



DevOps Mentorship program

Amazon API Gateway

Alma Beganović

Sadržaj

- Šta predstavlja API?
 - Primjer osnove aplikacije
 - *Requests / responses*
- Uvod u *API Gateway*
 - Definicija, protokoli i vrste
- Kreiranje *API Gateway*
 - Metode, *stages* i integracija
- Sigurnost
 - *IAM policies, Custom domains*, klijentski certifikati i *WAF*
- Autentifikacija i autorizacija
- Monitoring alati
- DEMO

Šta predstavlja *API*?

- *API – application programming interface*
- *Software* mehanizam koji pojednostavljuje *development*



Detalji implementacije

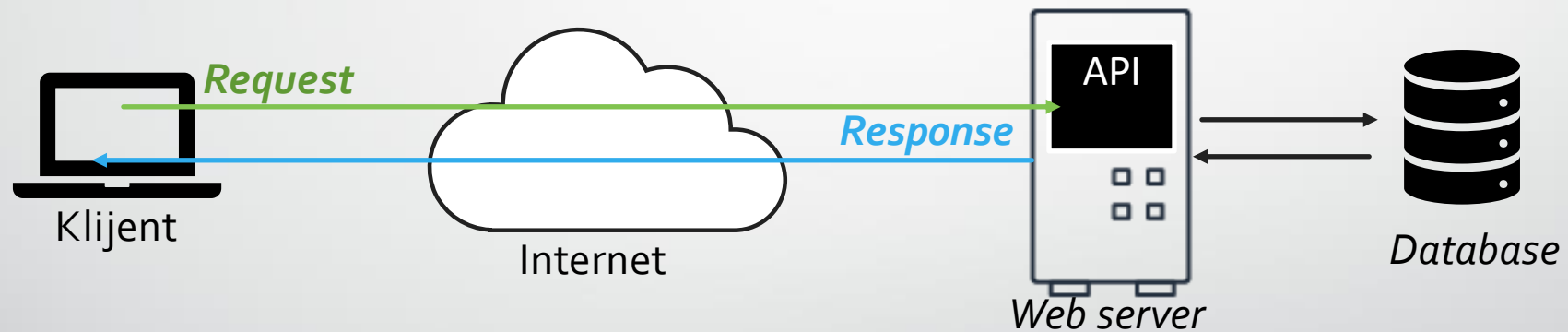


Izlaganje samo onih
objekata ili akcija koje su
developeru potrebne

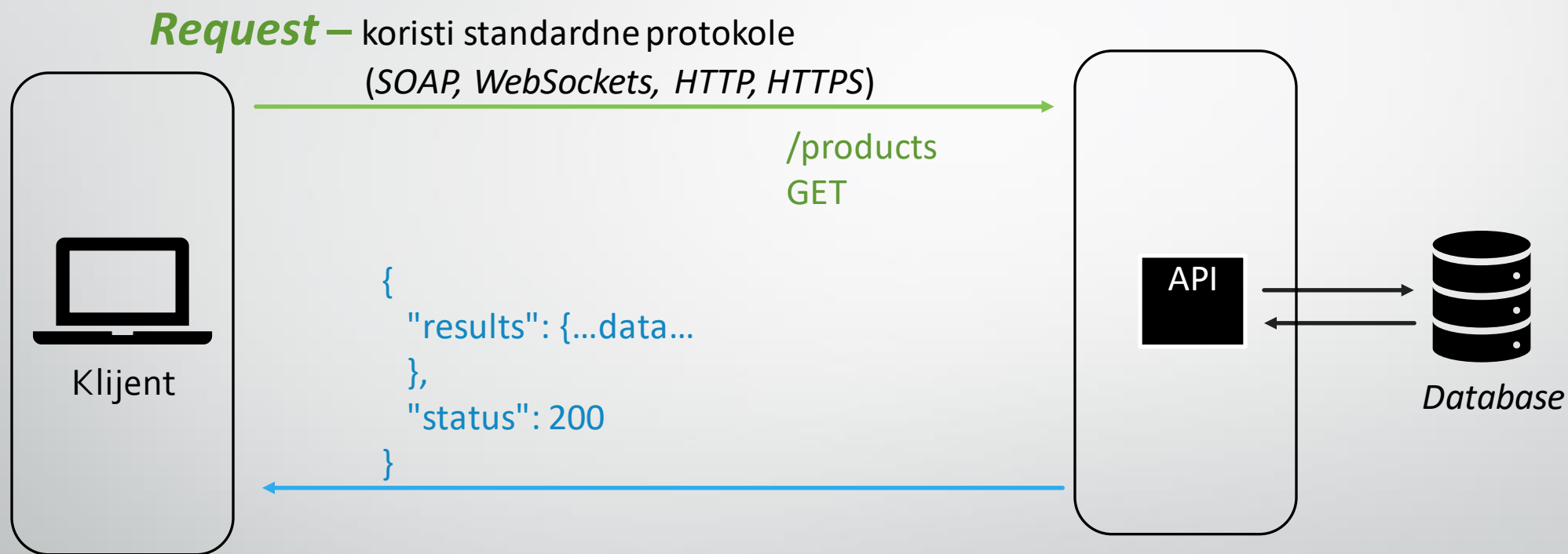


Način komunikacije *provider - user*

Primjer osnovne aplikacije



Requests - Responses



Response – podaci i statusni kodovi



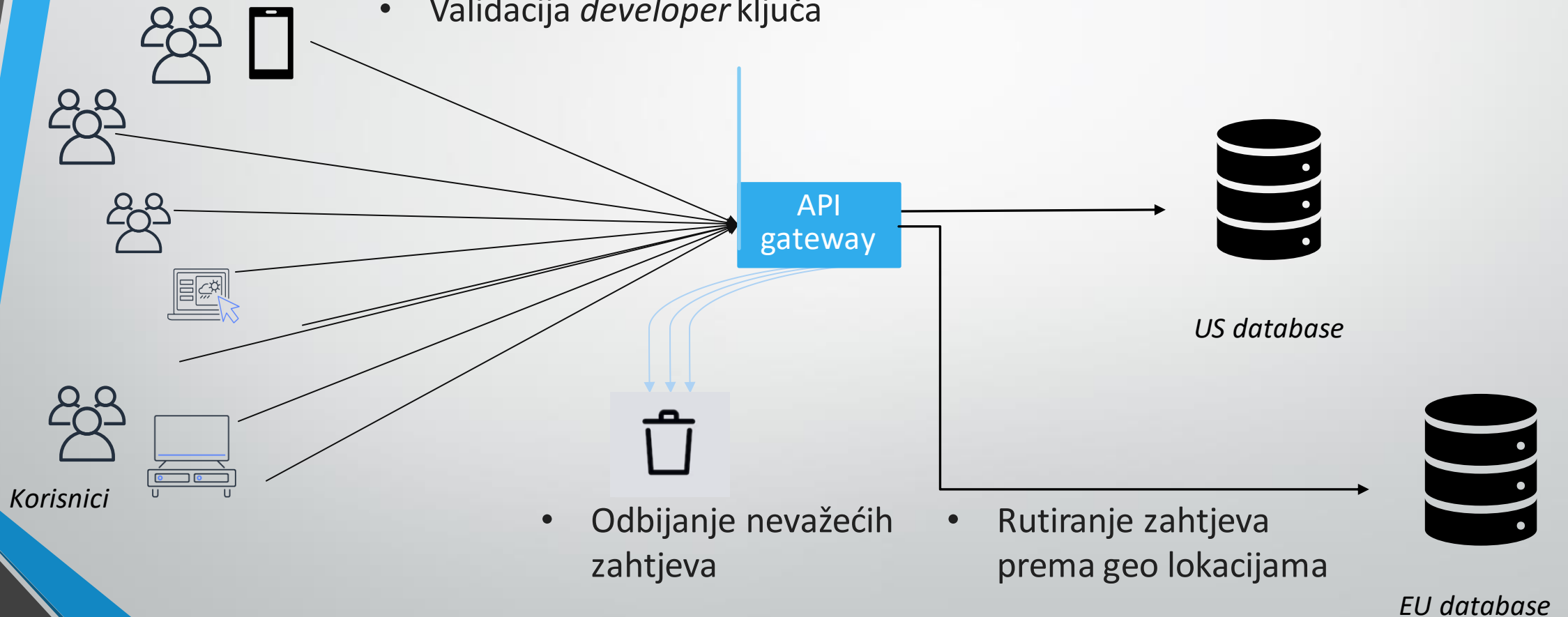
Status codes:

- 20X – 200, 201 uspješni odgovori
- 40X – 403, 412 greška na strani klijenta
- 50X – 500, 501 greška na strani servera

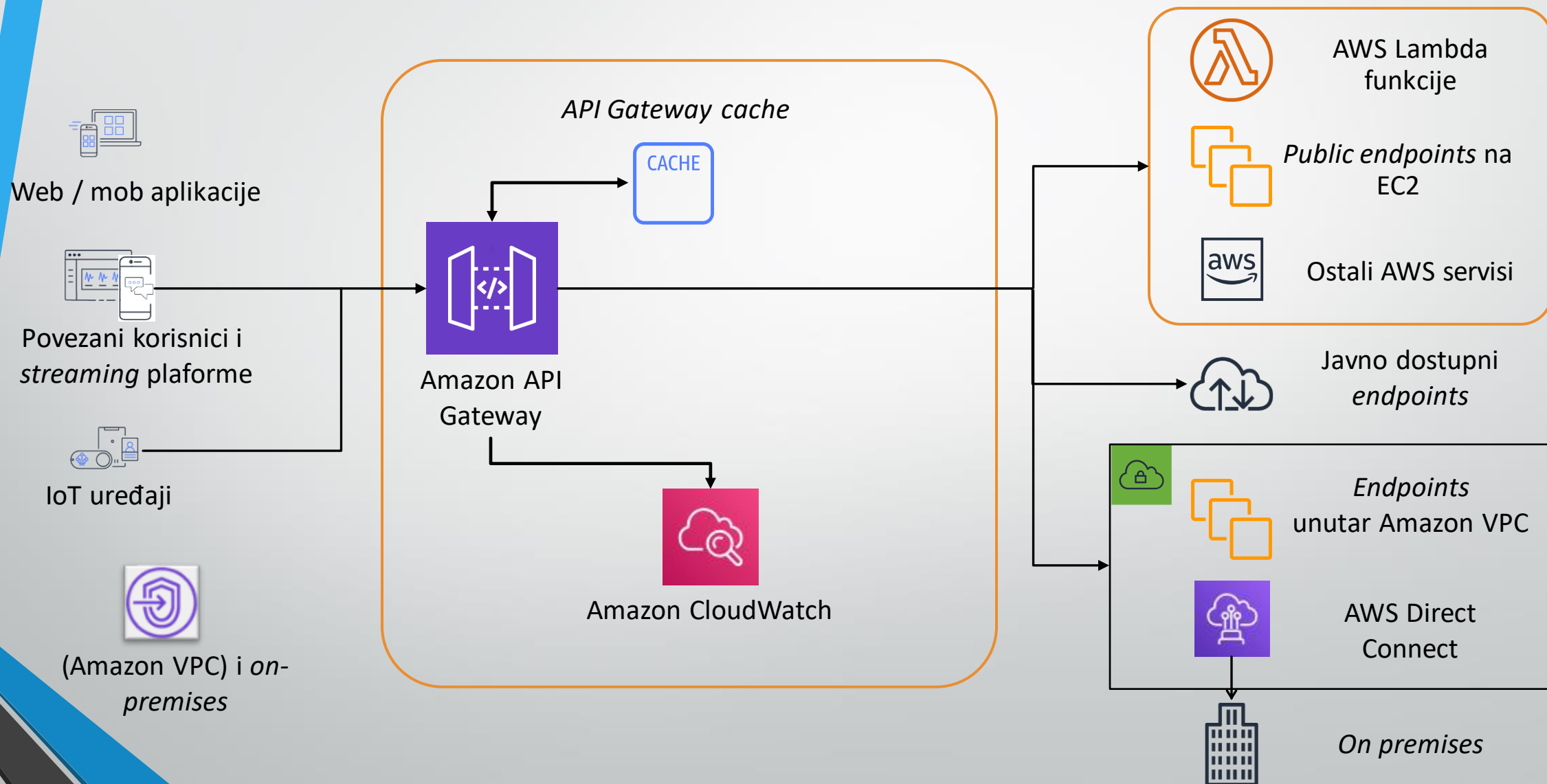
API gateway je proxy

- Ograničava *requests rate*
- Prihvata ili odbija zahtjeve
- Validacija *developer* ključa

- Visoko dostupan i skalabilan servis



Amazon API Gateway



API Gateway – endpoint vrste

- *Regional* – klijenti se nalaze u istoj regiji
- *Edge-optimized* – koristi se *CloudFront*
- *Private* – pristup samo unutar VPC-a

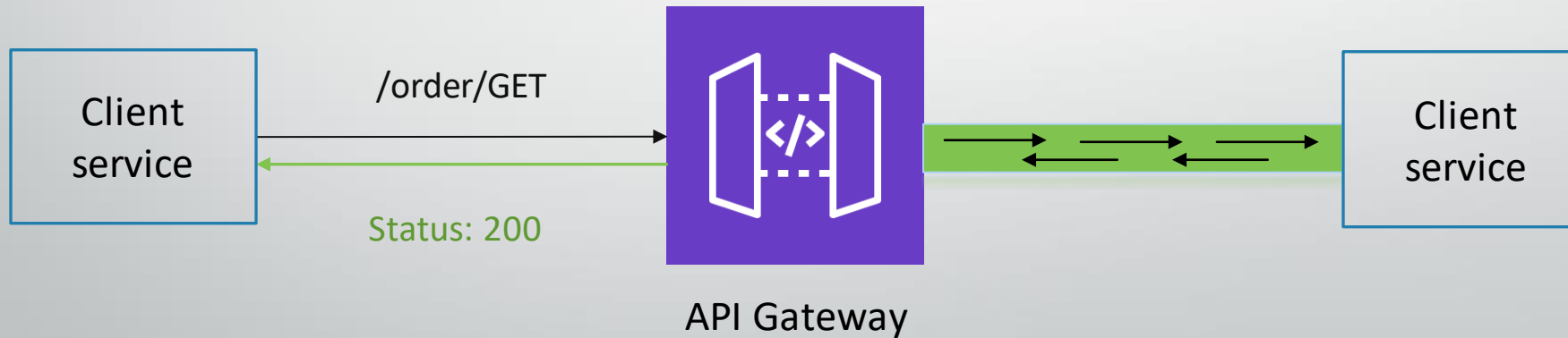
Koje protokole podržava *API Gateway*?

RESTful

- *Request/response*
- HTTP metode (GET, POST)
- *short-lived* komunikacija
- *stateless*

WebSockets

- dvosmjerni komunikacijski kanal
- *long-lived* komunikacija
- *stateful*



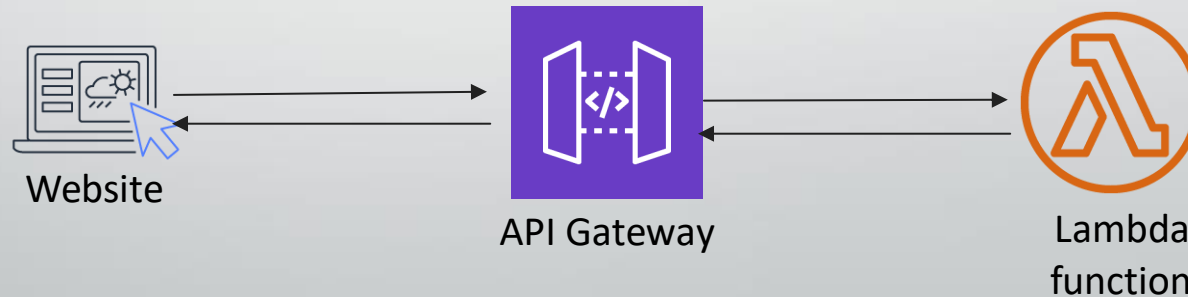
Vrste *RESTful API Gateway*-a

REST API

- Developer ima potpunu kontrolu nad API zahtjevima i odgovorima
- Podržava pogodnosti koje nisu dostupne sa HTTP APIs

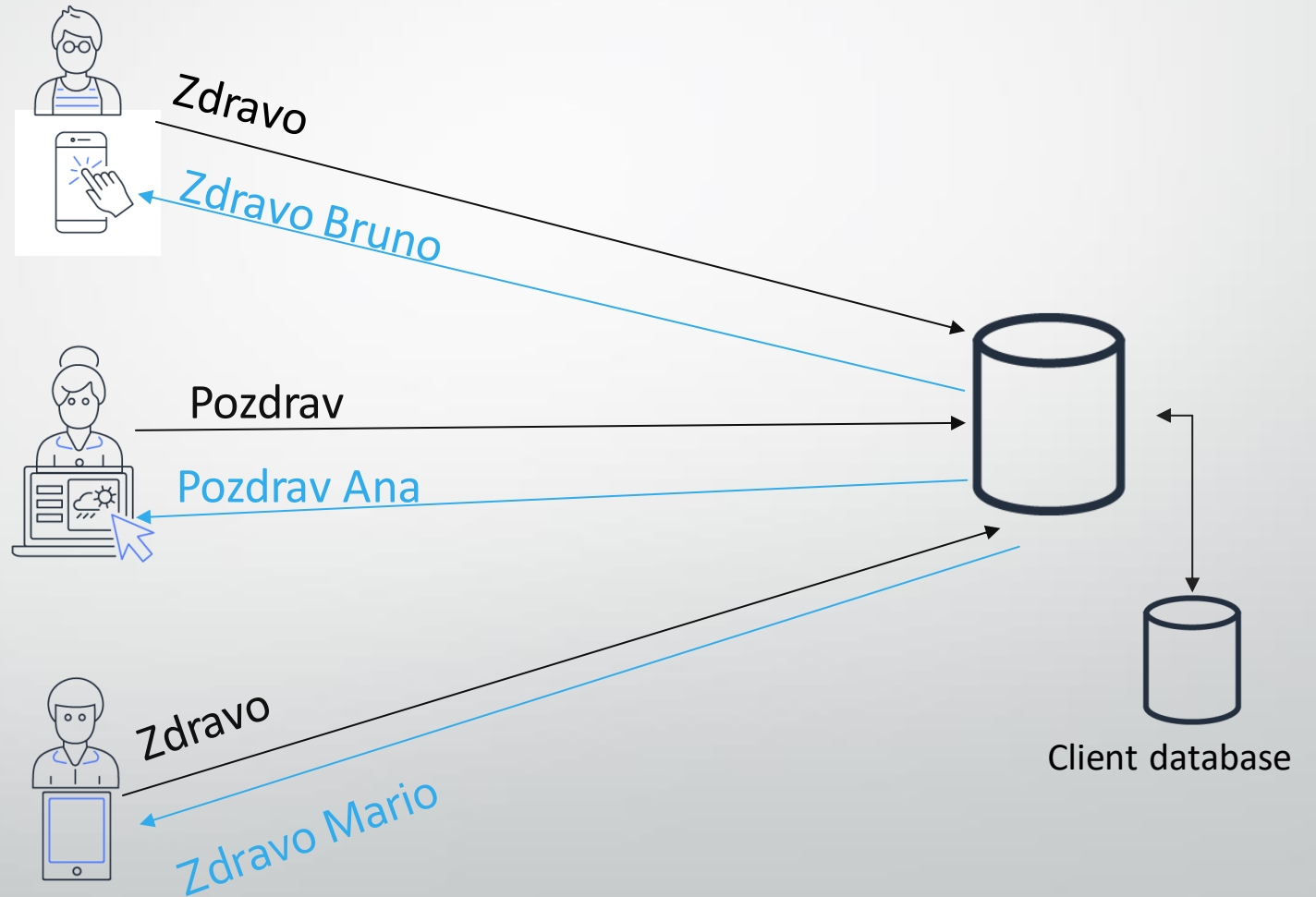
HTTP API

- Pojednostavljuje development APIs koji zahtijeva samo API proxy funkcionalnosti
- Niži troškovi i manje kašnjenje



WebSockets

Real-time, dvosmjerna komunikacija



API Gateway management

Develop



AWS Management
Console



AWS Command Line
Interface (AWS CLI)

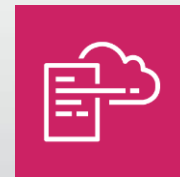


OpenAPI Specification
(Swagger)

Deploy



AWS Serverless Application Model
(AWS SAM)



AWS CloudFormation



AWS Cloud Development Kit
(AWS CDK)



Kako kreirati REST API?

Kreiranje REST ili HTTP API

Kreiranje pomoću:

- AWS CLI
- API Gateway console

Struktura za REST i HTTP APIs

`https://{restapi_id}.execute-api.{region}.amazonaws.com/{stage_name}/`

`{restapi_id}`

API identifier

`{region}`

The AWS Region

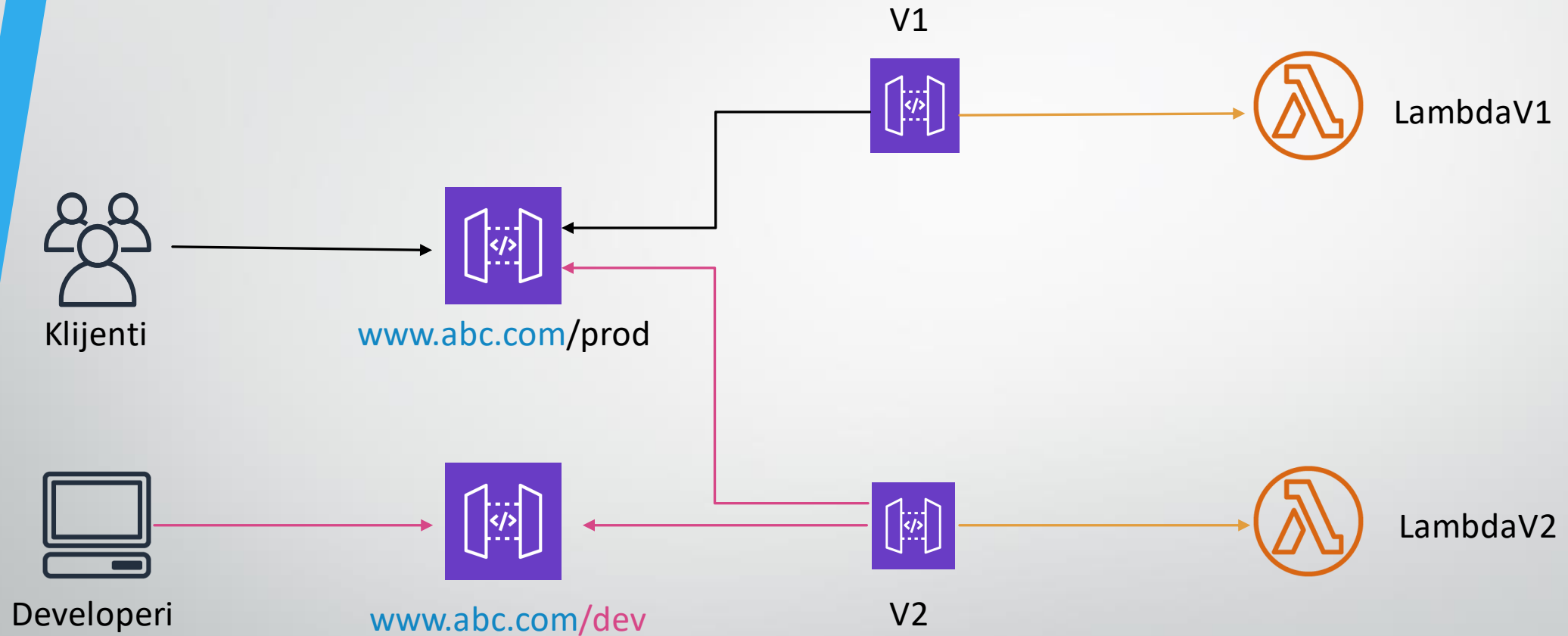
`{stage_name}`

Stage name of the API
deployment

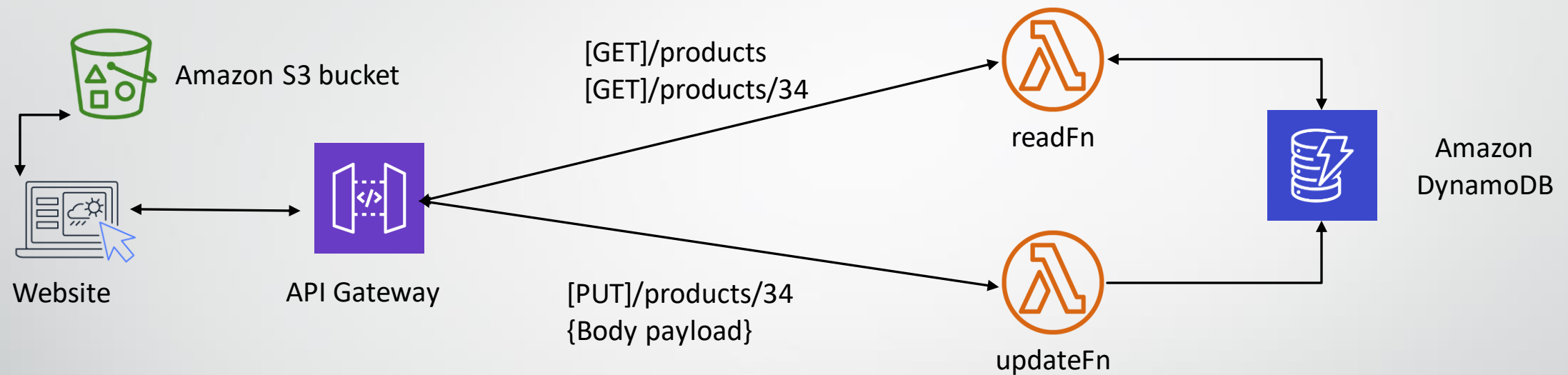
Za šta nam služe *stages* ?

- *Stages* predstavljaju *snapshots* za API:
 - Imenujete ih po želji
 - Identifikuju se na osnovu *API ID* i *stage name*
 - Ukjučeni su u URL koji se koristi za pozivanje API-a
- Developeri kreiraju različite *stages* kako bi:
 - razlikovali verzije development okruženja (primjer: dev i prod okruženje)
 - povezali različite *stages* sa različitim *backends* verzijama koristeći *stage variables*
 - optimizovali određeni *deployment* – primjer: *caching*

API Gateway- upotreba *Stages*



Metode i resursi



#svi objekti sa putanje /products

[GET] <https://api-id.execute-api.us-east-2.amazonaws.com/products>

#određeni objekat sa ID (34)

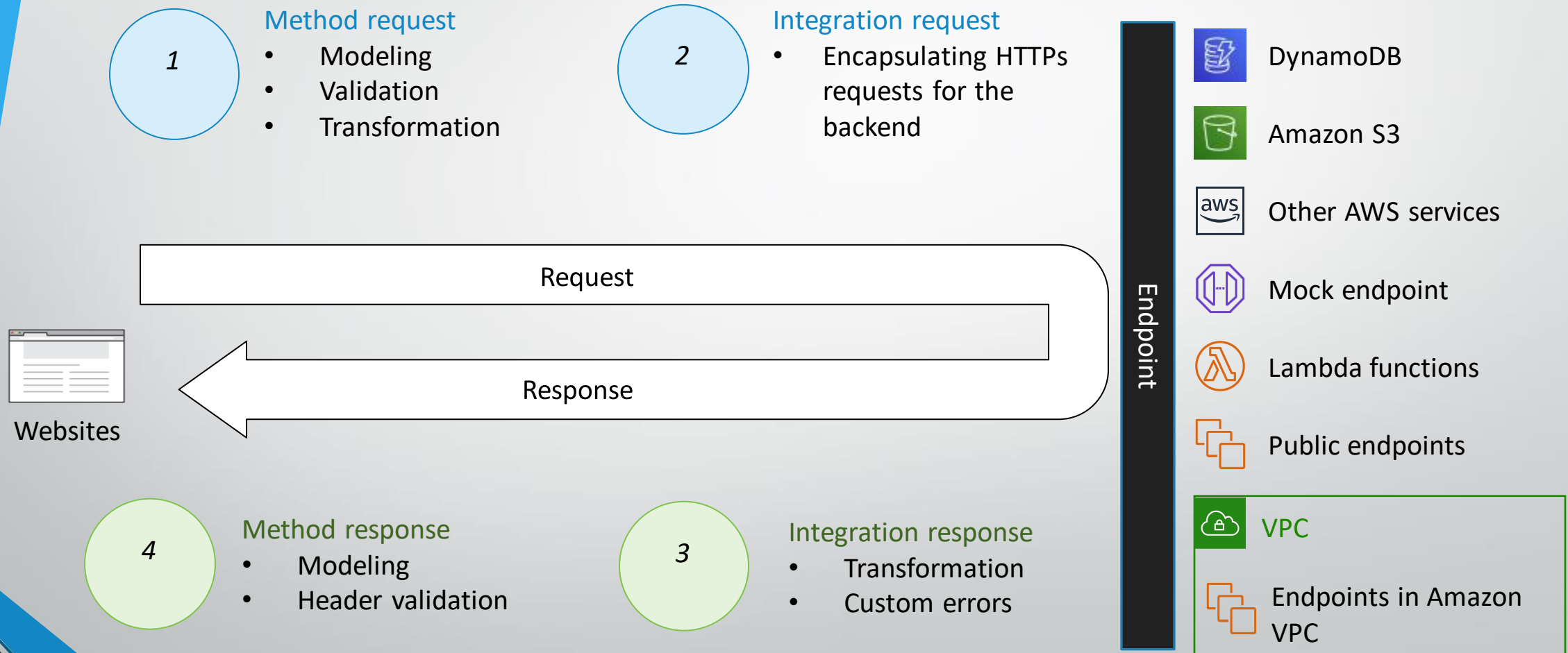
[GET] <https://api-id.execute-api.us-east-2.amazonaws.com/products/34>

#update određenog objekta sa ID (34)

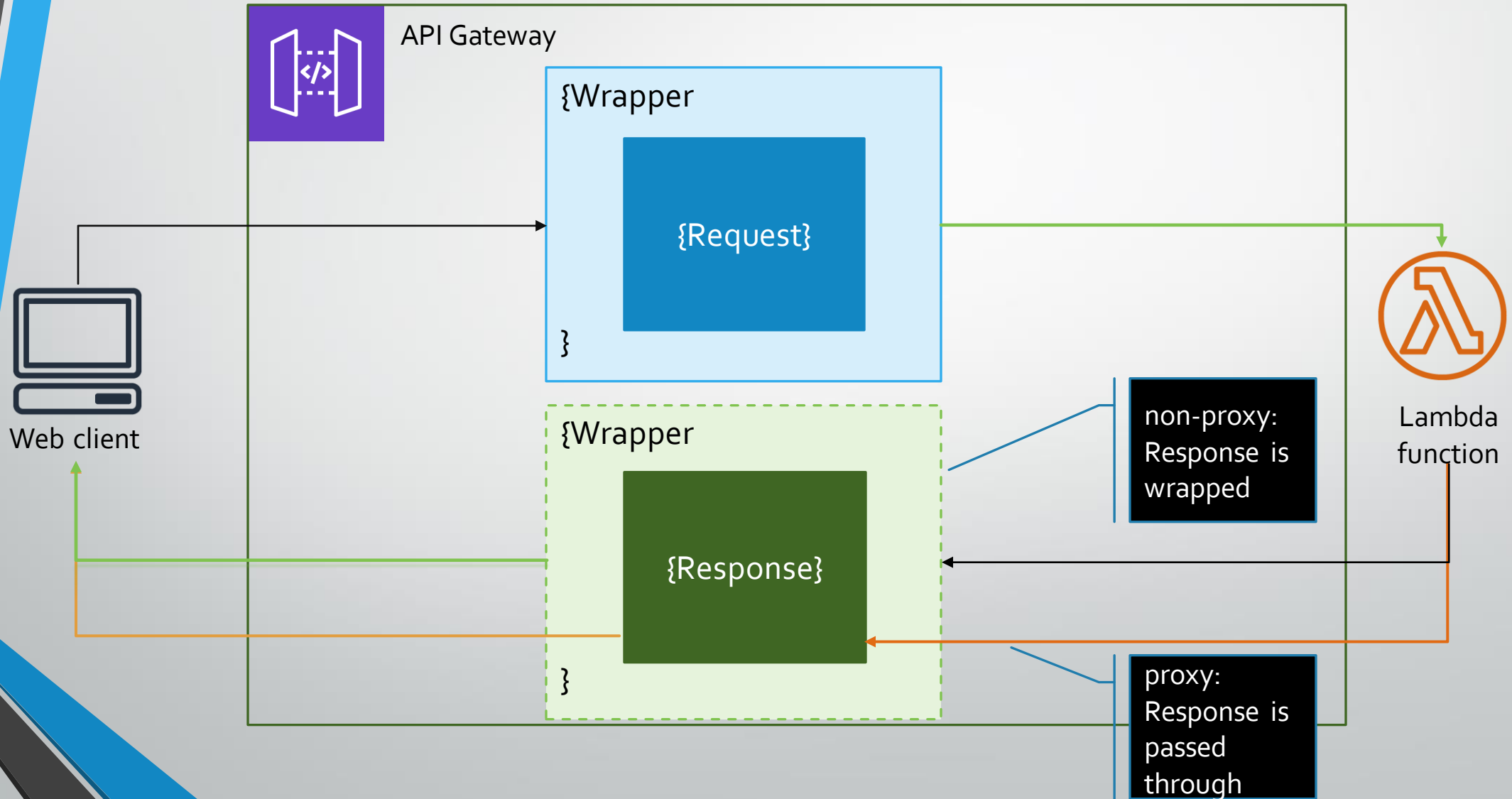
[PUT] <https://api-id.execute-api.us-east-2.amazonaws.com/products/34>

[BODY] #some keys and values

Primjeri integracijskog toka



Lambda non-proxy vs. lambda proxy

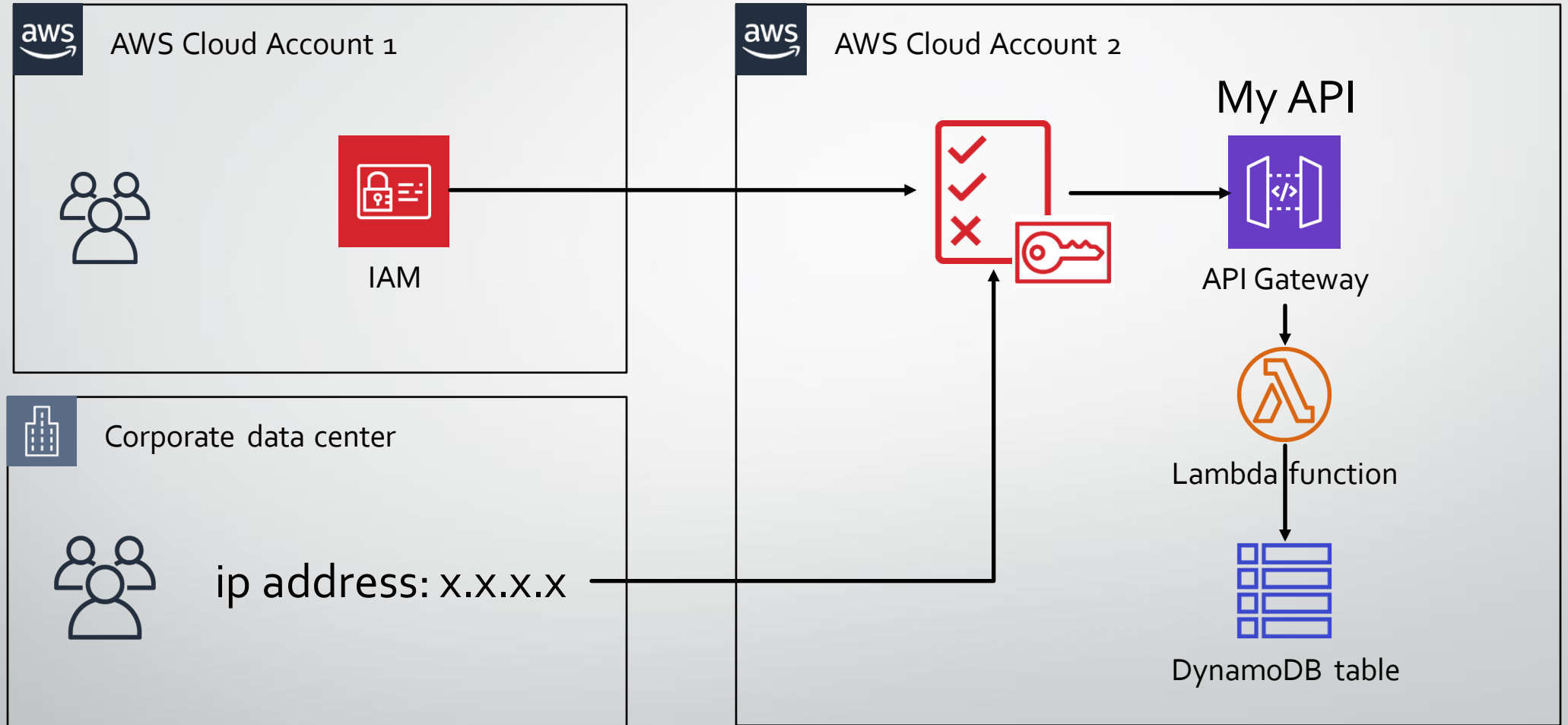




Kako zaštititi API od
neželjenog saobraćaja ?




IAM resource policies



Custom domains

<https://12345.execute-api.us-east-1.amazonaws.com/prod>

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

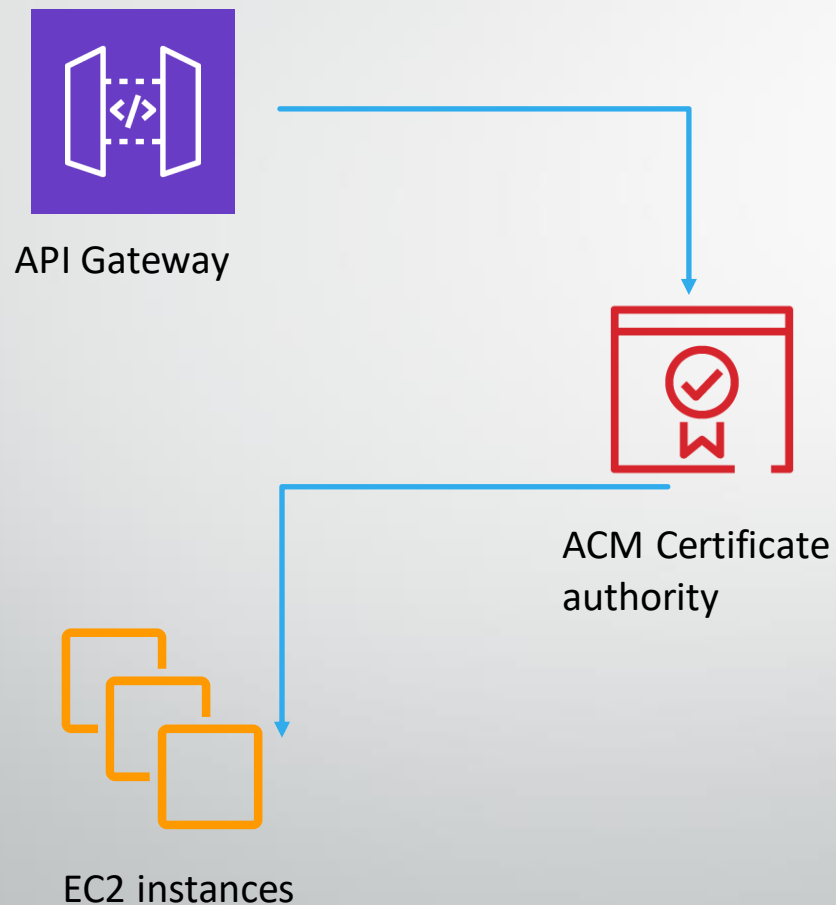


Secure Sockets Layer
(SSL) certifikati kojima
upravljamo kroz AWS
Certificate
Manager (ACM)

Podrška wildcard (*)
domene

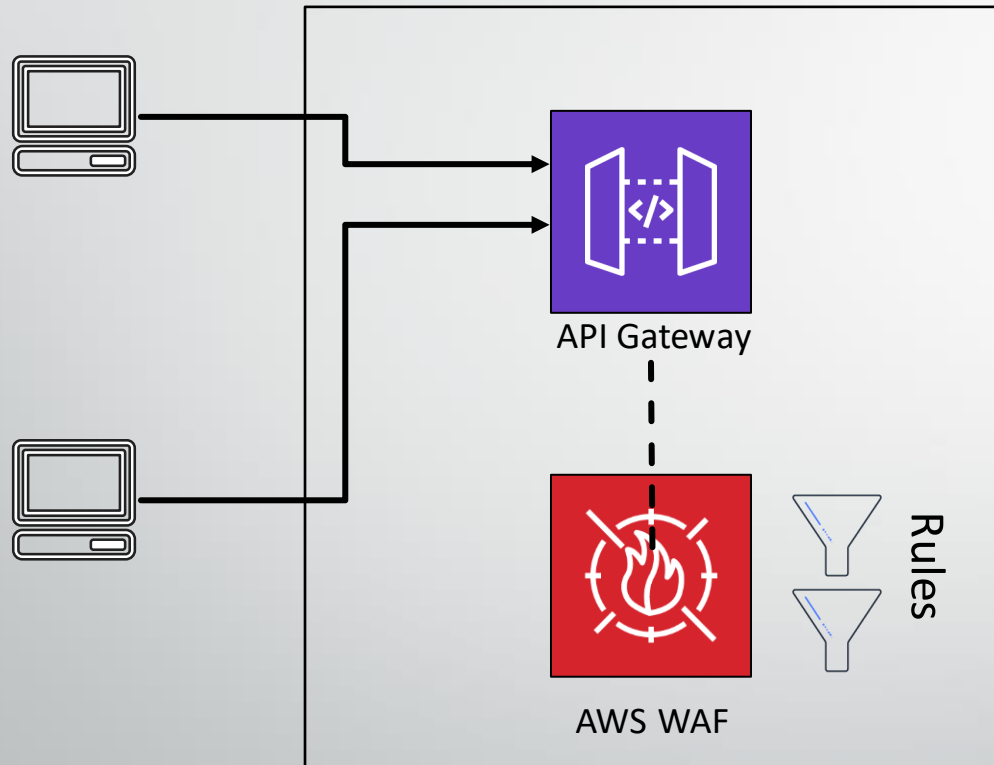
Podrška nekoliko domena
koristeći različite putanje za
mapiranje

Client certificates



- generisanje *client-side* SSL certifikata koji će koristiti API Gateway
- Backend strana verifikuje da je zahtjev stigao od API Gateway koristeći *public key*
- Trajanje certifikata: 365 dana

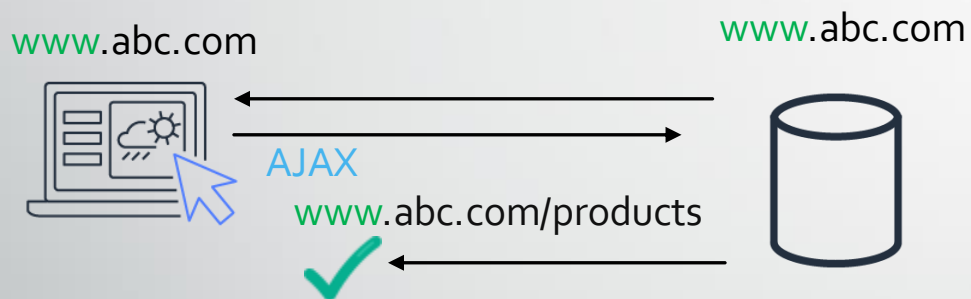
AWS WAF – *Web Application Firewall*



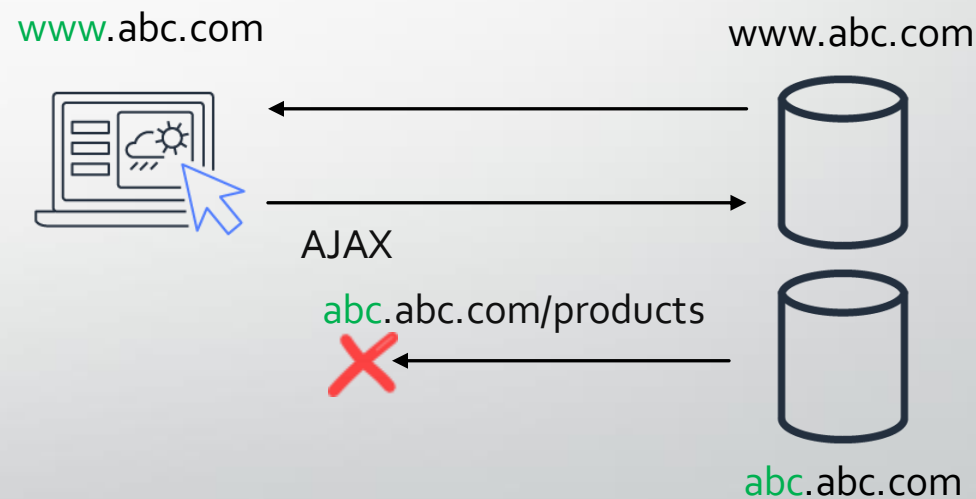
- Štiti APIs od čestih napada kao što su *SQL injection* i *cross-site scripting* (XSS)
- Upoređivanje određenog *string*-a ili zaglavlja
- Blokiranje zahtjeva na osnovu njihovog porijekla:
 - Određeni opseg IP adresa
 - Određena država ili regija
 - Određeni *user agents*, botovi , te *content scrapers*

Cross-origin resource sharing (CORS)

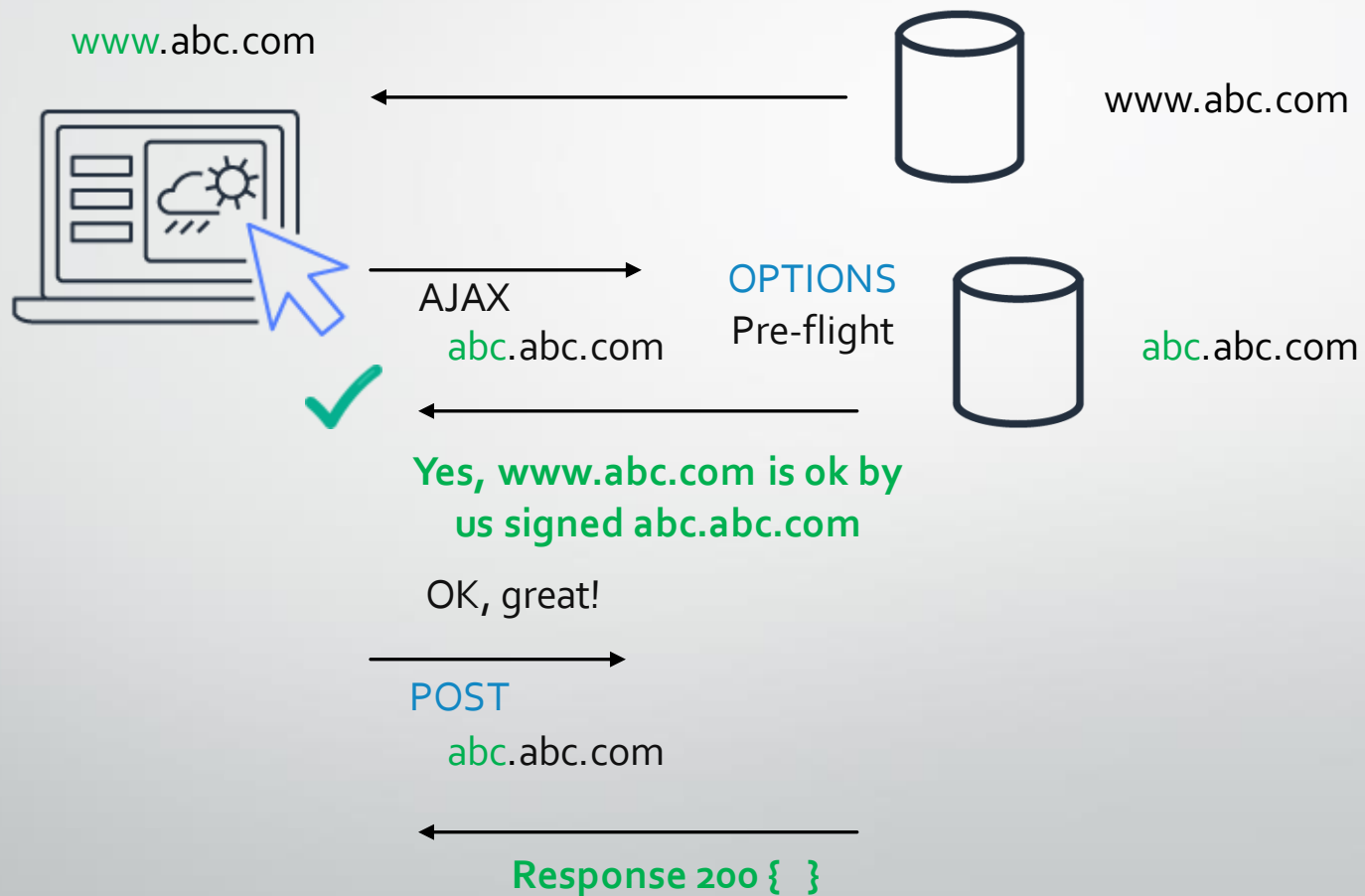
Same domain



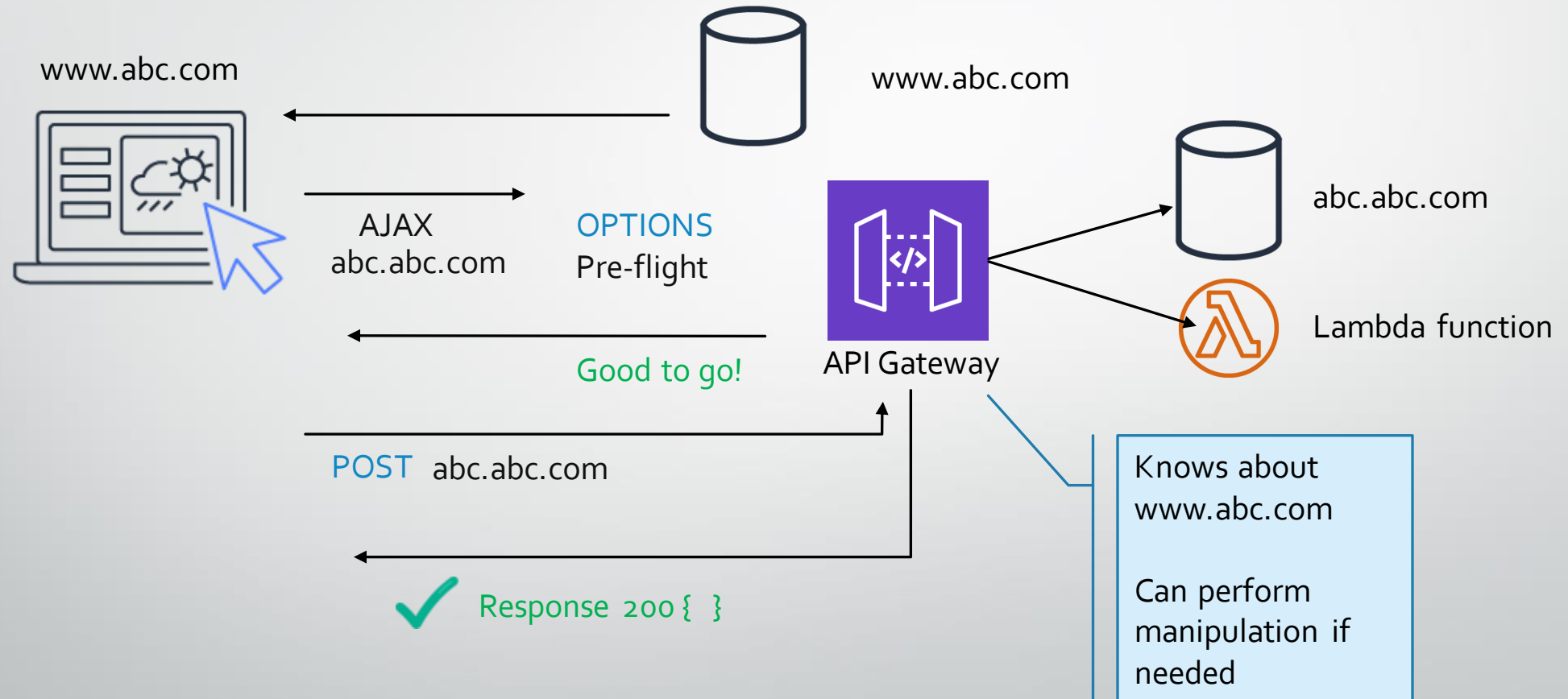
Cross-domain



Cross-origin zahtjevi sa CORS podrškom

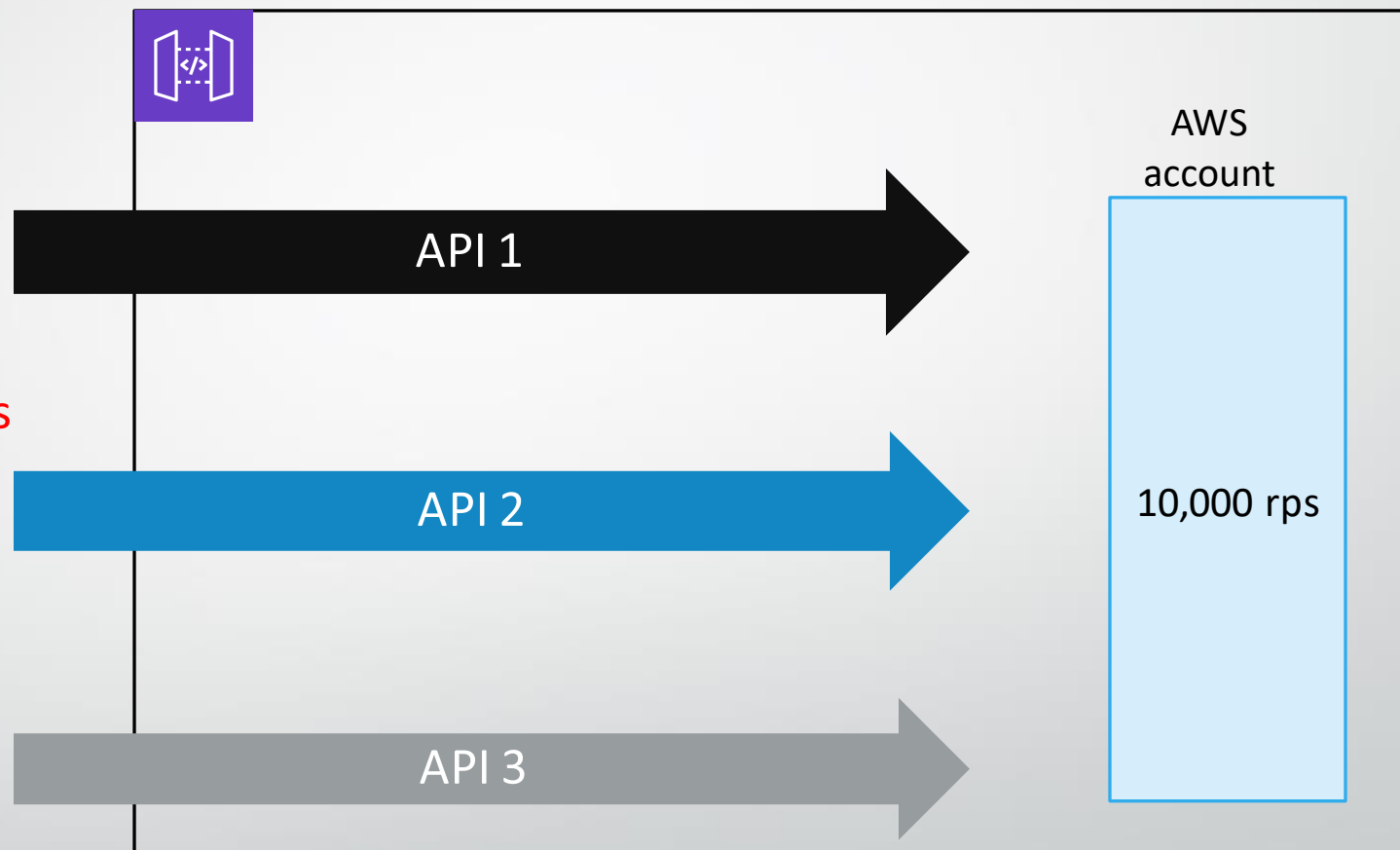


API Gateway sa CORS



Account-level rate limiting (throttling)

throttling limit po regiji: 10,000* rps
**Soft limit*



Autentifikacija i autorizacija REST APIs

None

otvoreni pristup

IAM

Koristi *IAM* i *AWS credentials* za pristup



Amazon
Cognito



JSON Web
Token (JWT)

JWT-based

Koristi Amazon Cognito (REST APIs) or drugi *JWT-based authorizer* (HTTP APIs)



API Gateway

Backend

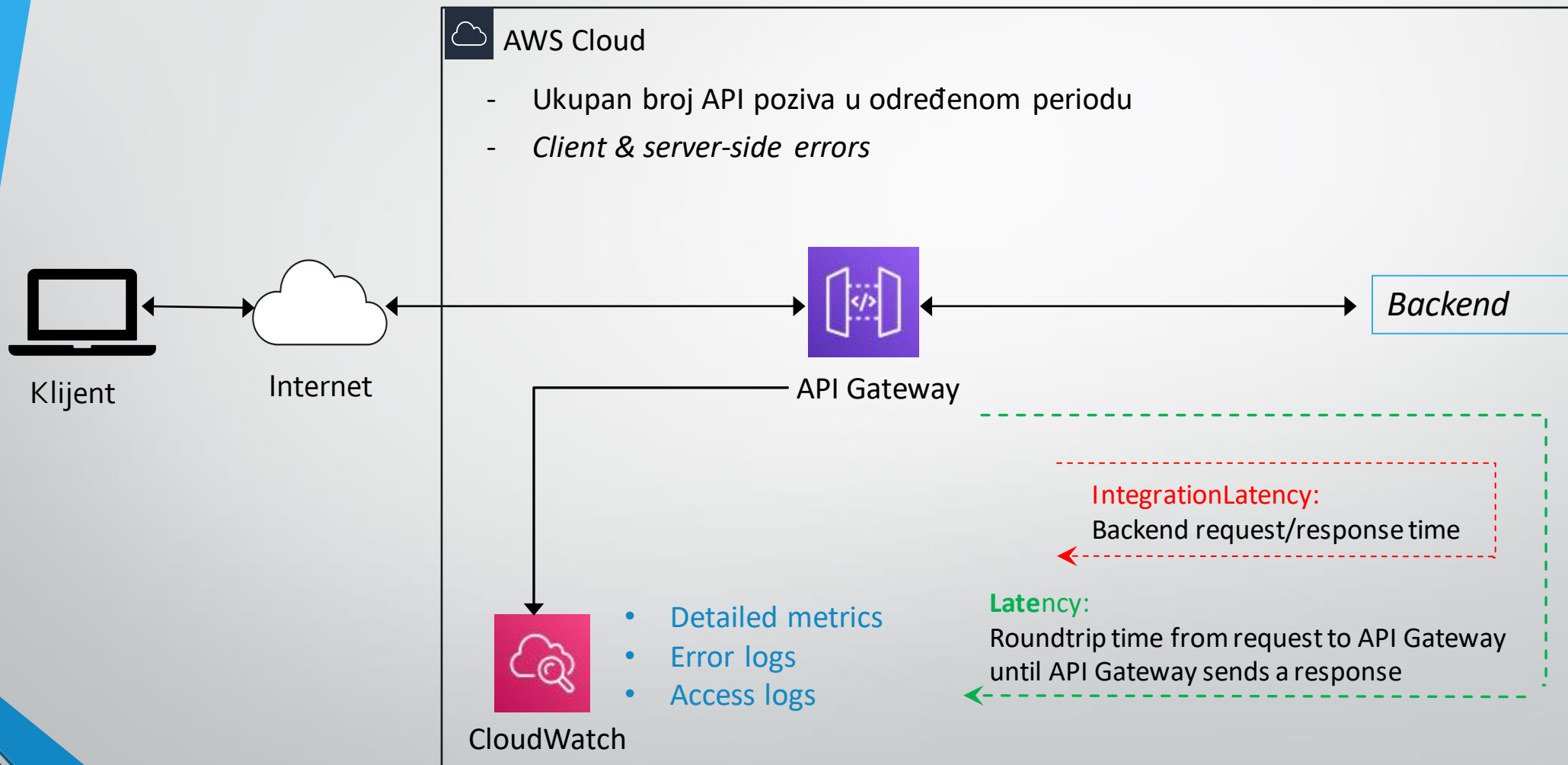


Lambda
function

Lambda authorizers

Koristi se lambda funkcija za provjeru *token-a* (kao što su *OAuth* ili *Security Assertion Markup Language* [SAML]) ili se zahtijevaju parametri za odobravanje pristupa

Monitoring REST APIs



Ostali monitoring servisi



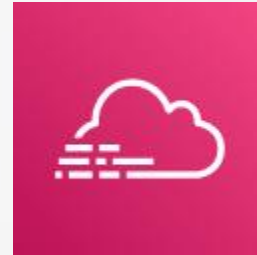
AWS X-Ray

Prati i analizira zahtjeve
end-to-end



AWS Config

Procjena i pregled
ažuriranja konfiguracije



AWS CloudTrail

Upravlja pozivima koji su
upućeni prema API Gateway-u
od strane korisnika, role ili nekog
drugog AWS servisa

DEMO

Integracija API Gateway + Lambda proxy

