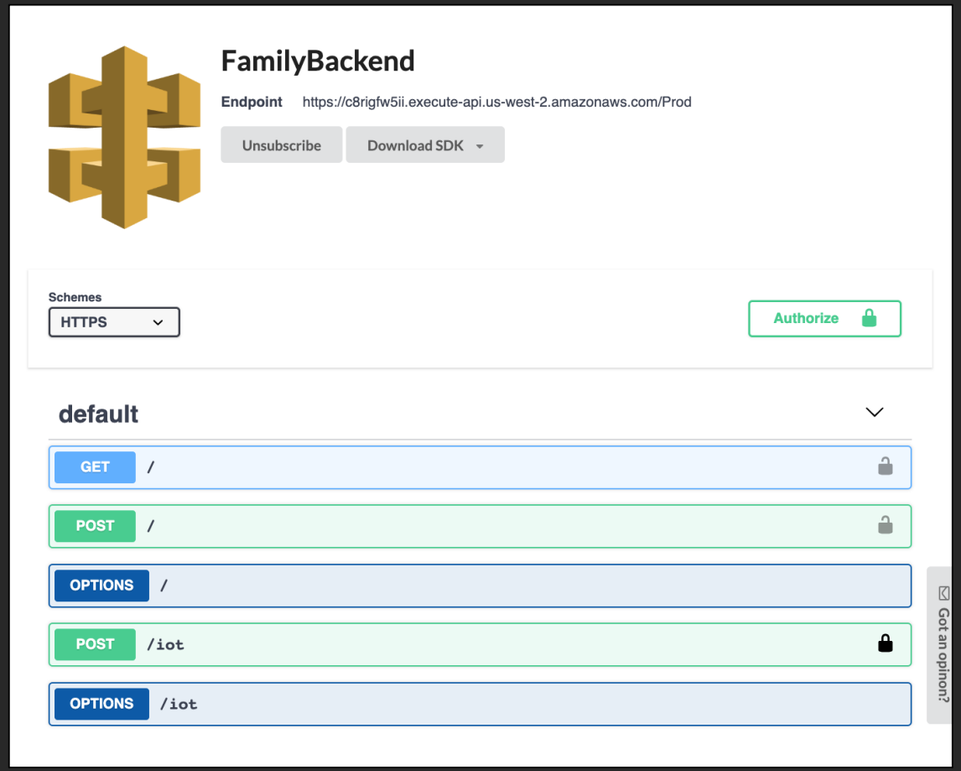


API registration & key generation

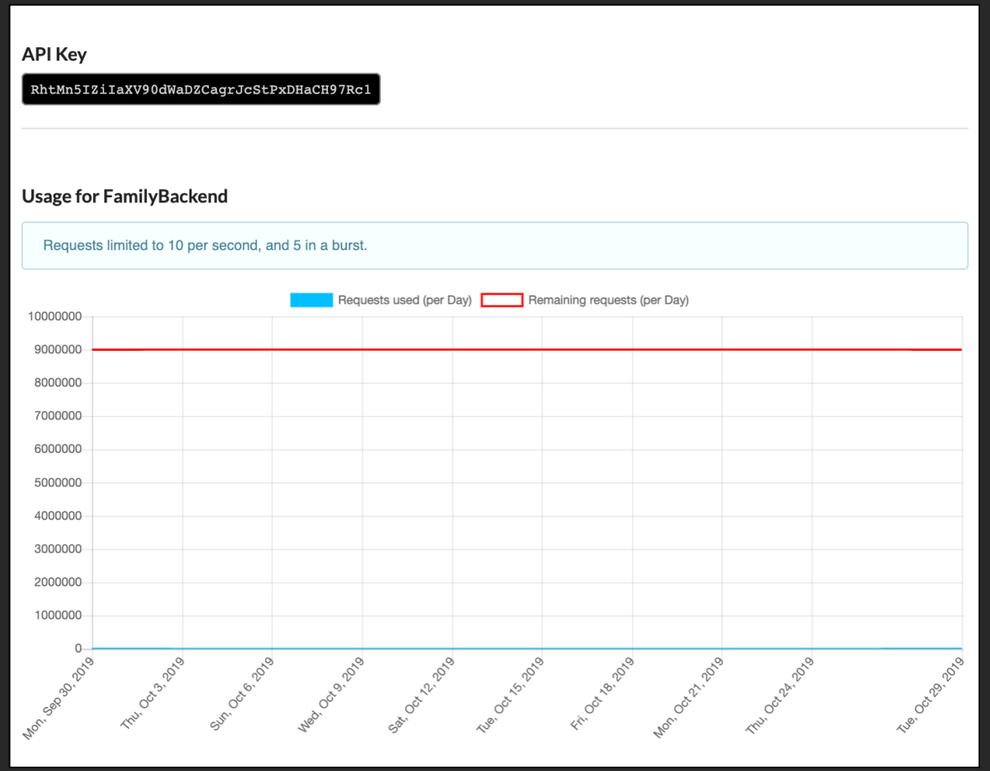


API monitoring and usage

Developers can subscribe to usage plans with their automatically generated API key



Usage statistics are available for subscribed users



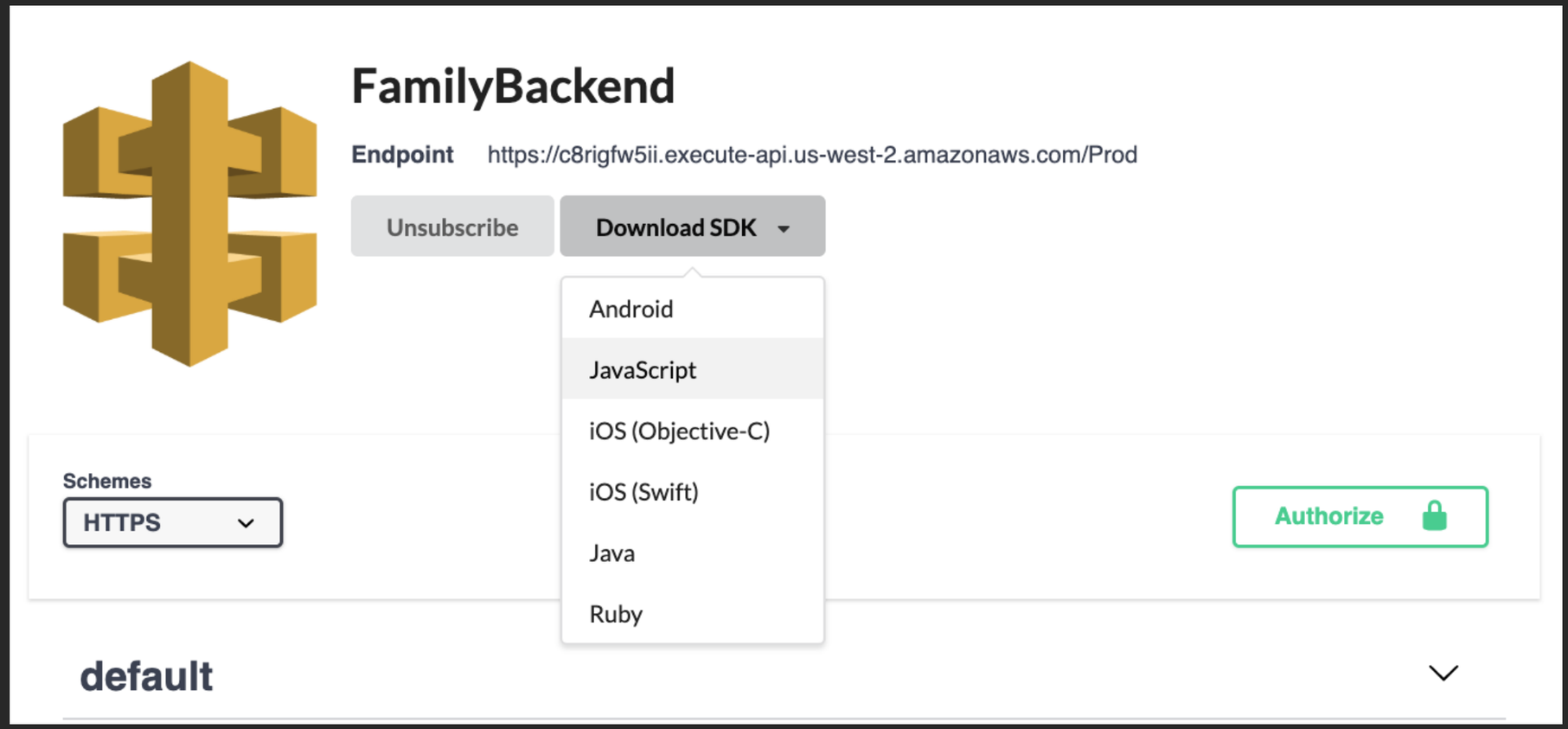
Developer portal



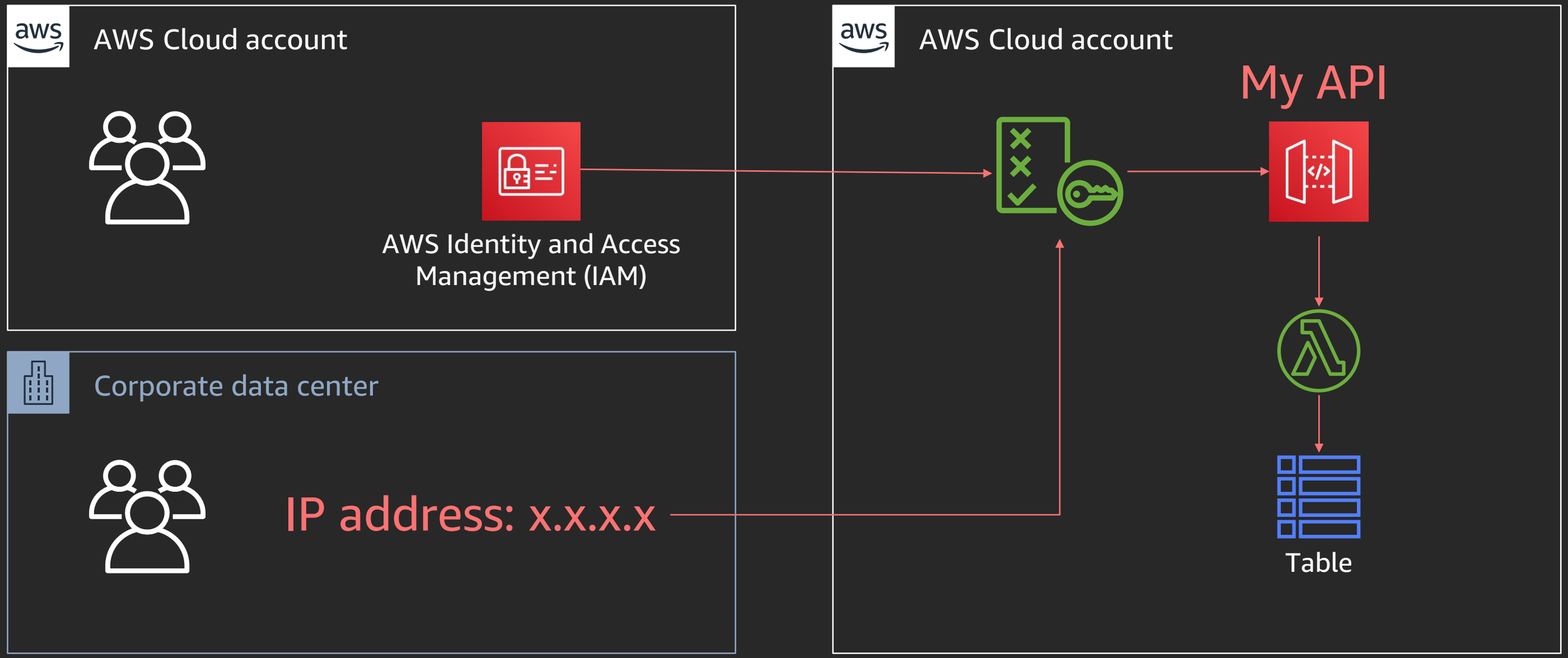
SDK generation

- Request signing with credentials or API key
- Request structure
- Request dependencies

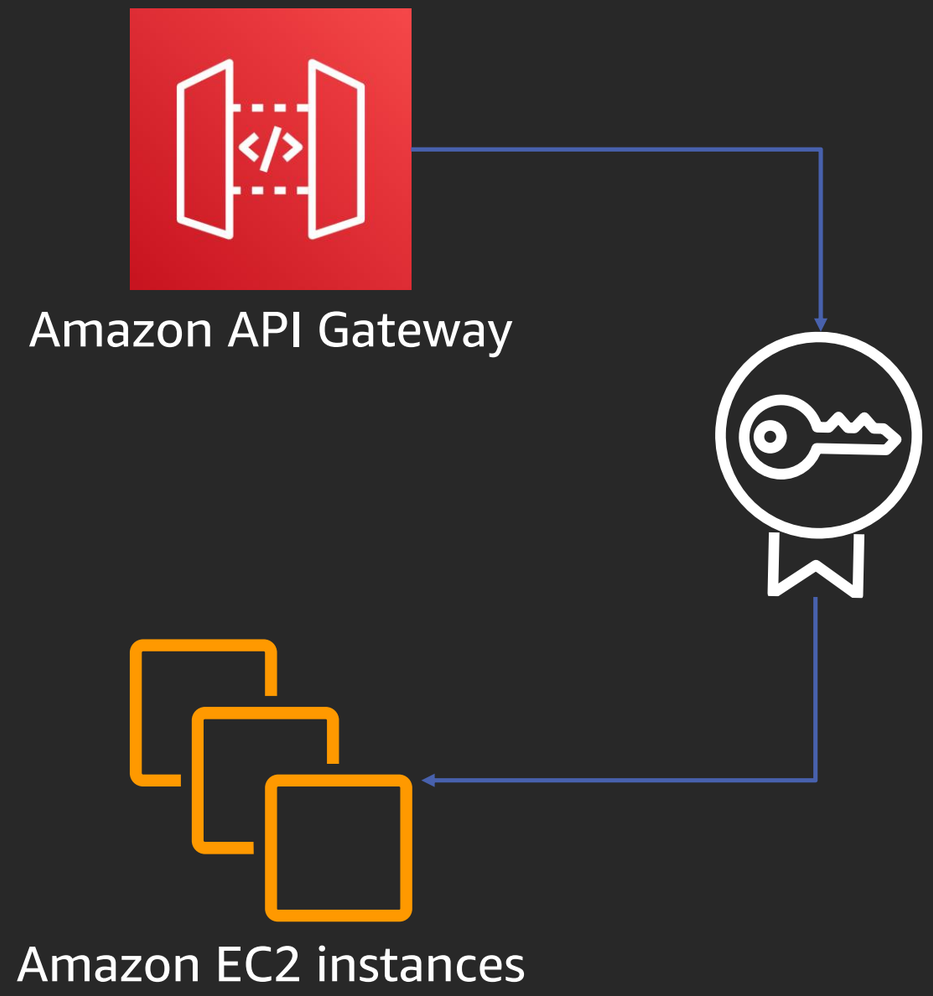
Developers can generate the client SDKs for multiple platforms



Resource policies



Client certificates



- Generate client-side SSL certificate by using the API Gateway
- Allow backend to verify request coming from API Gateway by using public key
- Expires after 365 days

Custom domains

~~https://*12345*.execute-api.*us-east-1*.amazonaws.com/*prod*~~

https://*.*mydomain.com/api-one*

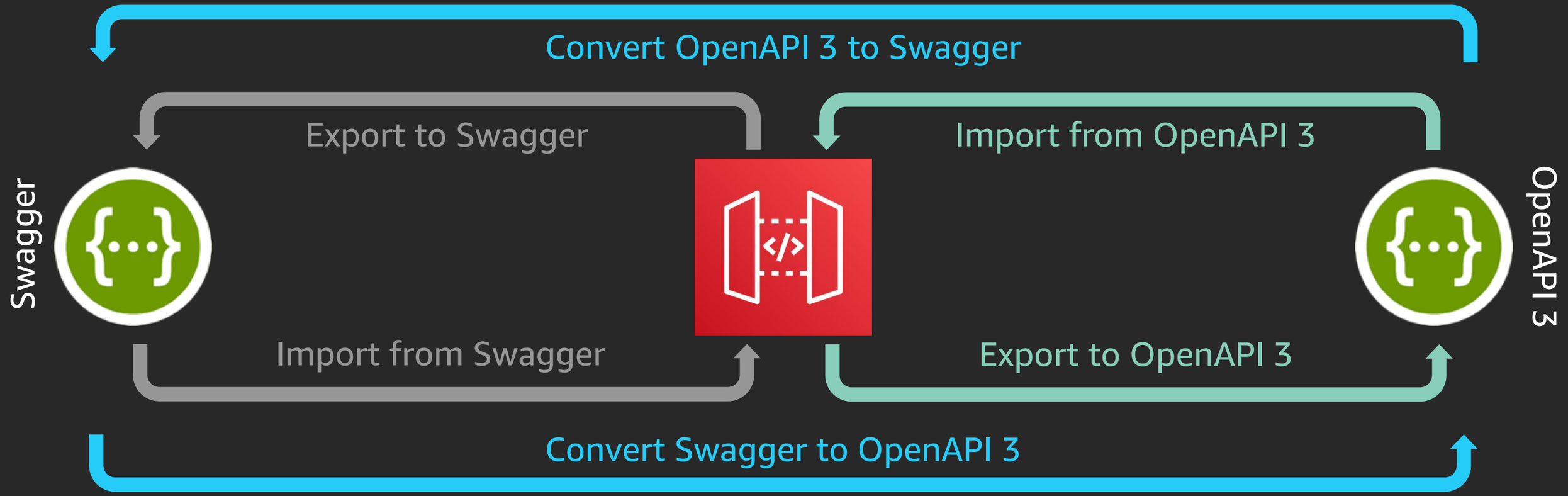


SSL certs managed through AWS Certificate Manager (ACM)

Supports wildcard (*) domains

Supports multiple domains through base path mapping

Swagger/OpenAPI 3 import & export



Postman extensions

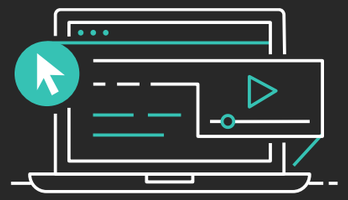
API Gateway extensions

JSON

YAML

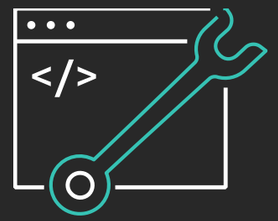
Learn serverless with AWS Training and Certification

Resources created by the experts at AWS to help you learn modern application development



Free, on-demand courses on serverless, including

- Introduction to Serverless Development
- Getting into the Serverless Mindset
- AWS Lambda Foundations
- Amazon API Gateway for Serverless Applications
- Amazon DynamoDB for Serverless Architectures



Additional digital and classroom trainings cover modern application development and computing

Visit the Learning Library at https://aws.training

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws training and certification

Thank you!

Eric Johnson

@edjgeek

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey in the mobile app.

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.