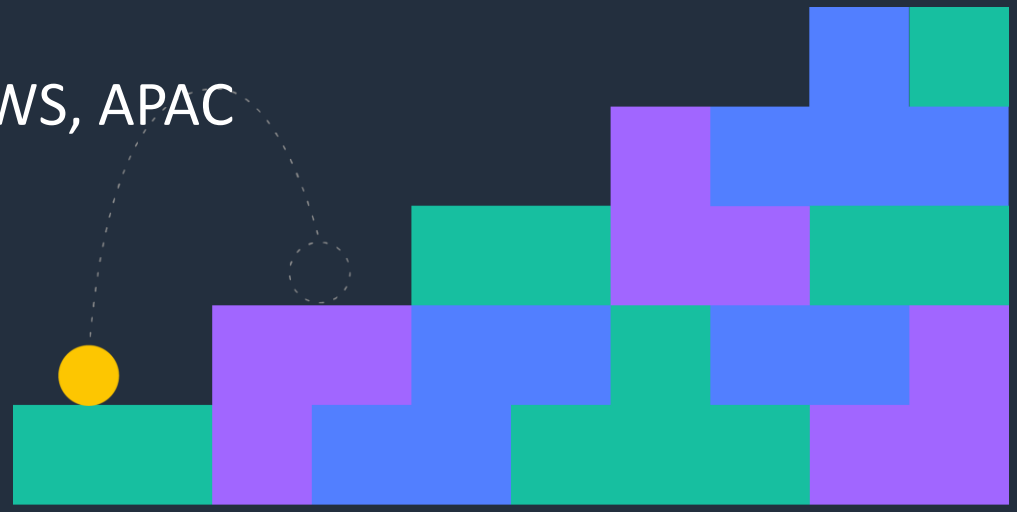
AWS Quick Start

A Practitioner's Guide to Securing Your Cloud (Like an Expert)

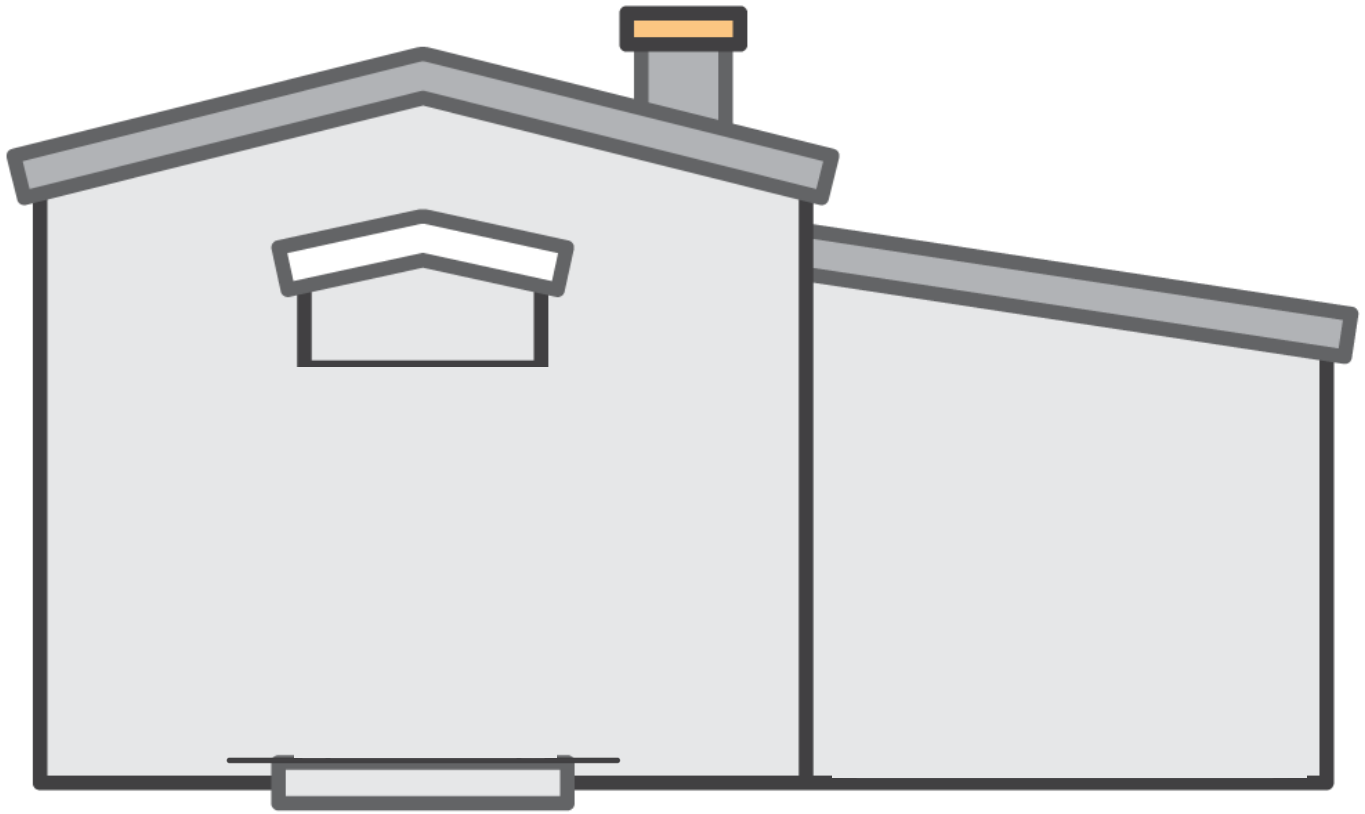
Gabe Hollombe, Senior Technical Evangelist, AWS, APAC

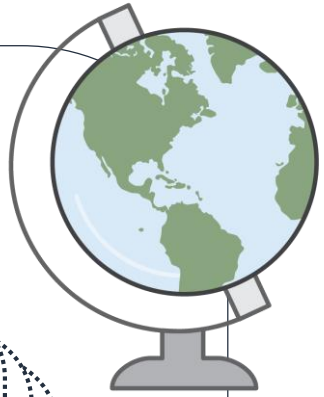


Agenda: Develop your cloud security know-how

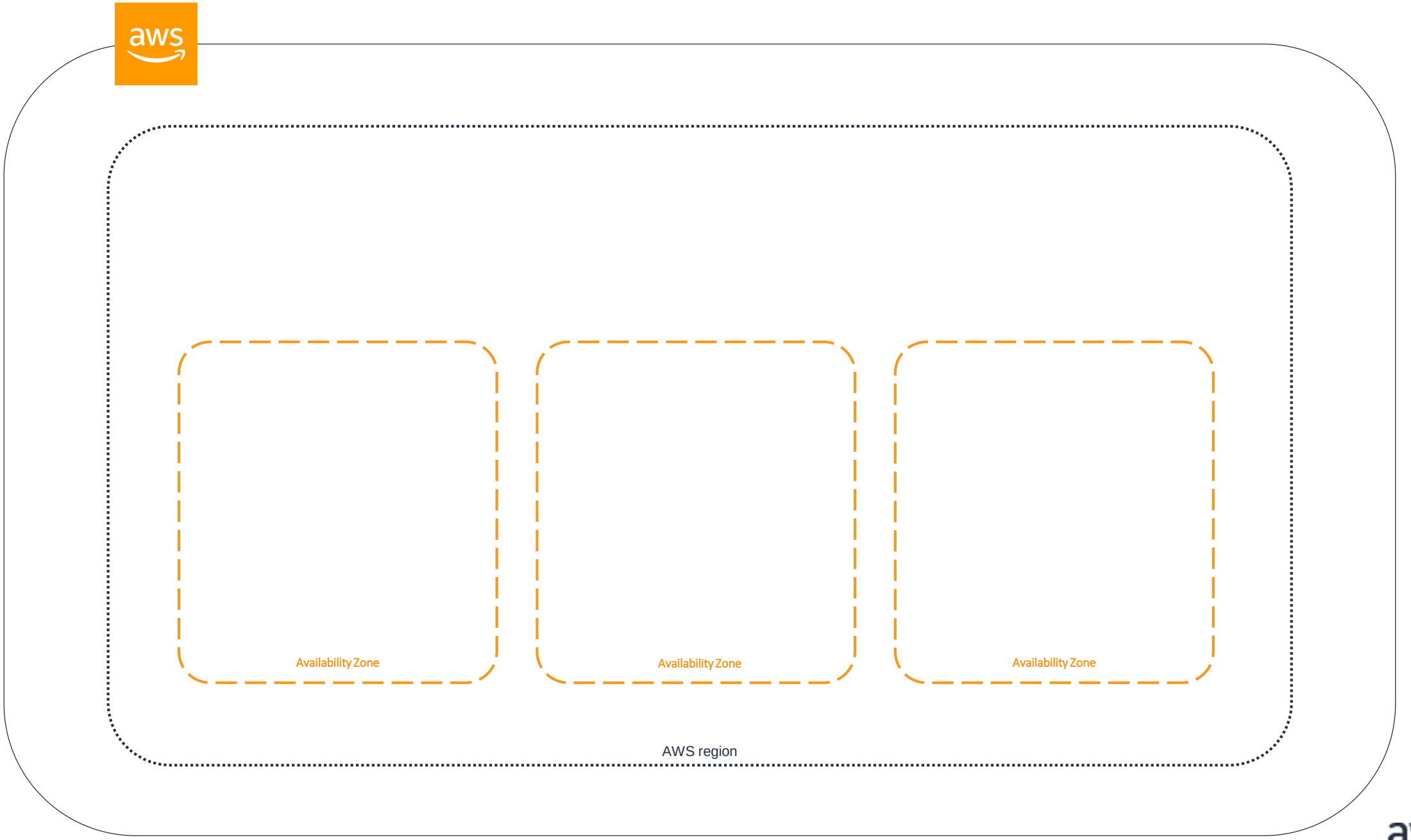
- Become familiar with the different types of AWS resources
- Quickly get up to speed with a practical overview of AWS's identity-based and network-based security controls
- Know how to interpret and implement AWS security controls

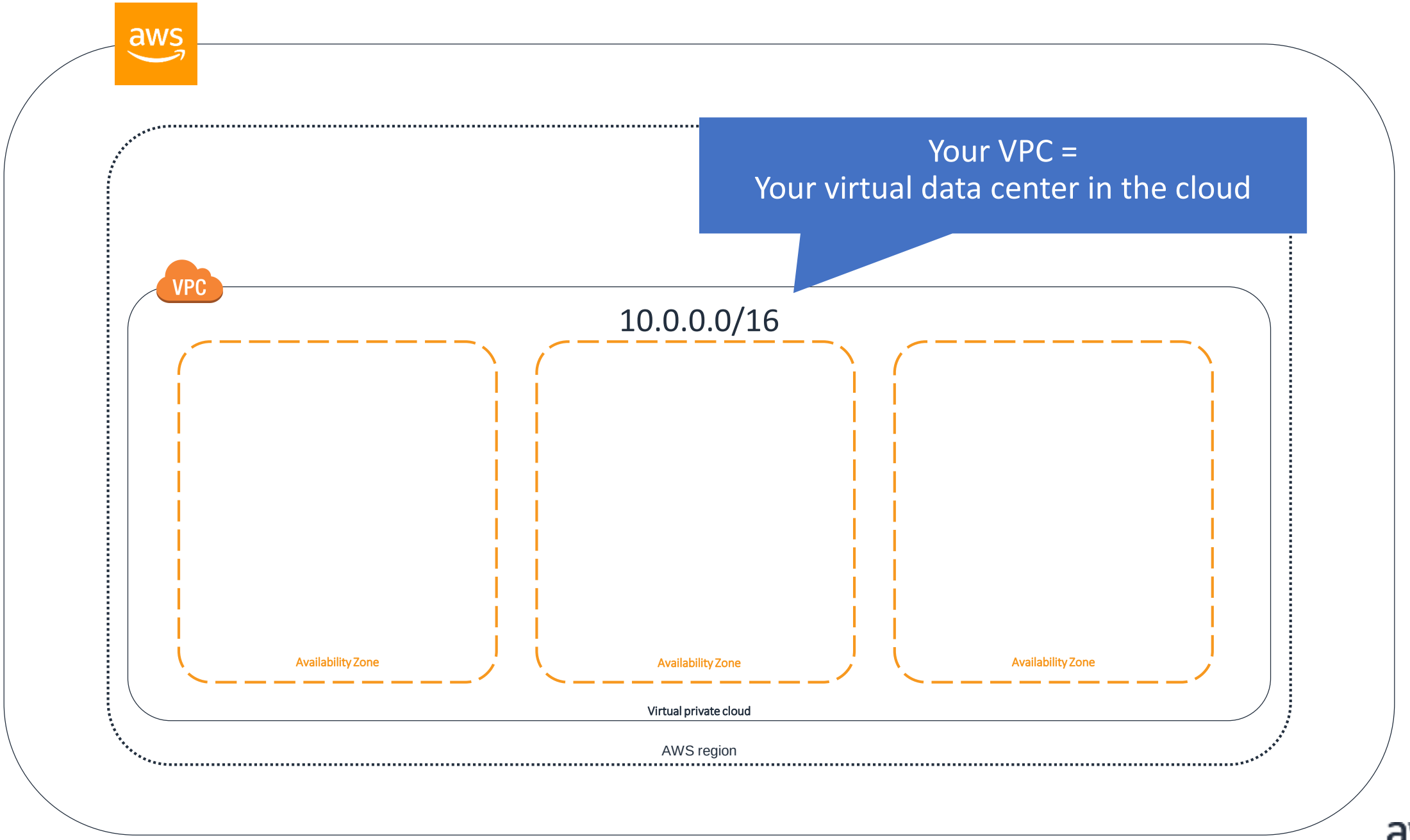
Where’s my [AWS] stuff?

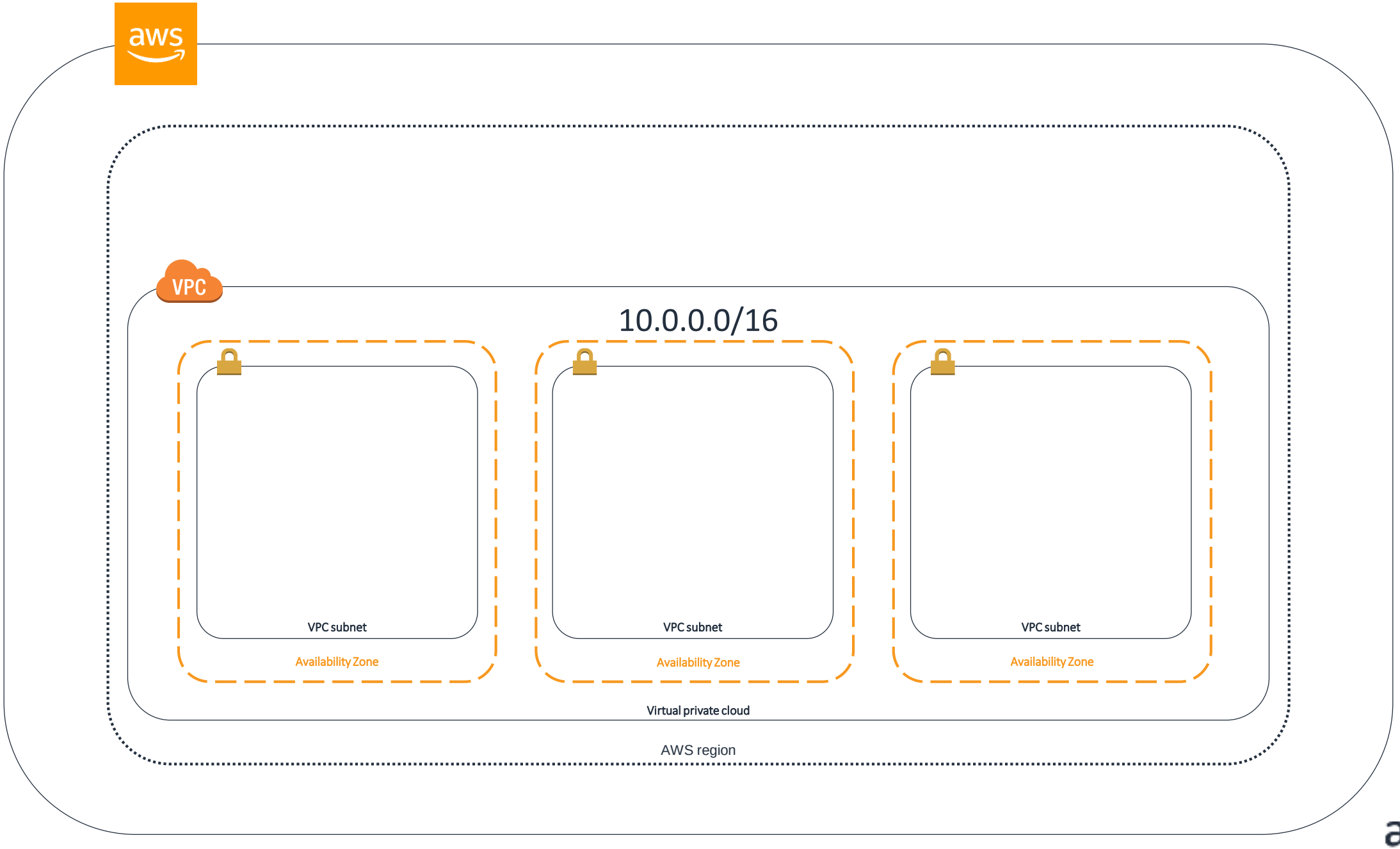


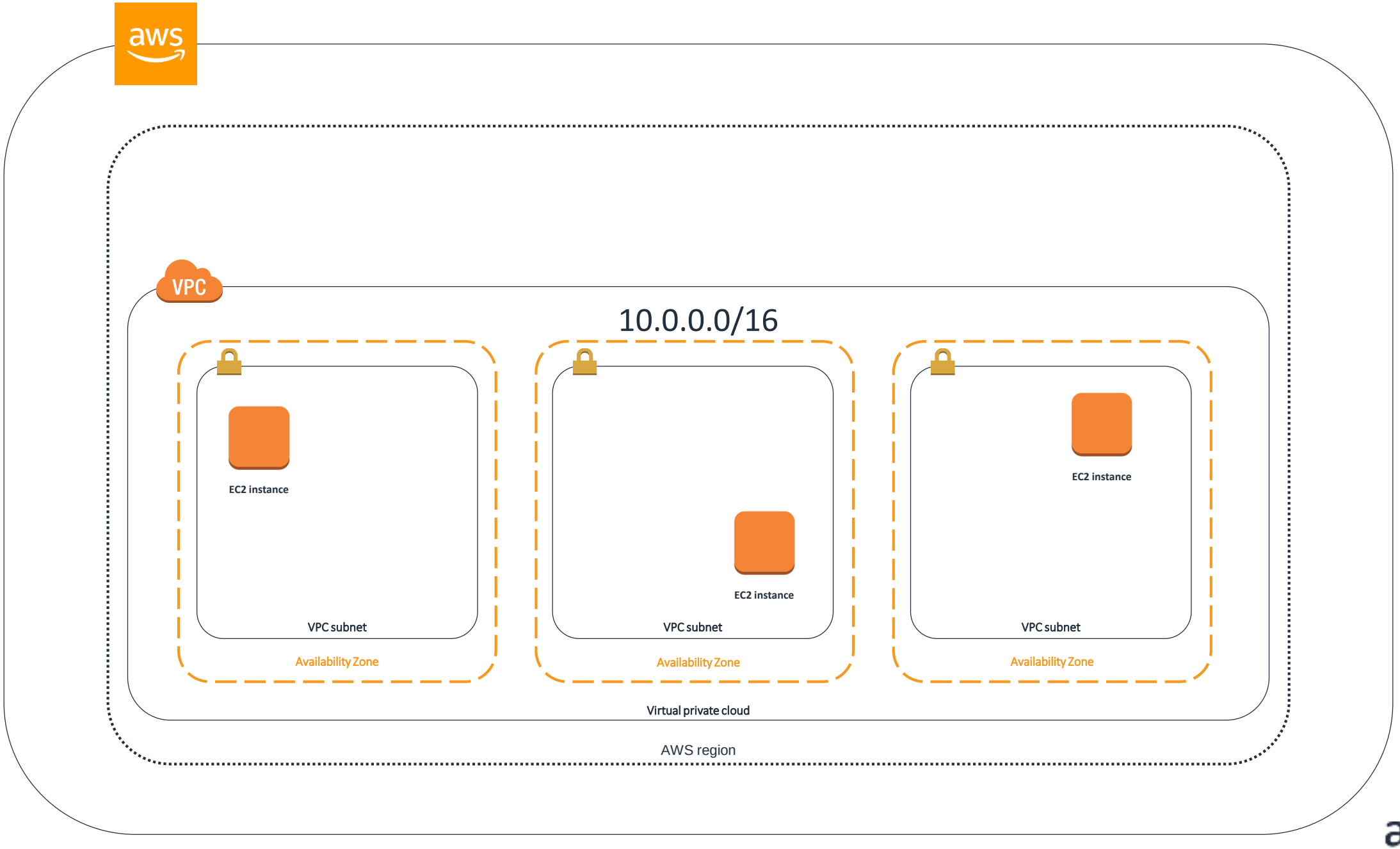


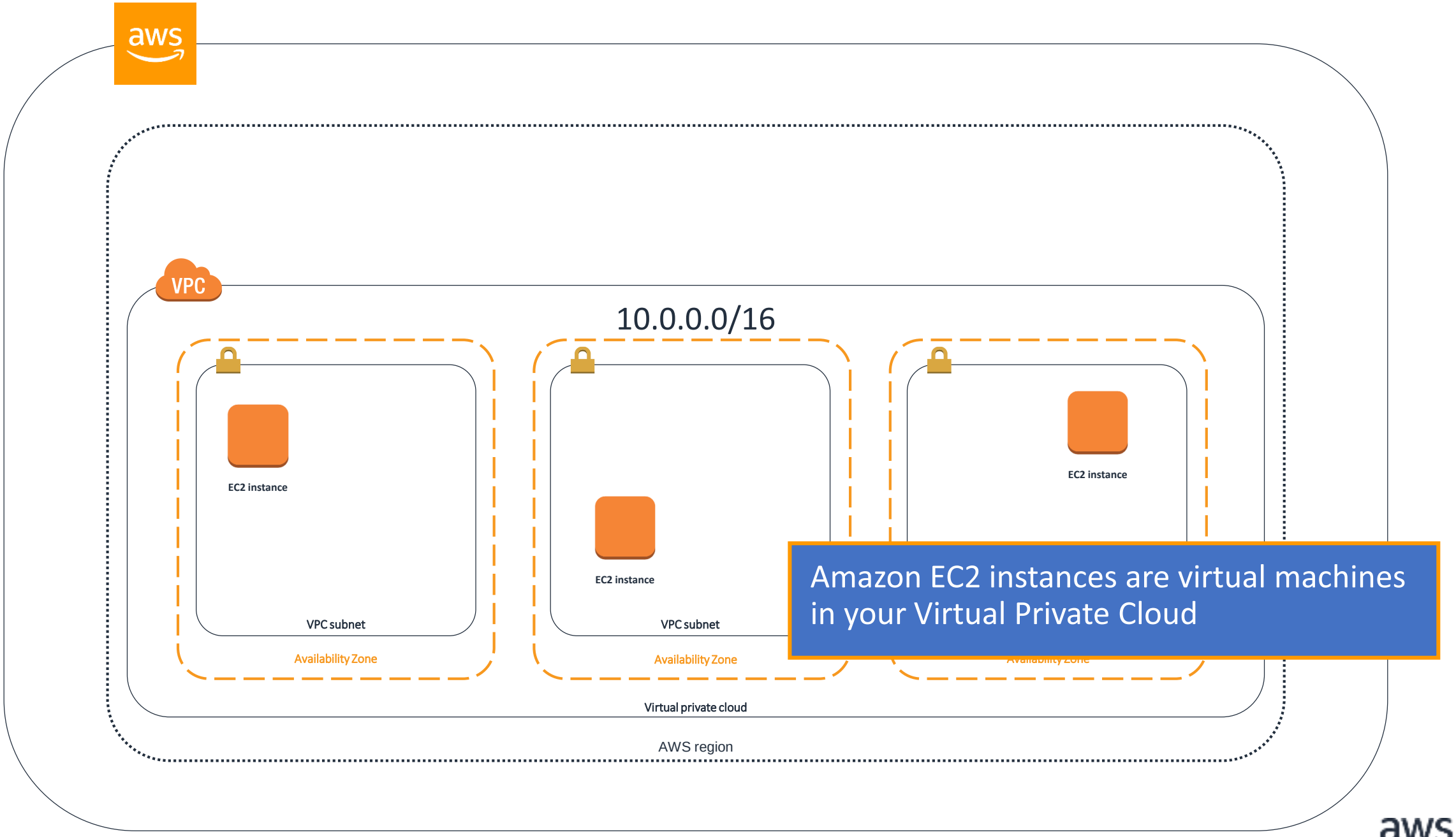
AWS region



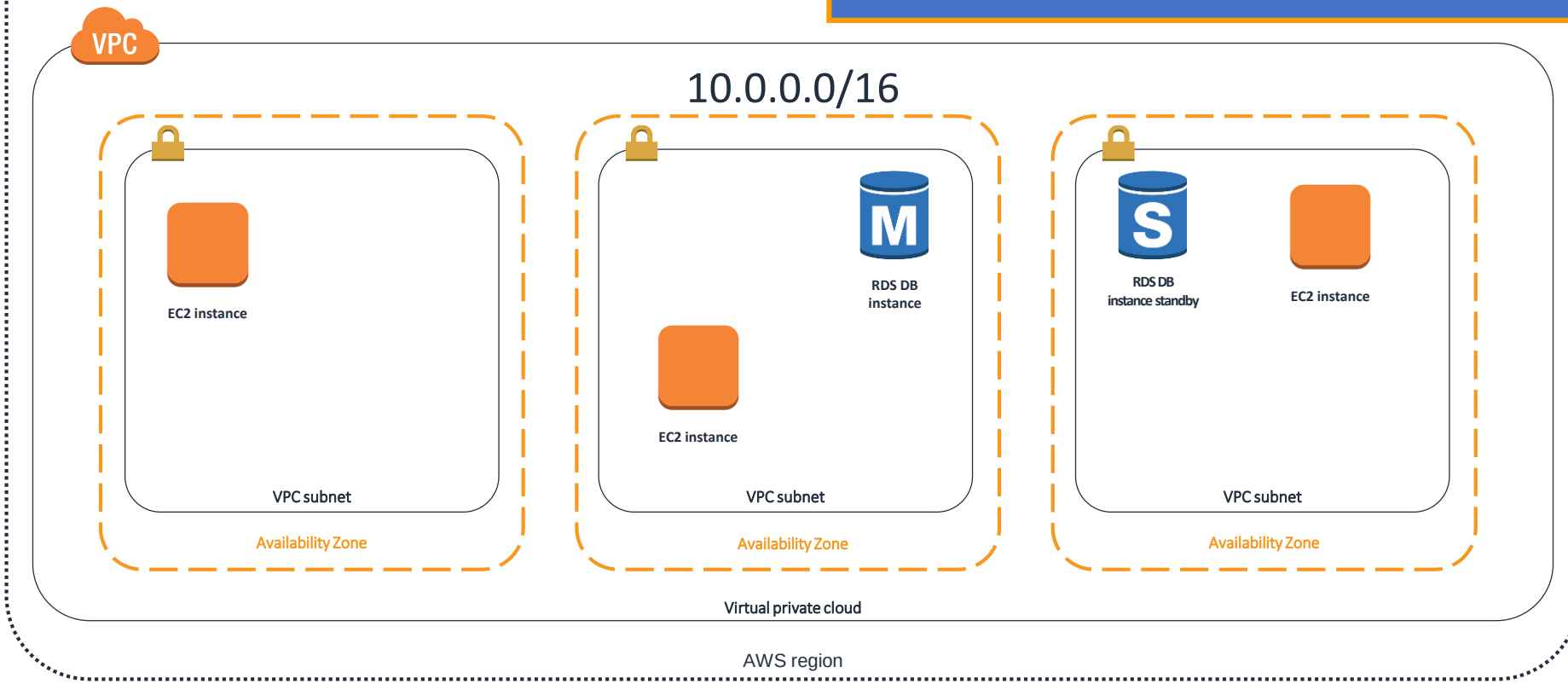




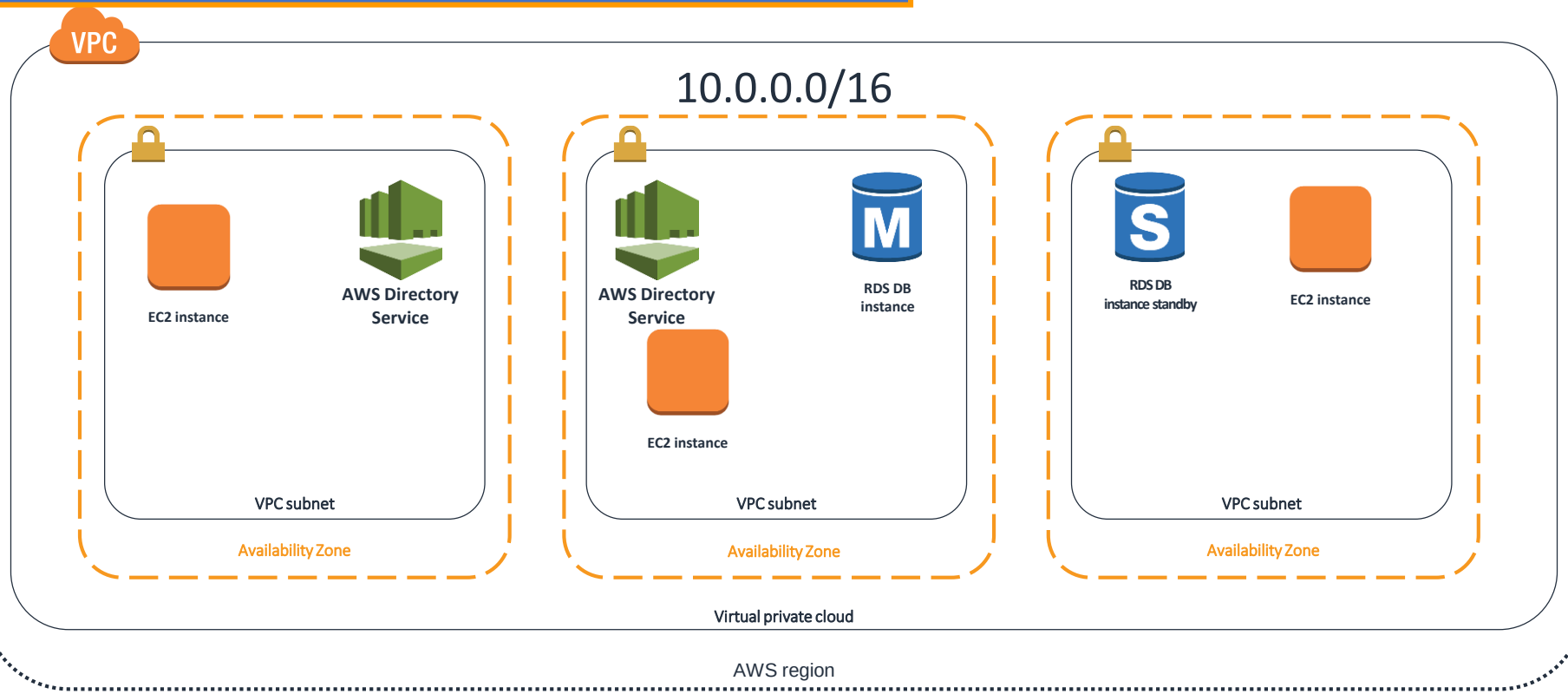


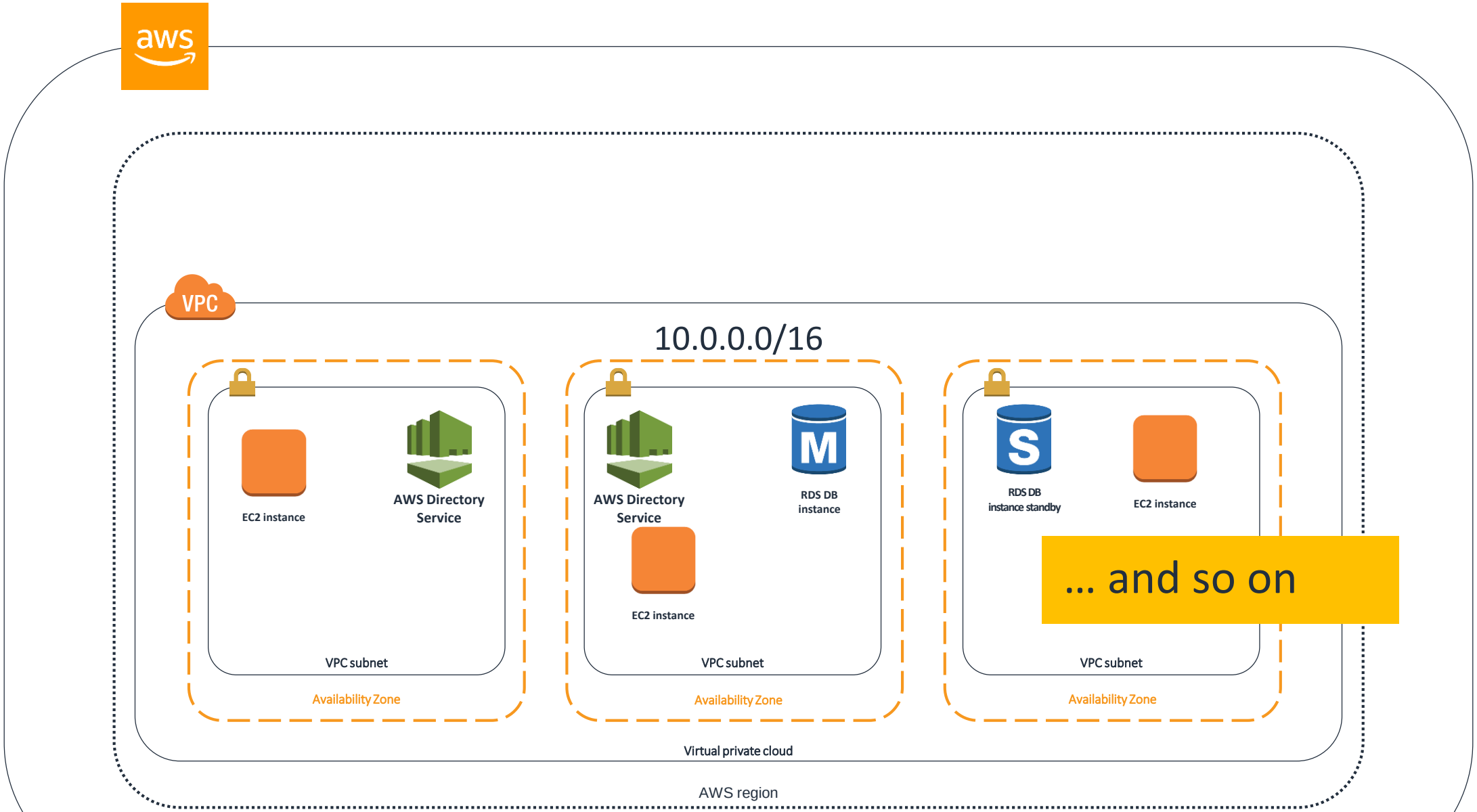


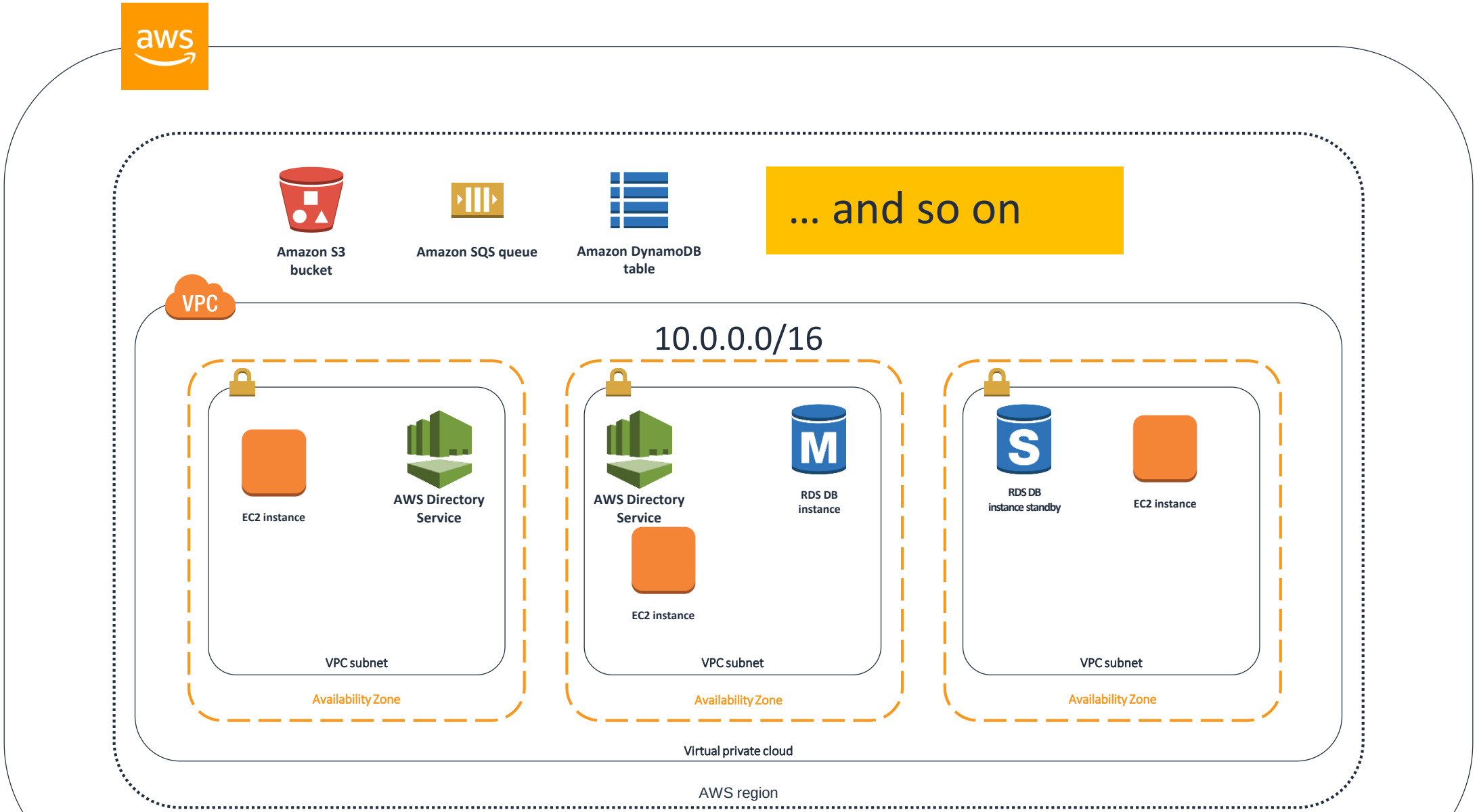
Amazon RDS databases run in your Virtual Private Cloud

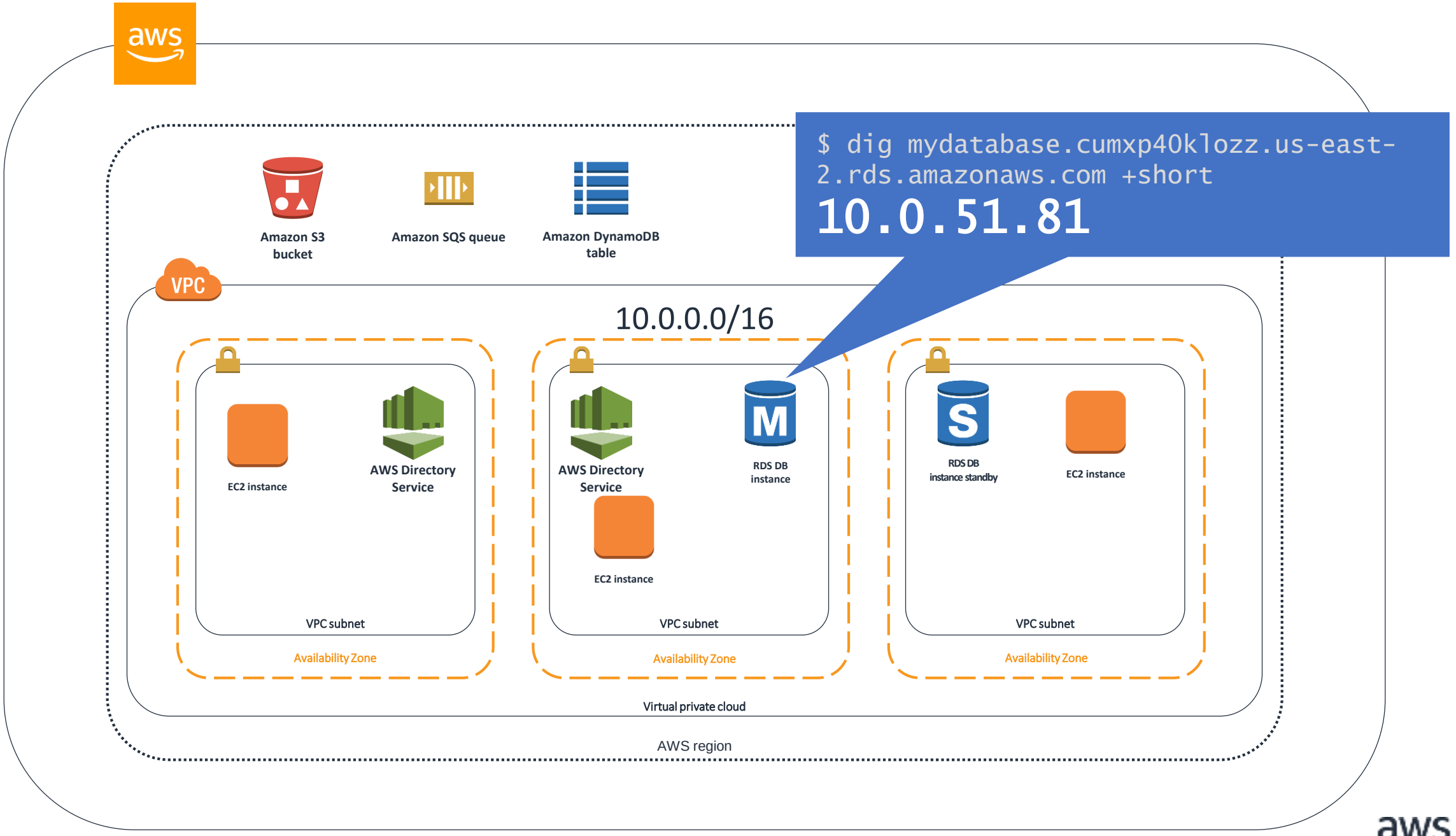


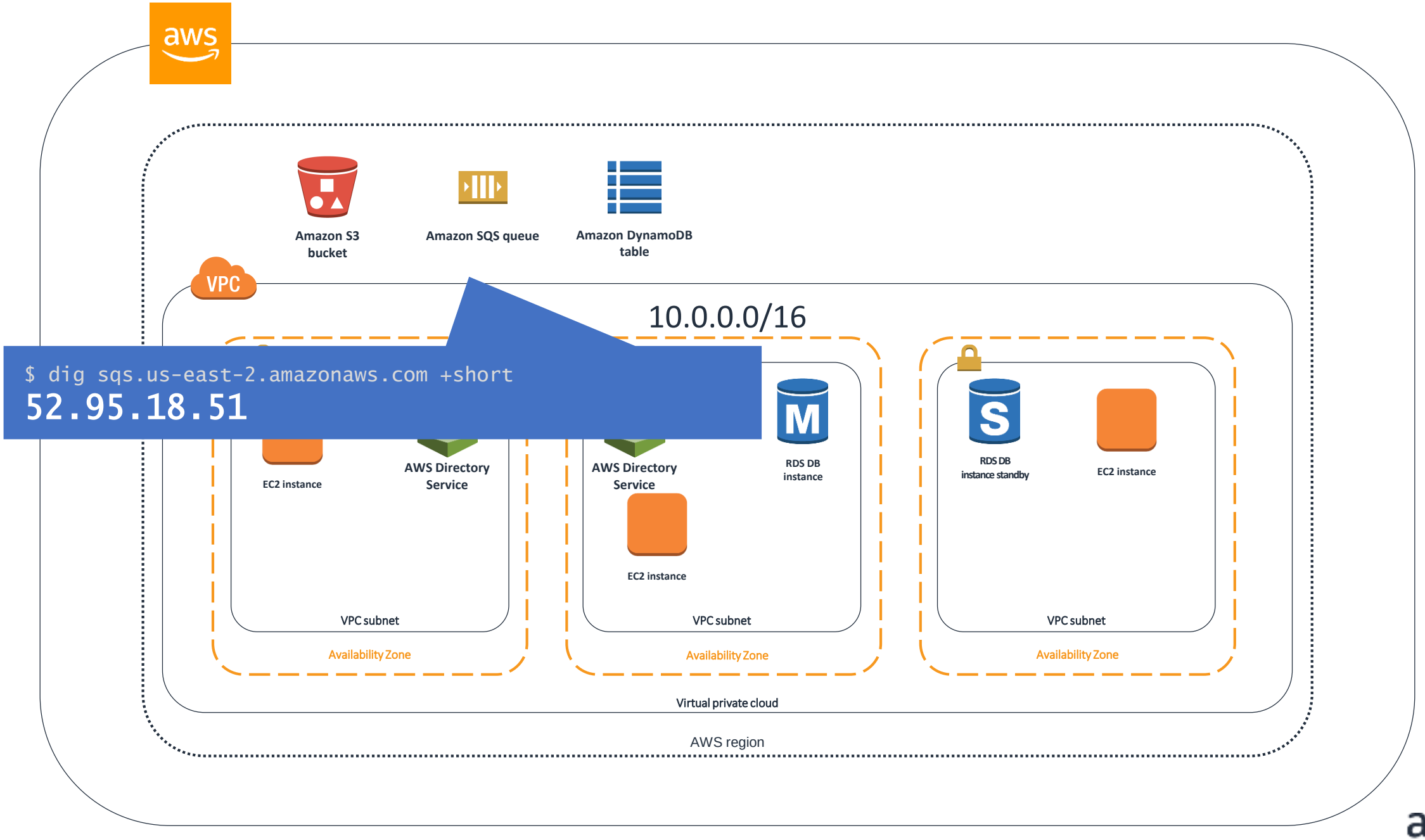
AWS Directory Service domain controllers run in your Virtual Private Cloud

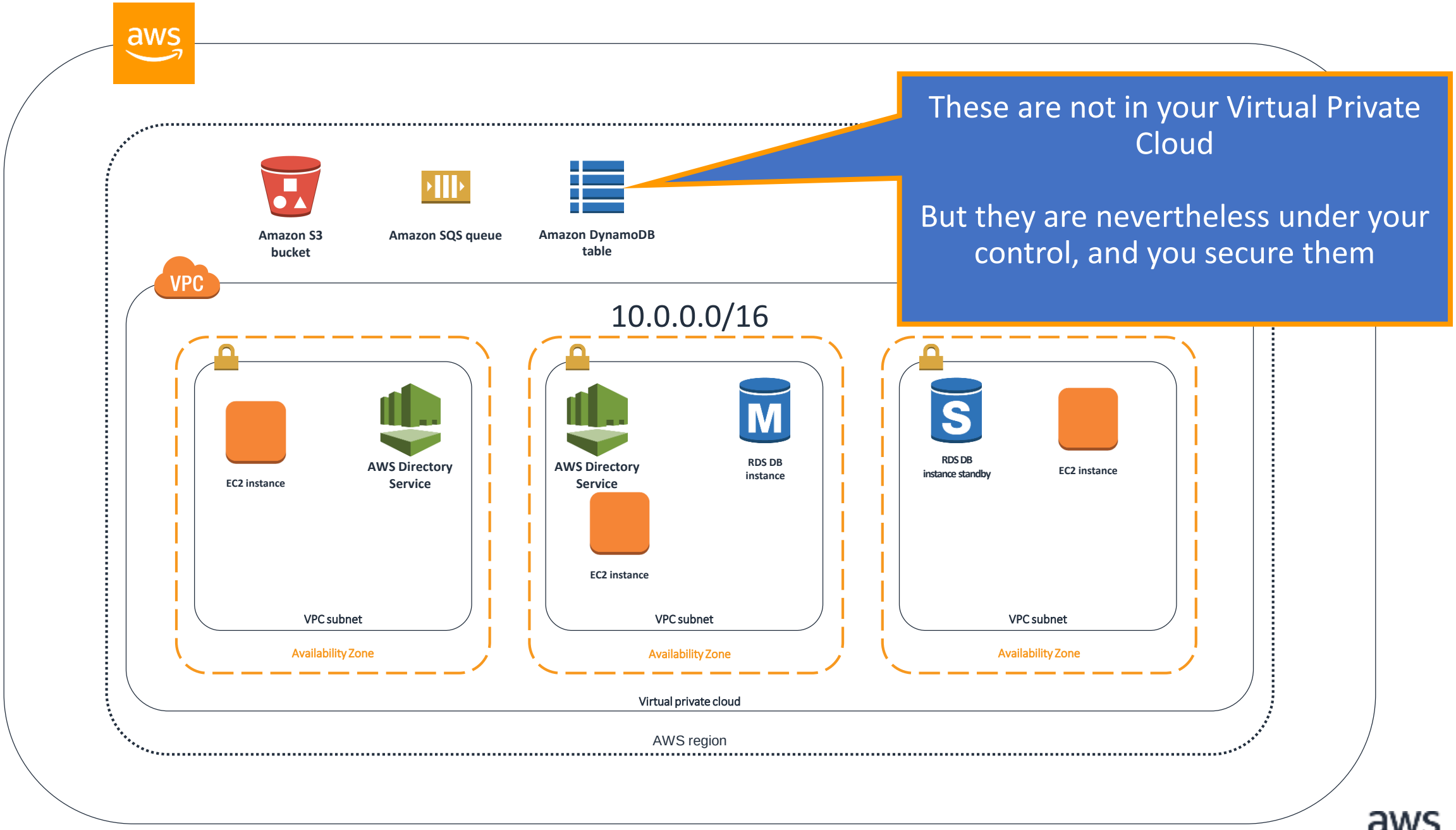






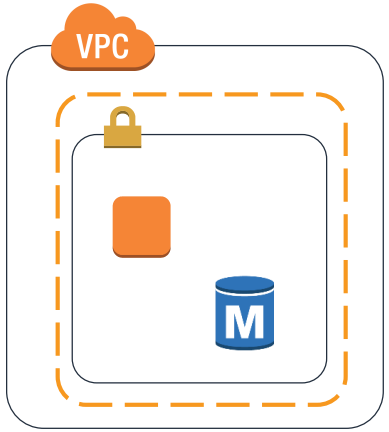




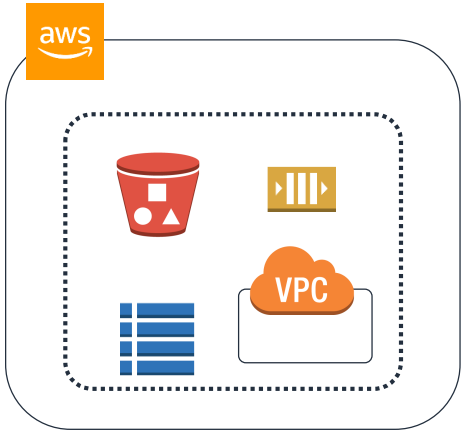


Determining a method for securing AWS resources

- If it’s in your VPC
- Identity and Access Management (IAM) permissions
- VPC network security controls



- If it’s not in your VPC
- Identity and Access Management (IAM) permissions



Practical introduction to IAM: Identity and Access Management

The ABCs of AWS Identity and Access Management (IAM)

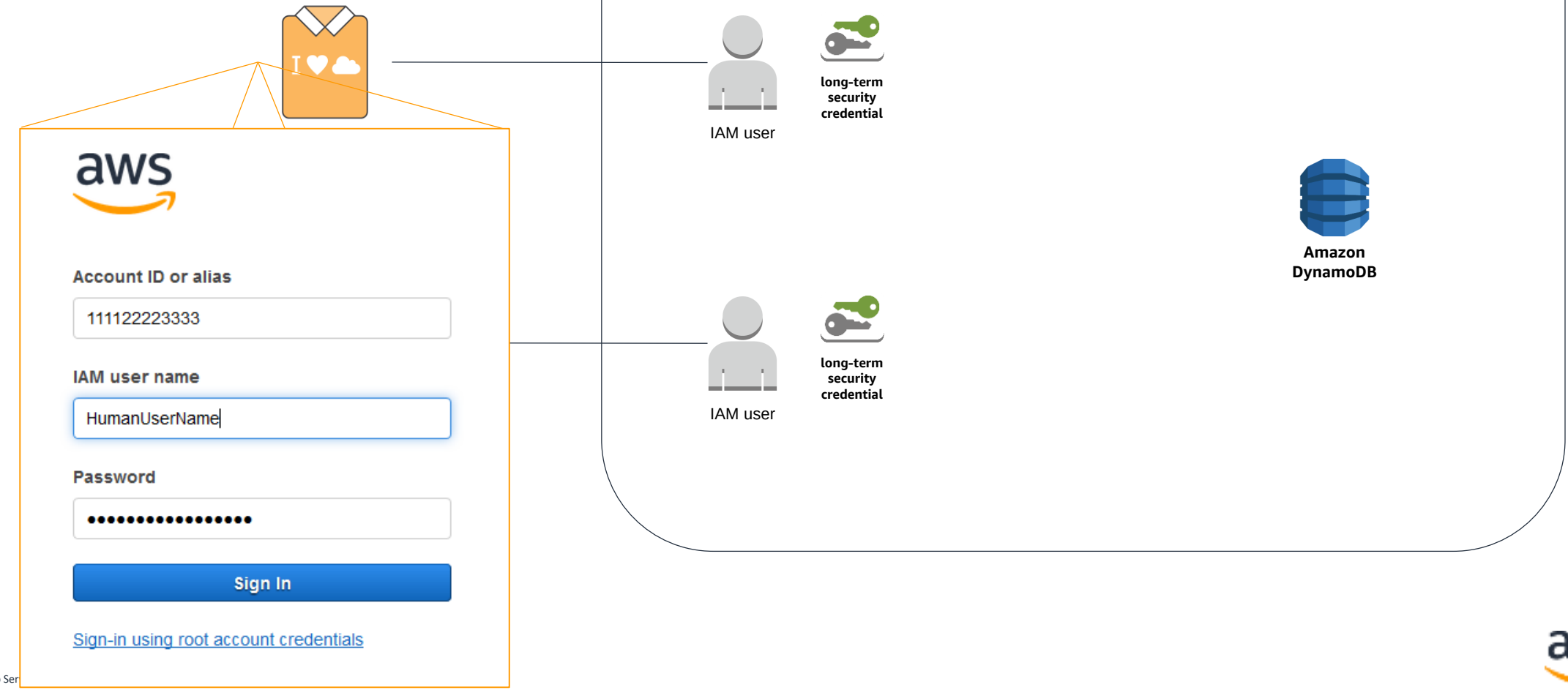
- **I: Identity.** IAM lets you create identities in your AWS Account who can make authenticated requests to AWS.

- **AM: Access Management.** IAM is your tool for defining who has permissions to do what to which resources in IAM.

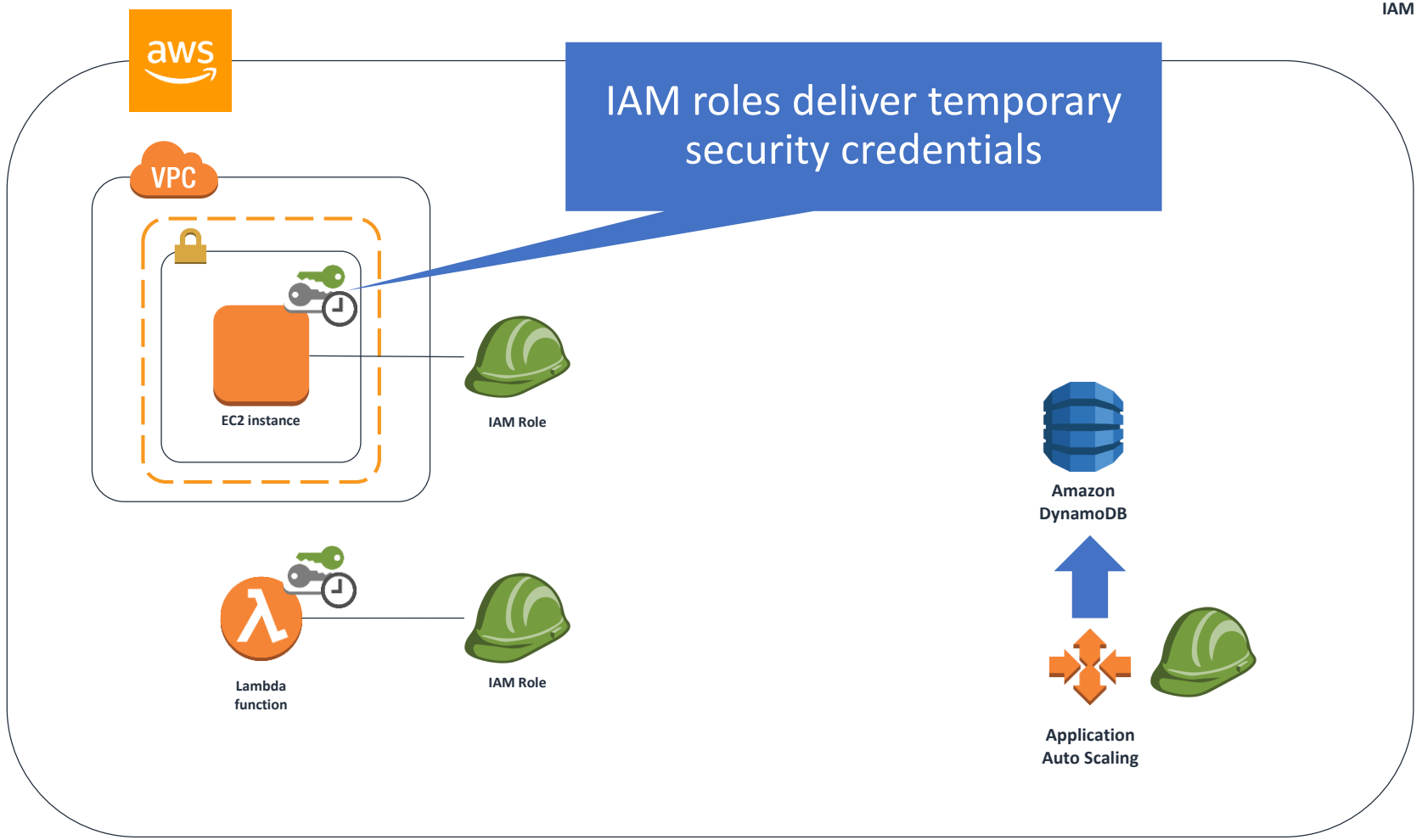
- **IAM is the AWS-wide permissions control system.** So you need to know it.

aws

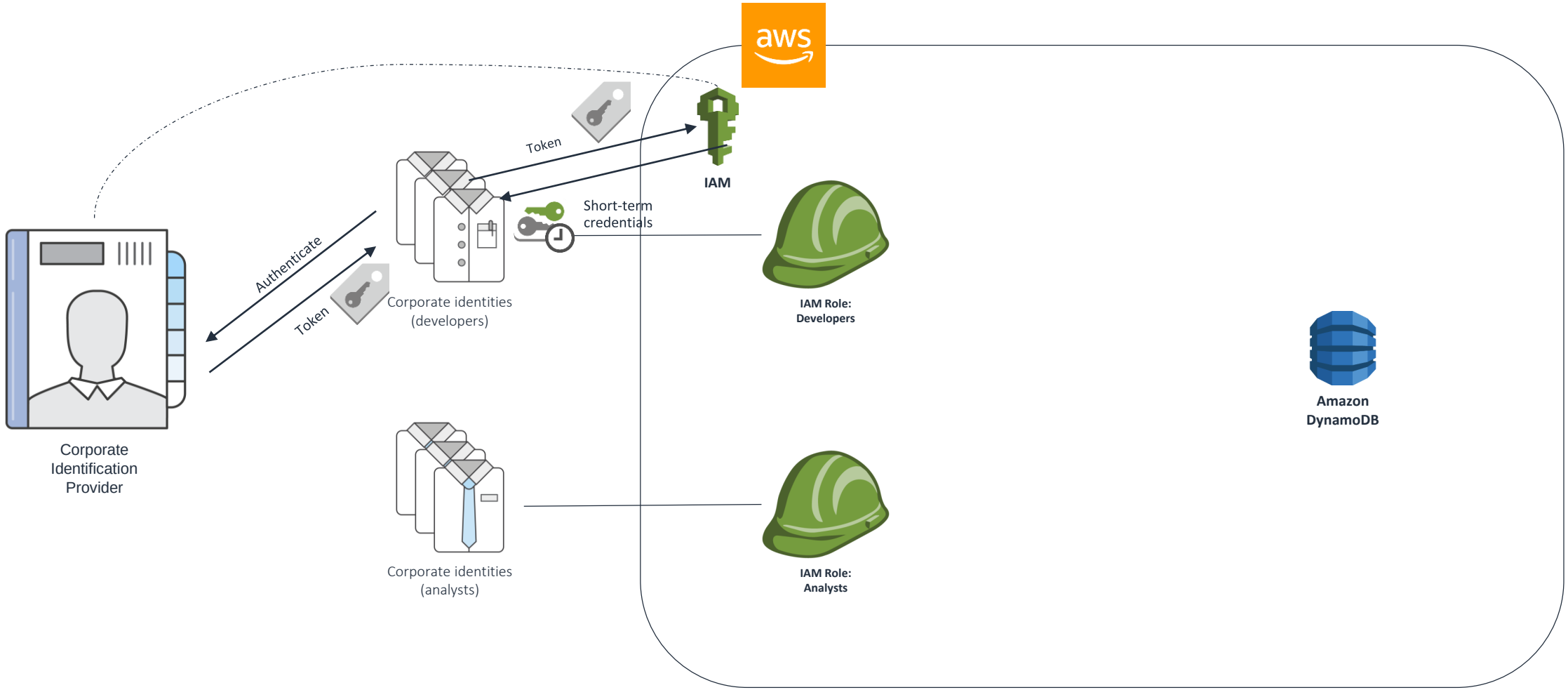
I is for Identity: Humans ➔ IAM Users



I is for Identity: Robots ➔ IAM roles



I is for Identity: Humans with external identities



Term: IAM principal

IAM

- An **IAM principal** is an identity defined within an AWS Account

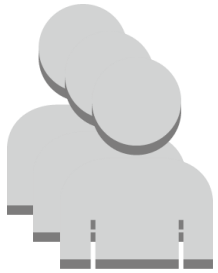
aws

IAM Roles

IAM roles are for

- Automated processes
- AWS Services
- Federated identities

IAM roles authenticate using short-lived credentials



IAM Users

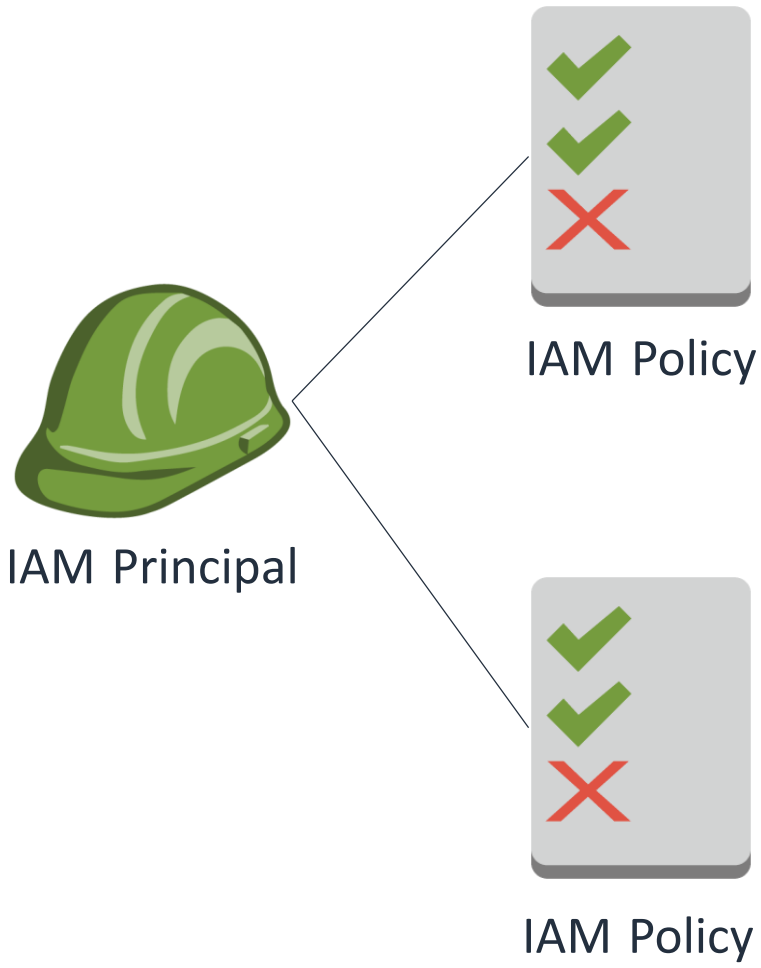
IAM users are for

- Direct human access

IAM users authenticate using long-lived credentials

aws

Term: IAM policy



- Every AWS service supports authorization via IAM policy
- AWS authorizes every API call against the IAM policies that apply
- IAM policies can be attached to IAM roles, users, and groups
- Later in this talk: Other places IAM policy can be attached

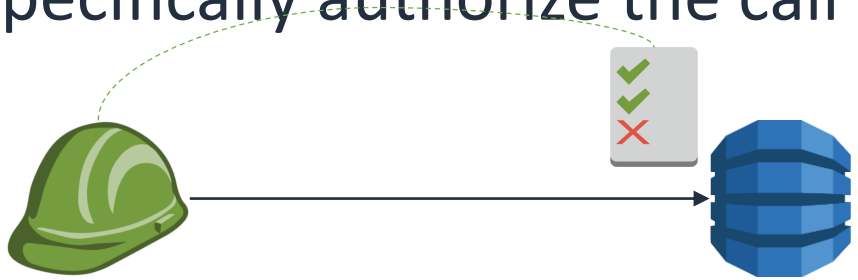
Where does IAM policy matter?

Everywhere in AWS

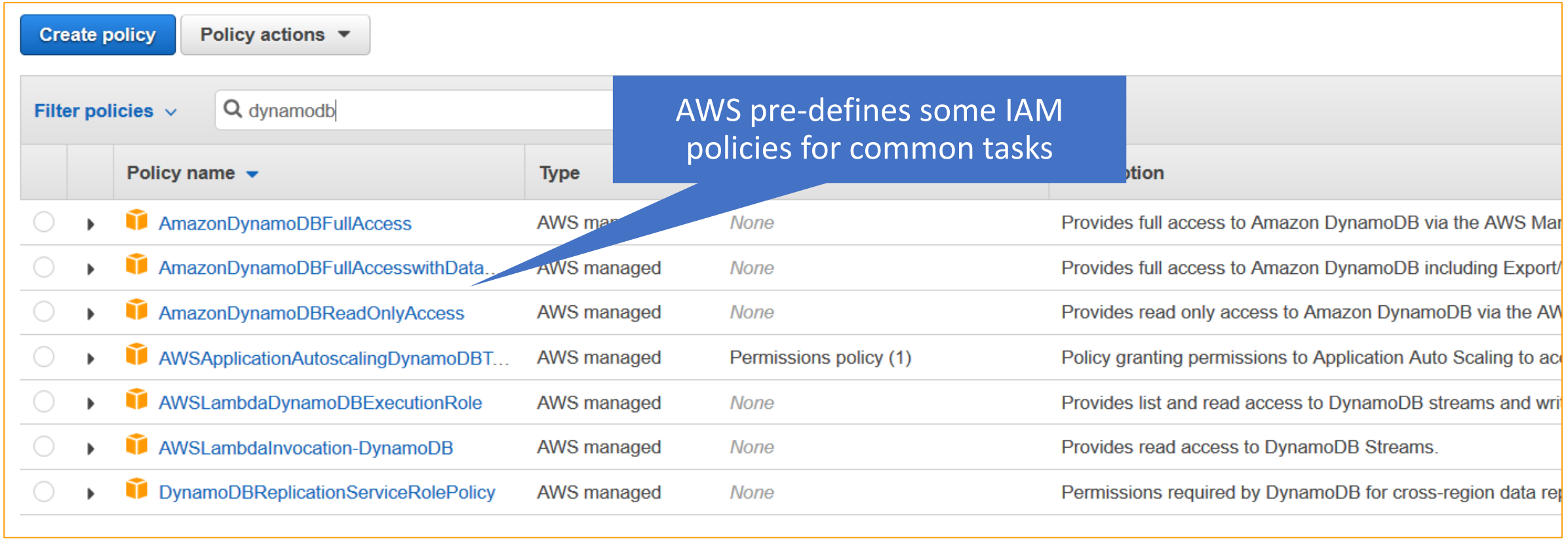
For an authenticated call to succeed

- The request must have a valid signature for an IAM principal

- IAM policy must specifically authorize the call



AWS-managed IAM policies



Reading an IAM policy


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Allow or deny?

What can (or can't) you do?

What can (or can't) you do it to?

In English: Allowed to take all DynamoDB actions

aws

Writing more granular IAM Policies: Actions


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:BatchGetItem",
        "dynamodb:GetItem",
        "dynamodb:Query"
      ],
      "Resource": "*"
    }
  ]
}
```

In English: Allowed to take only a few specific DynamoDB actions

aws

Writing more granular IAM Policies: Resource-level IAM Policies

In English: Allowed to take specific DynamoDB actions on a specific table and its indexes

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:BatchGetItem",
        "dynamodb:GetItem",
        "dynamodb:Query",
      ],
      "Resource": [
        "arn:aws:dynamodb:us-east-2:111122223333:table/MyTableName",
        "arn:aws:dynamodb:us-east-2:111122223333:table/MyTableName/index/*"
      ]
    }
  ]
}
```

This is an Amazon Resource Name (ARN).
All AWS services use them, and they always follow this format

aws

Term: Amazon Resource Name (ARN)

- **Resource:** A thing in AWS. Examples: S3 bucket, DynamoDB table, EC2 instance, VPC. Even IAM principals have ARNs.
- **ARN:** A fully-qualified name for that resource, used throughout AWS

- `arn:aws:dynamodb:us-east-2:111122223333:table/MyTableName`
- `service region accountId service-specific name`

aws

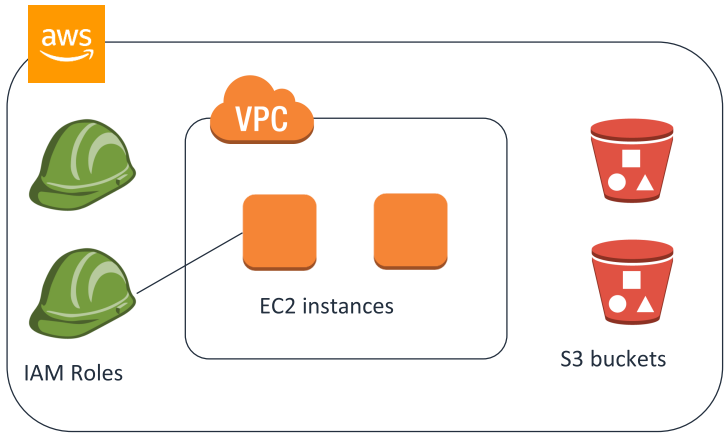
Writing more granular IAM policies: Conditions


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:*“
      ],
      "Resource": "*",
      "Condition": {
       "StringEquals": {
         "aws:RequestedRegion": [
           "us-east-2"
         ]
       }
    }
  ]
}
```

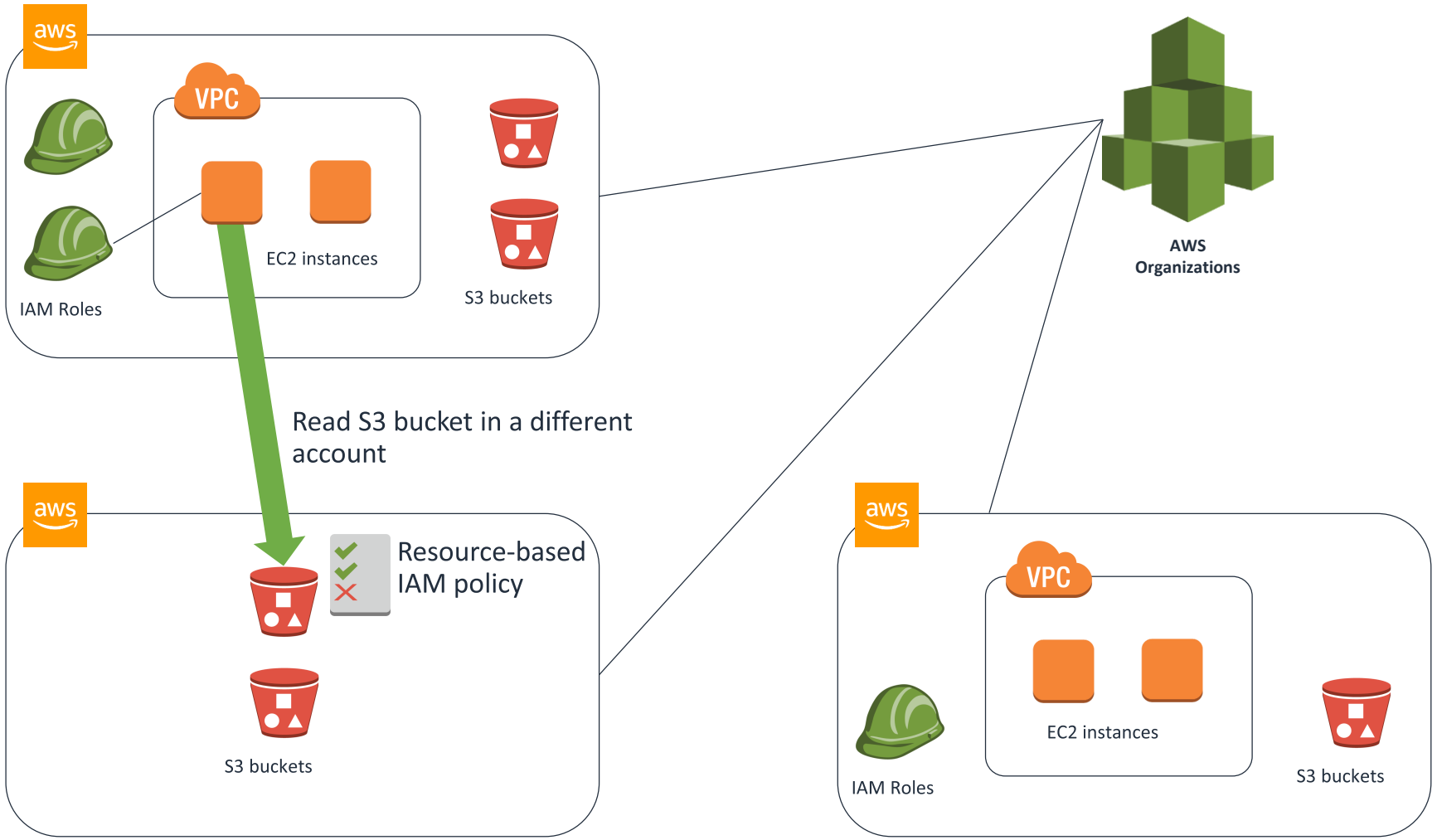
In English: Allowed to use DynamoDB only in the us-east-2 region

aws

Securing AWS resources across multiple accounts



Securing AWS resources across multiple accounts

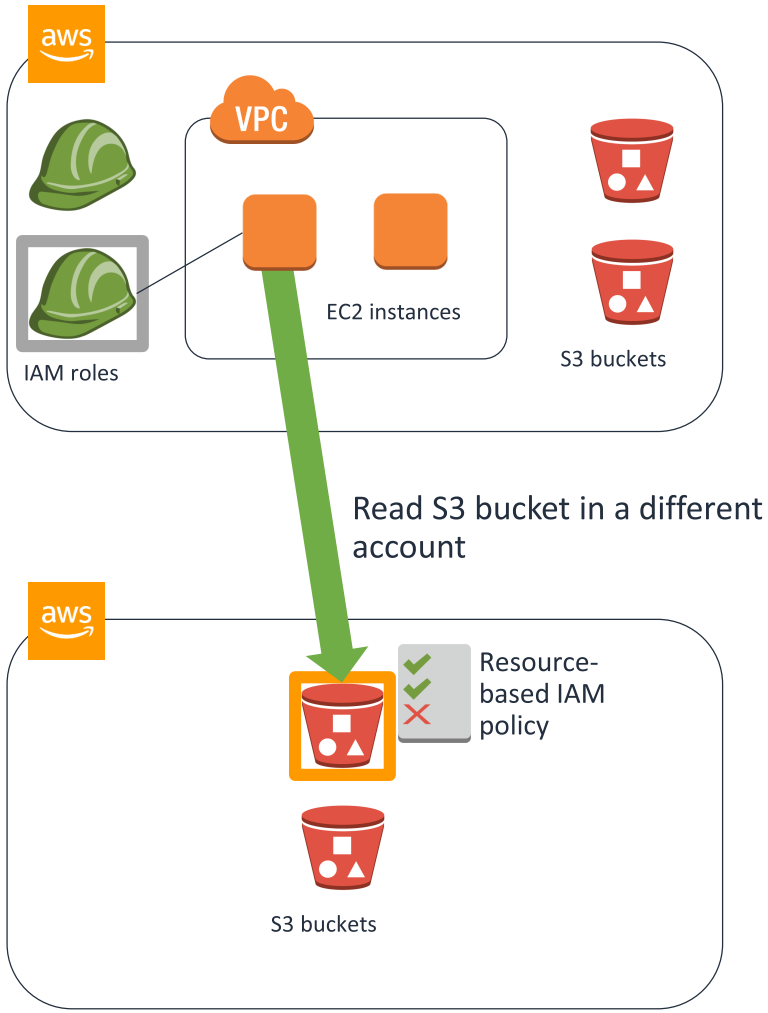


Example: Resource-based policy

In English: The “MyRole” IAM Role in account 444455556666 (a different account) can read objects from this bucket under /some/path/

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal“: {
        "AWS": [ {
            "arn:aws:iam::444455556666:role/MyRole"
      } ],
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::my-s3-bucket/some/path/*"
    }
  ]
}
```

IAM Authorization of cross-account access

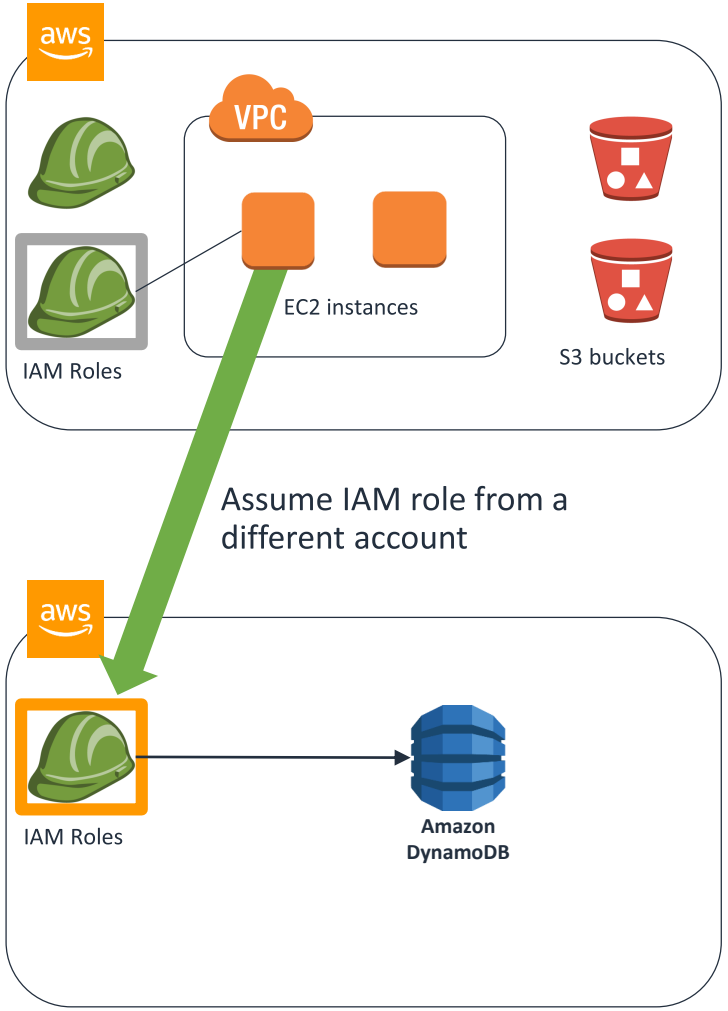


Authorization decision:

1. Does the S3 bucket have a policy allowing access from the calling IAM principal?
2. Does the calling IAM principal have a policy allowing access to this S3 bucket?

Cross-account access is disallowed unless there is a resource-based policy

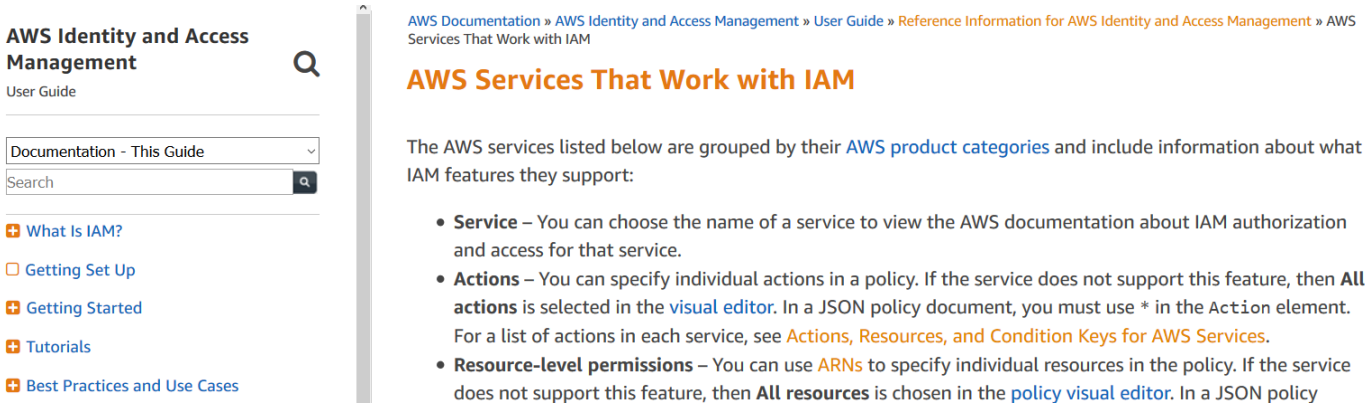
IAM authorization of cross-account access



IAM roles can be configured to allow cross-account access

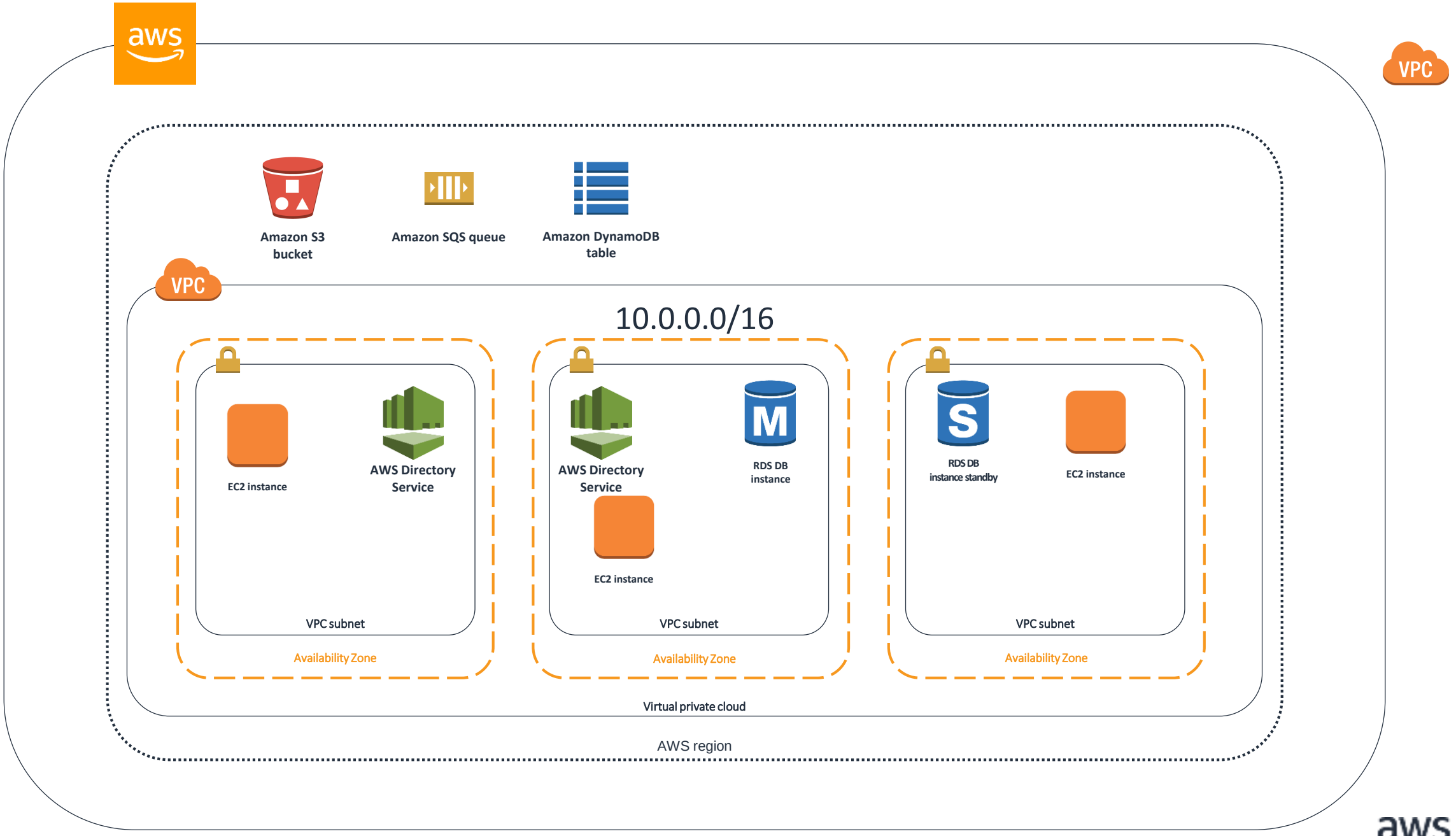
Assuming an IAM role in another account gives you access to whatever that role had permission to

The IAM Reference

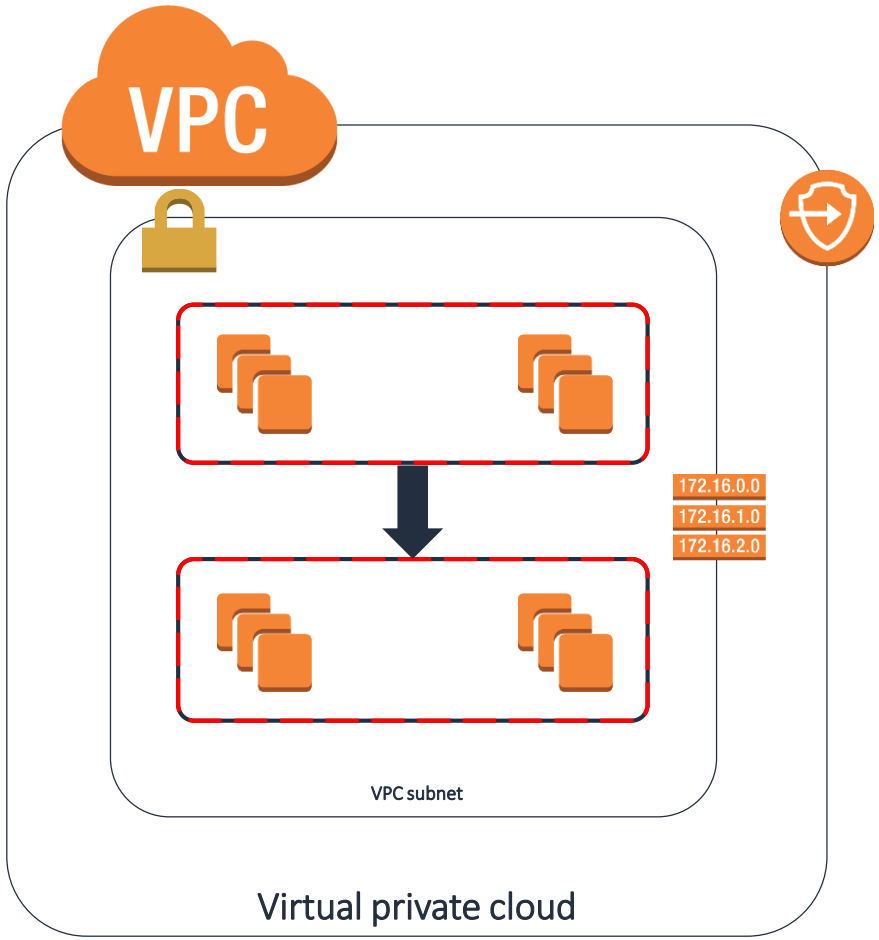


Service	Actions	Resource-level permissions	Resource-based policies	Authorization based on tags	Temporary credentials	Service-linked roles
Application Auto Scaling	Yes	Yes	No	No	Yes	Yes
Amazon EC2 Auto Scaling	Yes	Yes	No	No	Yes	Yes
AWS Batch	Yes	No	No	No	Yes	No
Amazon Elastic Compute Cloud (Amazon EC2)	Yes	Yes	No	Yes	Yes	Yes[1]
AWS Elastic Beanstalk	Yes	Yes	No	No	Yes	Yes
Amazon Elastic						

Practical introduction to Virtual Private Cloud network security

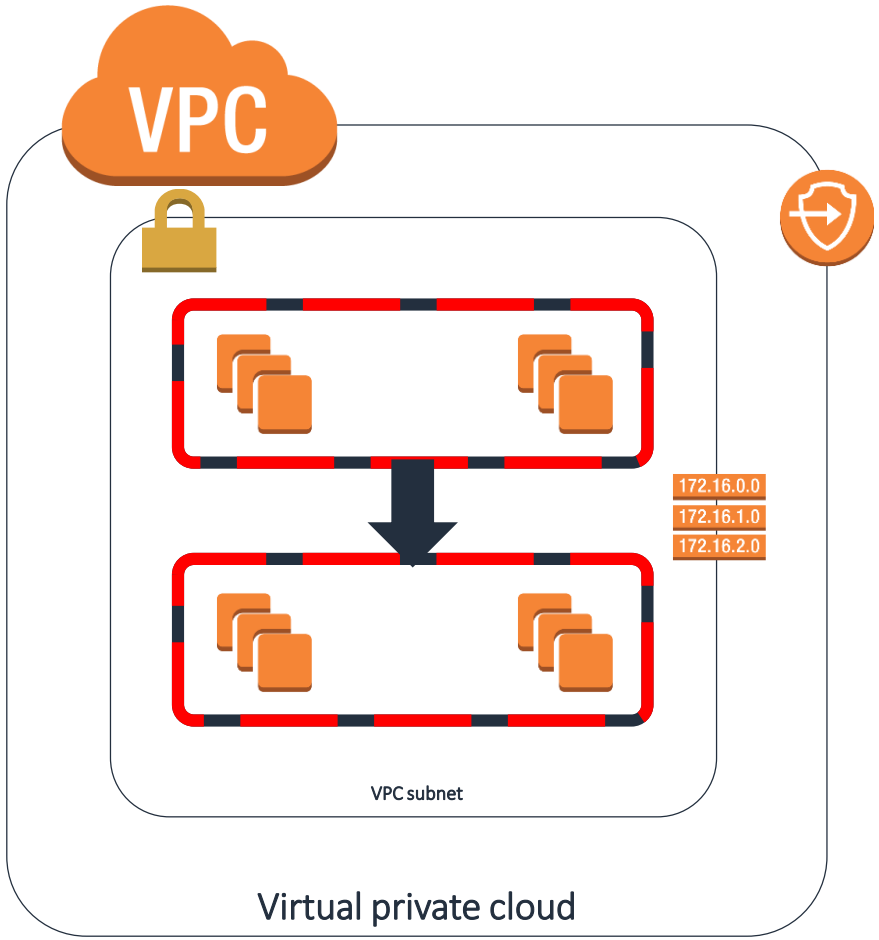


Secure connectivity with Amazon VPC



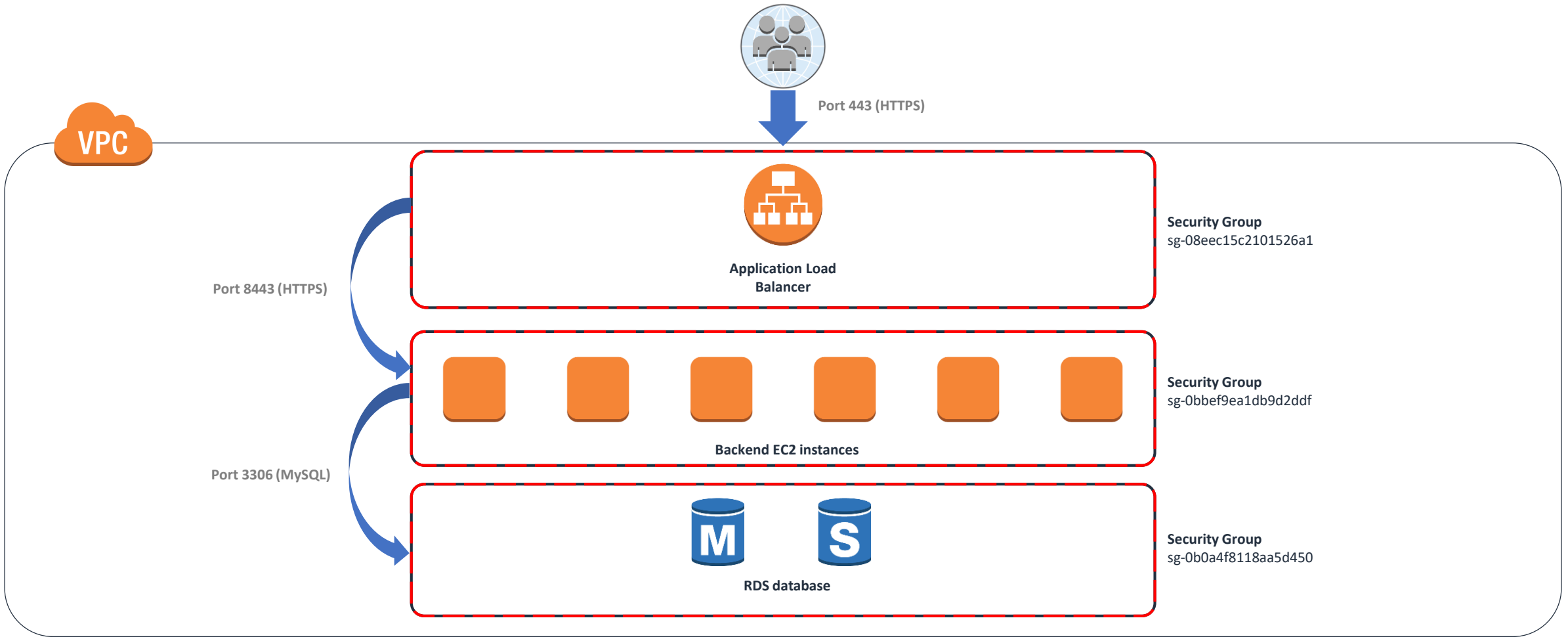
- **Security Groups:** Authorize only the traffic you expect
- **Routing:** Route traffic headed out of your VPC only to expected destinations
- **VPC Endpoints:** Create specific, least-privilege points of connectivity

Secure connectivity with Amazon VPC

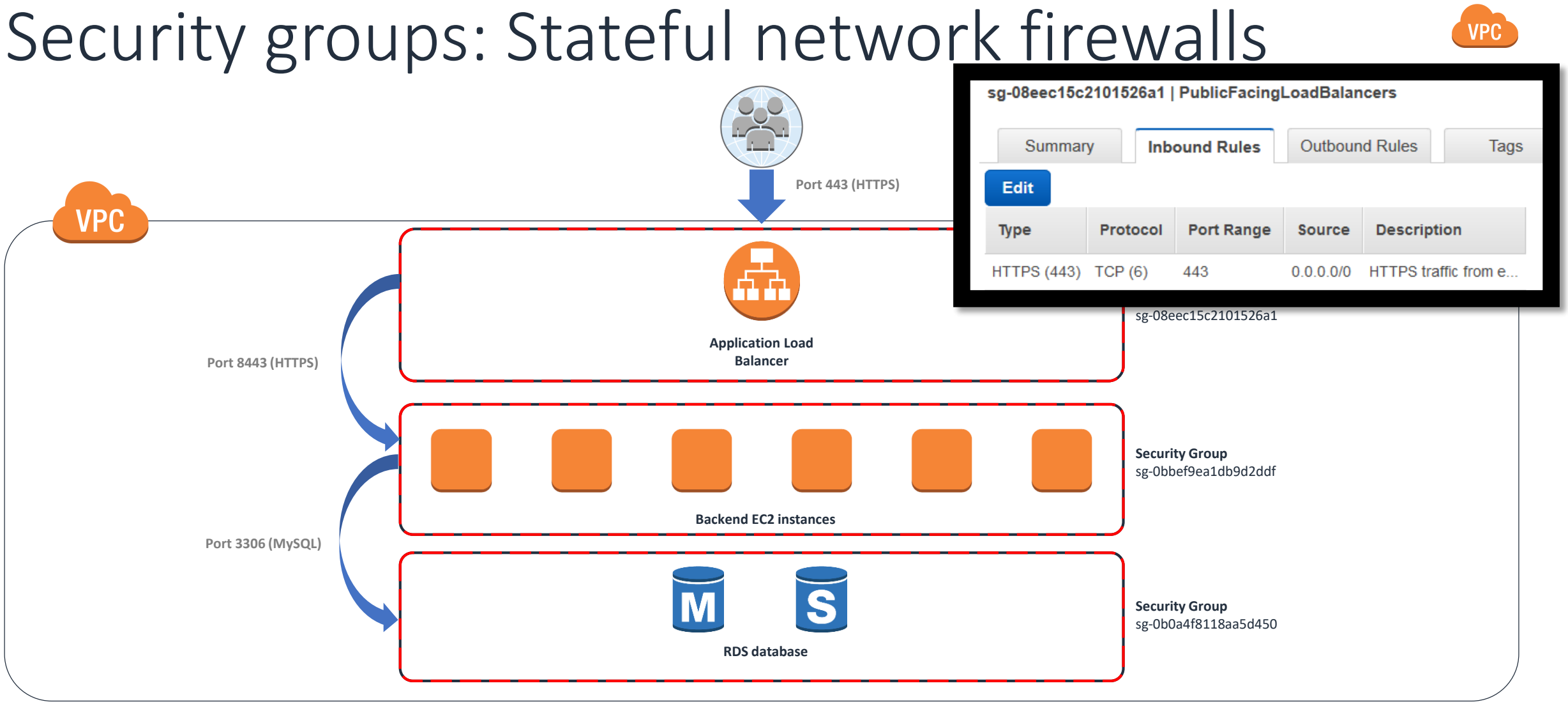


- **Security Groups:** Authorize only the traffic you expect
- **Routing:** Route traffic headed out of your VPC only to expected destinations
- **VPC Endpoints:** Create specific, least-privilege points of connectivity

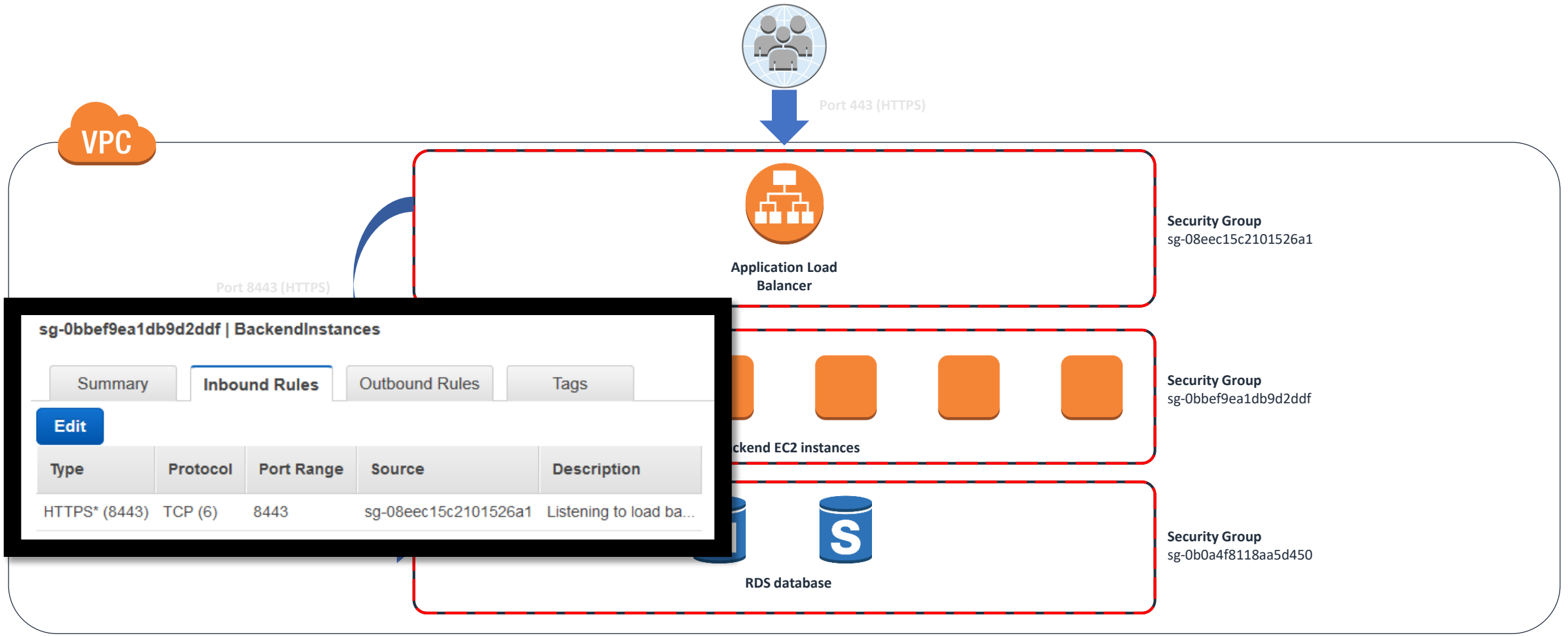
Security groups: Stateful network firewalls



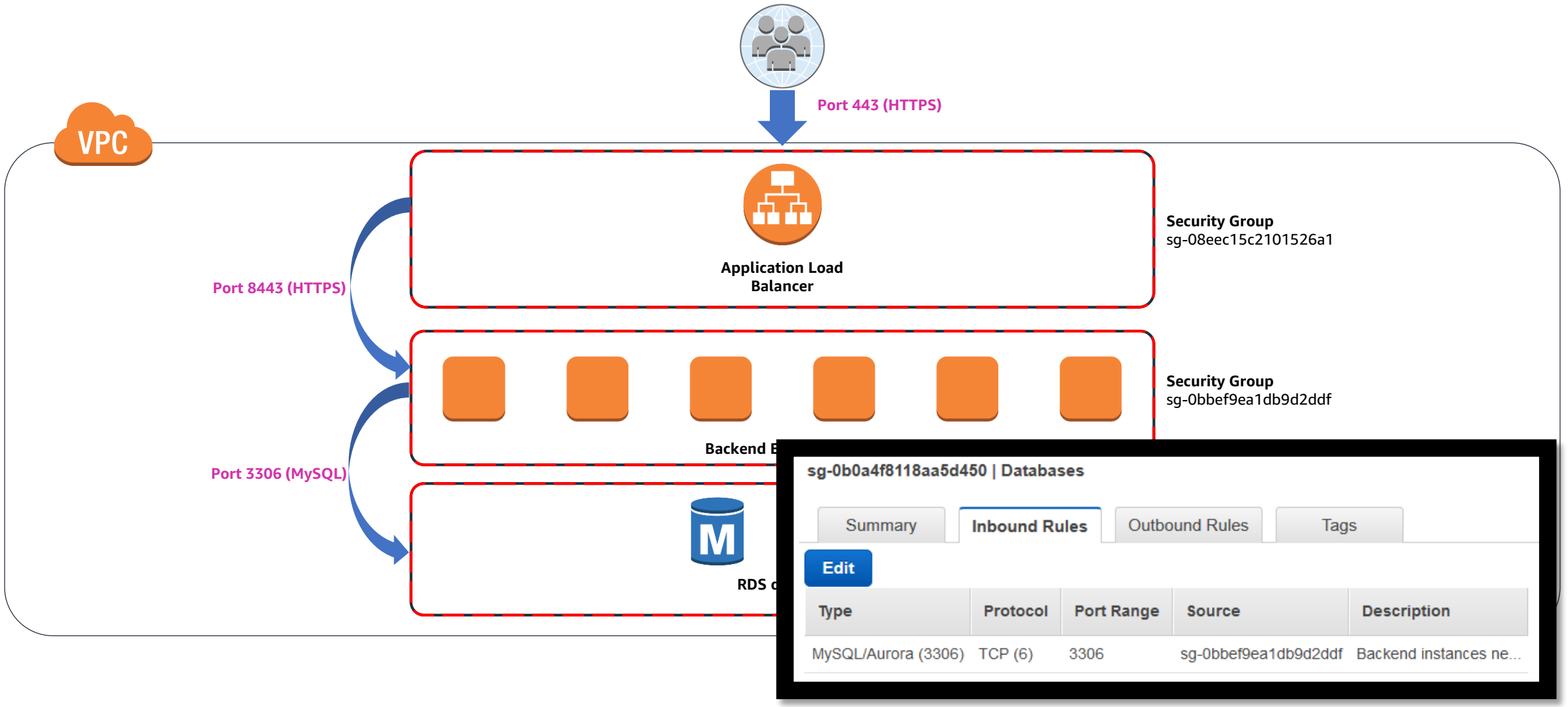
Security groups: Stateful network firewalls



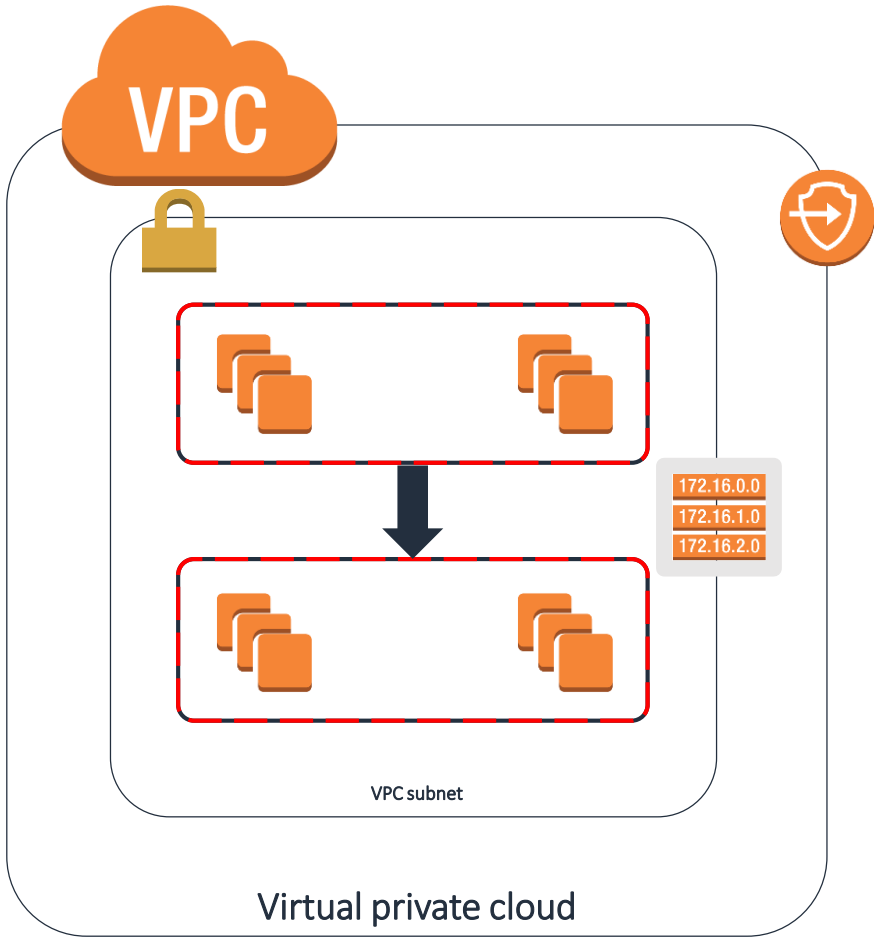
Security groups: Stateful network firewalls



Security Groups: Stateful network firewalls

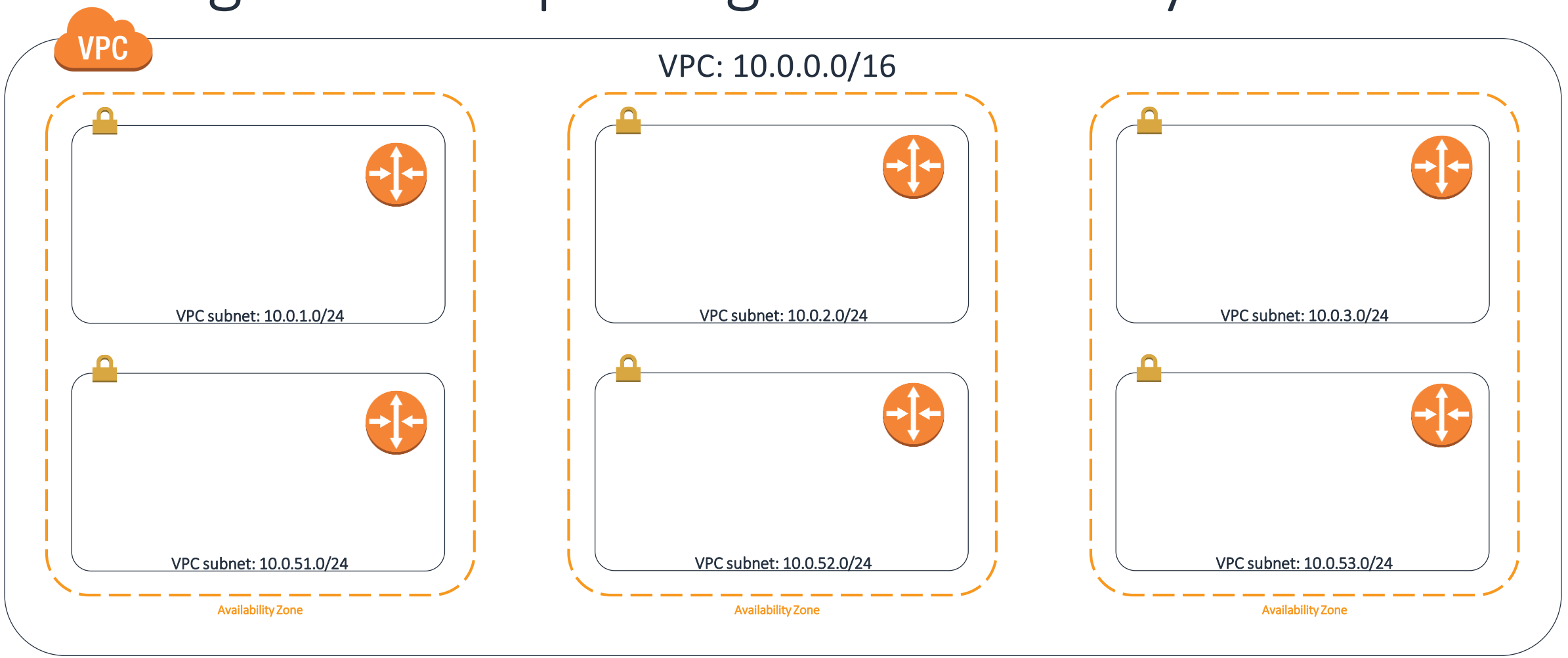


Secure connectivity with Amazon VPC

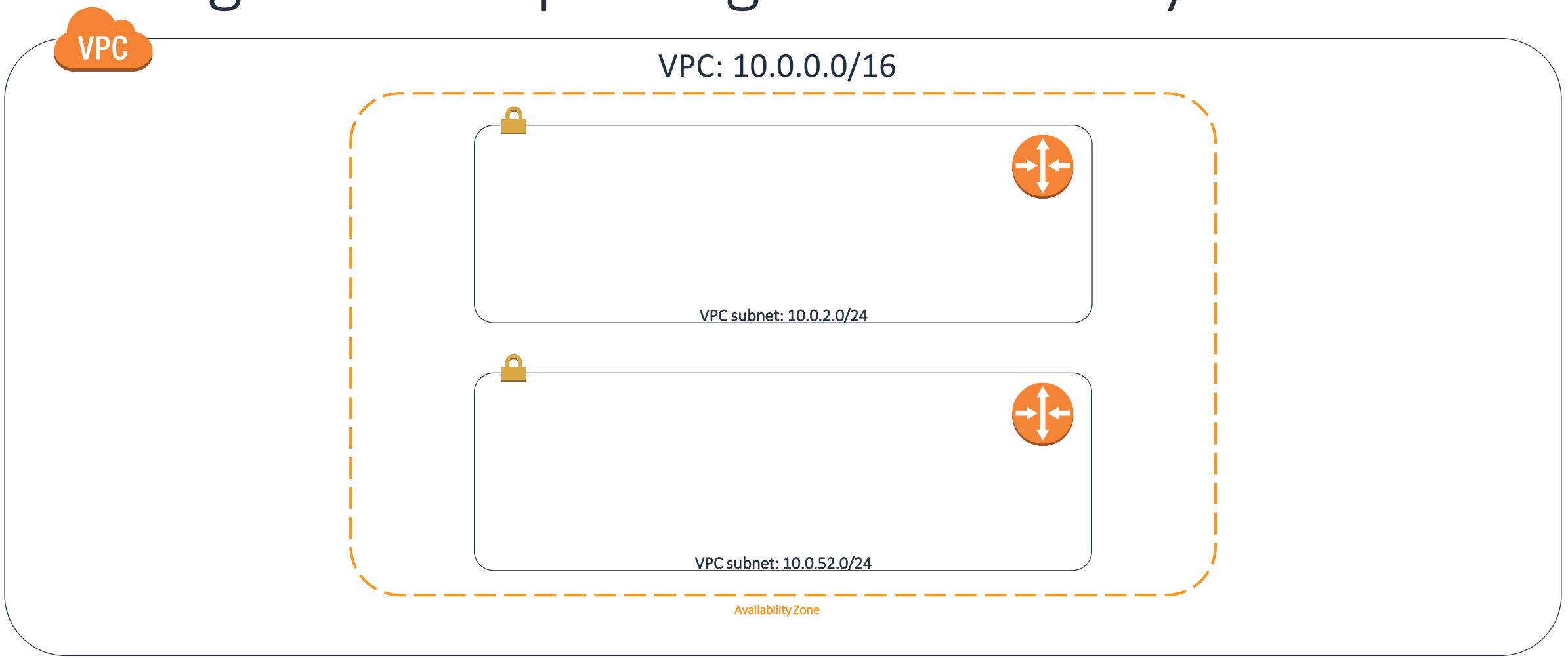


- **Security Groups:** Authorize only the traffic you expect
- **Routing:** Route traffic headed out of your VPC only to expected destinations
- **VPC Endpoints:** Create specific, least-privilege points of connectivity

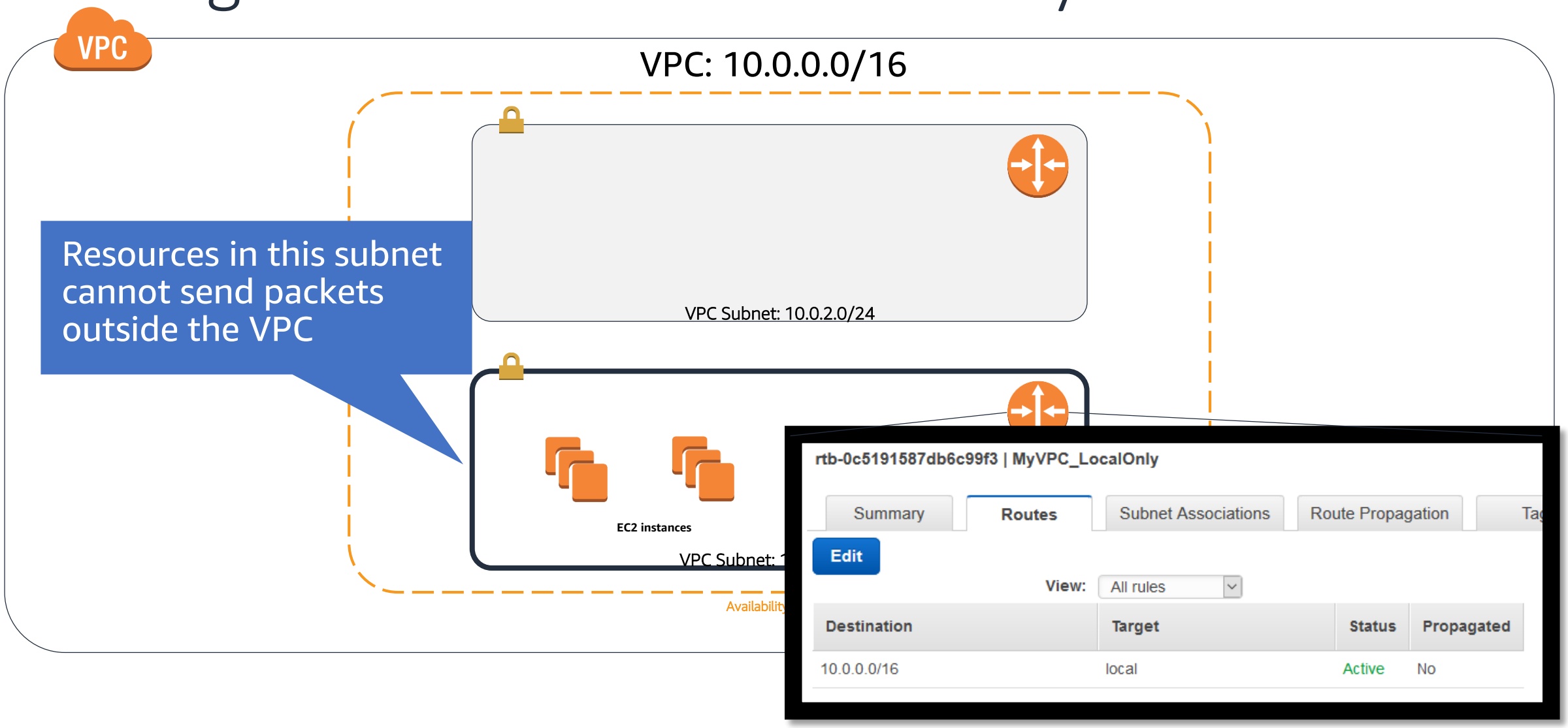
Routing for least-privilege connectivity



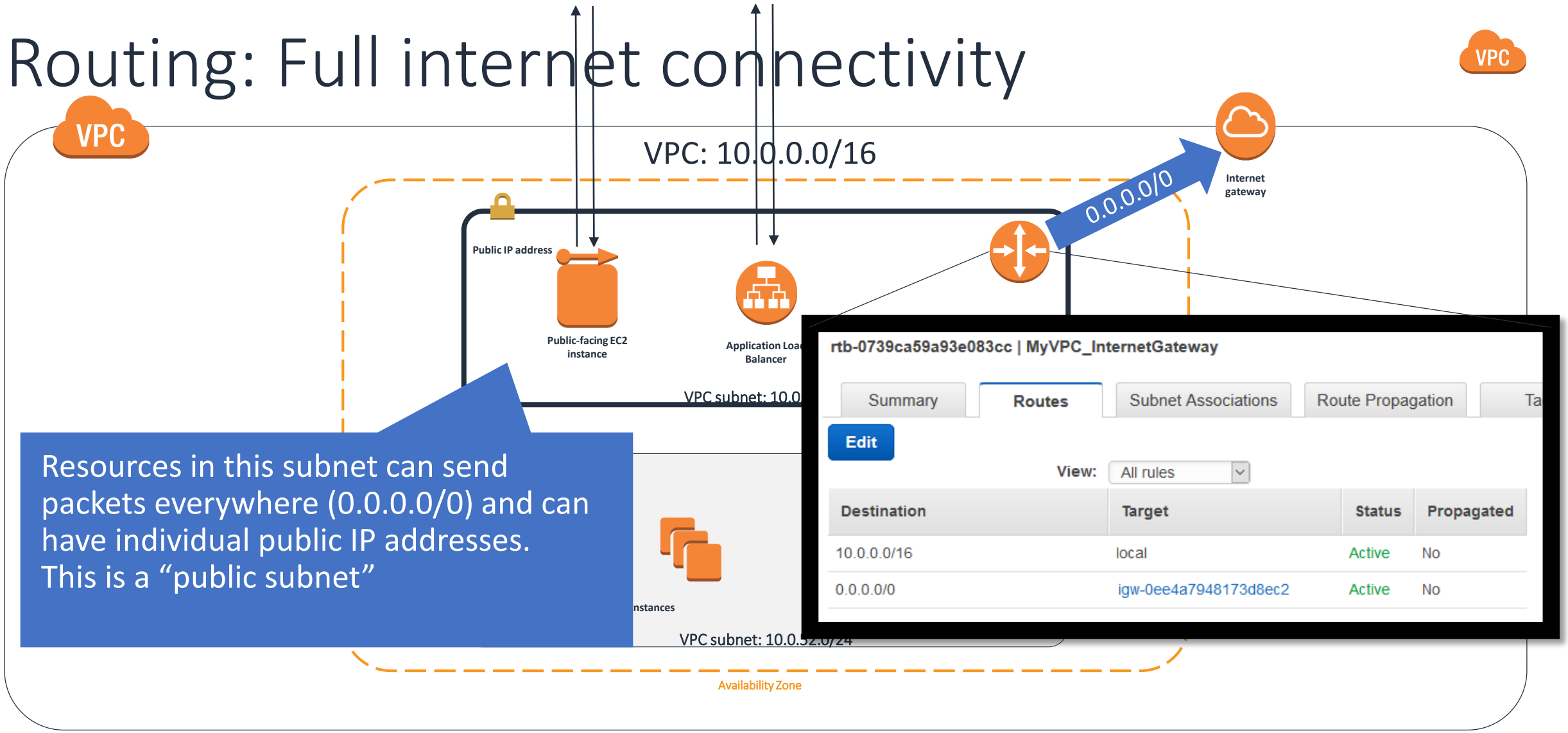
Routing for least-privilege connectivity



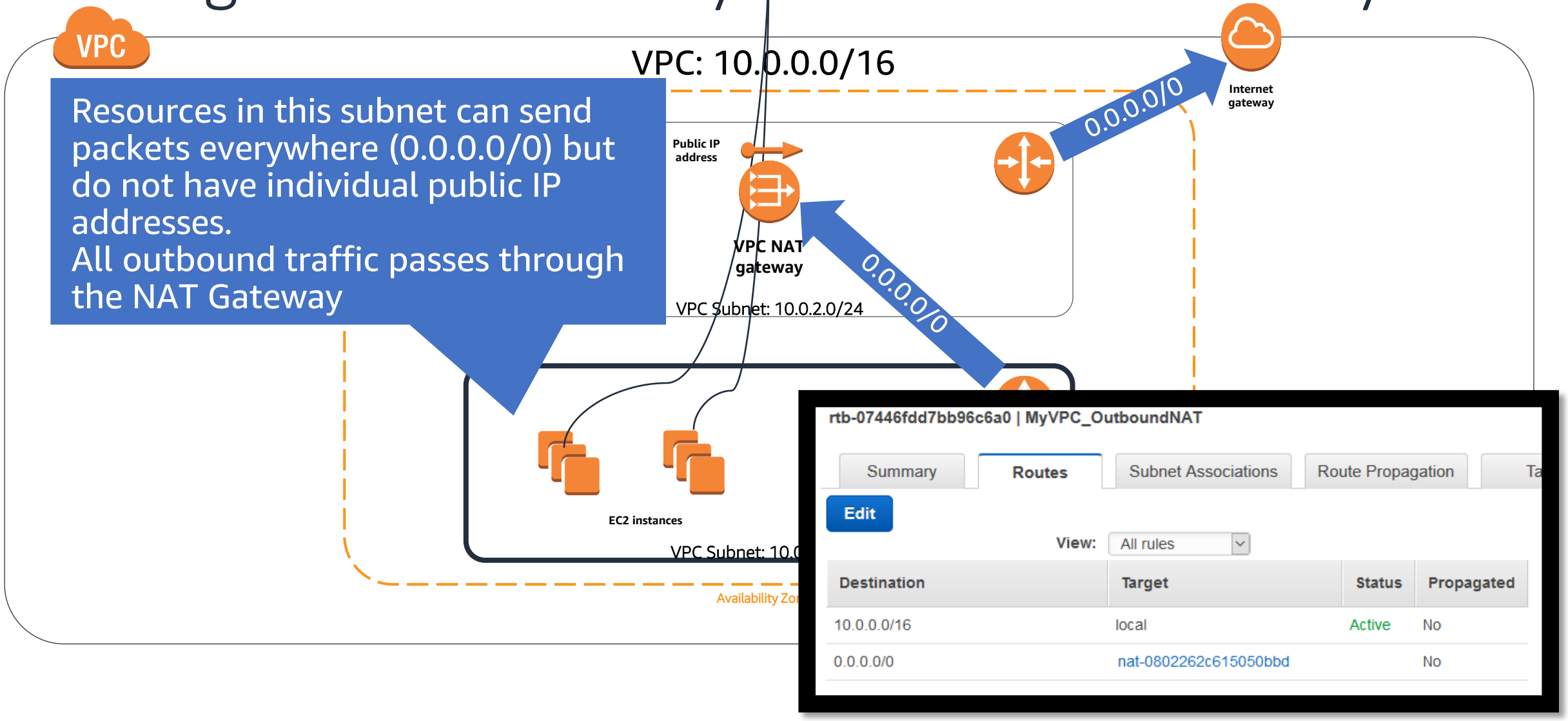
Routing: No outbound connectivity



Routing: Full internet connectivity

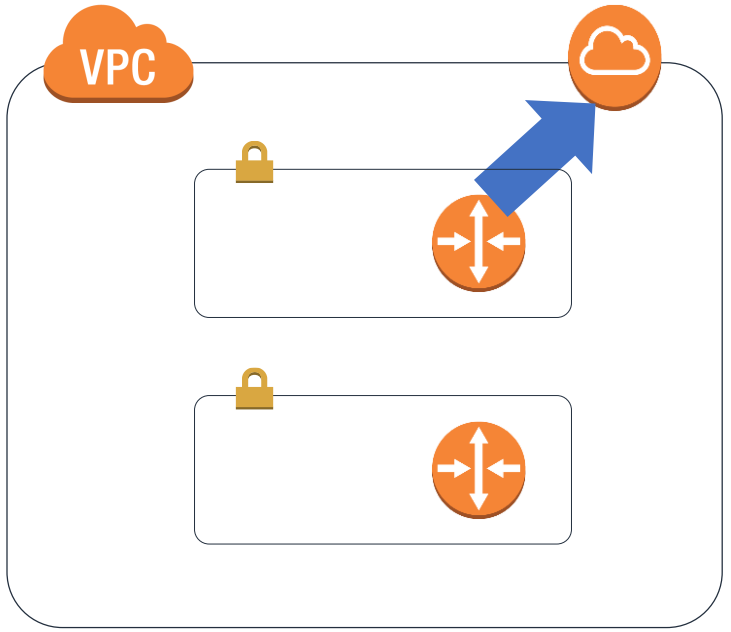


Routing: Outbound-only internet connectivity

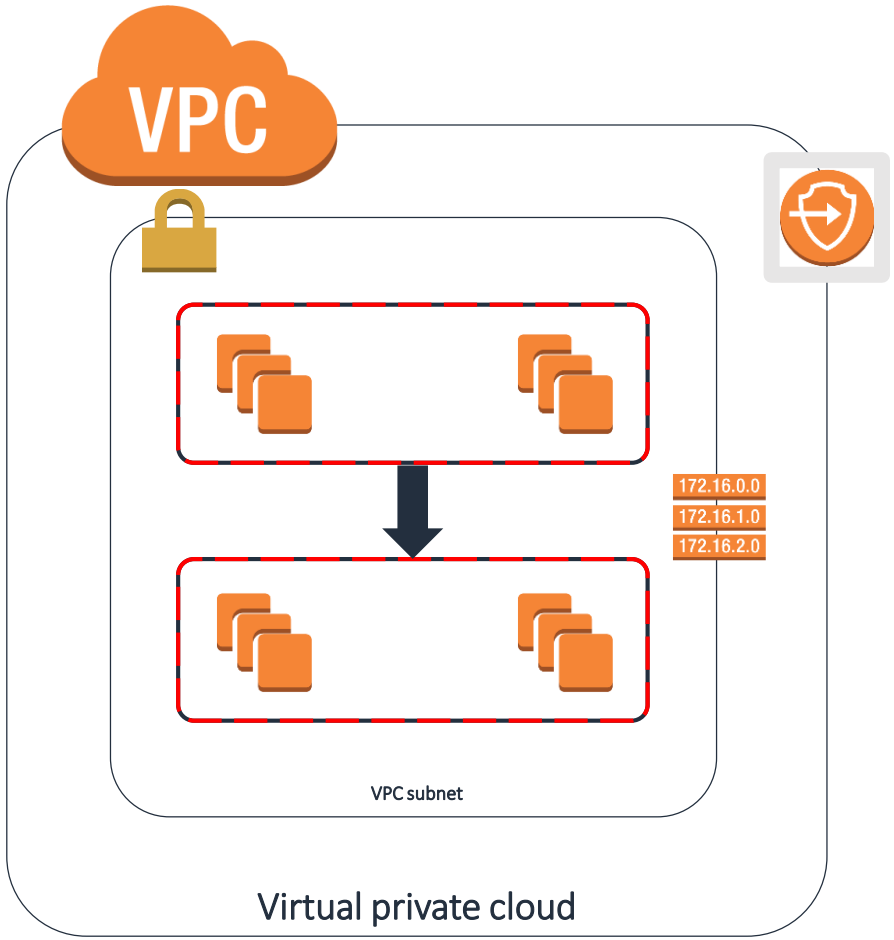


Routing for least privilege: Summary

- AWS offers a variety of routing options
- Determine the different routing needs of different parts of your workload, and put them in different subnets
- Have only the routes you need in each subnet.



Secure connectivity with Amazon VPC



- **Security Groups:** Authorize only the traffic you expect
- **Routing:** Route traffic headed out of your VPC only to expected destinations
- **VPC Endpoints:** Create specific, least-privilege points of connectivity

What we didn’t talk about

- Encryption

AWS Key Management Service

AWS Certificate Manager

- Visibility and detective controls

AWS CloudTrail

VPC Flow logs

- Higher-level security services

Amazon GuardDuty

Amazon Inspector

…

Thank You

Gabe Hollombe, AWS

Twitter & LinkedIn: @gabehollombe

Thank You for Attending AWS Quick Start

We hope you found it interesting! A kind reminder to **complete the survey.**
Let us know what you thought of today's event and how we can improve the event experience for you in the future.


aws-apac-marketing@amazon.com


twitter.com/AWSCloud


facebook.com/AmazonWebServices


youtube.com/user/AmazonWebServices


slideshare.net/AmazonWebServices


twitch.tv/aws