

AWS Quick Start

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

Gabe Hollombe, Senior Technical Evangelist, AWS, APAC

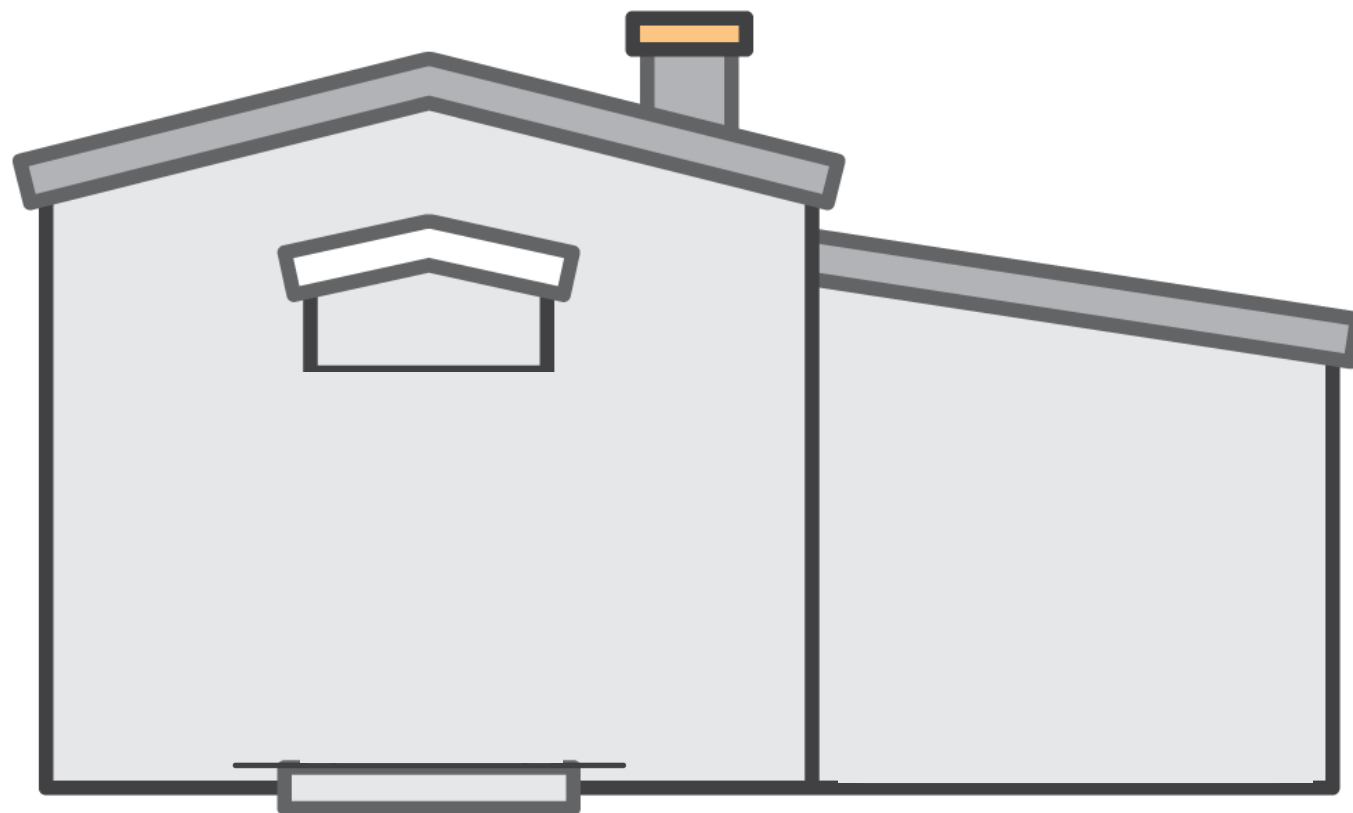


Agenda: Develop your cloud security know-how

- 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



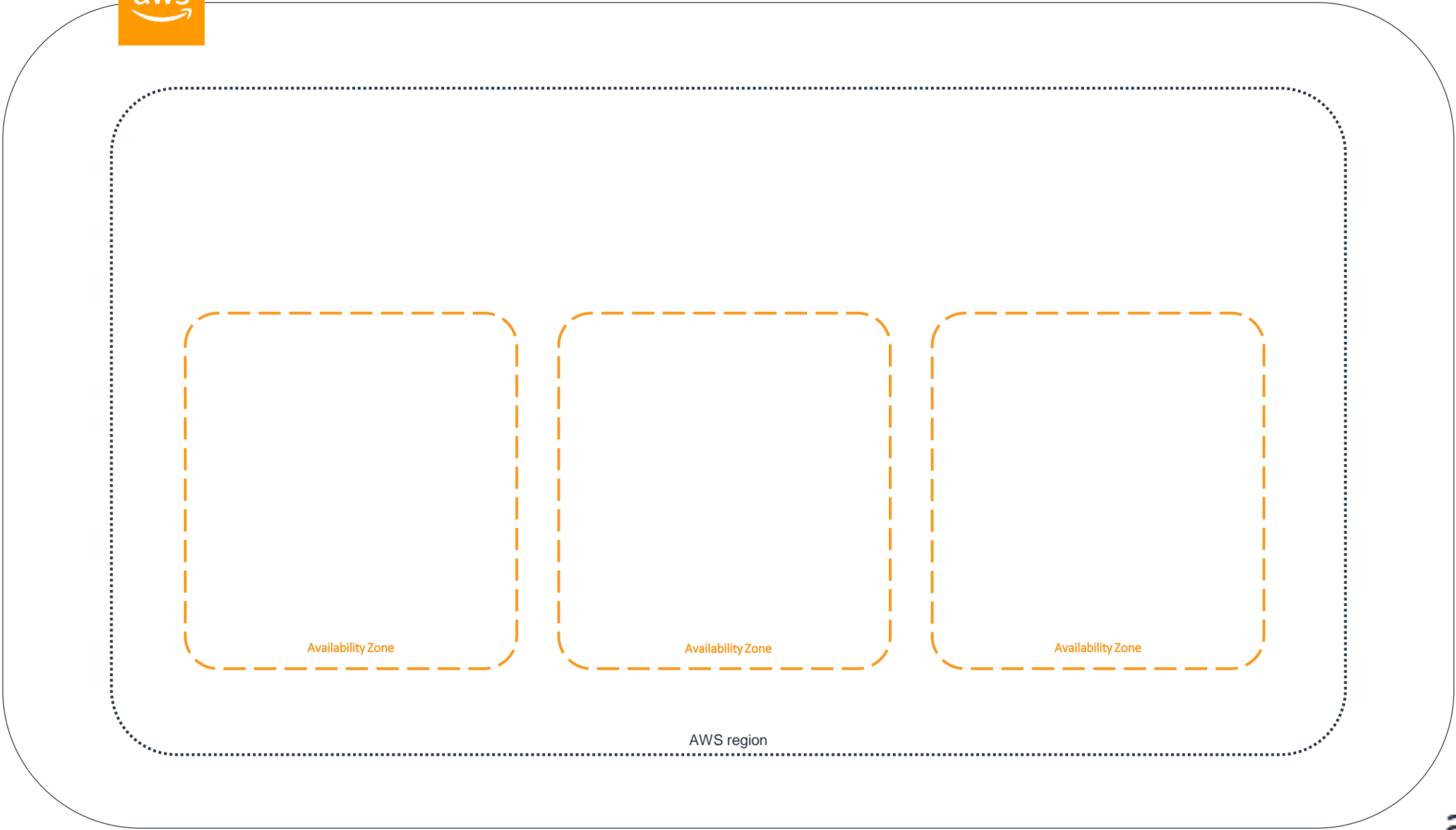
Where's my [AWS] stuff?





AWS region





Availability Zone

Availability Zone

Availability Zone

AWS region





Your VPC =
Your virtual data center in the cloud

VPC

10.0.0.0/16

Availability Zone

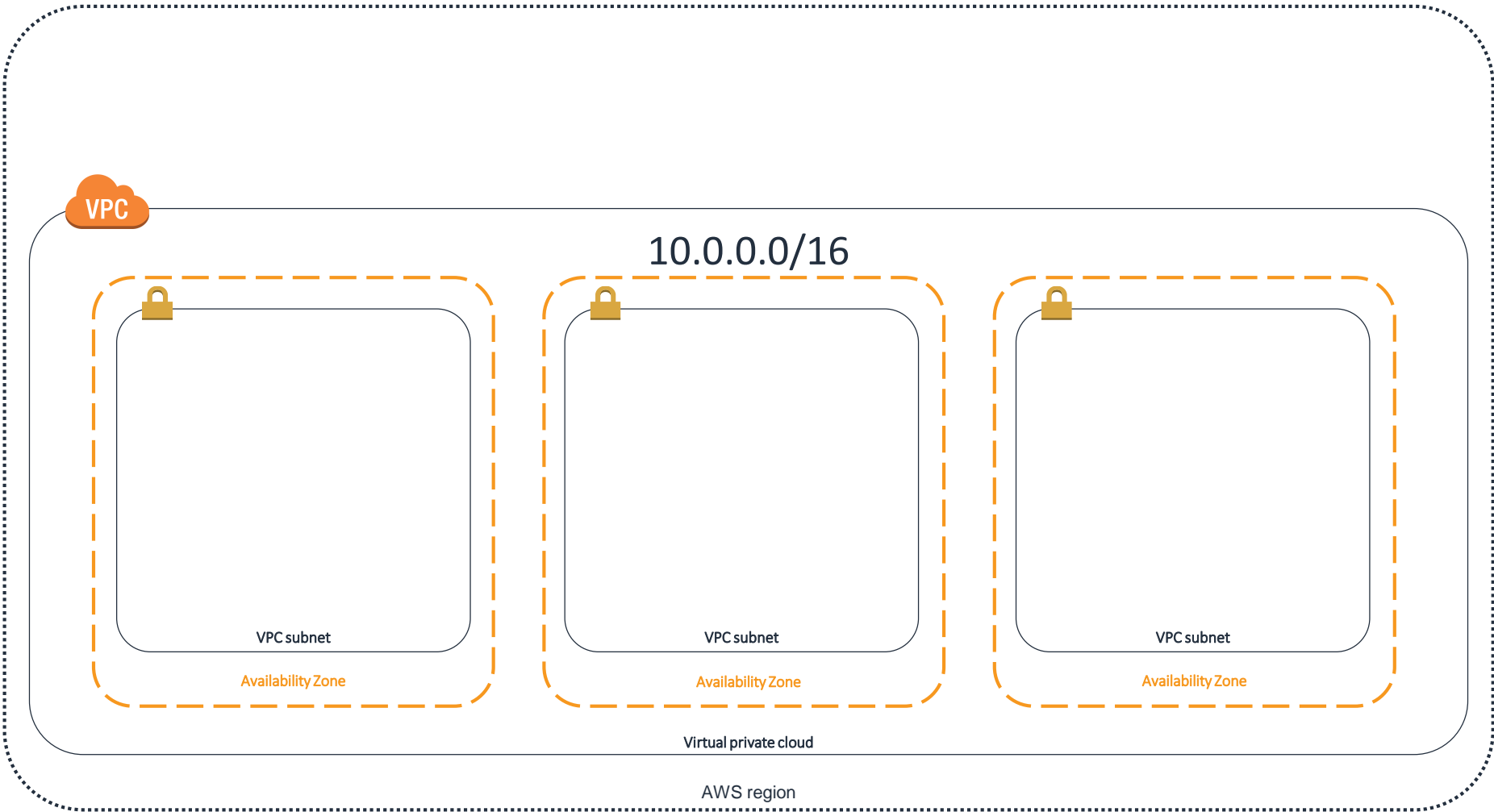
Availability Zone

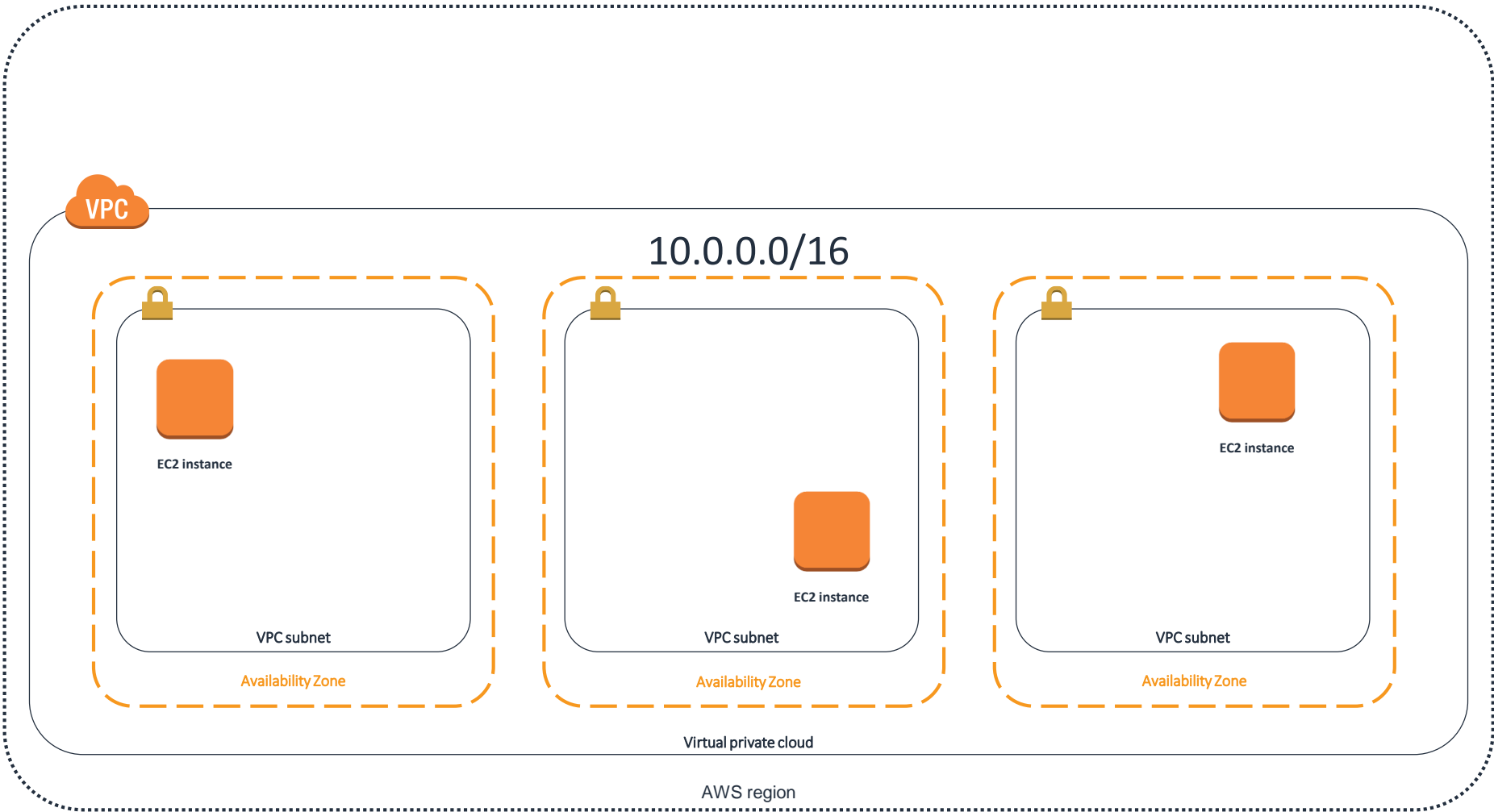
Availability Zone

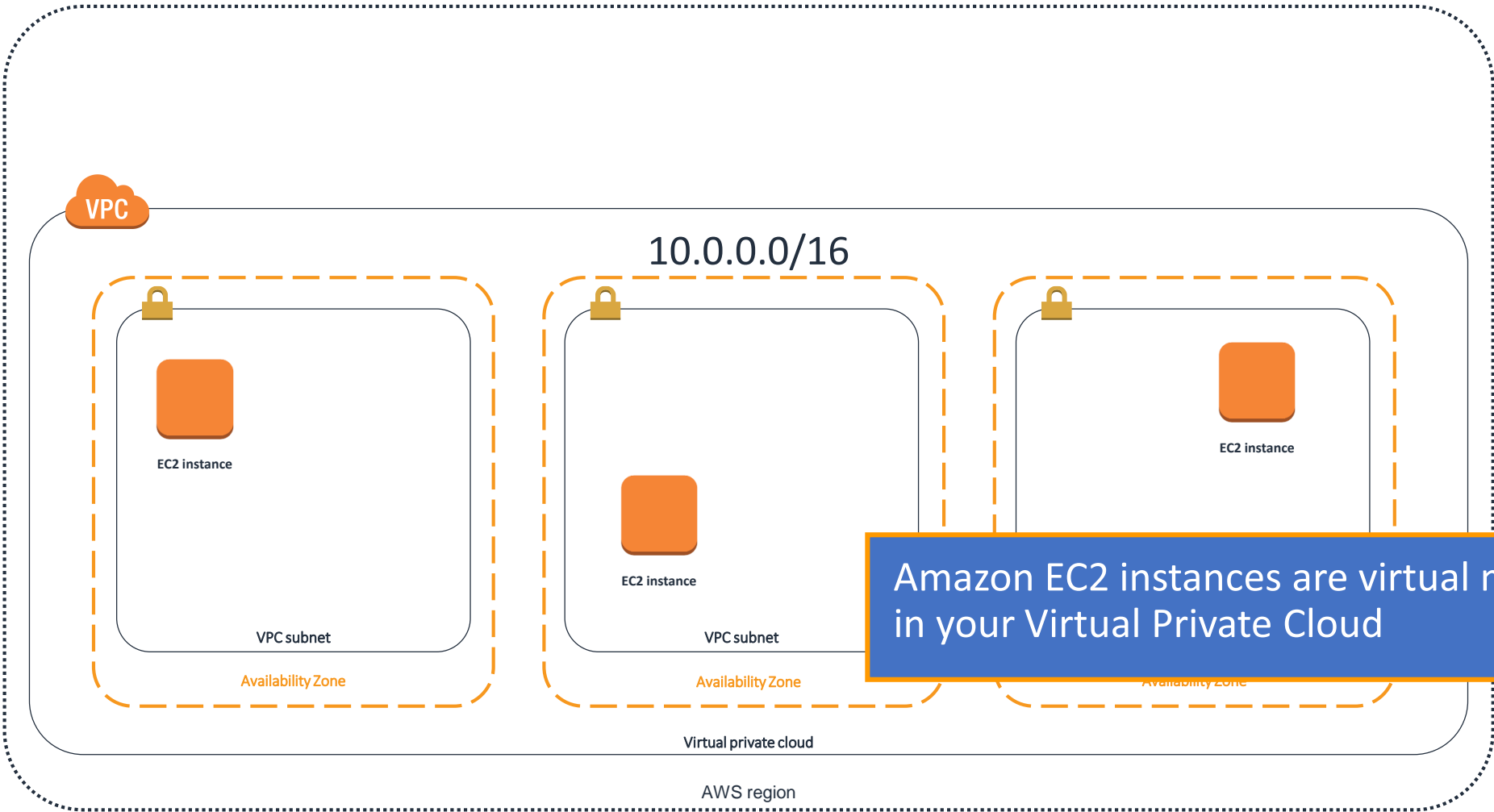
Virtual private cloud

AWS region







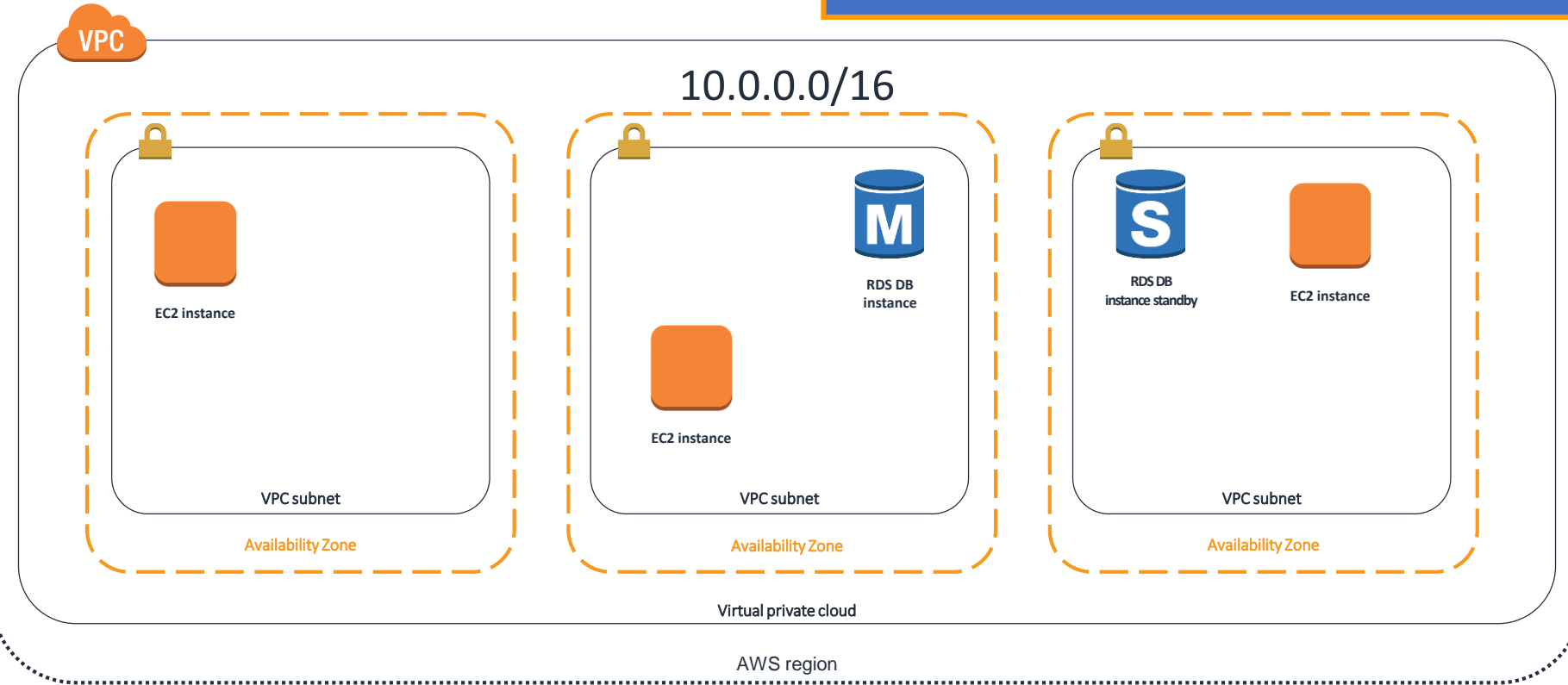


Amazon EC2 instances are virtual machines in your Virtual Private Cloud



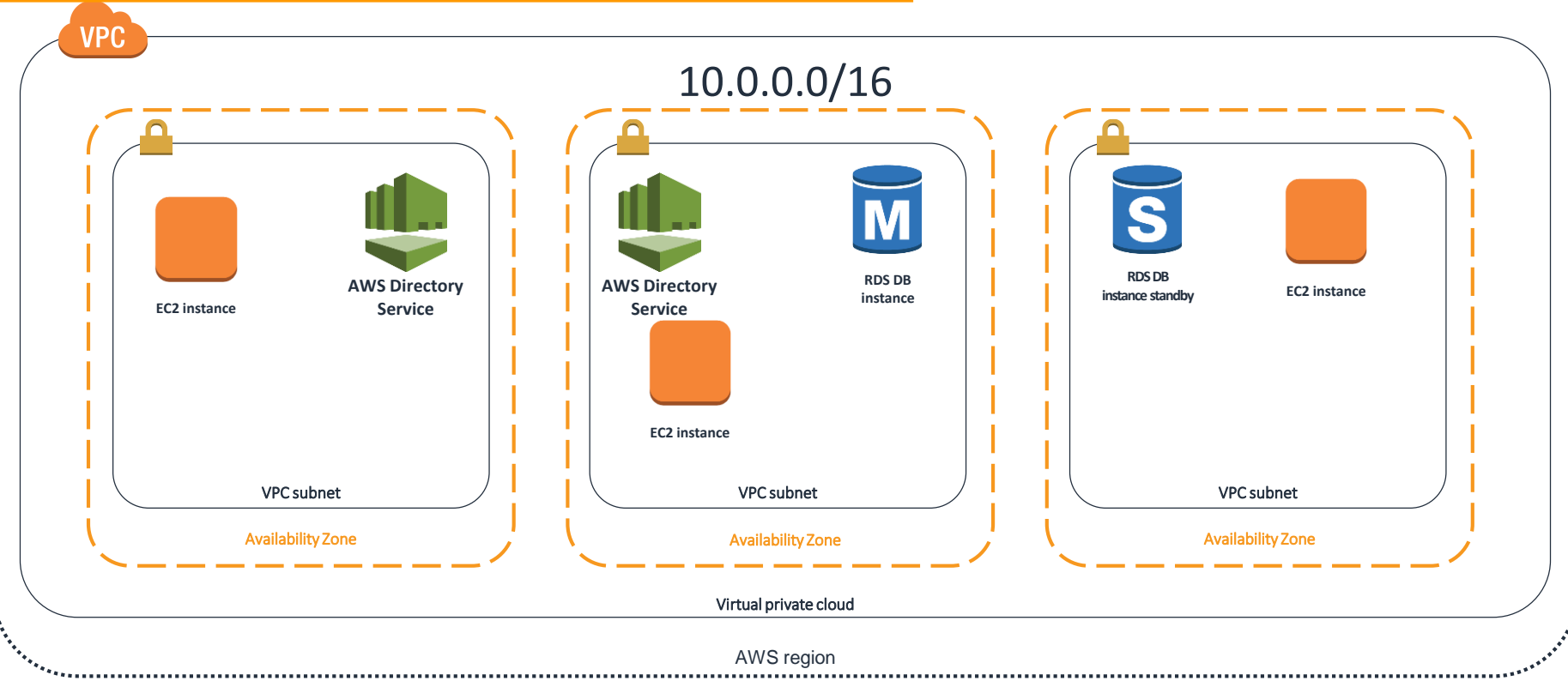


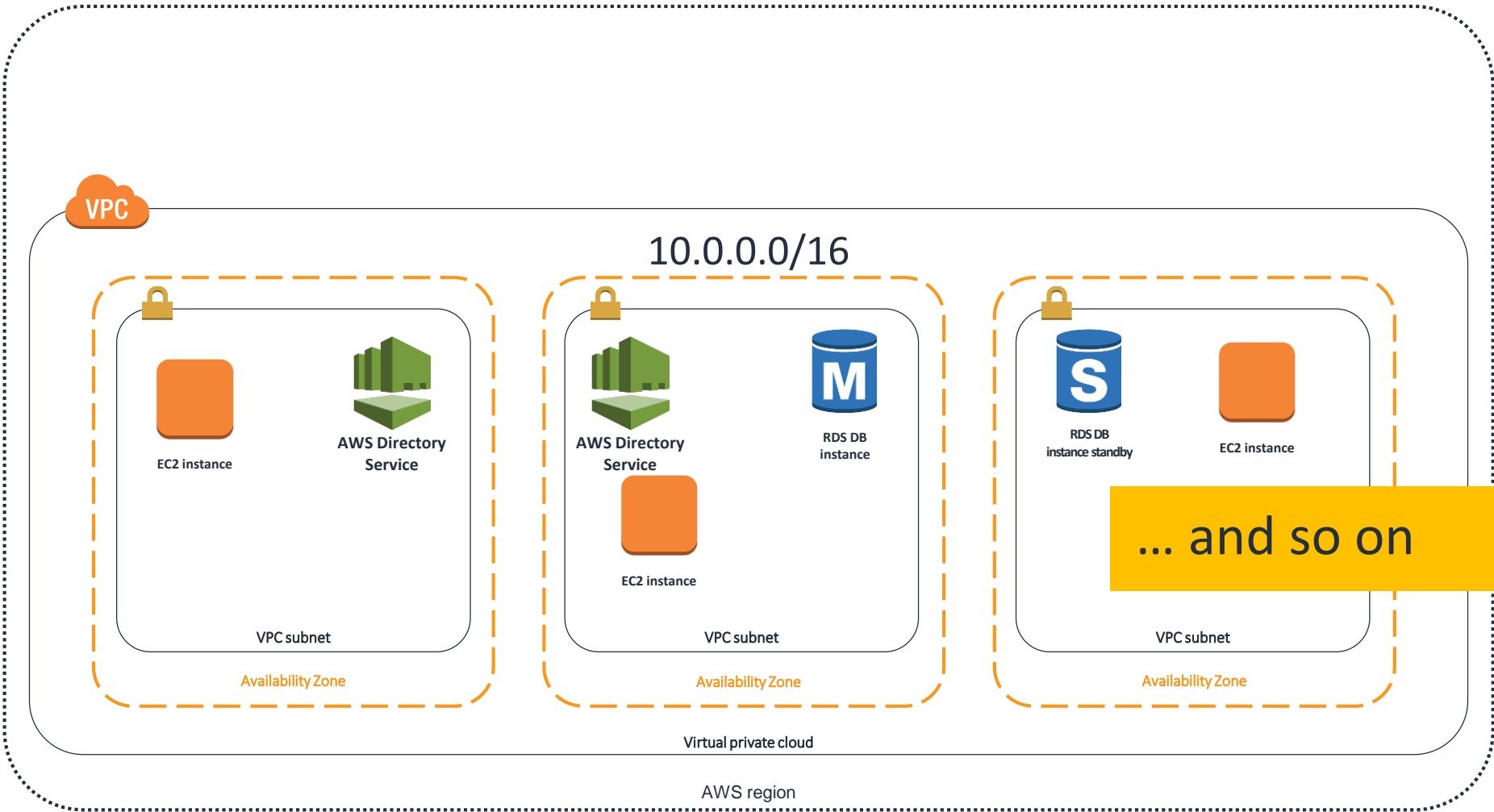
Amazon RDS databases run in your Virtual Private Cloud





AWS Directory Service domain controllers run in your Virtual Private Cloud







Amazon S3 bucket

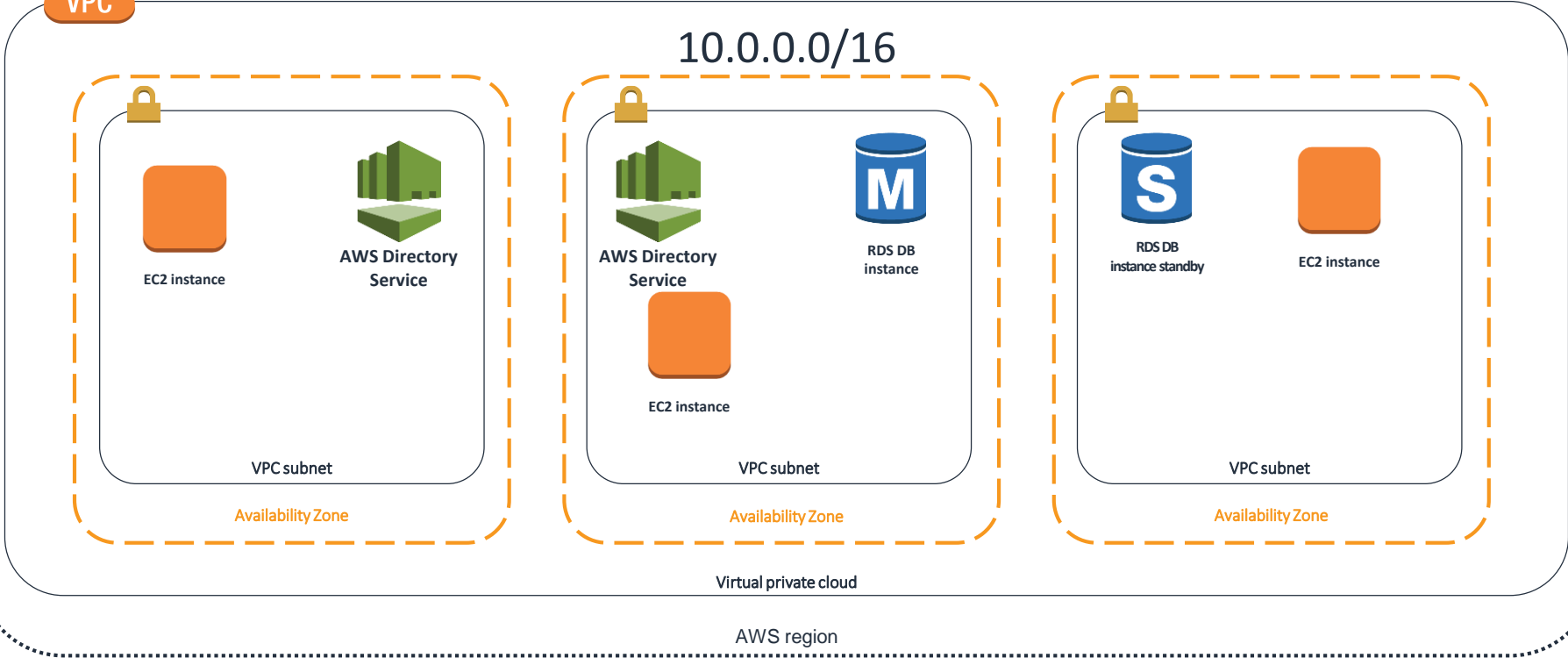


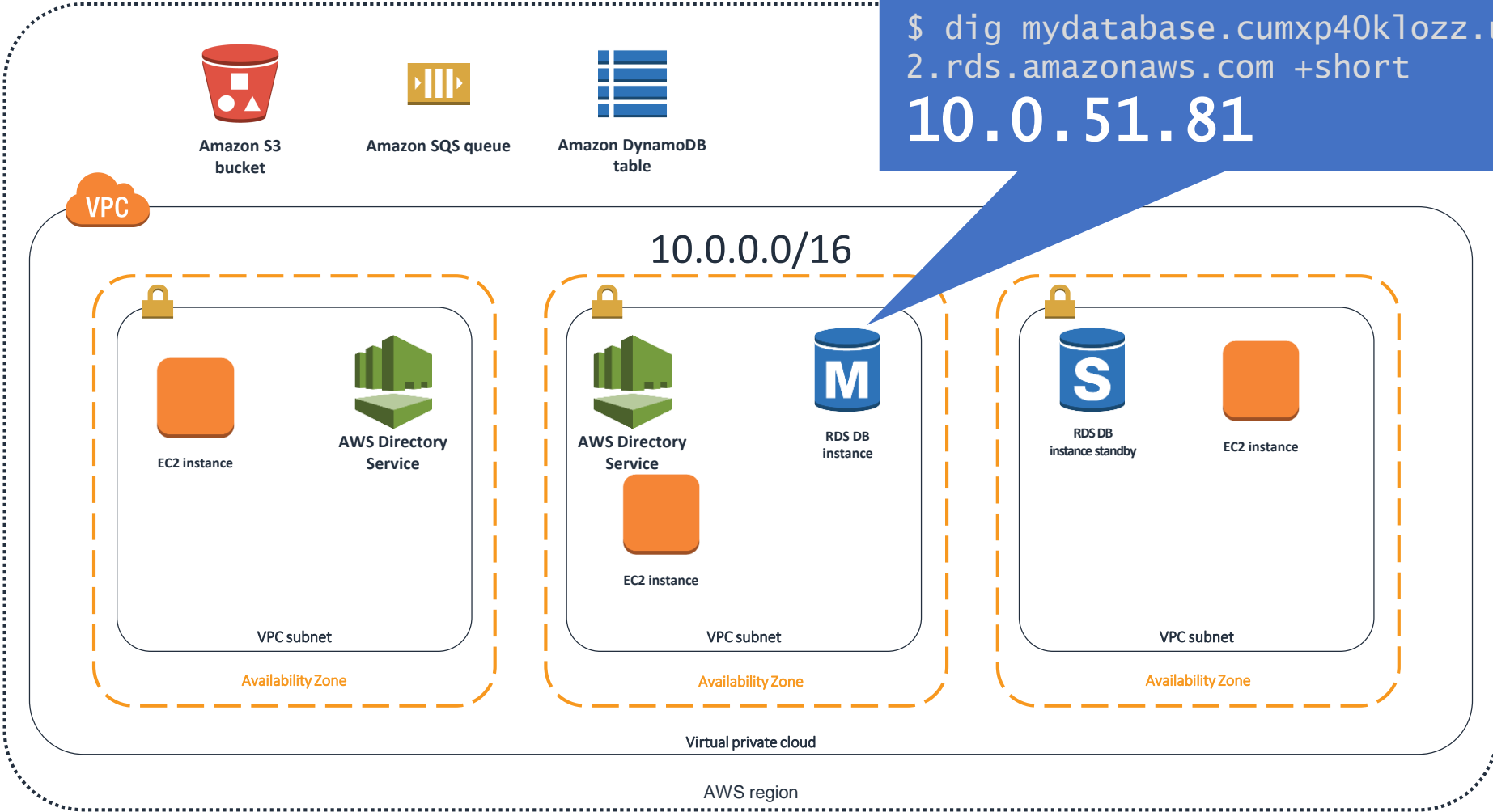
Amazon SQS queue



Amazon DynamoDB table

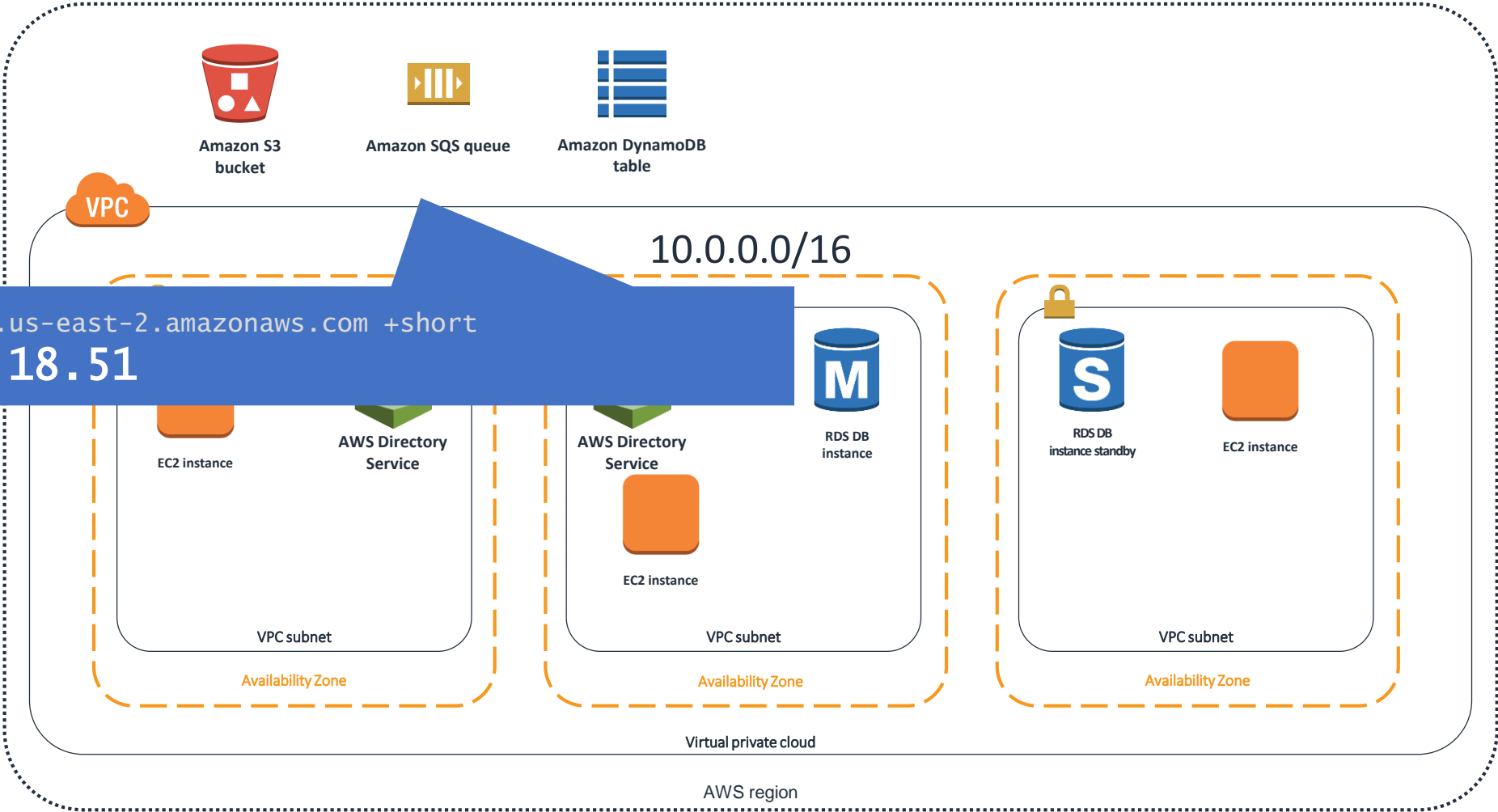
... and so on

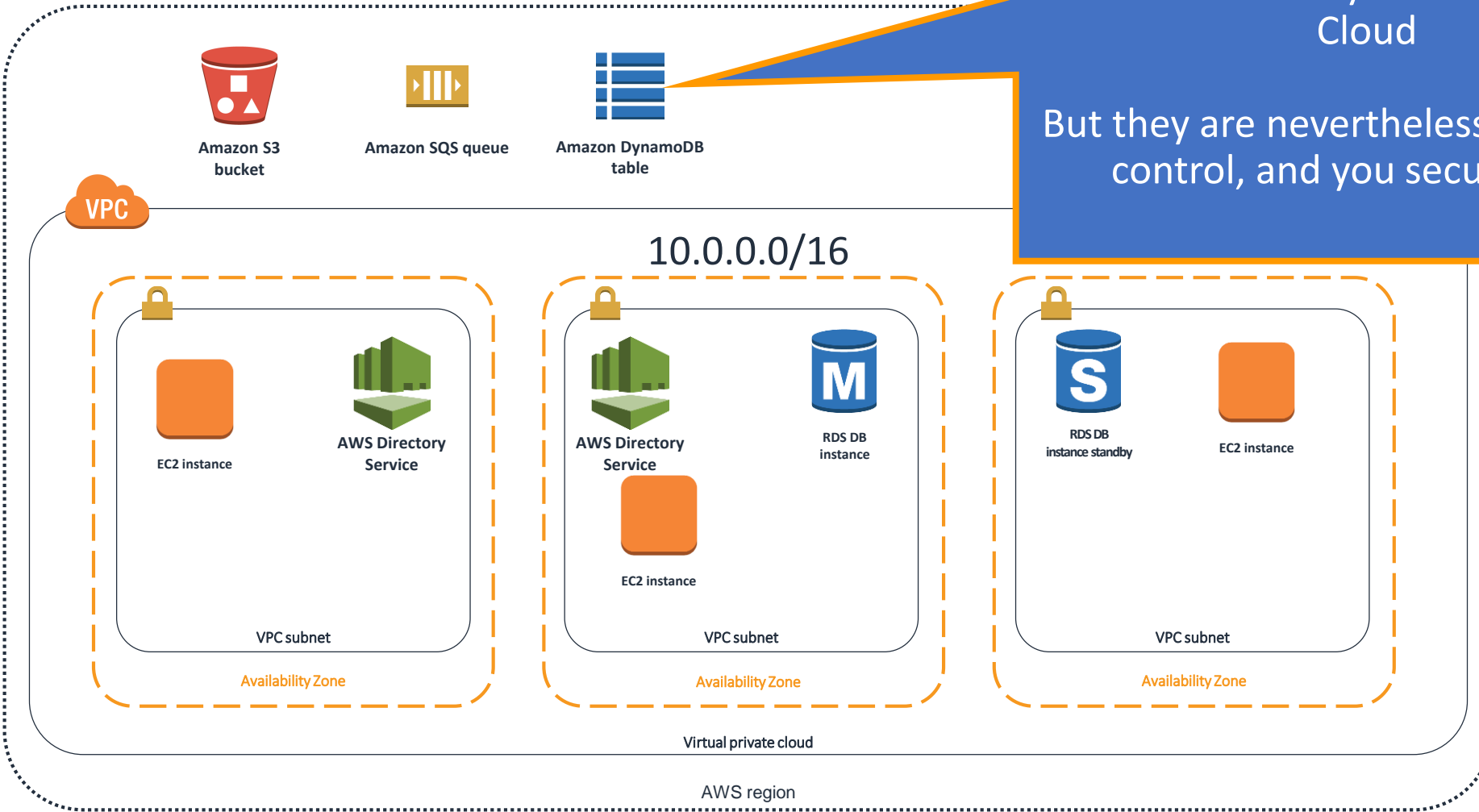






```
$ dig sqs.us-east-2.amazonaws.com +short  
52.95.18.51
```



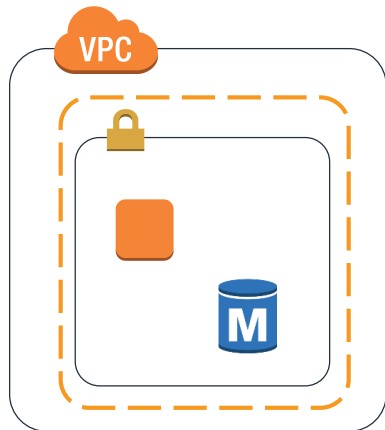


These are not in your Virtual Private Cloud
But they are nevertheless under your control, and you secure them

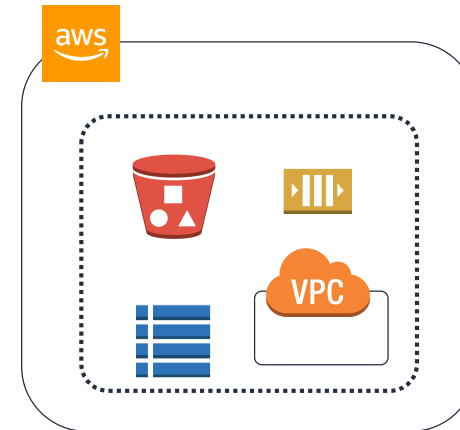


Determining a method for securing AWS resources

- 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)

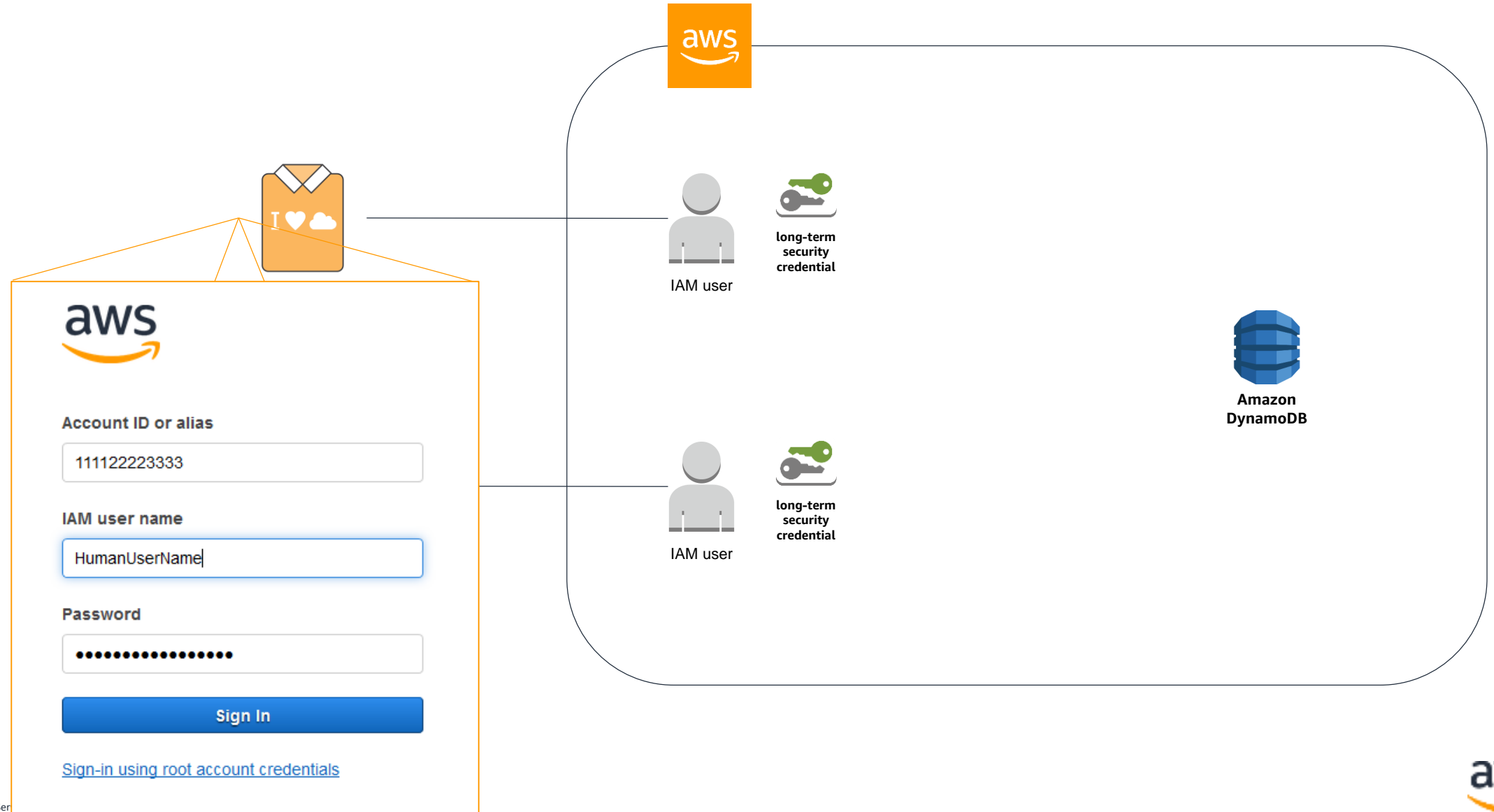
- **I: Identity.** IAM lets you create identities in your AWS Account who can make authenticated requests to AWS.
- **AM: Access Management.** IAM is your tool for defining who has permissions to do what to which resources in IAM.
- **IAM is the AWS-wide permissions control system.** So you need to know it.



I is for Identity: Humans → IAM Users



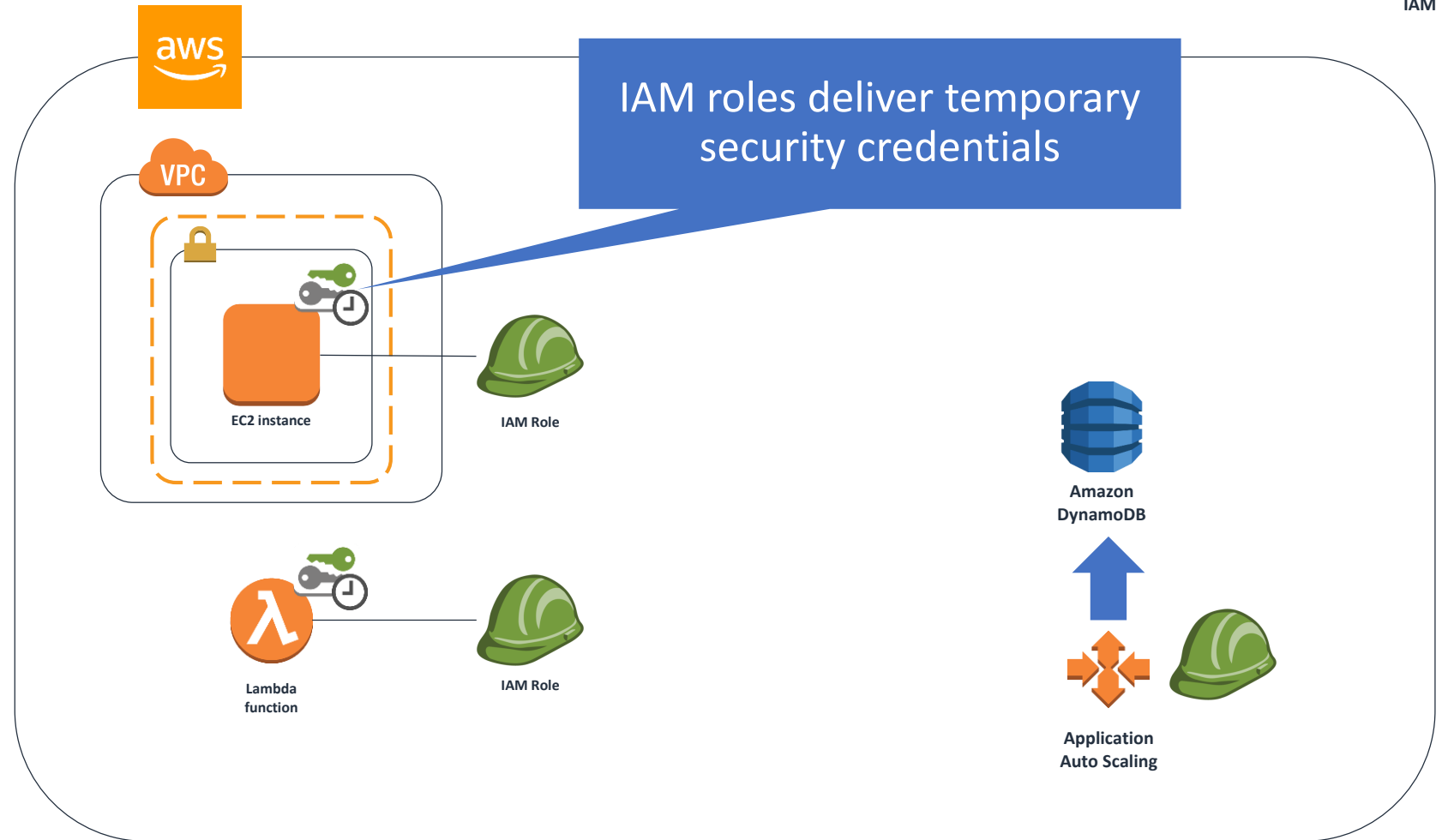
IAM



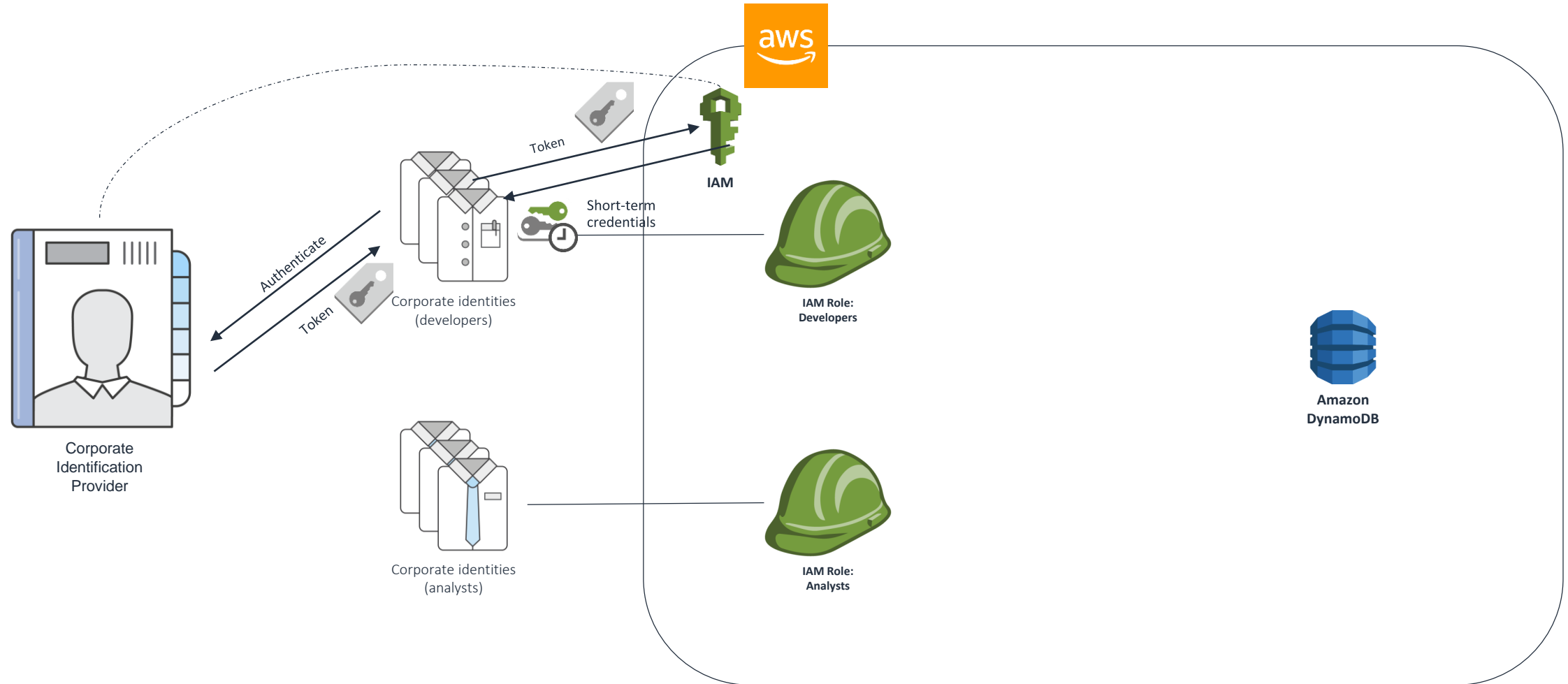
I is for Identity: Robots → IAM roles



IAM



I is for Identity: Humans with external identities



Term: IAM principal

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



IAM roles are for

- Automated processes
- AWS Services
- Federated identities



IAM Roles

IAM roles authenticate using short-lived credentials

IAM users are for

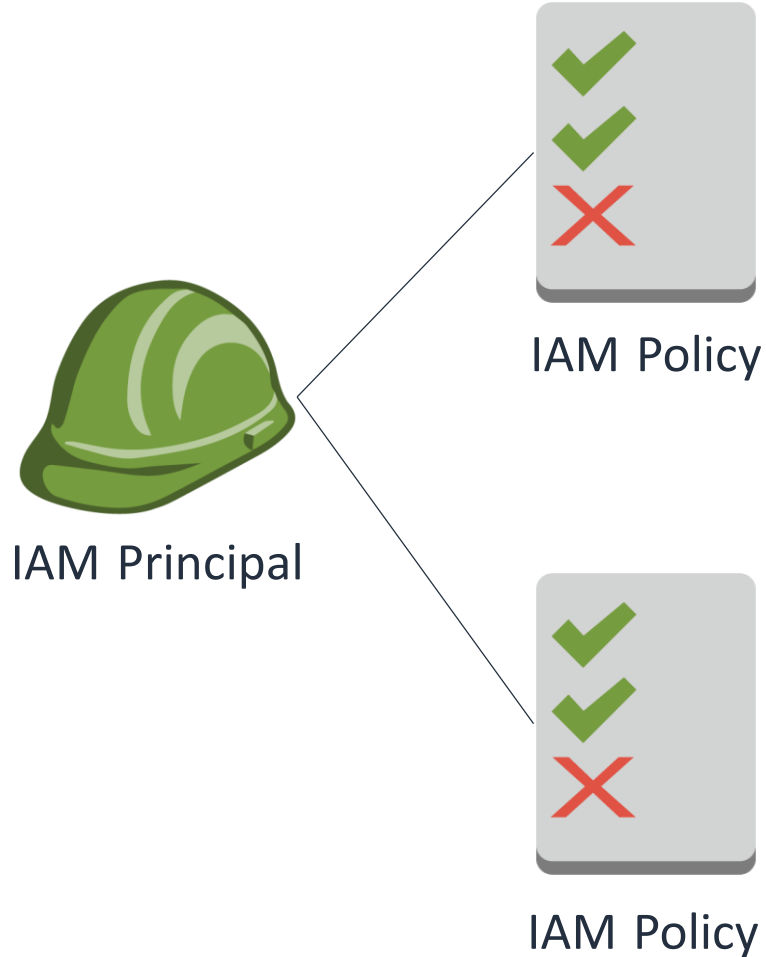
- Direct human access



IAM Users

IAM users authenticate using long-lived credentials

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



Create policy Policy actions

Filter policies

AWS pre-defines some IAM policies for common tasks

	Policy name	Type	Permissions	Description
<input type="radio"/>	AmazonDynamoDBFullAccess	AWS managed	None	Provides full access to Amazon DynamoDB via the AWS Man...
<input type="radio"/>	AmazonDynamoDBFullAccesswithData...	AWS managed	None	Provides full access to Amazon DynamoDB including Export/...
<input type="radio"/>	AmazonDynamoDBReadOnlyAccess	AWS managed	None	Provides read only access to Amazon DynamoDB via the AW...
<input type="radio"/>	AWSApplicationAutoscalingDynamoDBT...	AWS managed	Permissions policy (1)	Policy granting permissions to Application Auto Scaling to ac...
<input type="radio"/>	AWSLambdaDynamoDBExecutionRole	AWS managed	None	Provides list and read access to DynamoDB streams and writ...
<input type="radio"/>	AWSLambdaInvocation-DynamoDB	AWS managed	None	Provides read access to DynamoDB Streams.
<input type="radio"/>	DynamoDBReplicationServiceRolePolicy	AWS managed	None	Permissions required by DynamoDB for cross-region data rep...

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

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

Writing more granular IAM Policies: Resource-level IAM Policies

```
{
  "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/*"
      ]
    }
  ]
}
```

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

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



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`

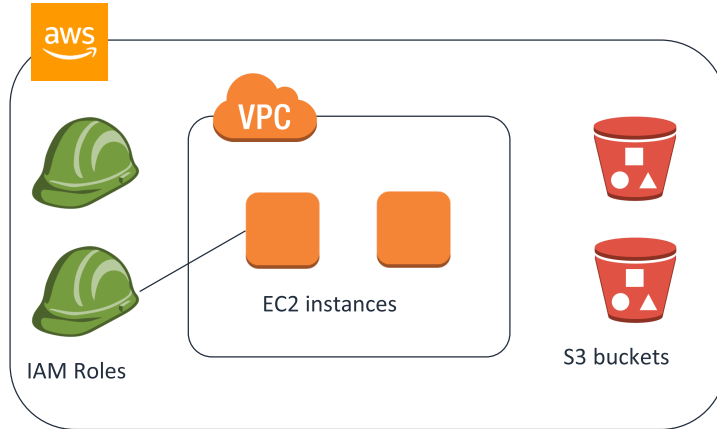
Writing more granular IAM policies:

Conditions

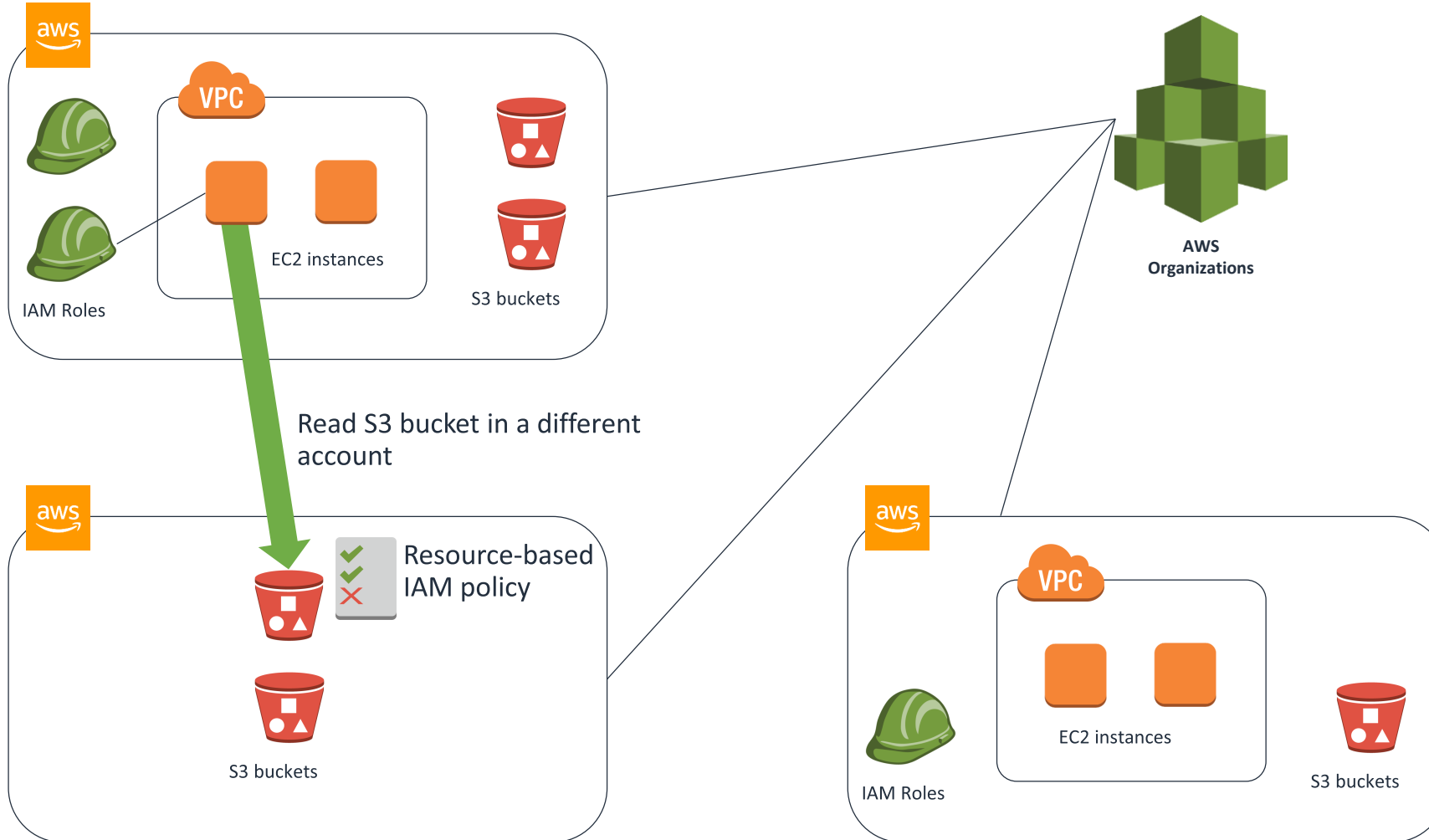
```
{
  "version": "2012-10-17",
  "statement": [
    {
      "effect": "Allow",
      "action": [
        "dynamodb:*"
      ],
      "resource": "*",
      "condition": {
        "stringEquals": {
          "aws:RequestedRegion": [
            "us-east-2"
          ]
        }
      }
    }
  ]
}
```

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

Securing AWS resources across multiple accounts



Securing AWS resources across multiple accounts



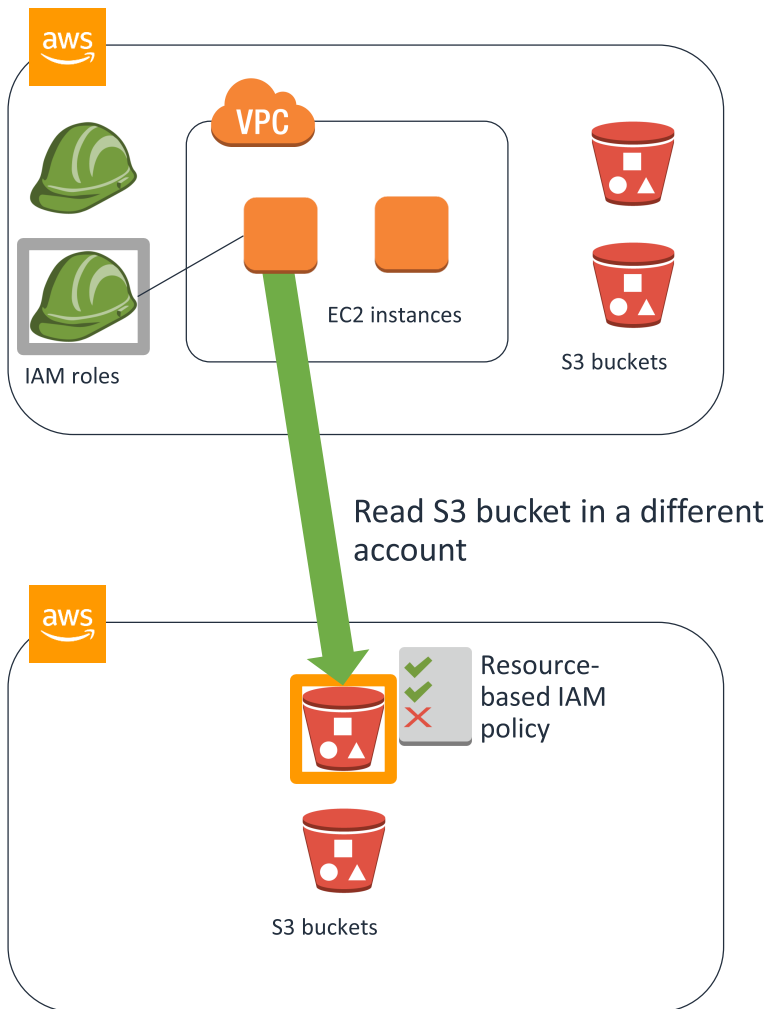
Example: Resource-based policy

```
{
  "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/*"
    }
  ]
}
```

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



IAM Authorization of cross-account access



Authorization decision:



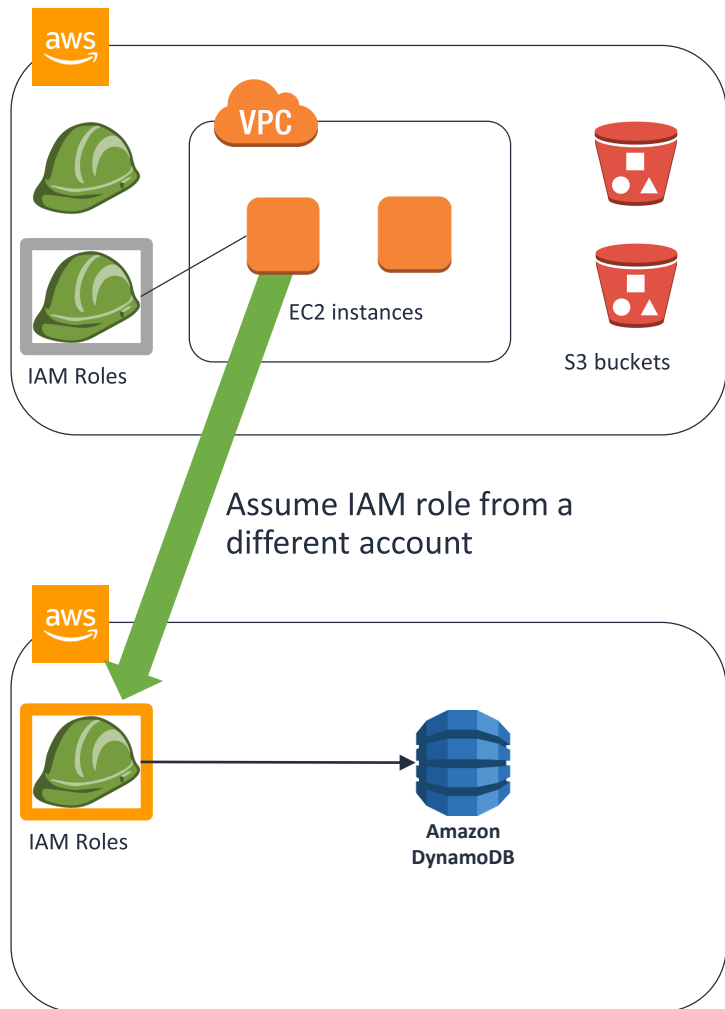
1. Does the **S3 bucket** have a policy allowing access from the calling IAM principal?



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



AWS Identity and Access Management

User Guide

Documentation - This Guide

Search

- [What Is IAM?](#)
- [Getting Set Up](#)
- [Getting Started](#)
- [Tutorials](#)
- [Best Practices and Use Cases](#)

[AWS Documentation](#) » [AWS Identity and Access Management](#) » [User Guide](#) » [Reference Information for AWS Identity and Access Management](#) » [AWS Services That Work with IAM](#)

AWS Services That Work with IAM

The AWS services listed below are grouped by their [AWS product categories](#) and include information about what IAM features they support:

- **Service** – You can choose the name of a service to view the AWS documentation about IAM authorization and access for that service.
- **Actions** – You can specify individual actions in a policy. If the service does not support this feature, then **All actions** is selected in the [visual editor](#). In a JSON policy document, you must use * in the Action element. For a list of actions in each service, see [Actions, Resources, and Condition Keys for AWS Services](#).
- **Resource-level permissions** – You can use [ARNs](#) to specify individual resources in the policy. If the service does not support this feature, then **All resources** is chosen in the [policy visual editor](#). In a JSON policy

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



Amazon S3 bucket



Amazon SQS queue



Amazon DynamoDB table

VPC

10.0.0.0/16



EC2 instance



AWS Directory Service

VPC subnet

Availability Zone



AWS Directory Service



RDS DB instance



EC2 instance

VPC subnet

Availability Zone



RDS DB instance standby



EC2 instance

VPC subnet

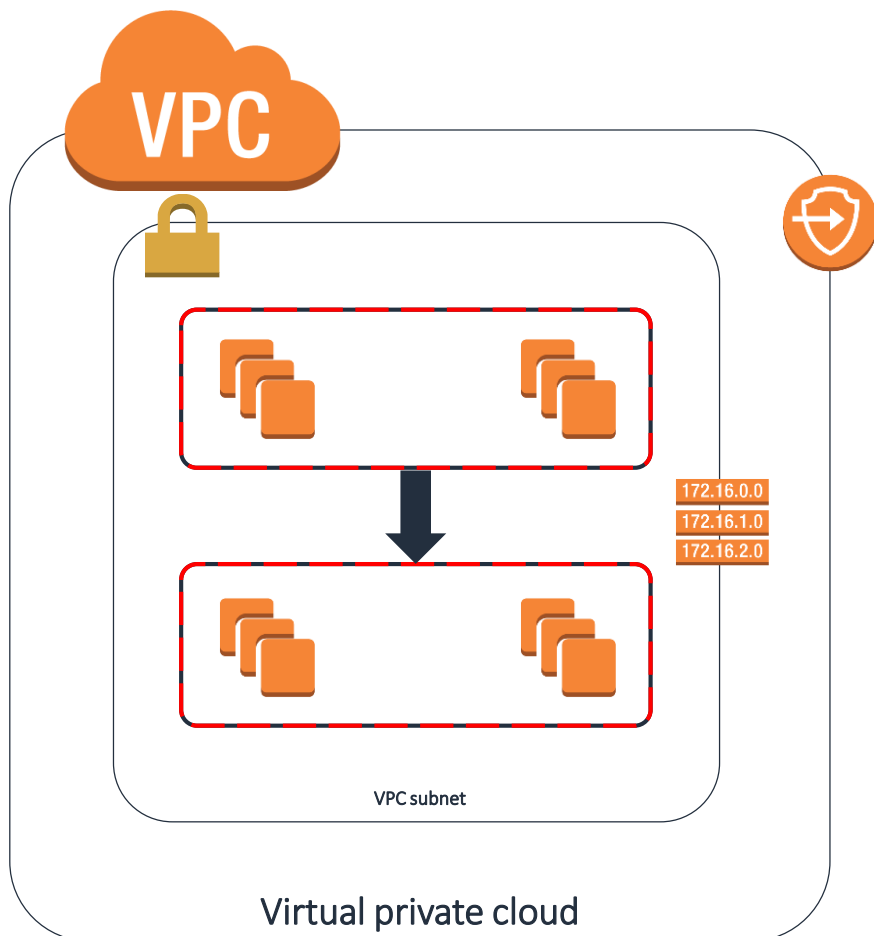
Availability Zone

Virtual private cloud

AWS region

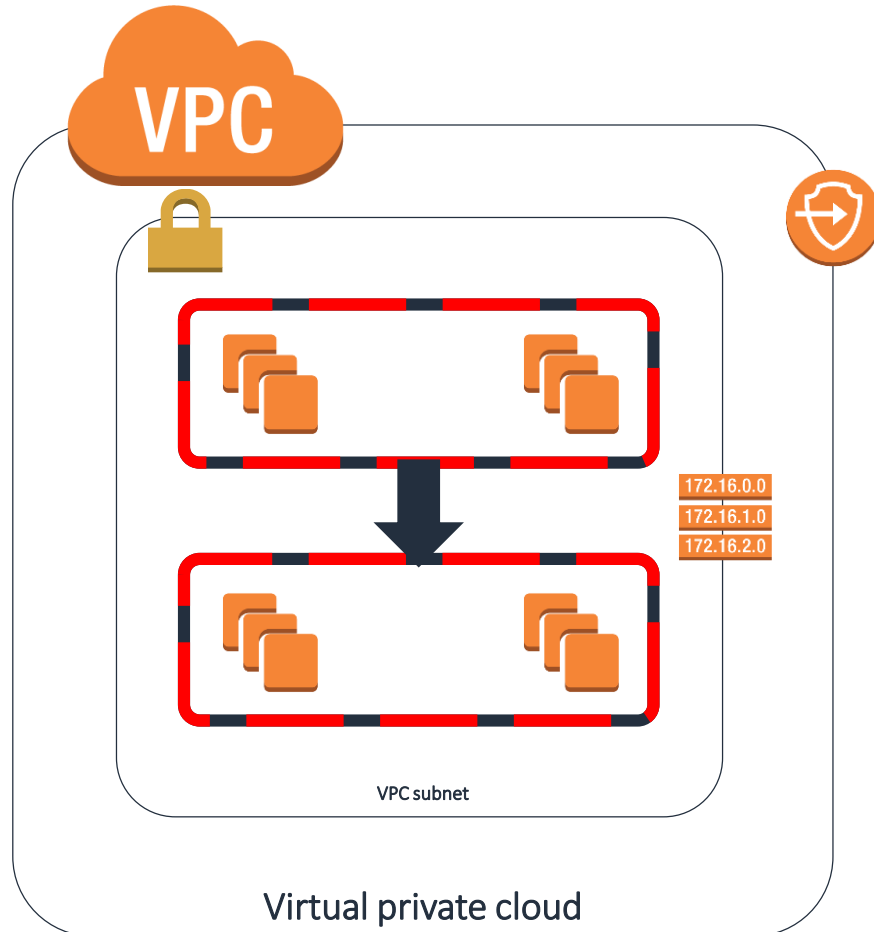


Secure connectivity with Amazon VPC



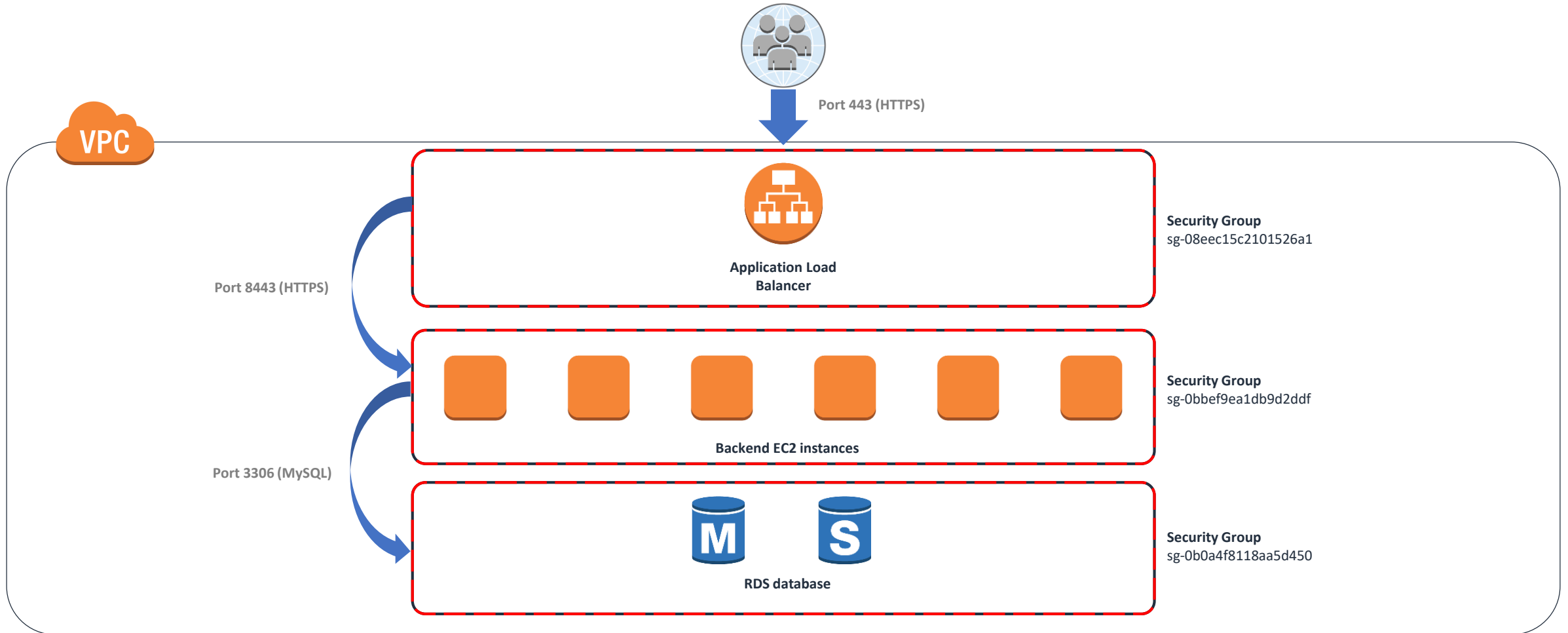
- **Security Groups:** Authorize only the traffic you expect
- **Routing:** Route traffic headed out of your VPC only to expected destinations
- **VPC Endpoints:** Create specific, least-privilege points of connectivity

Secure connectivity with Amazon VPC

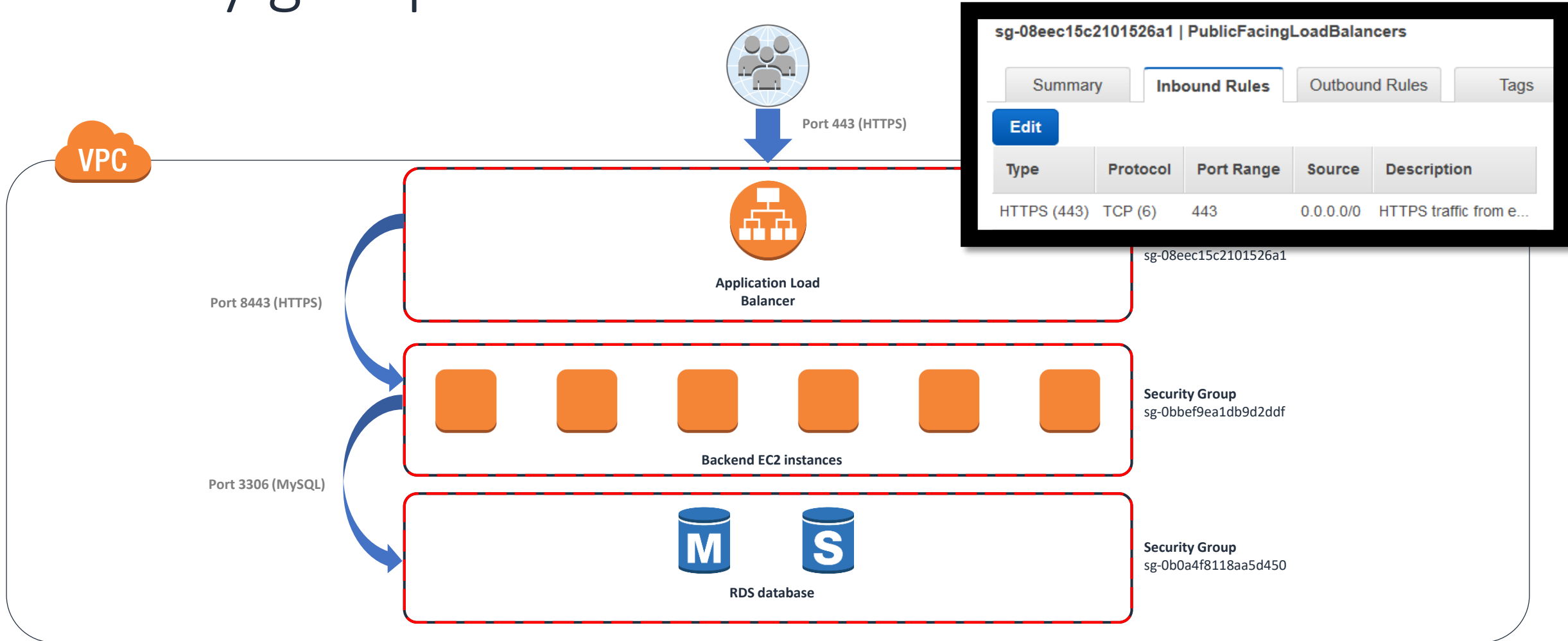


- **Security Groups:** Authorize only the traffic you expect
- **Routing:** Route traffic headed out of your VPC only to expected destinations
- **VPC Endpoints:** Create specific, least-privilege points of connectivity

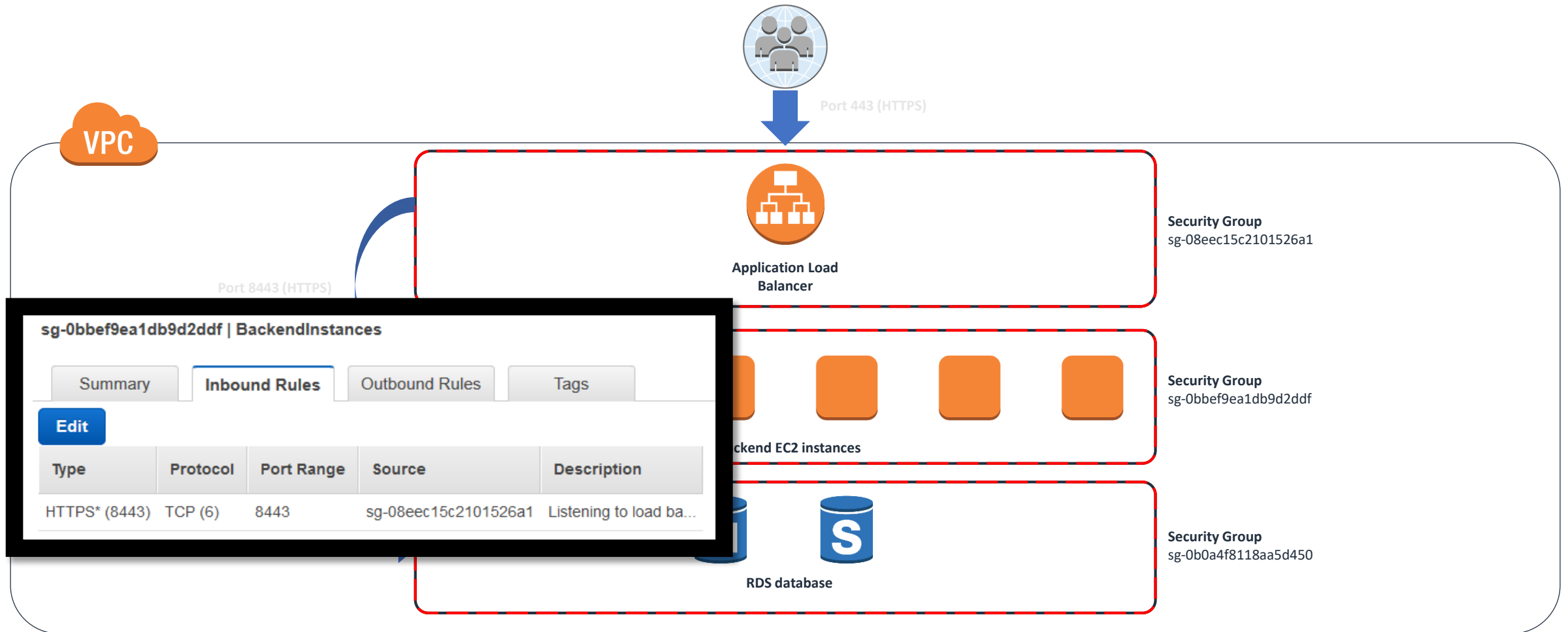
Security groups: Stateful network firewalls



Security groups: Stateful network firewalls



Security groups: Stateful network firewalls



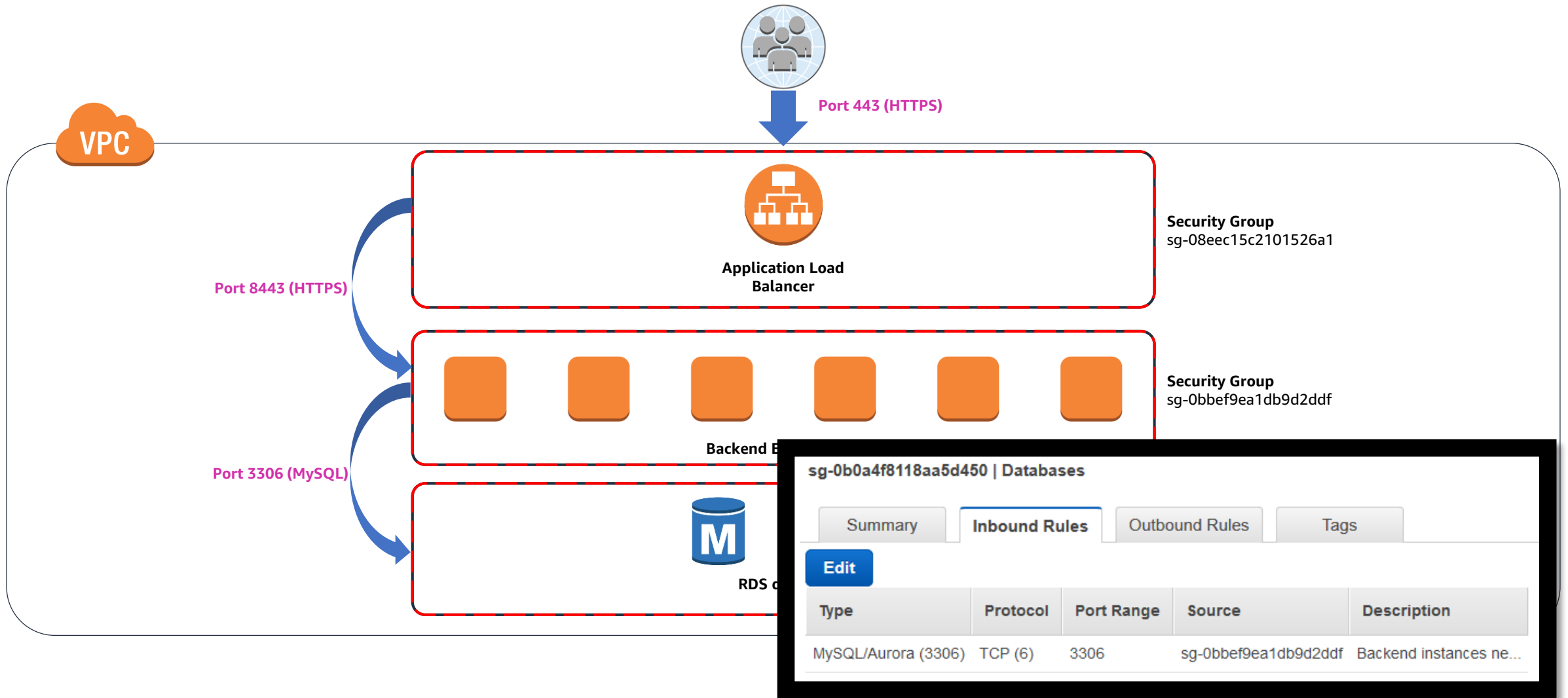
sg-0bbef9ea1db9d2ddf | BackendInstances

Summary | **Inbound Rules** | Outbound Rules | Tags

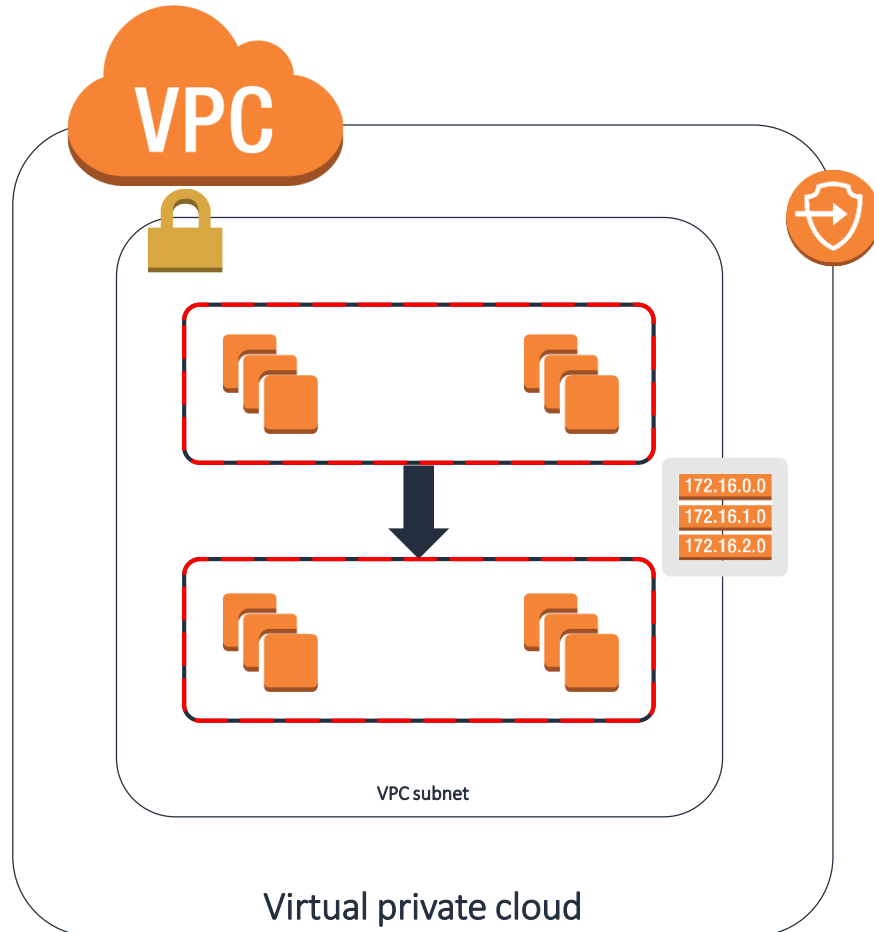
Edit

Type	Protocol	Port Range	Source	Description
HTTPS* (8443)	TCP (6)	8443	sg-08eec15c2101526a1	Listening to load ba...

Security Groups: Stateful network firewalls

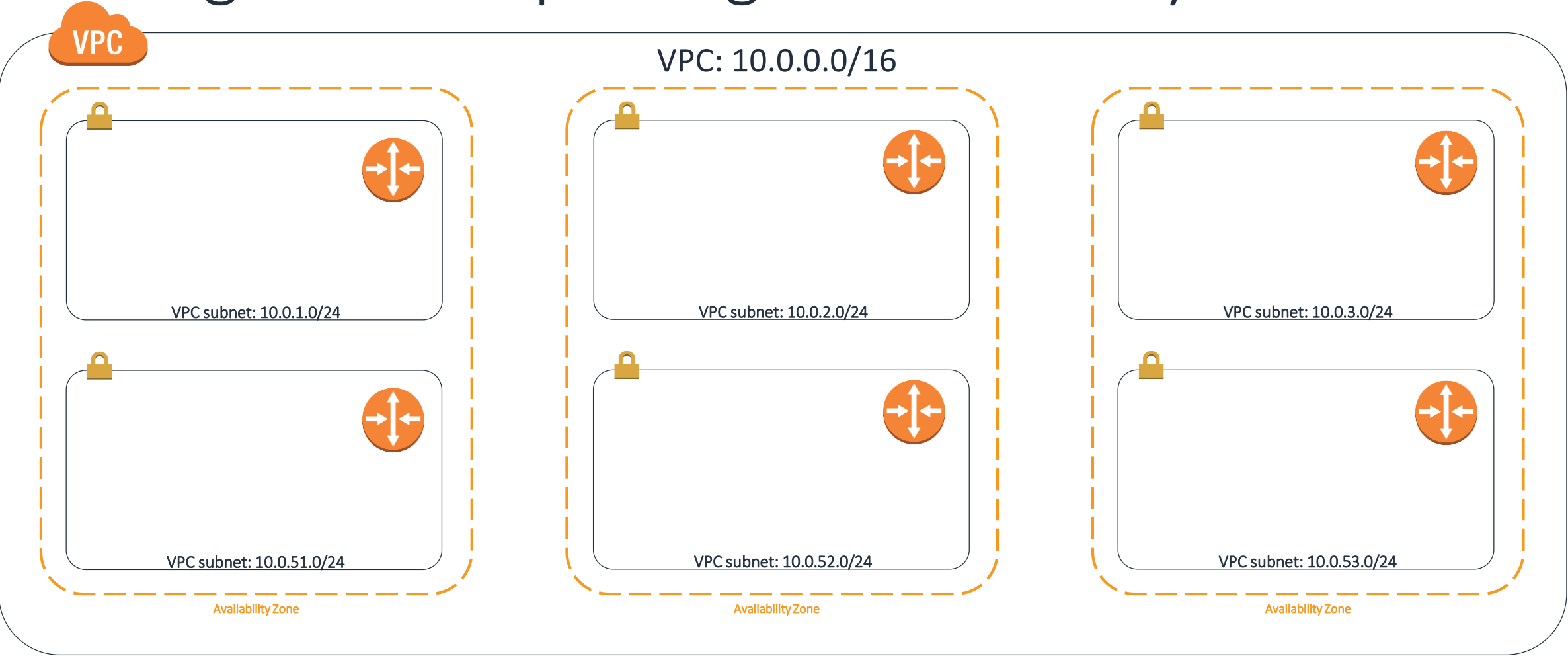


Secure connectivity with Amazon VPC

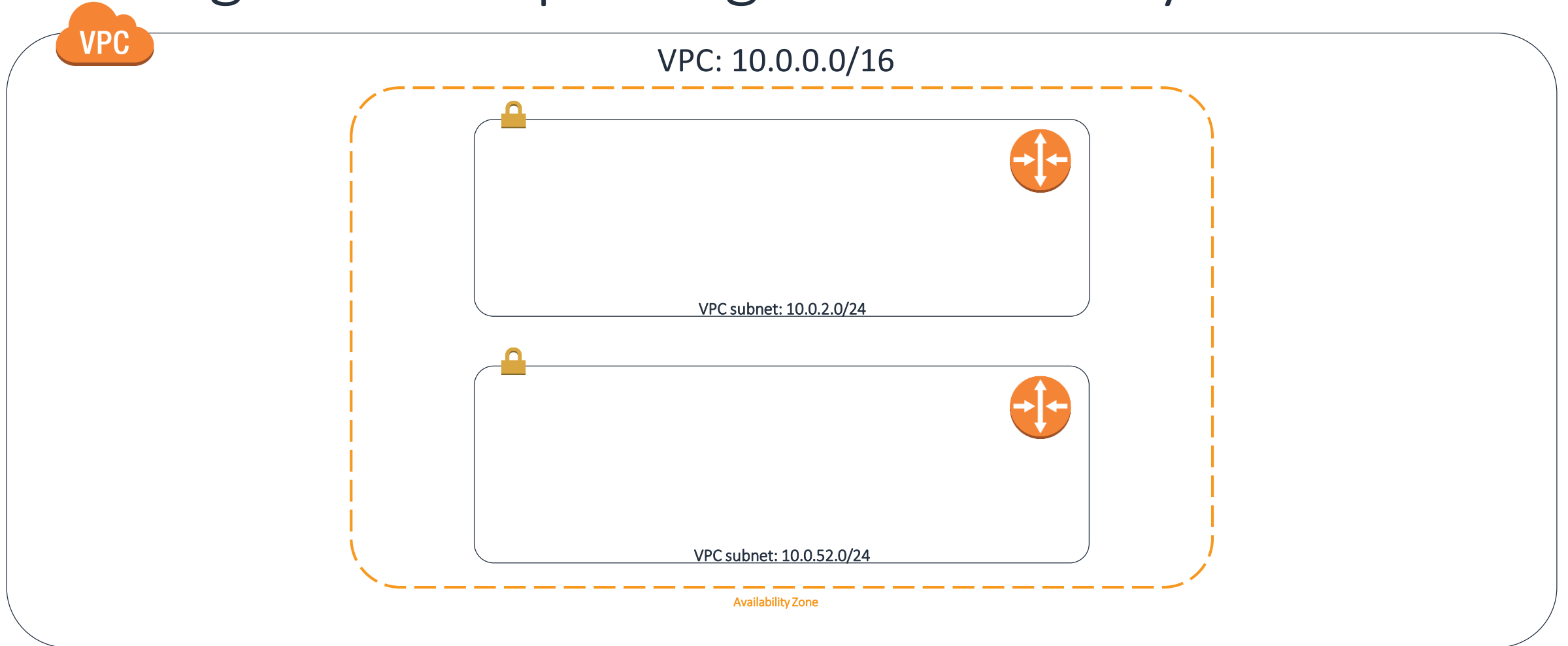


- **Security Groups:** Authorize only the traffic you expect
- **Routing:** Route traffic headed out of your VPC only to expected destinations
- **VPC Endpoints:** Create specific, least-privilege points of connectivity

Routing for least-privilege connectivity



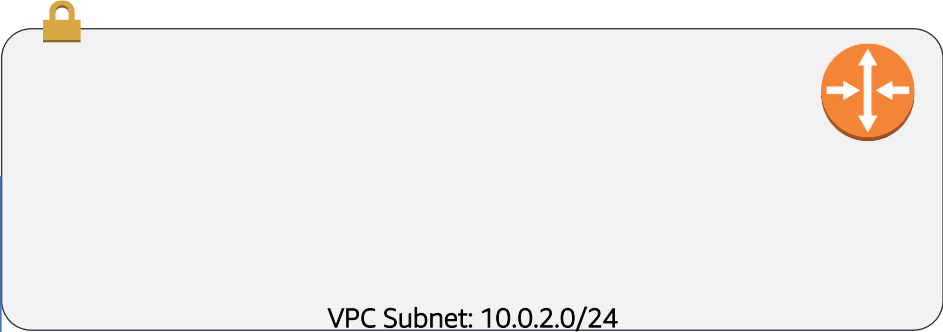
Routing for least-privilege connectivity



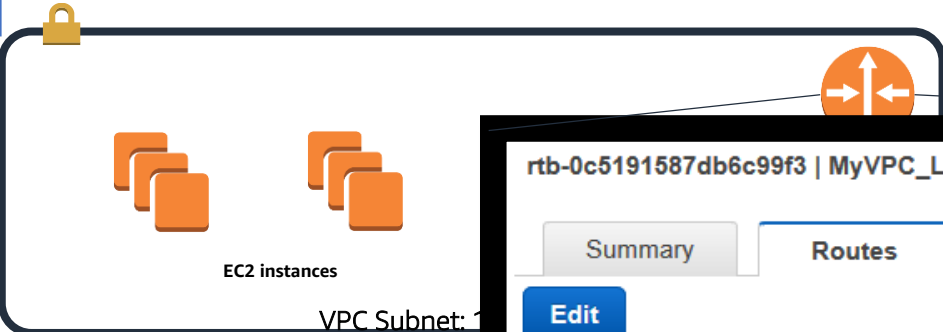
Routing: No outbound connectivity



VPC: 10.0.0.0/16



Resources in this subnet cannot send packets outside the VPC



rtb-0c5191587db6c99f3 | MyVPC_LocalOnly

Summary Routes Subnet Associations Route Propagation Tags

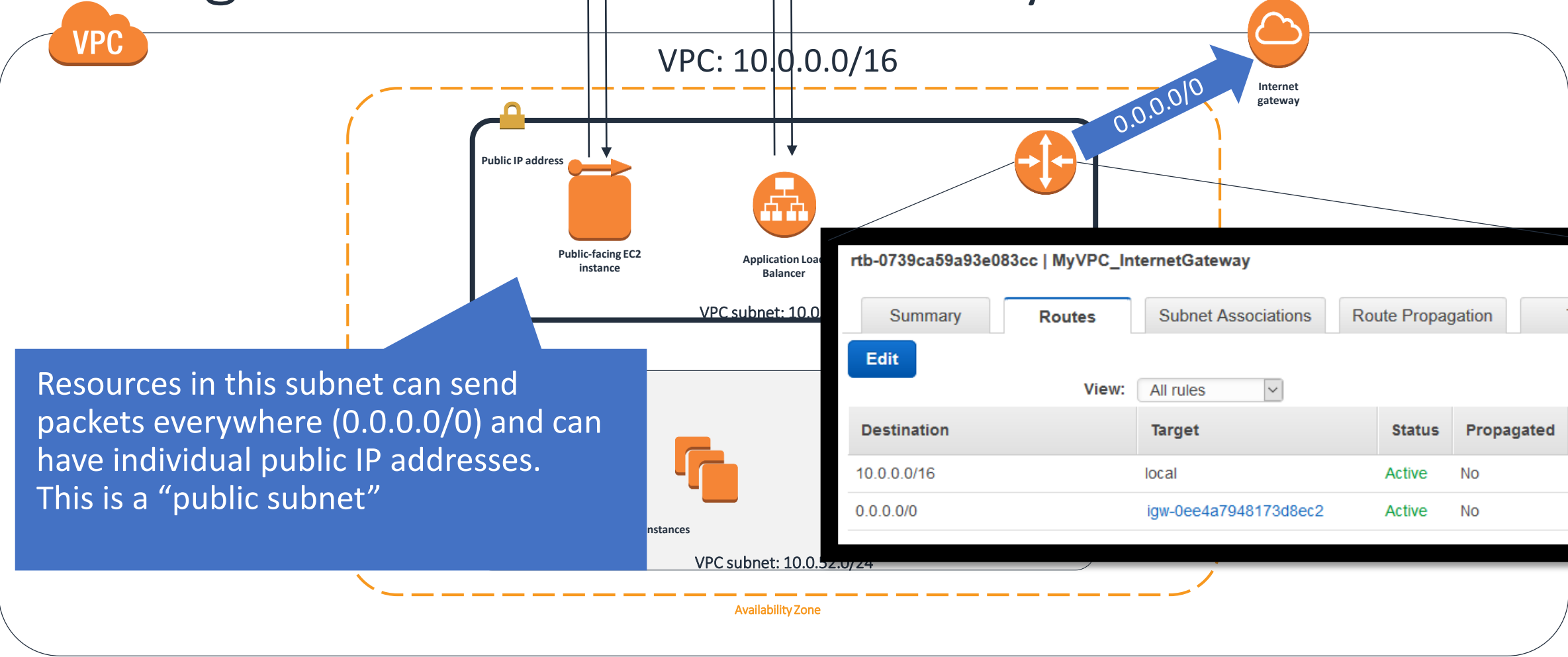
Edit

View: All rules

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No



Routing: Full internet connectivity



Resources in this subnet can send packets everywhere (0.0.0.0/0) and can have individual public IP addresses. This is a “public subnet”



Routing: Outbound-only internet connectivity



Resources in this subnet can send packets everywhere (0.0.0.0/0) but do not have individual public IP addresses. All outbound traffic passes through the NAT Gateway

VPC: 10.0.0.0/16

Public IP address



VPC NAT gateway

VPC Subnet: 10.0.2.0/24



0.0.0.0/0



Internet gateway



EC2 instances

VPC Subnet: 10.0.0.0/24

Availability Zone

rtb-07446fdd7bb96c6a0 | MyVPC_OutboundNAT

Summary Routes Subnet Associations Route Propagation

Edit

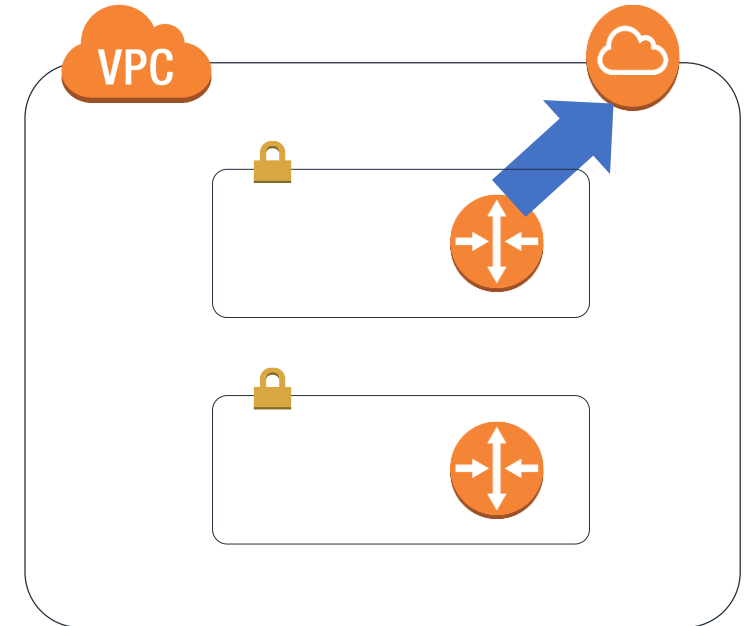
View: All rules

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-0802262c615050bbd		No

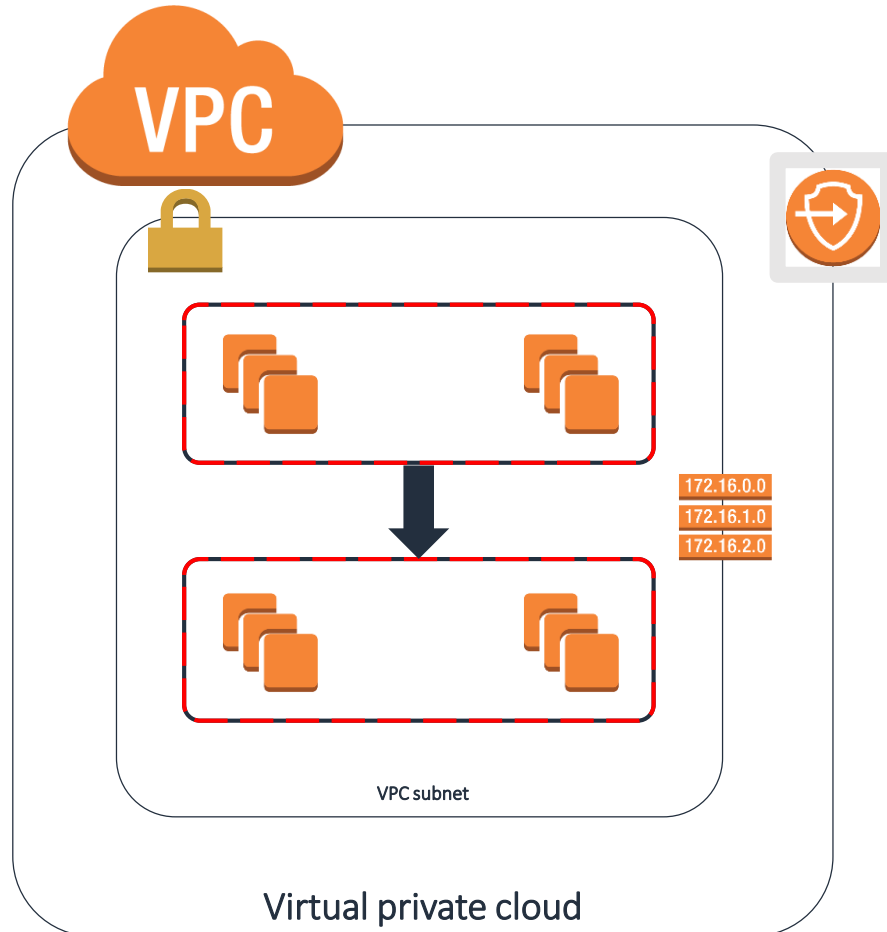


Routing for least privilege: Summary

- 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