
AWS
re:Invent

SVS313

Serverless API authentication for HTTP APIs on AWS

Leo Drakopoulos

Solutions Architect

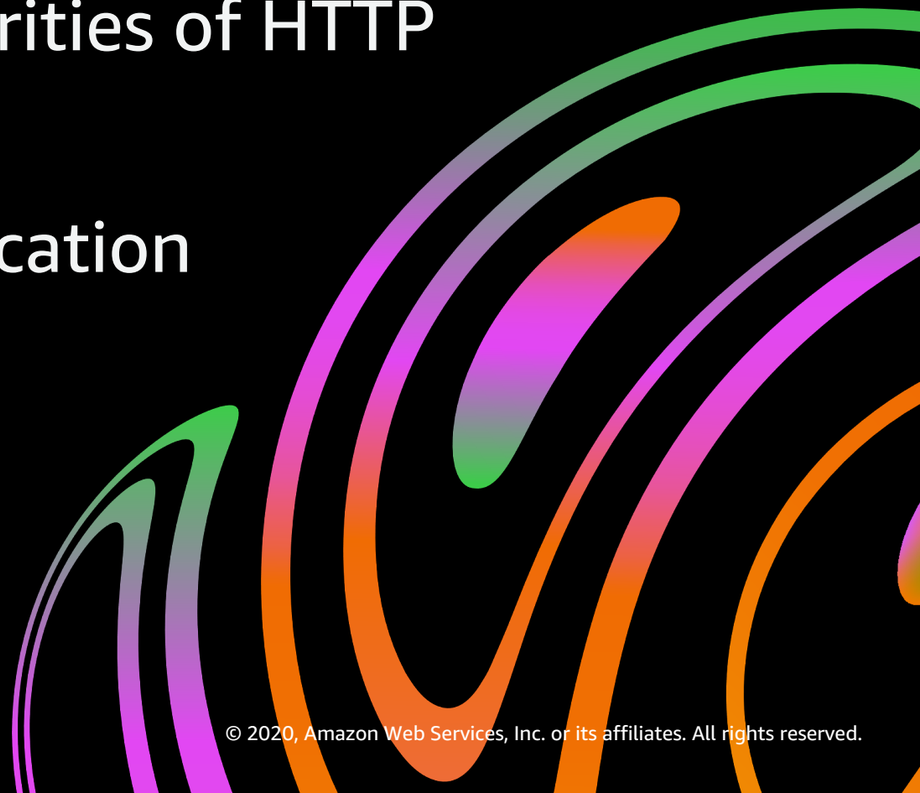
AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What to expect from the session

- 400-level session
- Learn how to implement the different types of authorization and authentication for HTTP APIs on Amazon API Gateway
- Highlight authorization differences and similarities of HTTP vs. REST APIs
- Learn how to implement mutual TLS authentication (mTLS) with your HTTP APIs



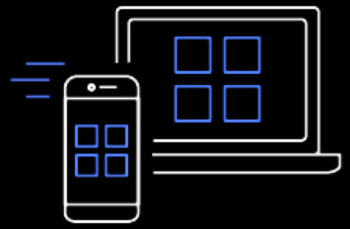
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

HTTP APIs for Amazon API Gateway

Improved cost efficiency, improved performance, and better usability compared to REST APIs



Cost efficiencies by up to 70 percent



Reduced application latency by up to 50 percent



Configure HTTP APIs easier and faster than before

Controlling and managing access to HTTP APIs

- JWT authorizers
- Lambda authorizers
- IAM authorization
- mTLS authentication

When to use each authorization method & why

	Use case
JWT authorizer	Support OAuth2 flows with minimal coding
Lambda authorizer	Leverage a Lambda function for your authorization flow
IAM authorization	AWS IAM credentials for authentication
mTLS authentication	Client certificate authentication; support regulatory requirements – e.g., *Open Banking*

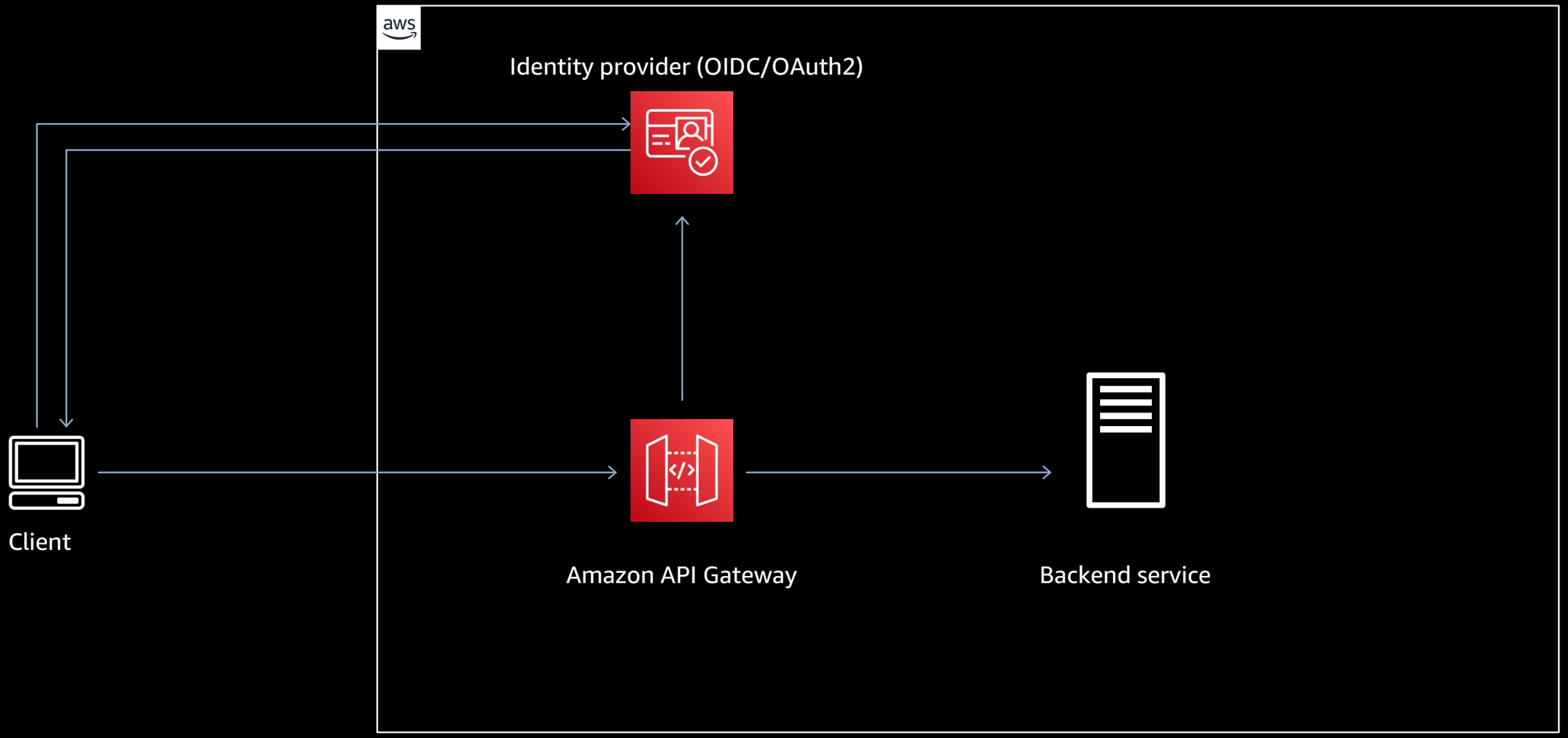
JWT authorizers



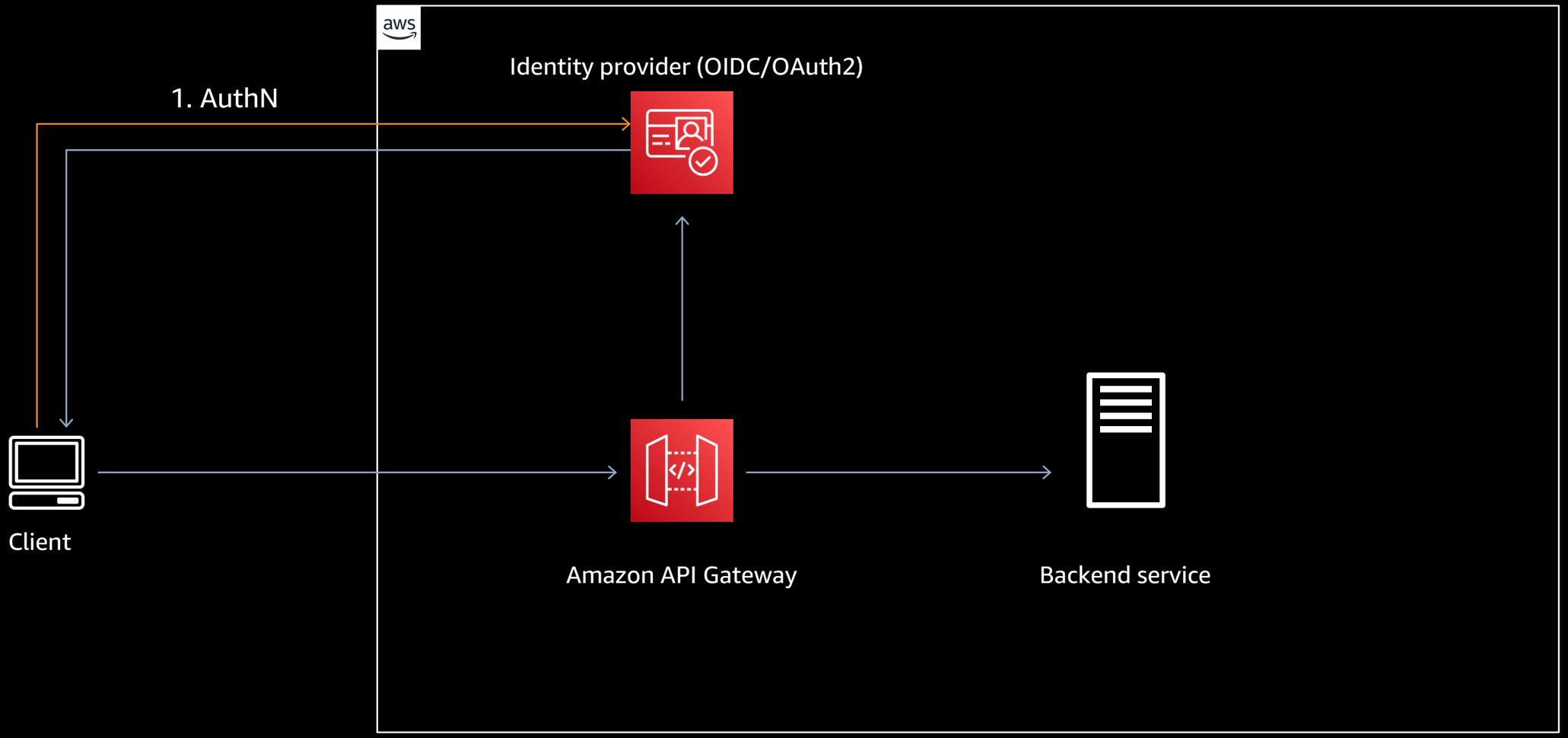
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

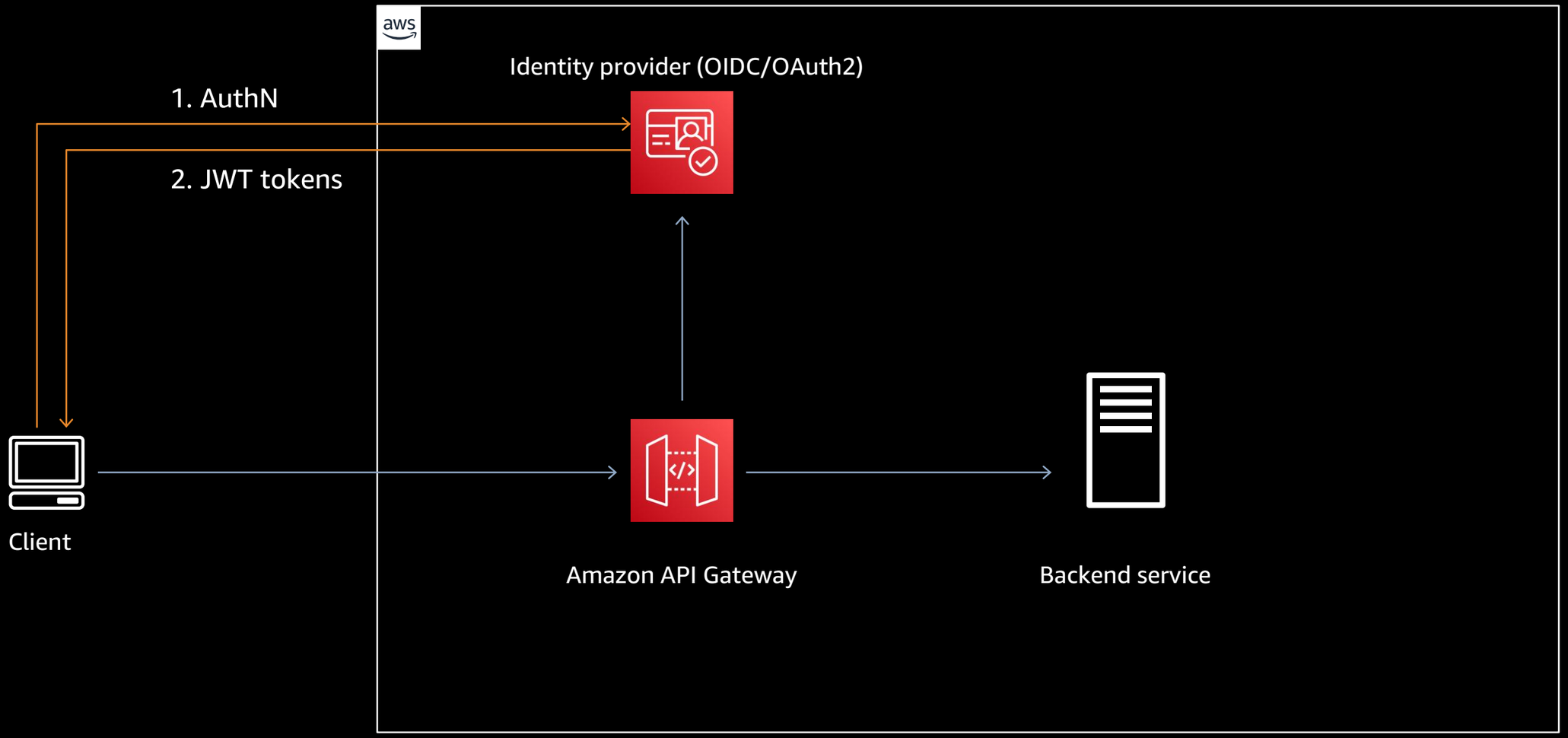
JWT authorizer flow



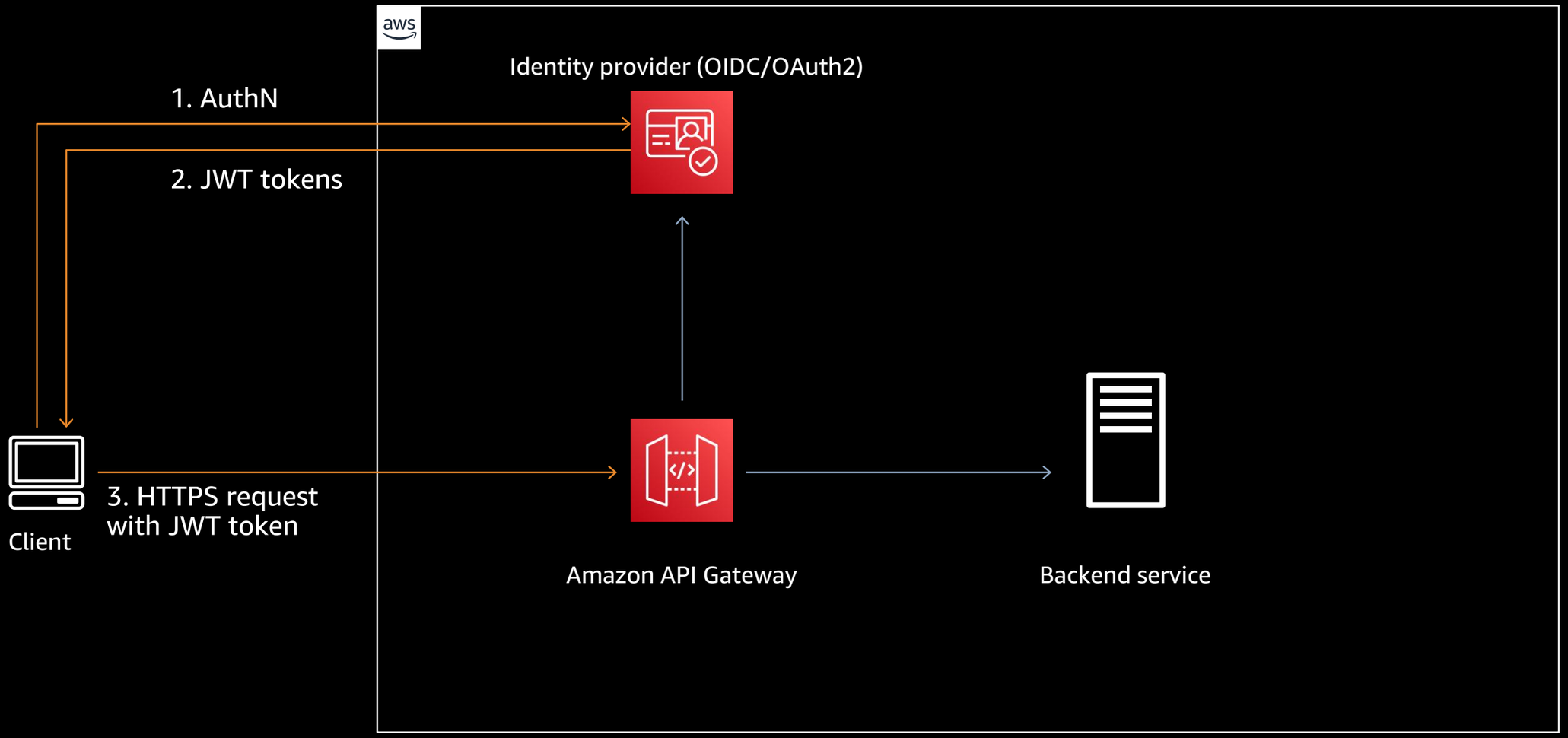
JWT authorizer flow



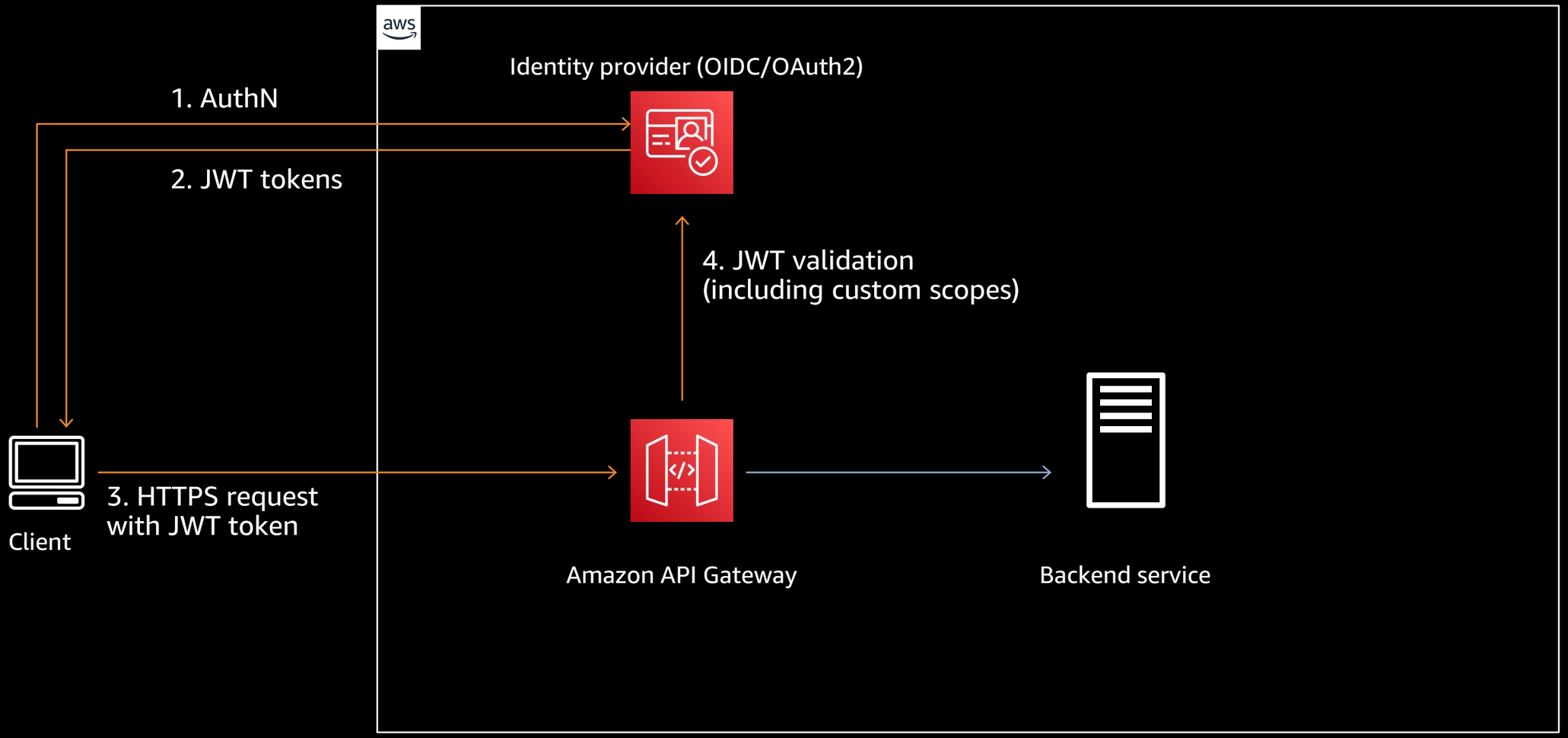
JWT authorizer flow



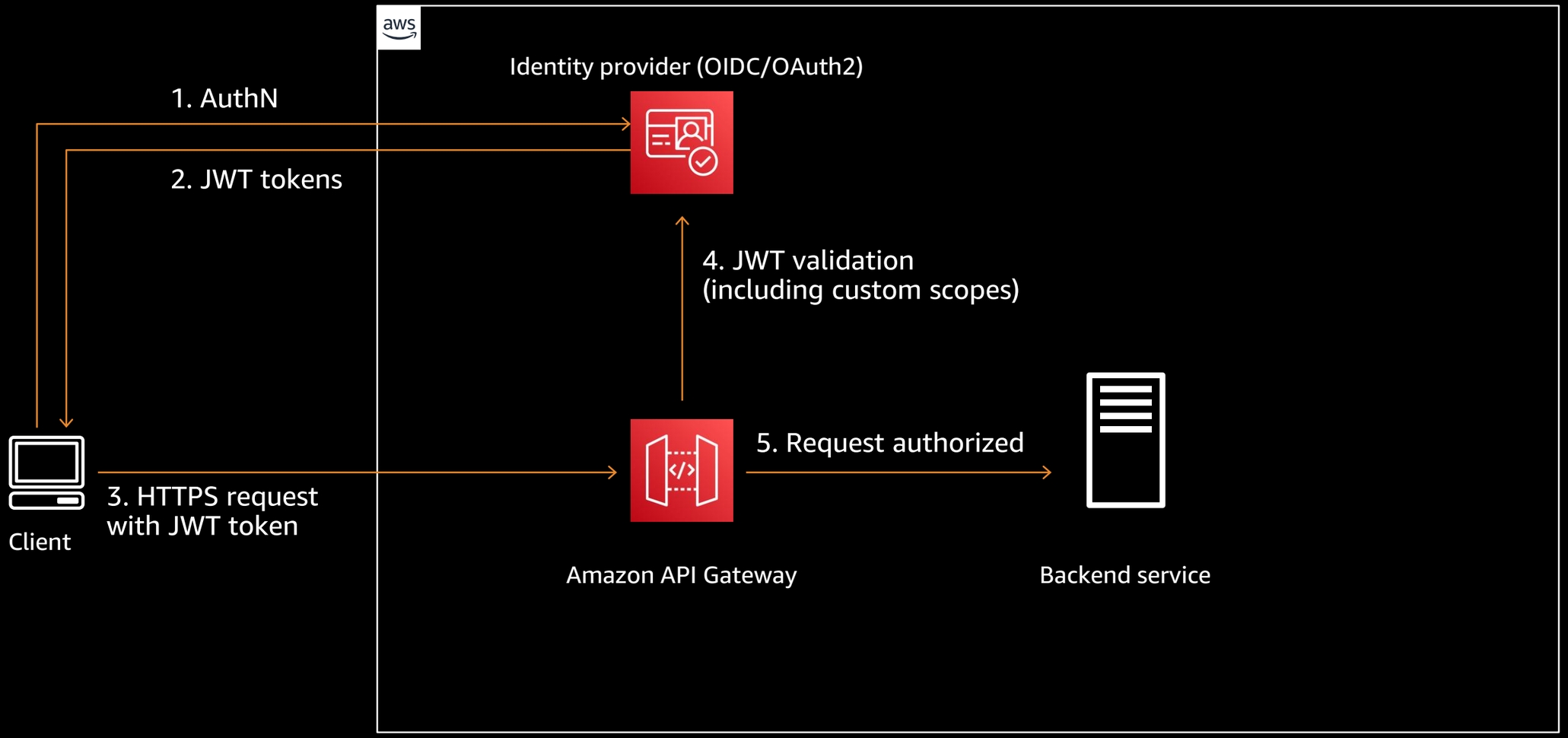
JWT authorizer flow



JWT authorizer flow



JWT authorizer flow



Lambda authorizers



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lambda authorizer payload formats

- v1.0 event payload format
  - Compatibility event format with REST API Lambda authorizer

- v2.0 event payload format
  - Very similar to the v1.0 payload format but with some breaking changes

You need to specify the event payload version using authorizerPayloadFormatVersion when creating an authorizer using AWS CLI, SDK, or CloudFormation

Lambda authorizer payload formats

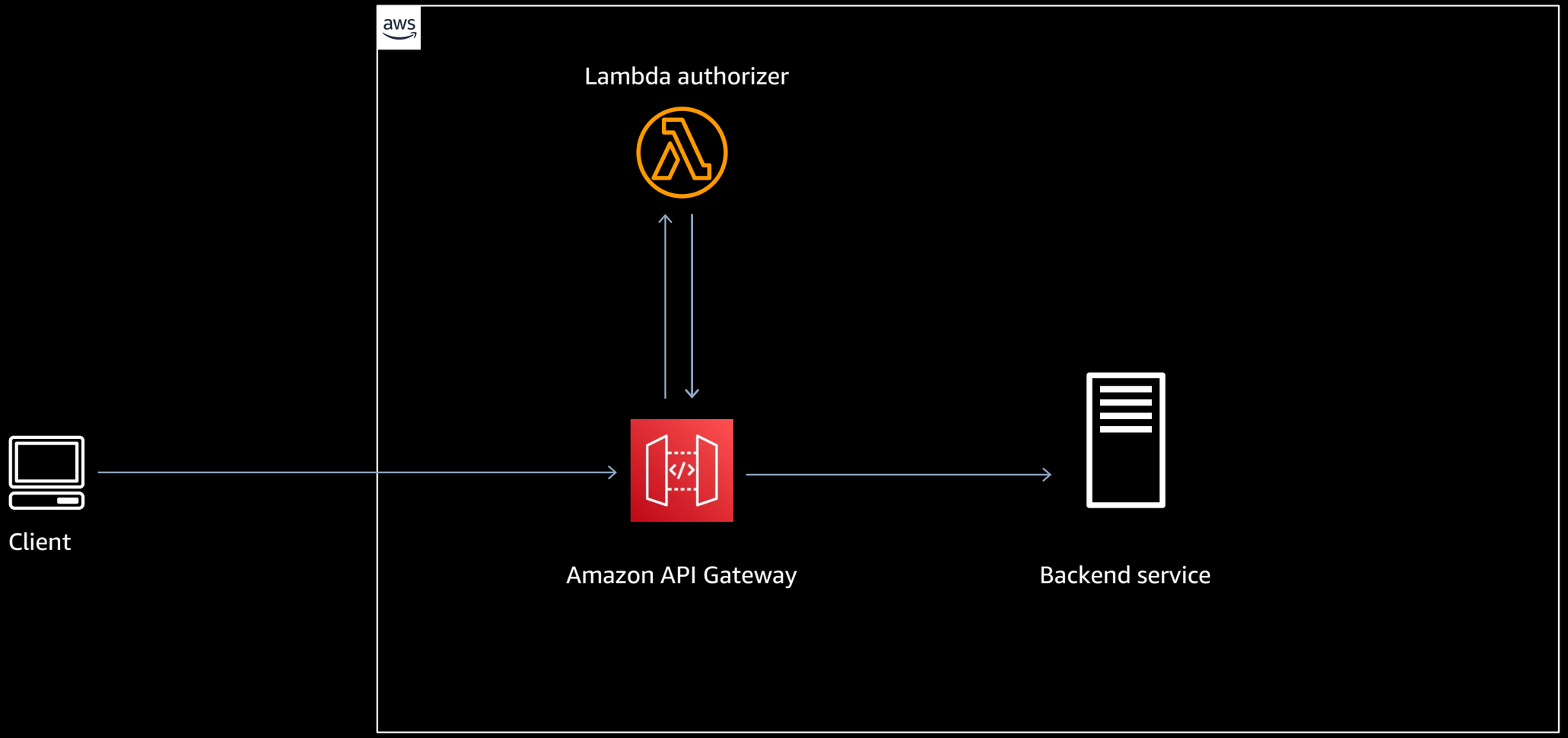
- v1.0 Lambda response format
  - Compatibility response format with REST API Lambda authorizer
  - Returning an IAM policy

- v2.0 Lambda response format
  - Returning a *Boolean value or an IAM policy

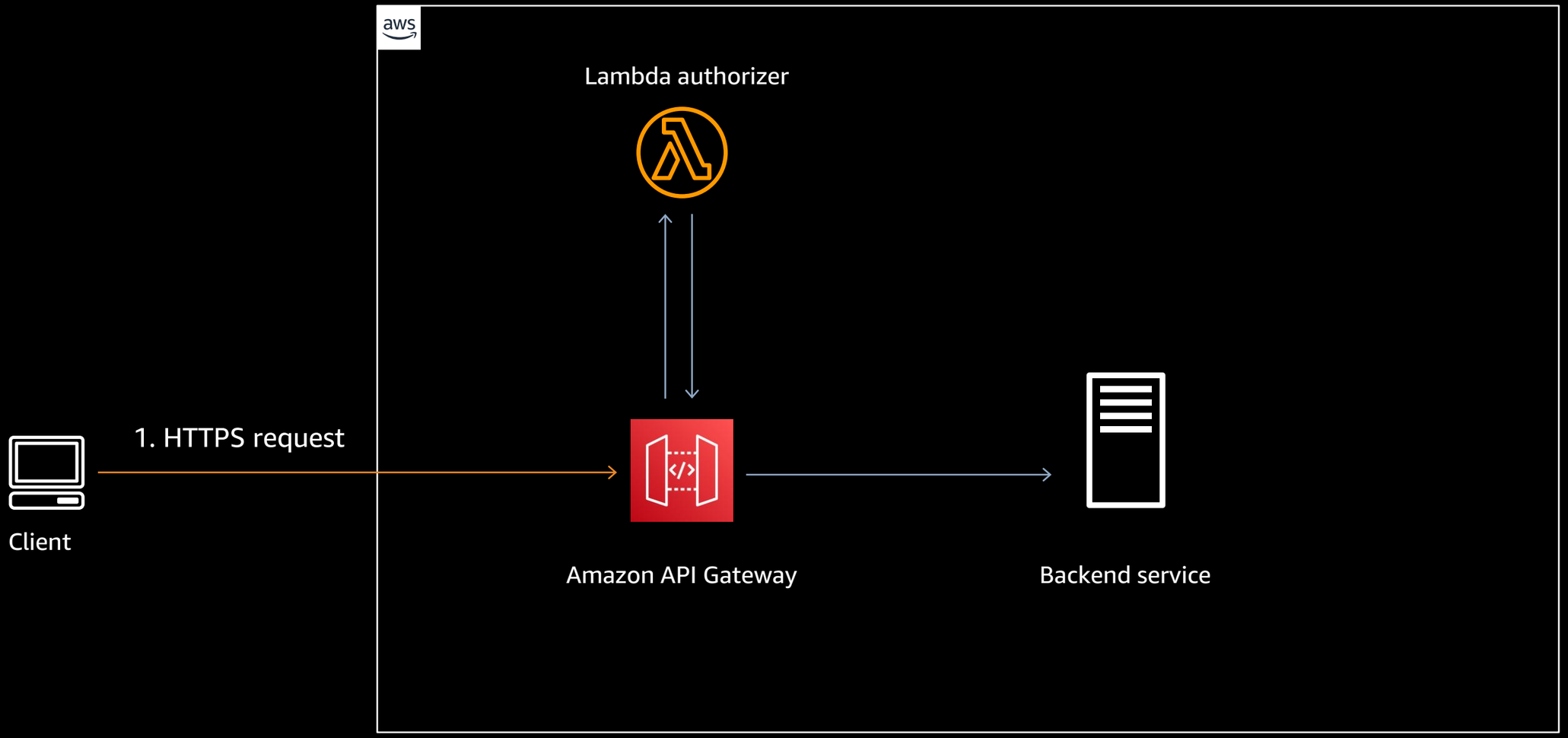
*Boolean (simple) response format

```
{
  "isAuthorized": true/false,
  "context": {
    "exampleKey": "exampleValue"
  }
}
```

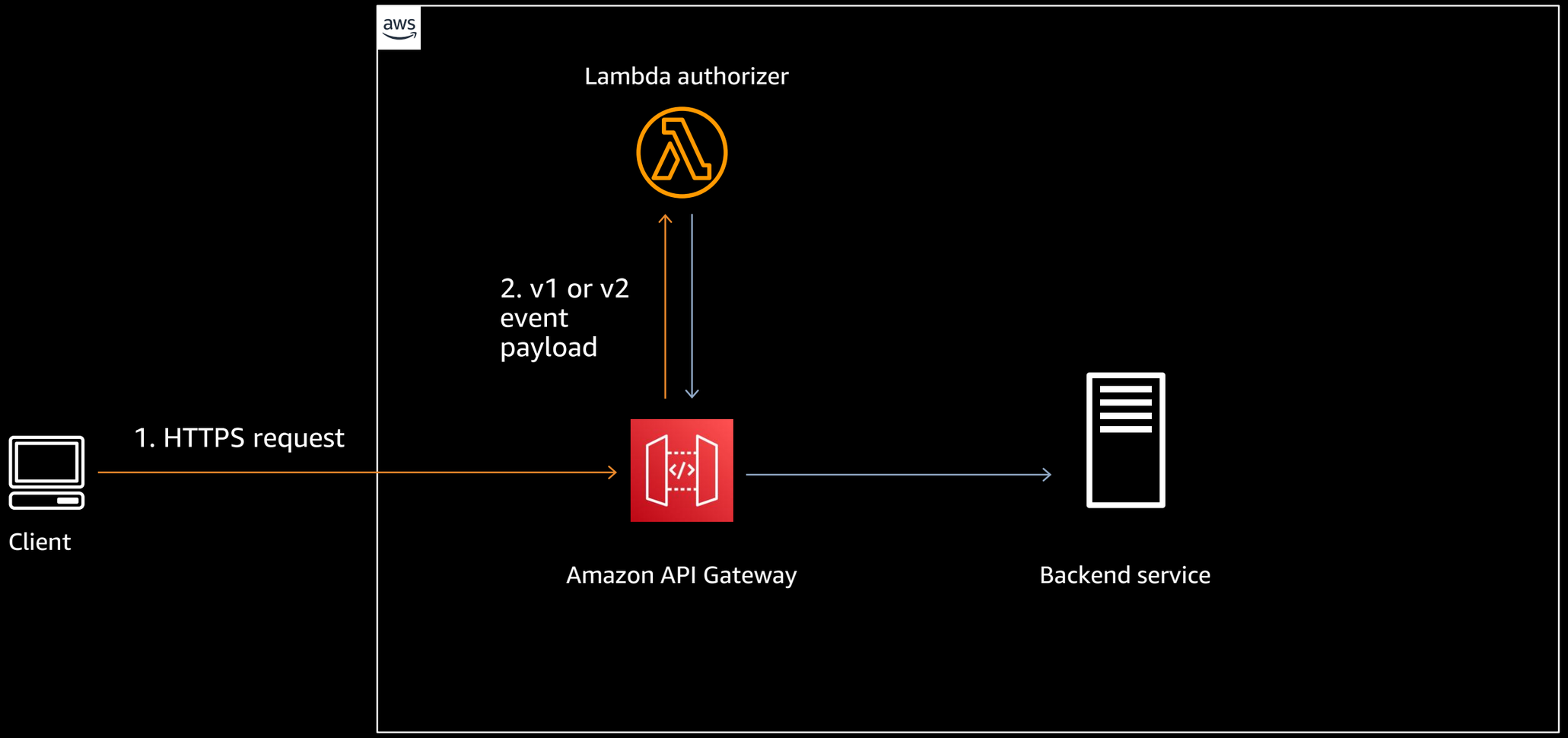
Lambda authorizer flow



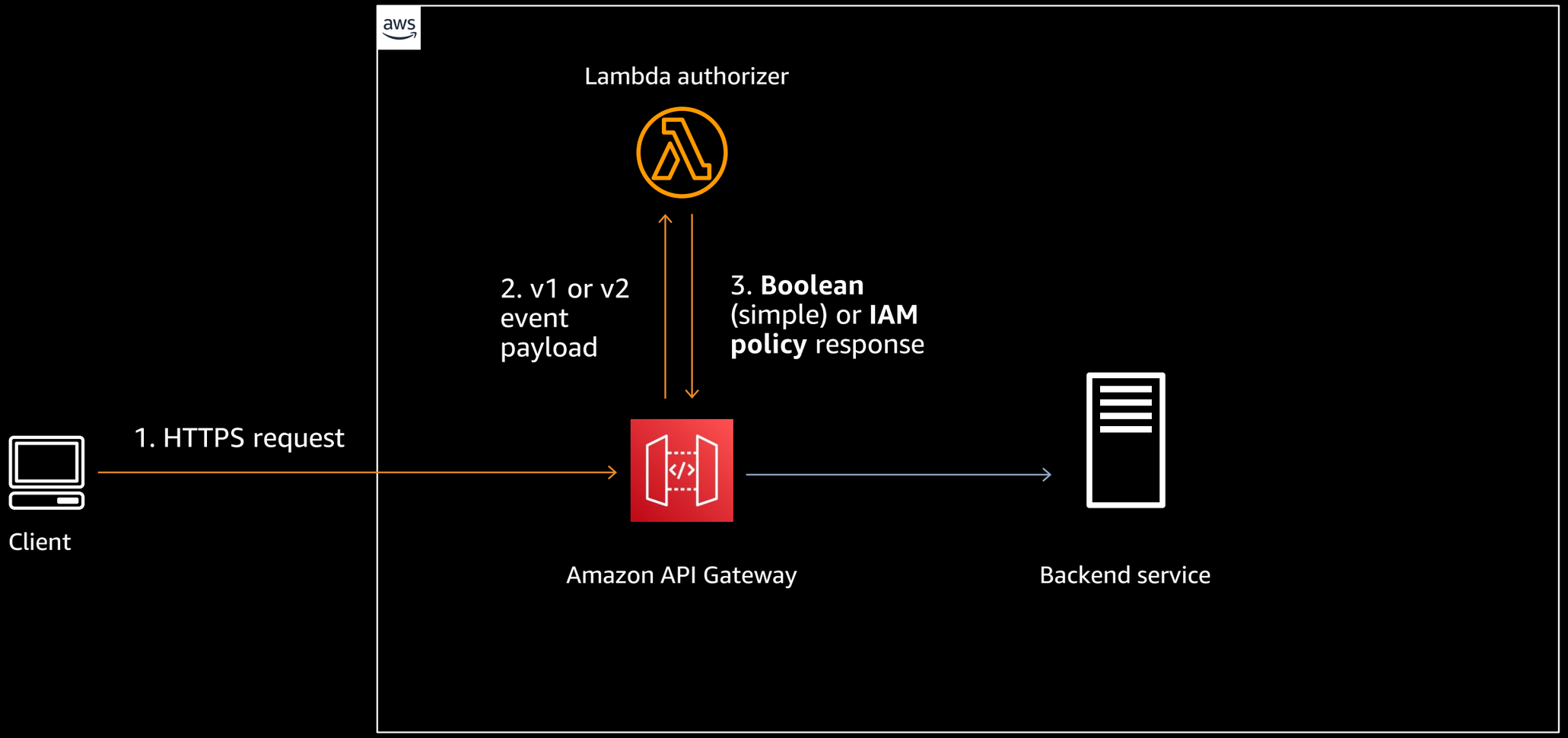
Lambda authorizer flow



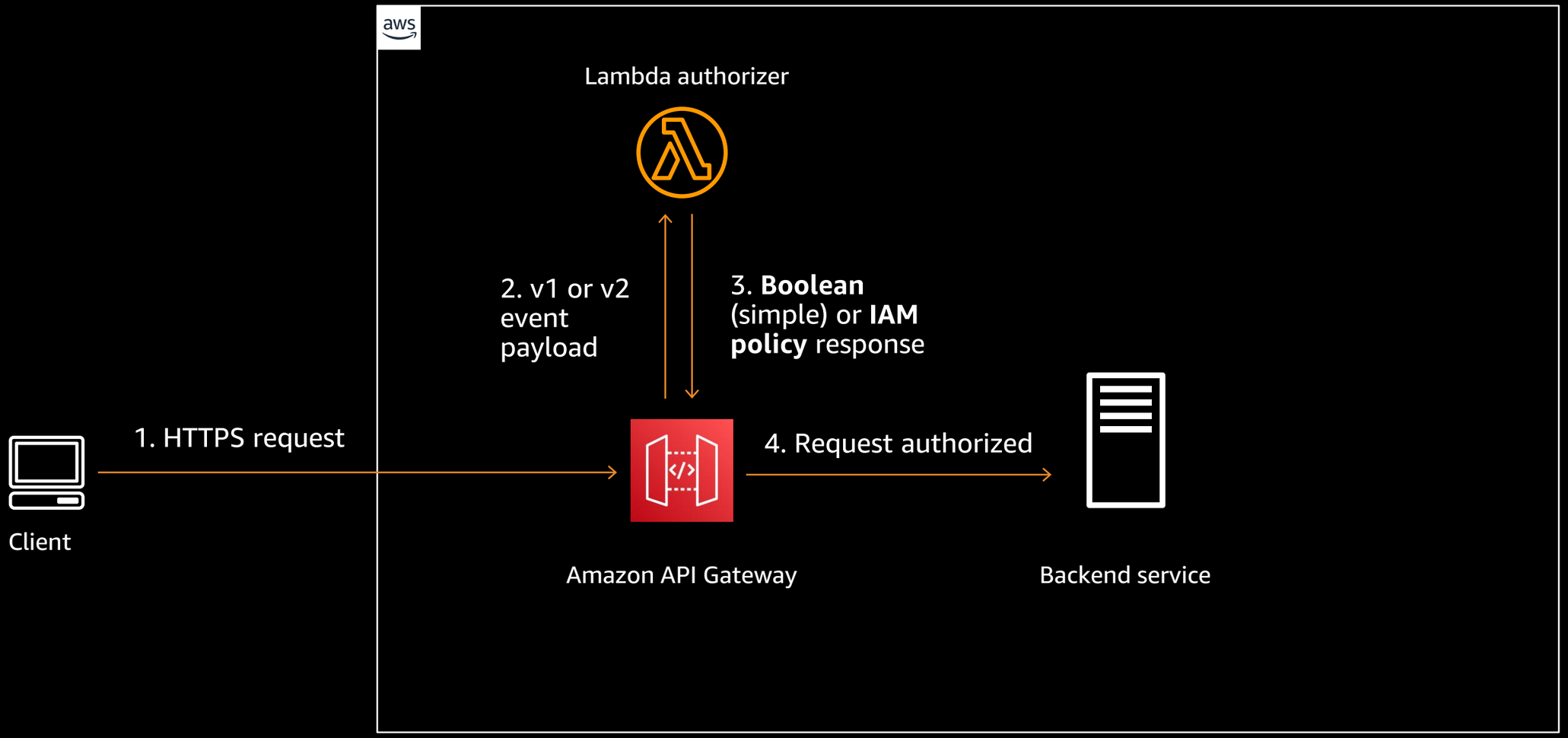
Lambda authorizer flow



Lambda authorizer flow



Lambda authorizer flow



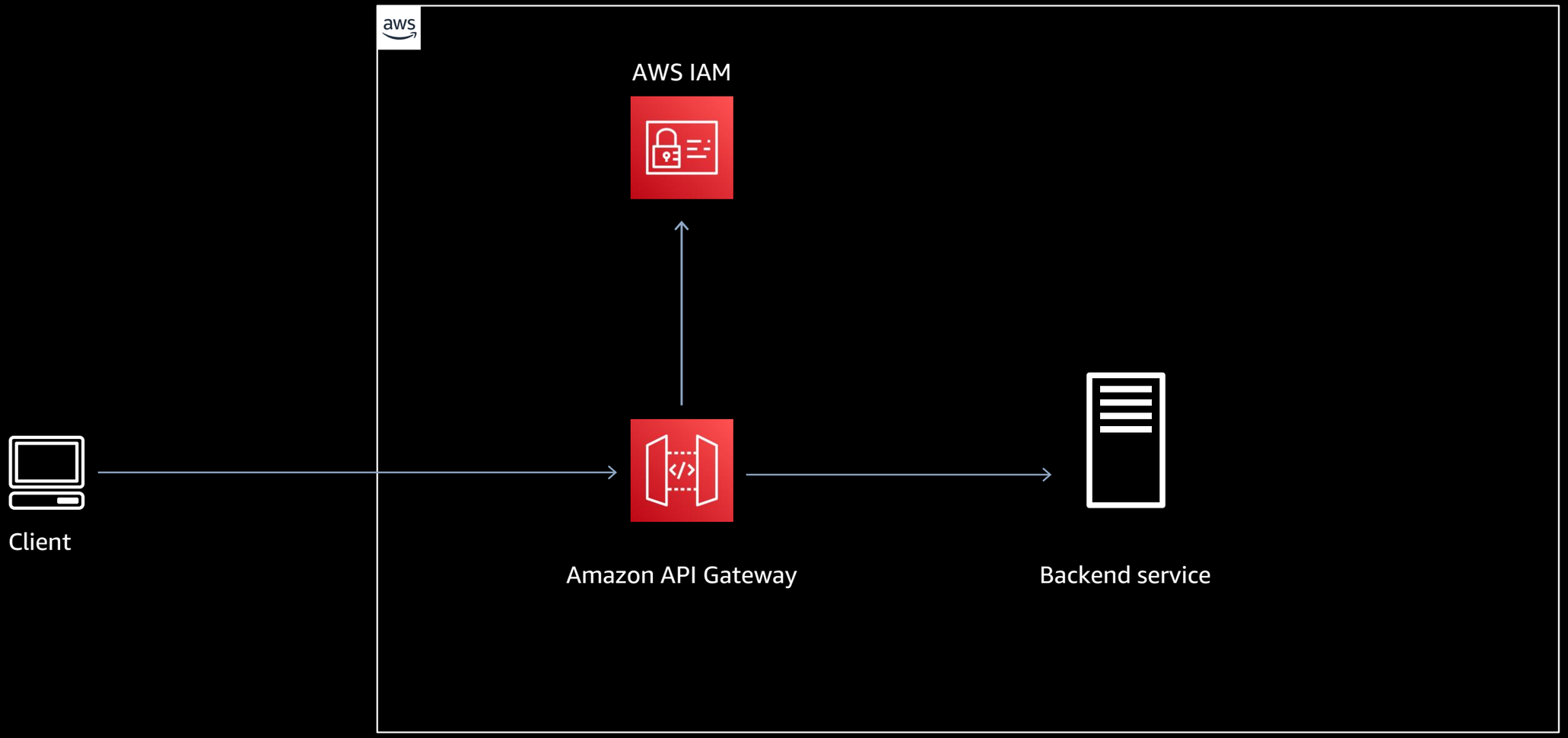
IAM authorization



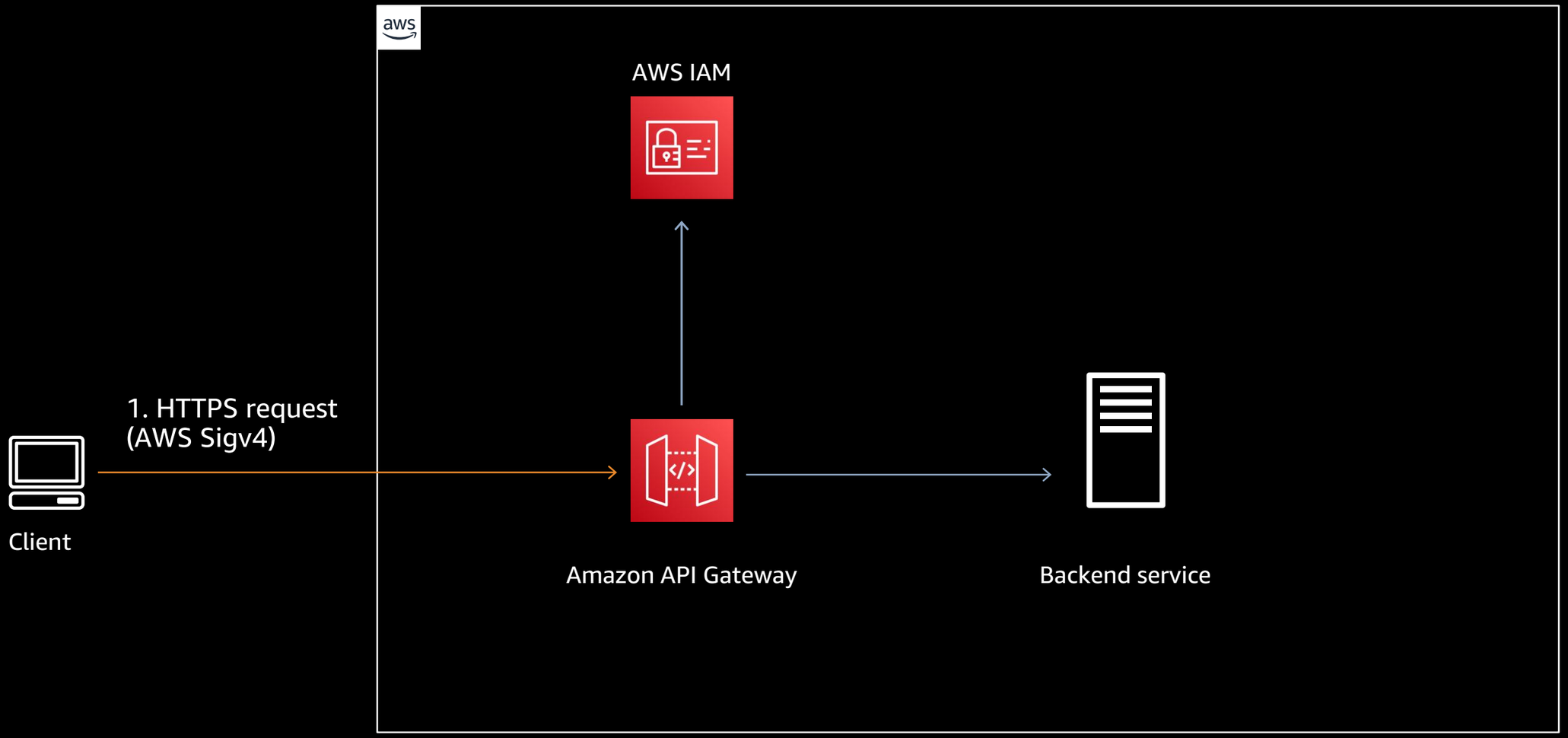
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

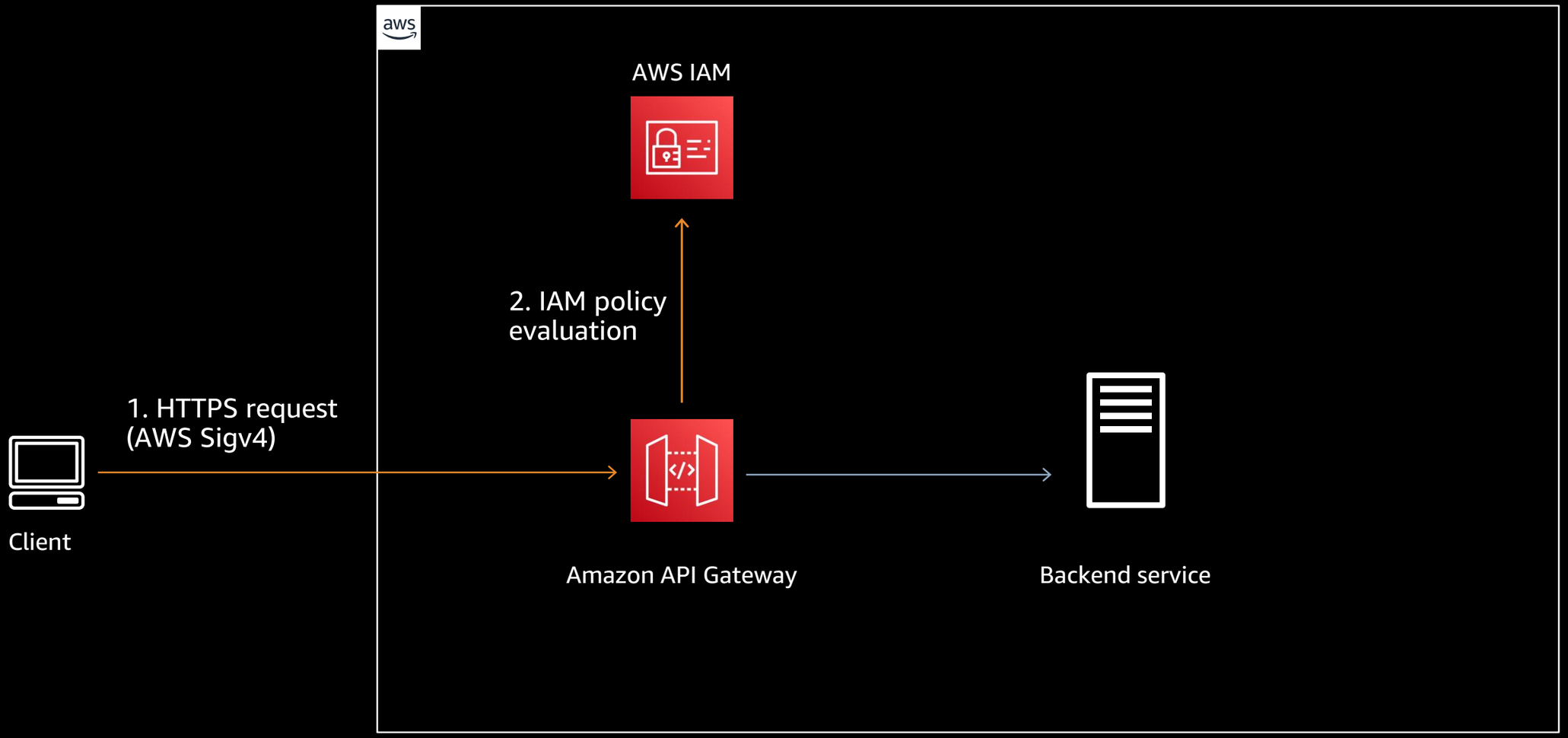
IAM authorizer flow



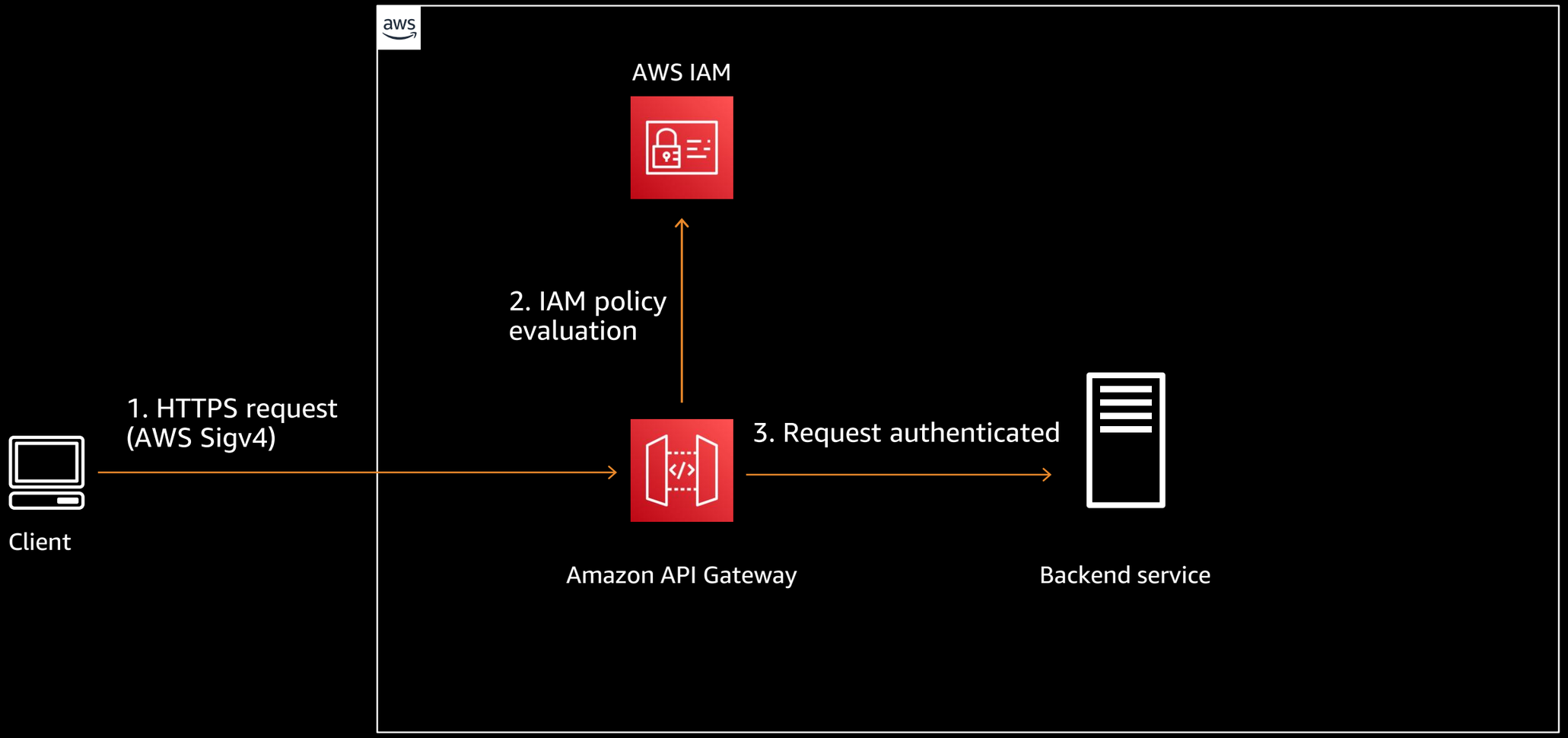
IAM authorizer flow



IAM authorizer flow



IAM authorizer flow



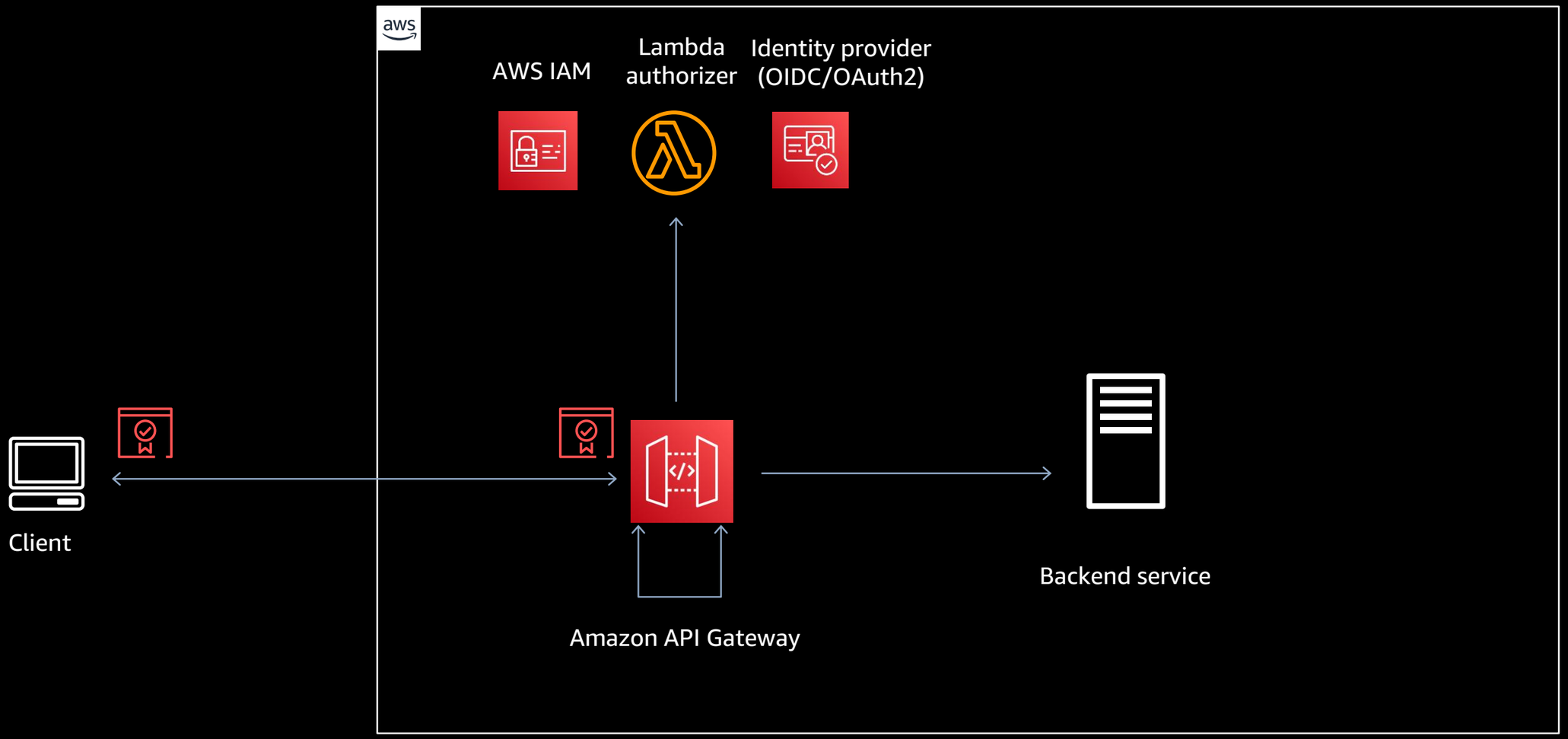
HTTP APIs and mTLS



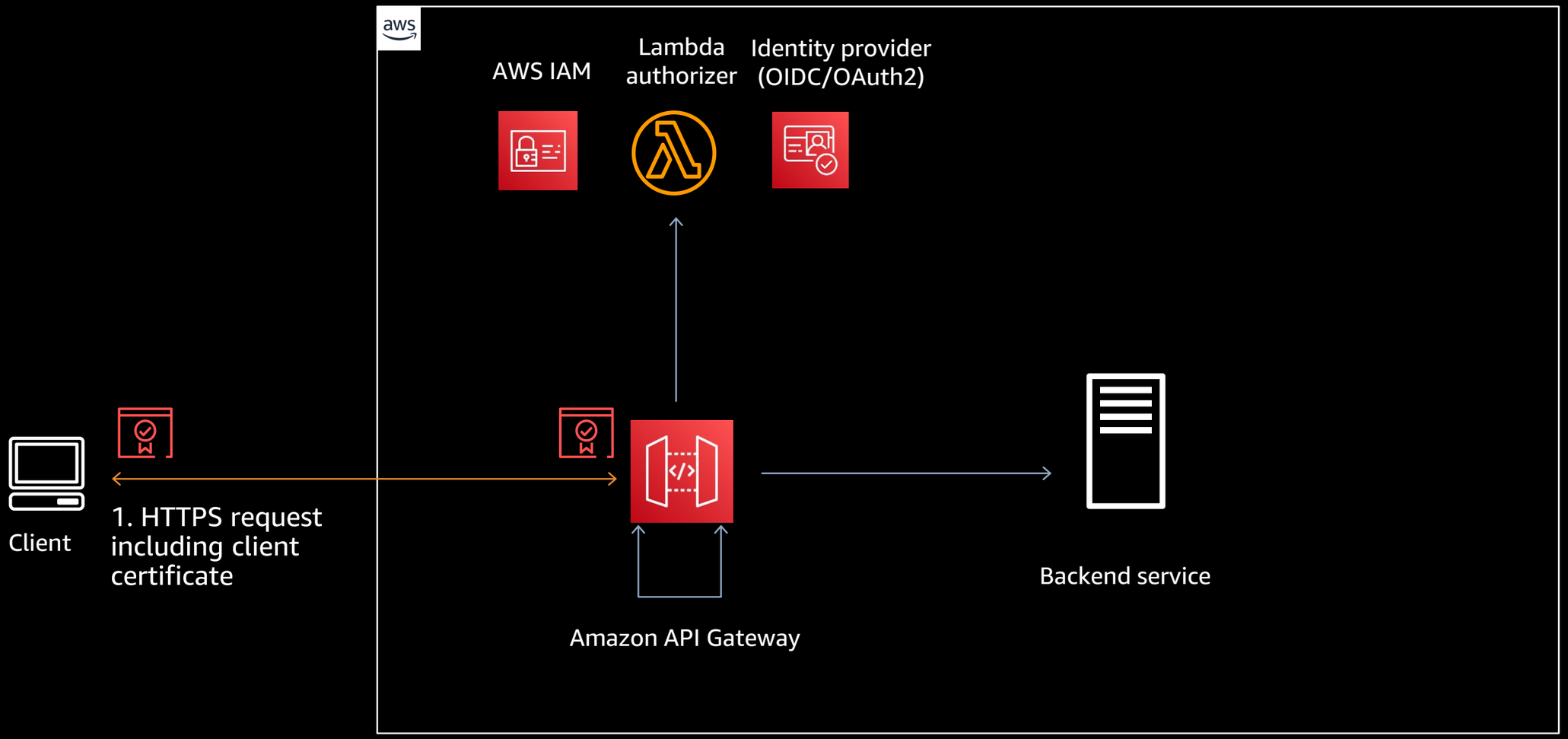
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

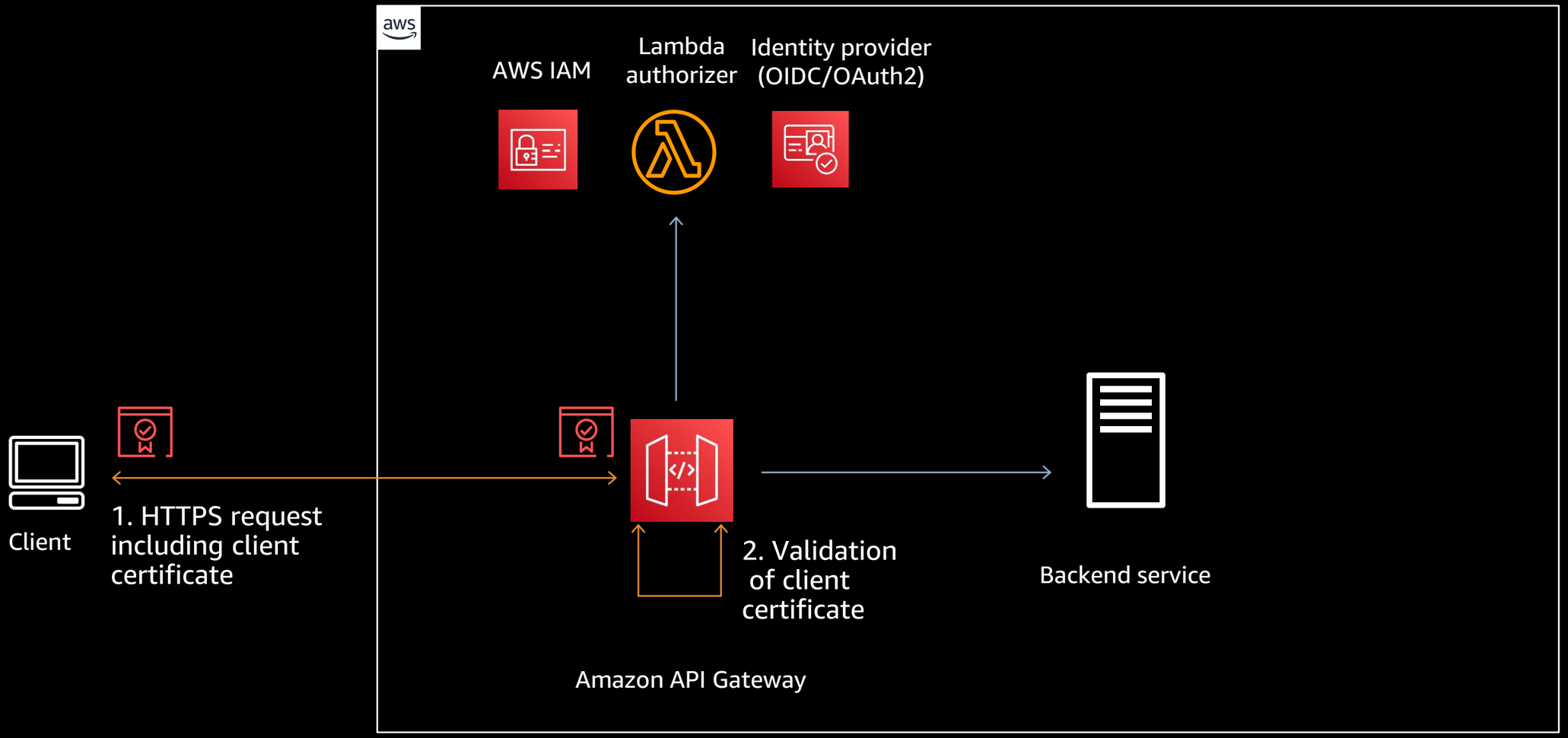
mTLS authentication



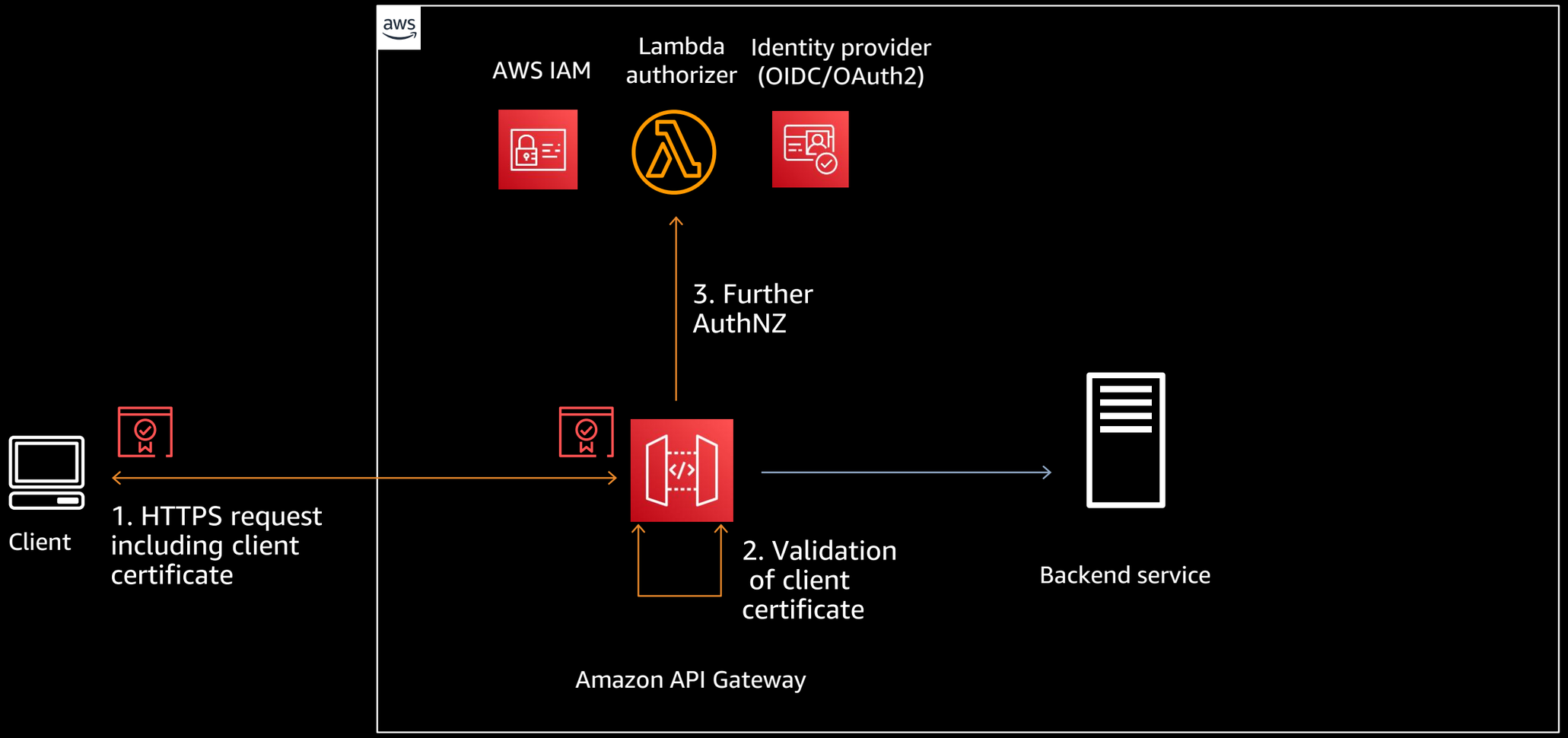
mTLS authentication



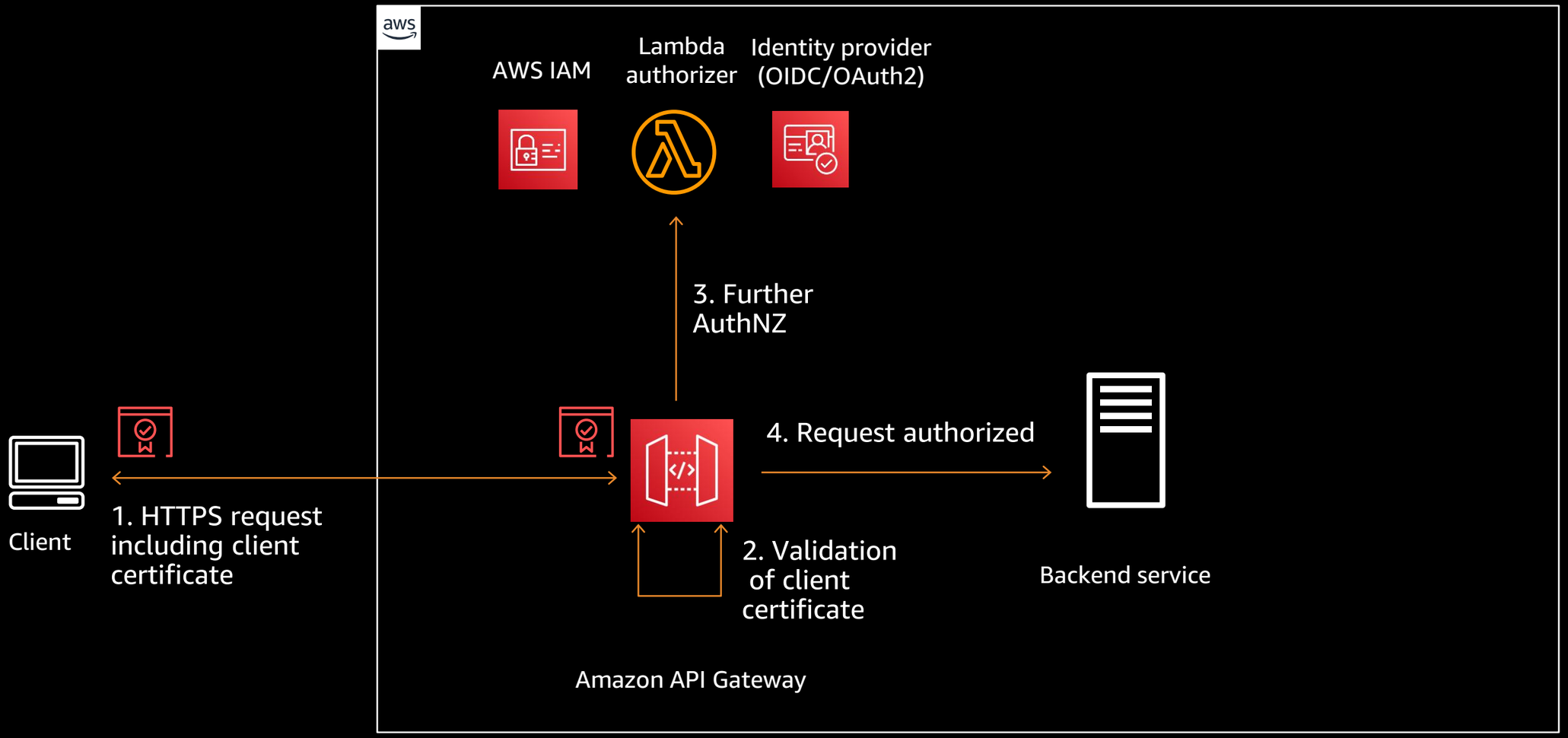
mTLS authentication



mTLS authentication



mTLS authentication



Wrap-up

- You can achieve many efficiencies by using HTTP APIs, such as improved cost, performance, and better usability

- HTTP APIs offer many flexible ways of authentication and authorization
  - JWT authorizer, Lambda authorizer, IAM authorization, mTLS authentication

- There is compatibility for Lambda authorizers between HTTP APIs and REST APIs on Amazon API Gateway

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.