Capgemini

CONSULTING.TECHNOLOGY.OUTSOURCING

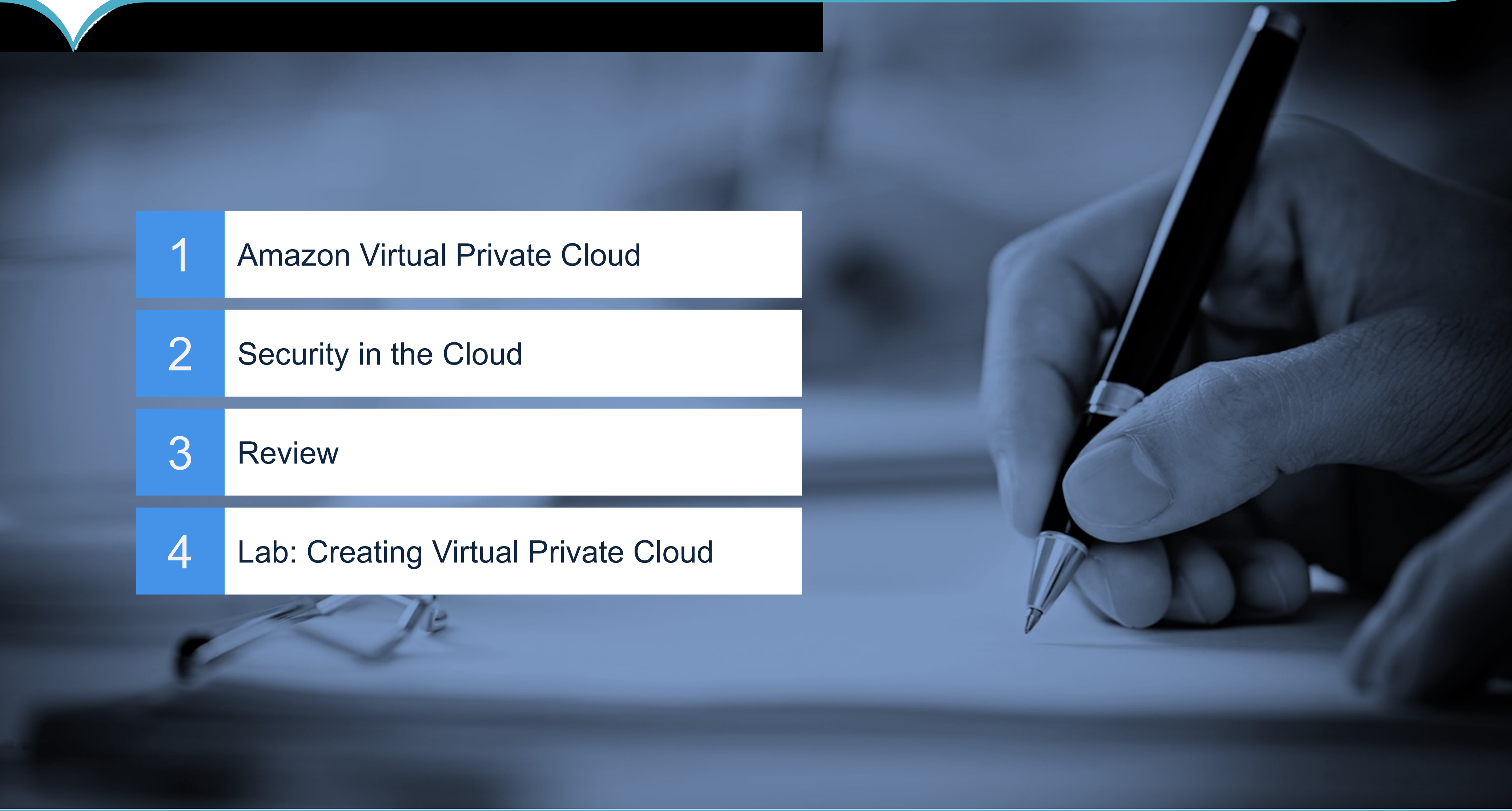
Networking in AWS Part 1

2019

People matter, results count.

Agenda

[redacted]



1 Amazon Virtual Private Cloud

2 Security in the Cloud

3 Review

4 Lab: Creating Virtual Private Cloud

Amazon Virtual Private Cloud

What is VPC?

Your private network space in the AWS Cloud

Provides logical isolation for your workloads

Allows custom access controls and security settings for your resources

Amazon VPC Specifics

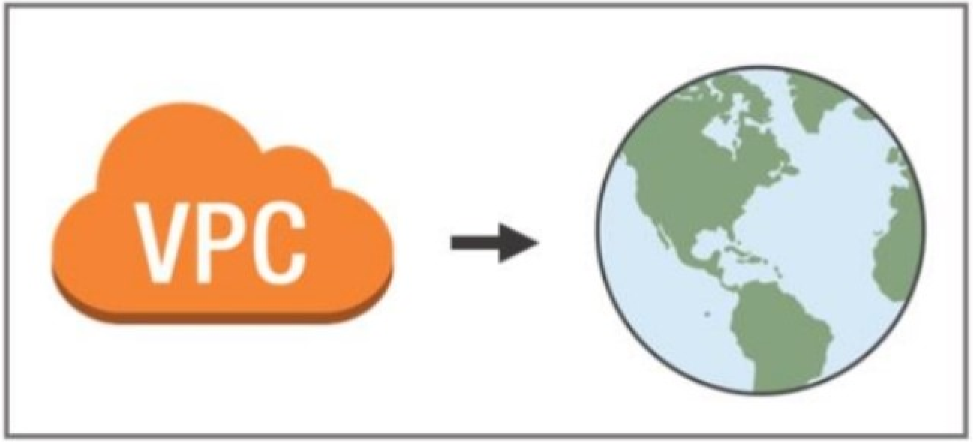
A VPC is a virtual network dedicated to your AWS account

Exists either in the IPv4 or IPv6 address ranges

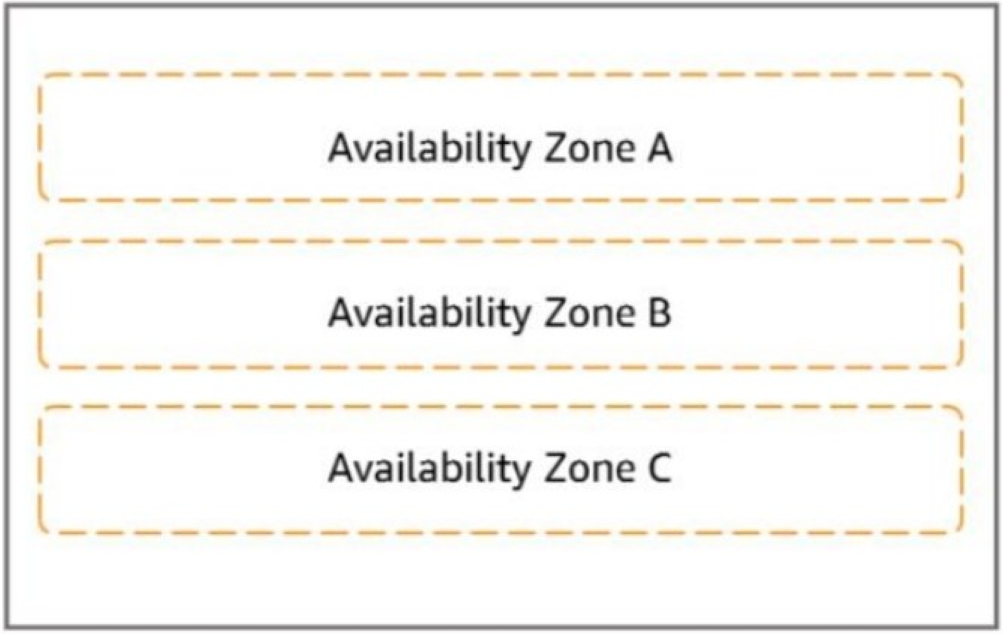
Enables you to create specific CIDR ranges for your resources to occupy

Provides strict access rules for inbound and outbound traffic

Deploying a VPC



VPCs deploy into **1** of the **18** AWS Regions



A VPC can host resources from **any** Availability Zone within its region

Using One VPC

There are limited use cases where one VPC could be appropriate:

- Small, single applications managed by one person or a very small team
- High-performance computing
- Identity management

For **most** use cases, there are two primary patterns for organizing your infrastructure:

Multi-VPC and Multi-account

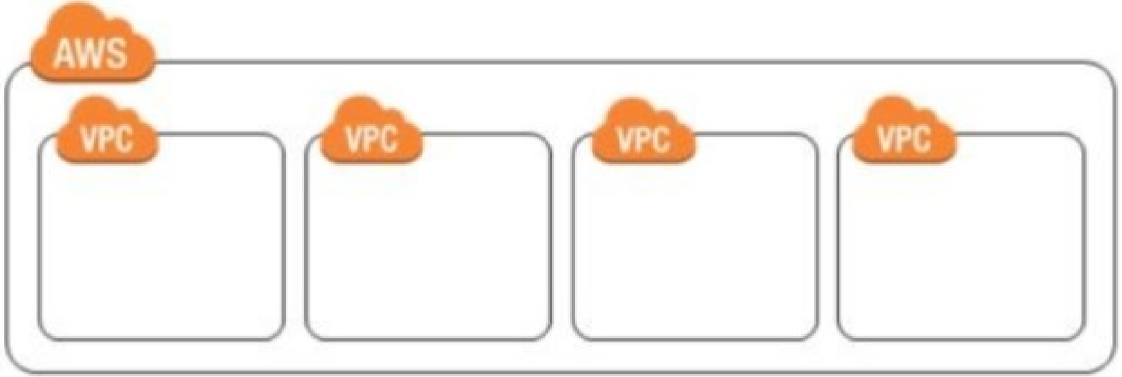
Multi VPC pattern

Best suited for:

- **Single team or single organization**, such as managed service providers
- Limited teams, which makes it easier to **maintain standards** and **manage access**

Exception:

- **Governance** and **compliance standards** may require greater workload isolation regardless of organizational complexity.



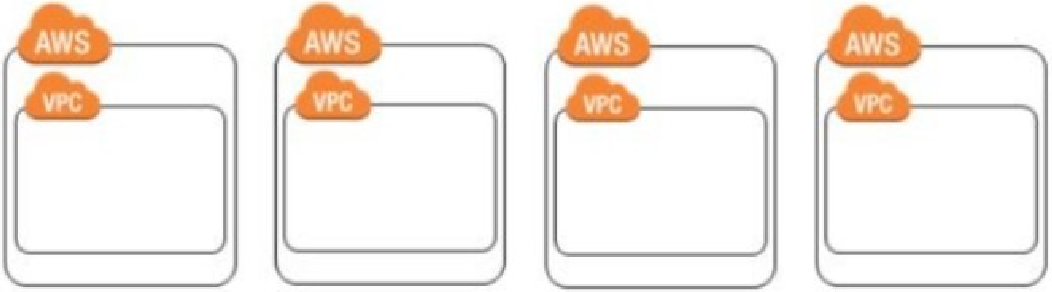
Multi-Account pattern

Best suited for:

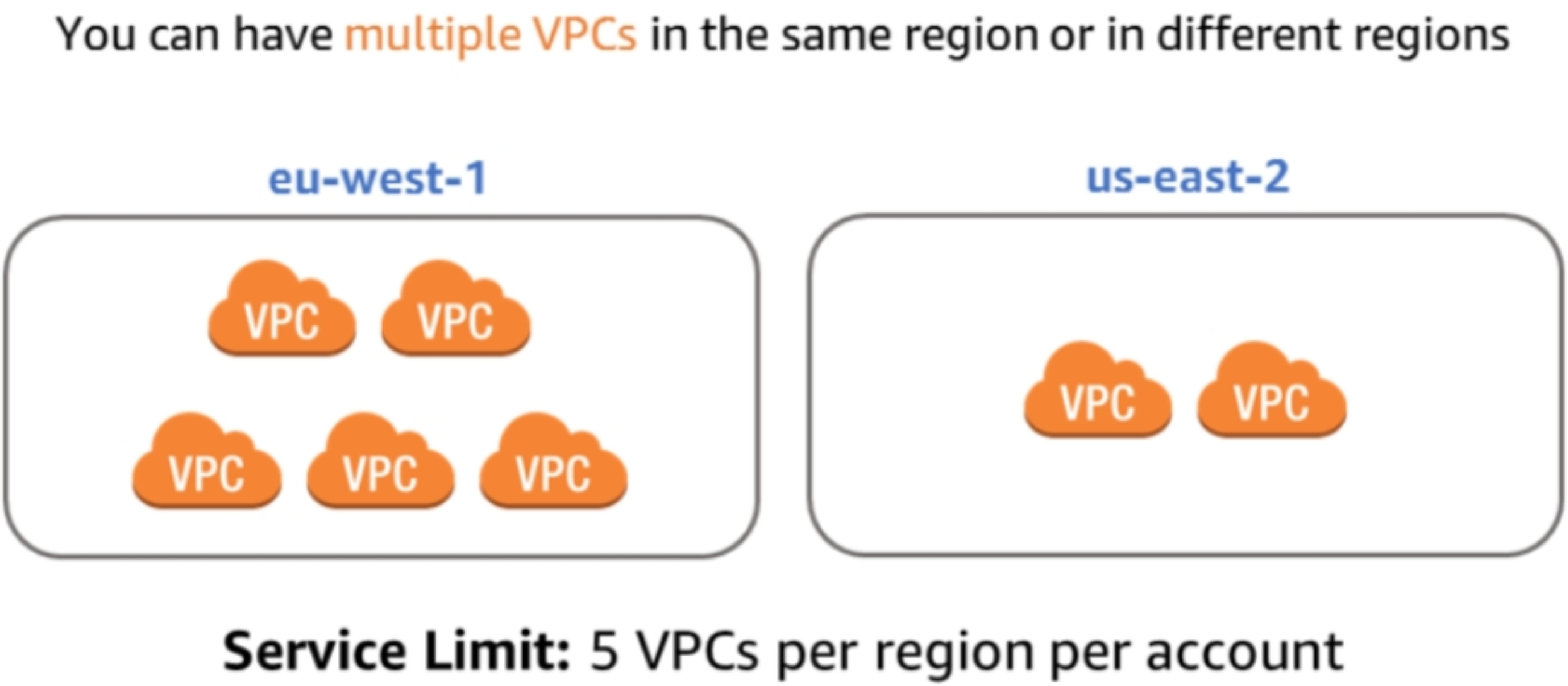
- **Large organization** and **organizations with multiple IT teams**
- **Medium-sized organizations** that anticipate growth

Why:

- **Managing access** and **standards** can be more challenging in more complex organizations.



VPC Limits



You can have multiple VPCs in the same region or in different regions

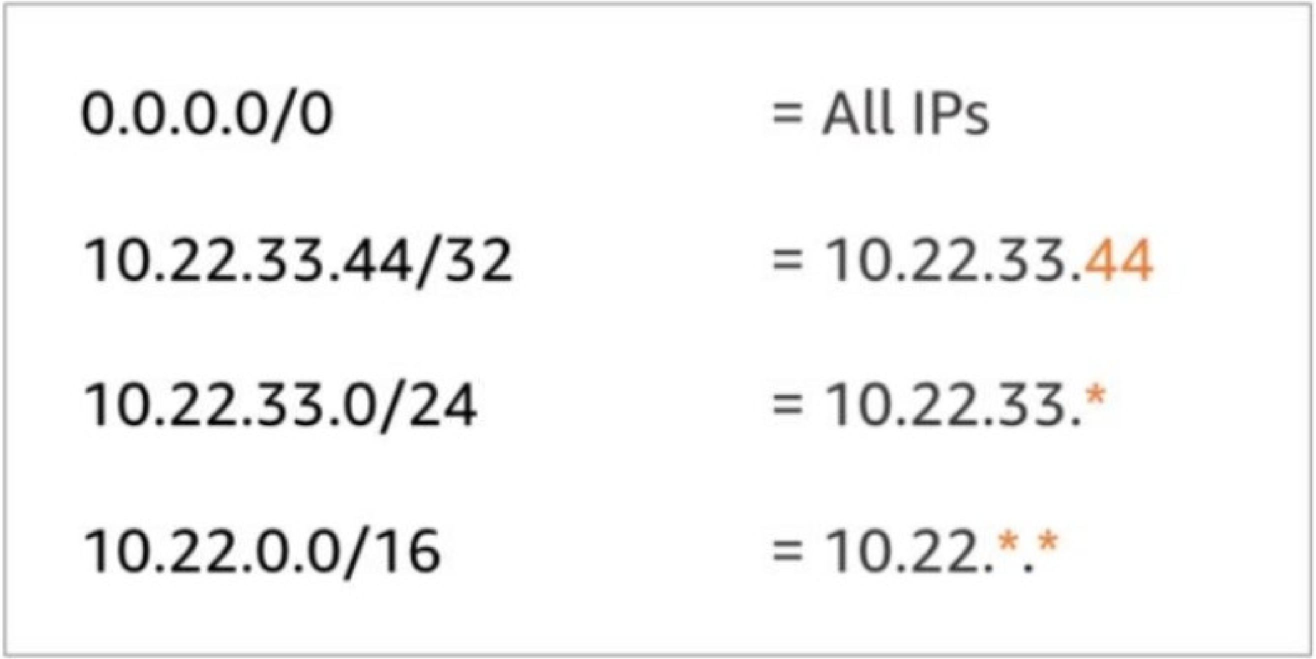
Service Limit: 5 VPCs per region per account

VPC and IP Addressing

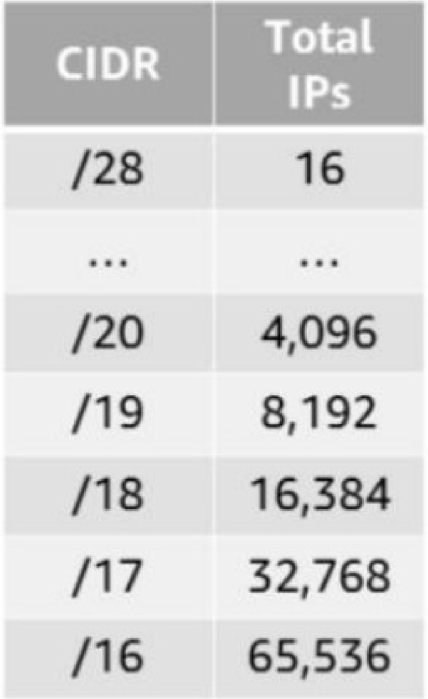
- Each VPC **reserves a range of private IP address** that you specify.
- Those private IP addresses can be used by resources deployed into that VPC.
- The IP range is defined using **Classless Inter-Domain Routing (CIDR)** notation
- Supports bringing **your own IP** prefixes

Example: **10.0.0.0/16 = all IPs from 10.0.0.0 to 10.0.255.255**

CIDR Example



0.0.0.0/0	= All IPs
10.22.33.44/32	= 10.22.33.44
10.22.33.0/24	= 10.22.33.*
10.22.0.0/16	= 10.22.*.*



CIDR	Total IPs
/28	16
...	...
/20	4,096
/19	8,192
/18	16,384
/17	32,768
/16	65,536

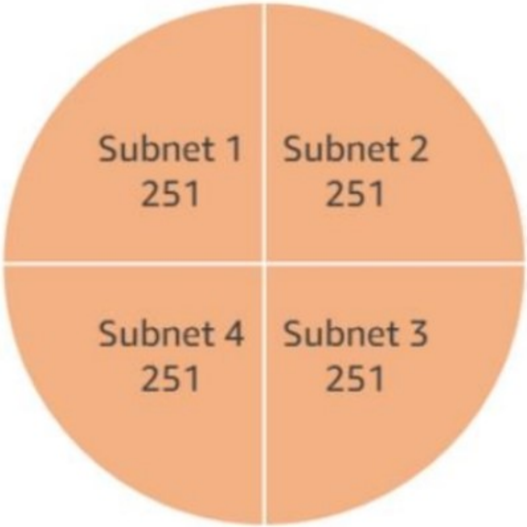
Using Subnet to Divide your VPC

Subnet is a segment or partition of a VPC's IP address range where you can isolate a group of resources.

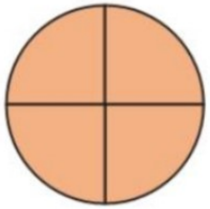
Example:

A VPC with **CIDR /22**

includes 1024 total IPs



Subnets: Key Attributes



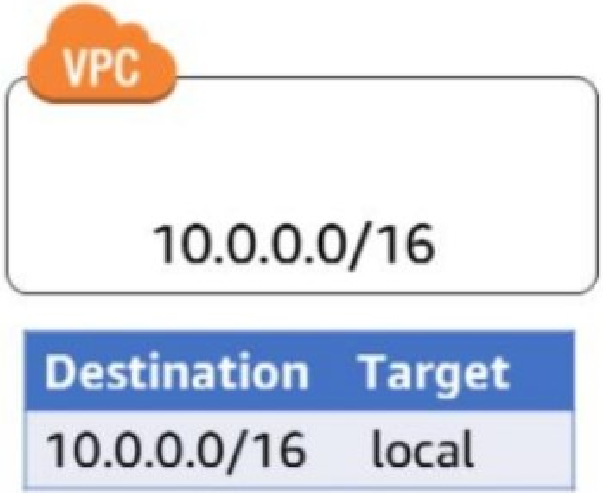
- Subnets are a subset of the VPC CIDR block
- Subnet CIDR blocks cannot overlap
- Each subnet resides entirely within one Availability Zone
- An Availability Zone can contain multiple subnets

AWS will reserve five IP addresses from each subnet

Route Tables: Directing Traffic Between VPC Resources

Route tables:

- Required to direct traffic between VPC resources
- Each VPC has a main (default) route table
- You can create custom route tables
- All subnets must have an associates route table



Destination	Target
10.0.0.0/16	local

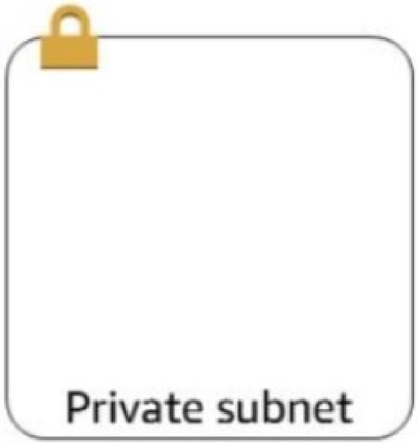
Best practice: Use custom route tables for each subnet

Subnets Allow Different Levels of Network Isolation

Use subnets to define internet accessibility.

Public subnets

- Include a routing table entry to an internet gateway to support inbound/outbound access to the public internet



Private subnets

- Do not have routing table entry to an internet gateway
- Are not directly accessible from the public internet
- Typically use a NAT gateway to support restricted, outbound public internet access

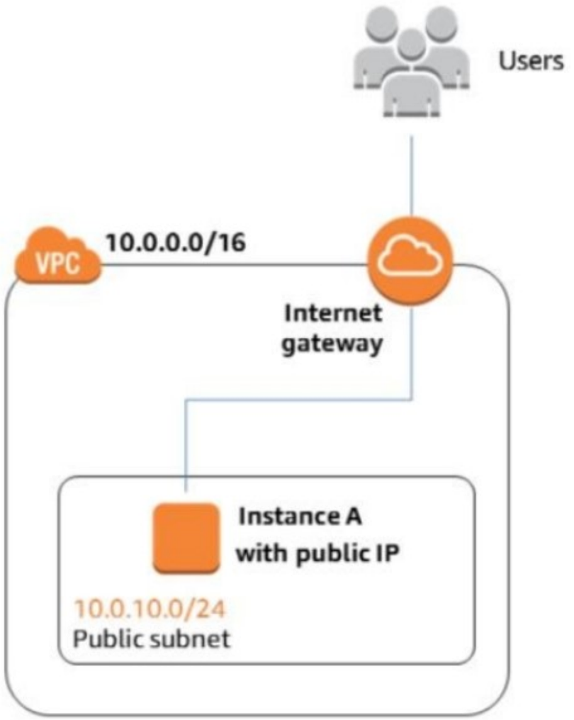
Connecting Public Subnets to the Internet

Internet Gateways

- Allows communication between instances in your VPC and the internet.
- Are horizontally scaled, redundant and highly available by default
- Provide a target in your subnet route tables from internet-routable traffic

Public route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>



Connecting Public Subnets to the Internet

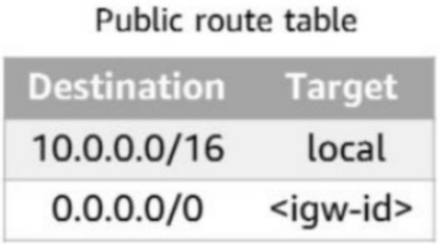
Internet Gateways

- Allows communication between instances in your VPC and the internet.
- Are horizontally scaled, redundant and highly available by default
- Provide a target in your subnet route tables from internet-routable traffic

Connecting Private Subnets to the Internet

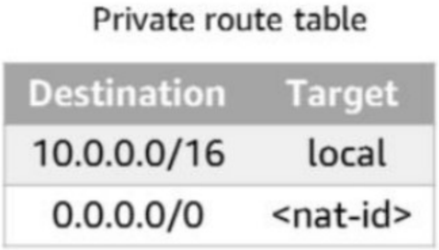
NAT Gateways

- Enable instances in the private subnet to initiate outbound traffic to the internet or other AWS services.
- Prevent private instances from receiving inbound traffic from the internet.



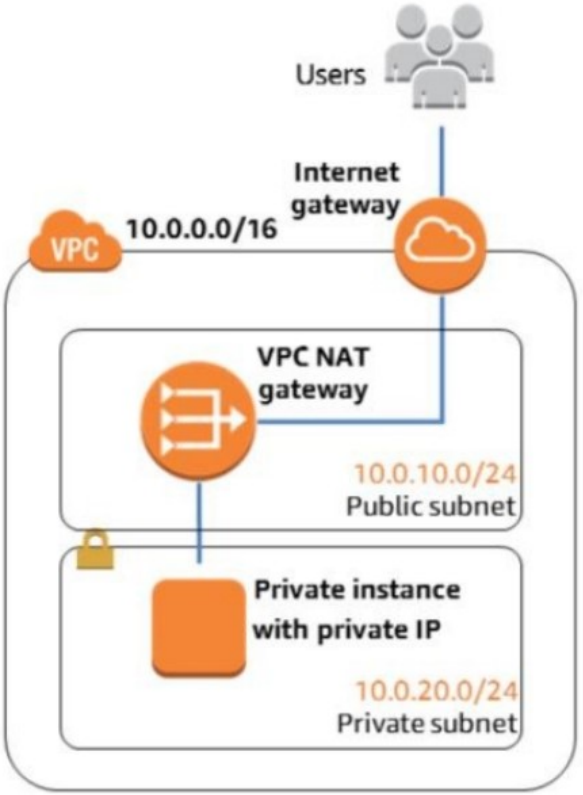
Public route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>



Private route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<nat-id>



Subnet Use Case Examples

Data store instances → private subnet

Batch processing instances → private subnet

Back-end instances → private subnet

Web application instances → Public or

private subnet

Subnet Recommendations

Consider larger subnets over small ones (/24 and larger)

Simplifies workload placement:

- Choosing where to place a workload among 10 small subnets is more complicated than with one large subnet.

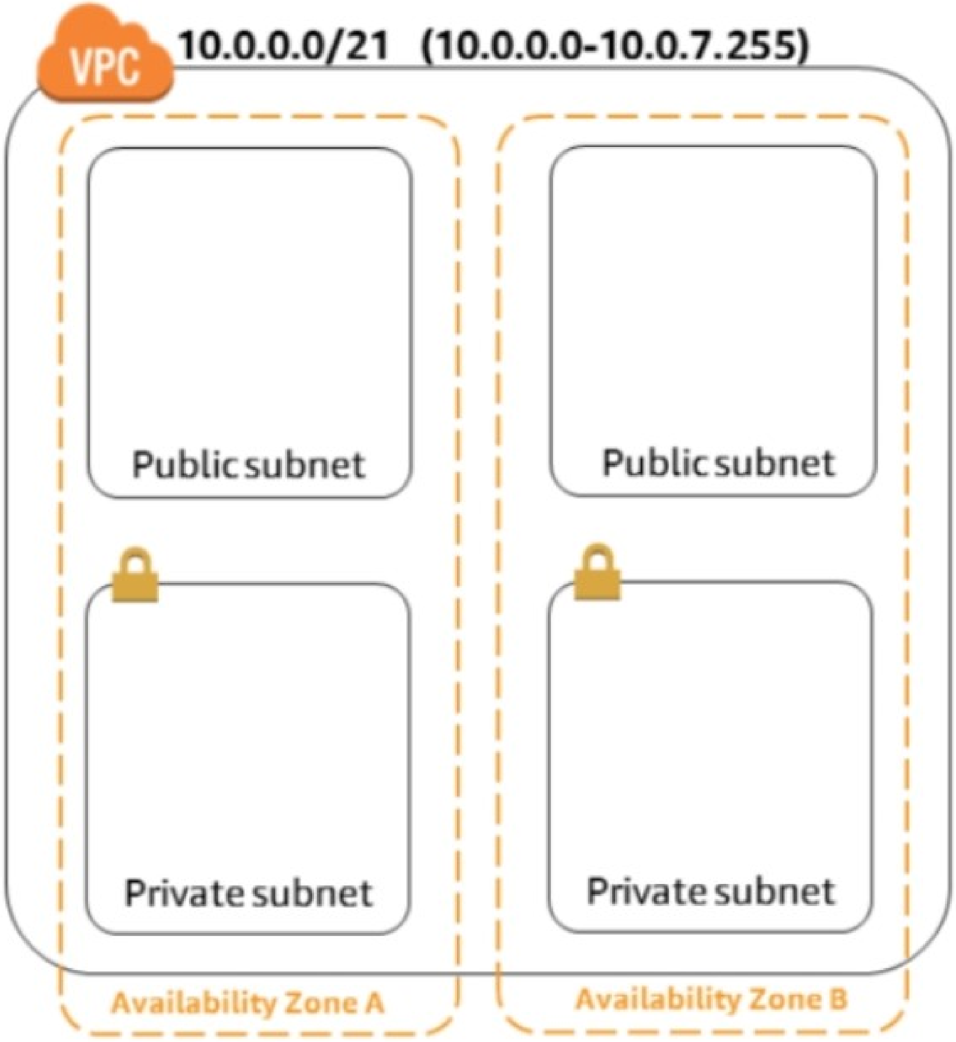
Less likely to waste or run out of IPs:

- If your subnet runs out of available IPs, you can't add more to that subnet.

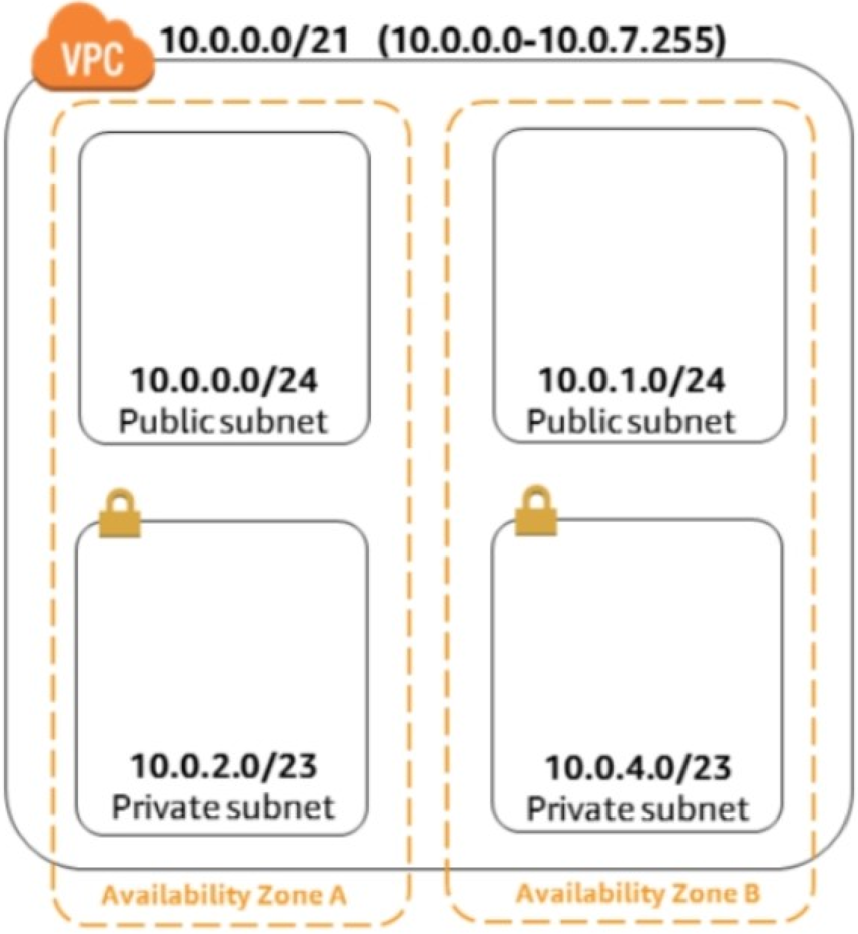
Basic Subnet Configurations

If you are unsure of the best way to set up your subnets:

Start with one public and one private subnet per Availability Zone.



Basic Subnet Configuration



Most architectures have significantly **more private resources than public** resources.

Allocate substantially **more IPs for private subnets** that for public subnets.

Elastic Network Interfaces

An elastic network interface is a

virtual network interface

that can be moved across EC2 instances in the same Availability Zone.

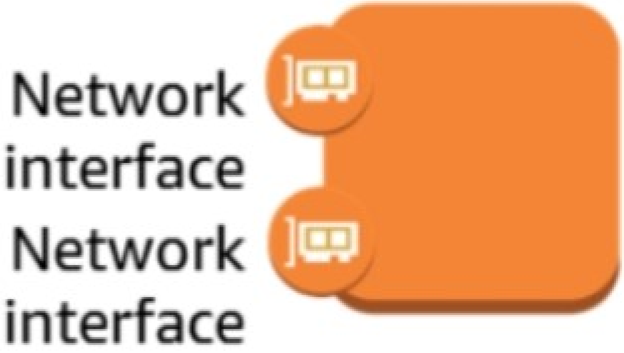
When moved to a new instance, a network interface maintains its:

- Private IP address
- Elastic IP address
- MAC address

Elastic Network Interfaces

Why have more than one network interface on an instance?

- If you need to:
  - Create a management network
  - Use network and security appliances in your VPC
  - Create dual-homed instances with workloads/roles on distinct subnets

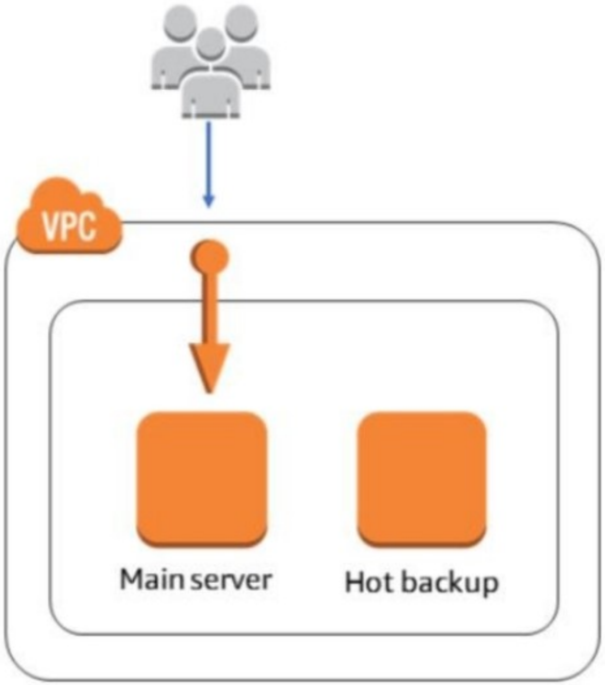


Elastic IP Addresses

- Can be associated with an instance or a network interface
- Able to re-associate and direct traffic immediately
- Five allowed per AWS Region

Elastic IP Addresses

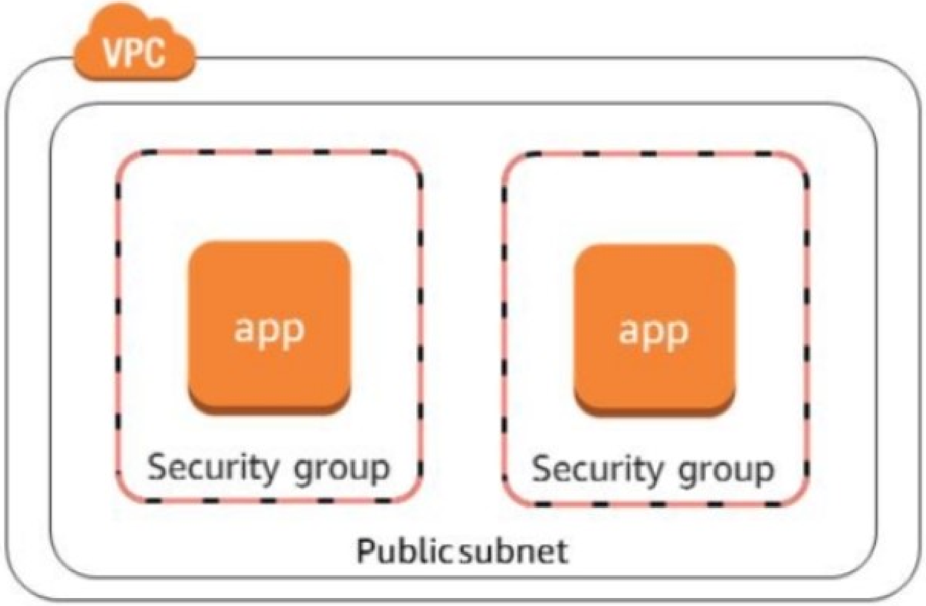
- Can be associated with an instance or a network interface
- Able to re-associate and direct traffic immediately
- Five allowed per AWS Region



Security in the Cloud

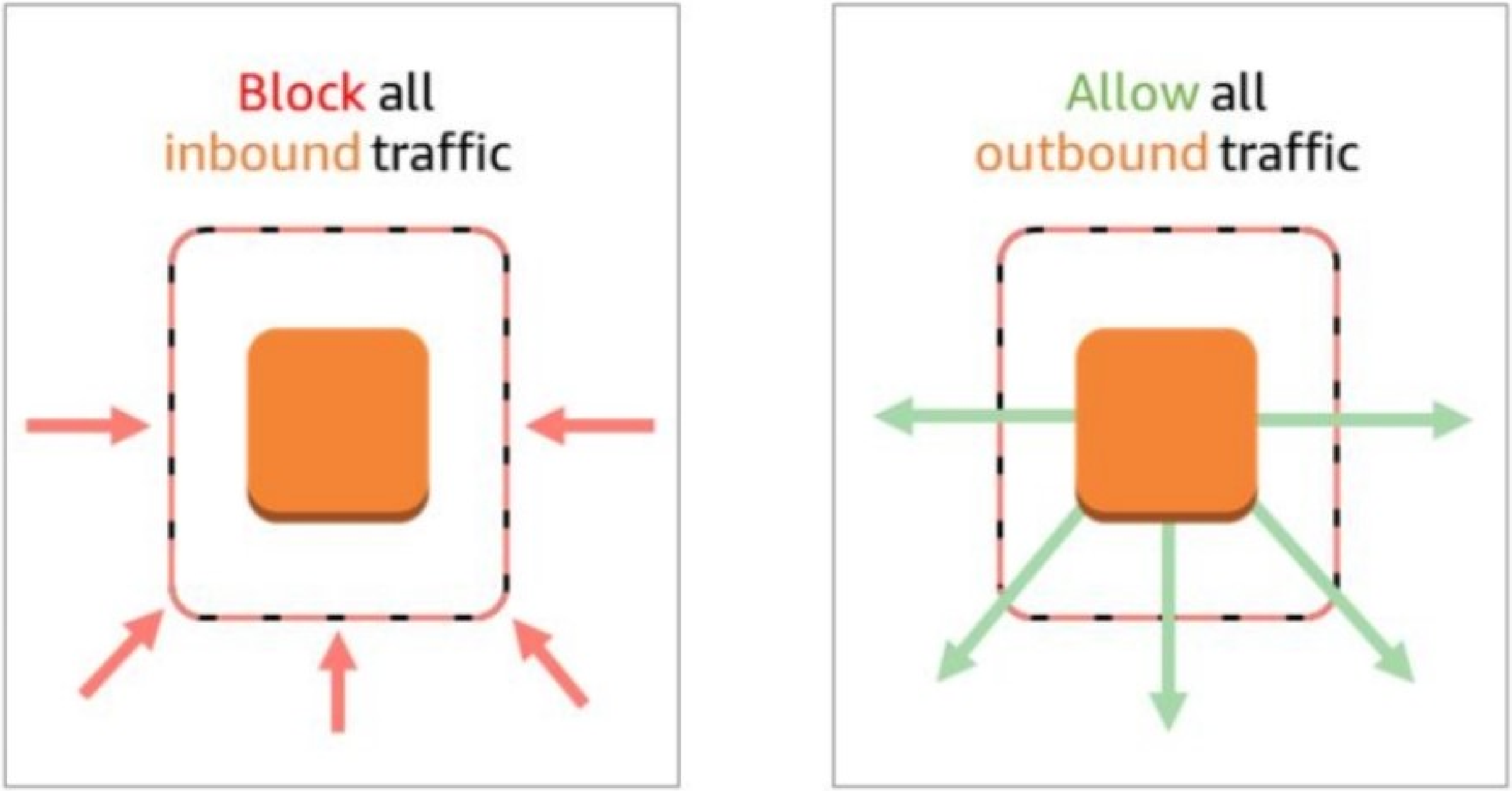
Security Groups

- Virtual firewalls that control inbound and outbound traffic into AWS resources
- Traffic can be restricted by any IP protocol, port or IP address
- Rules are stateful



Security Groups: By Default

New security groups:

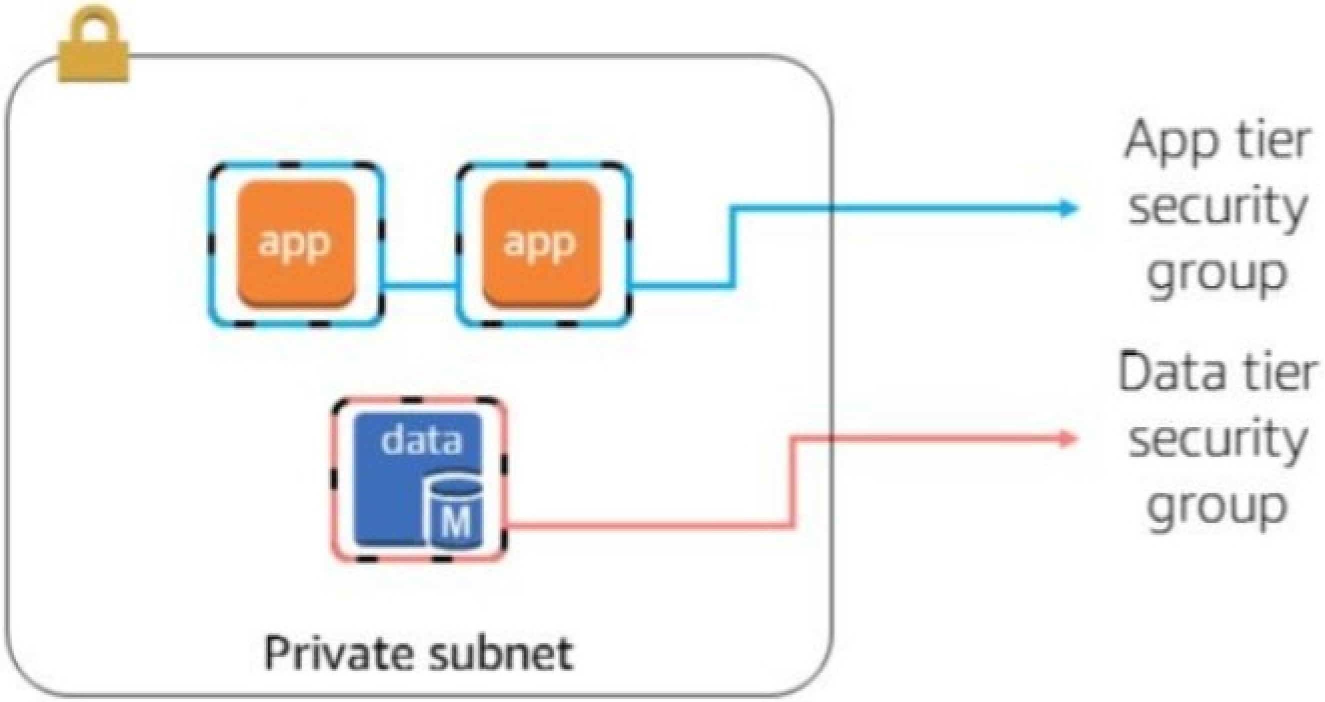


Block all inbound traffic

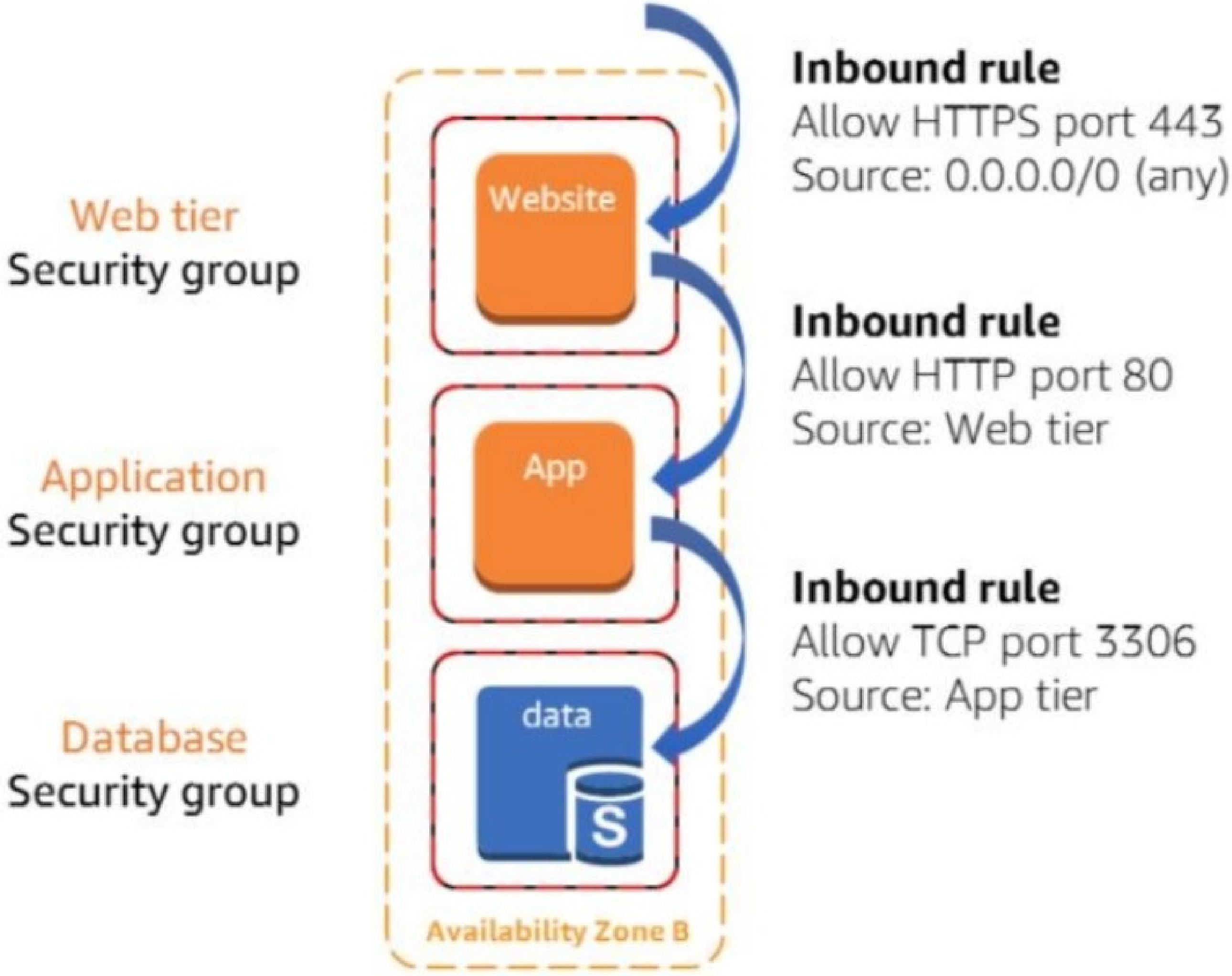
Allow all outbound traffic

Security Groups: Controlling Traffic

Most cloud organizations create security groups with **inbound rules for each functional tier**.



Security Groups: Chaining Diagram

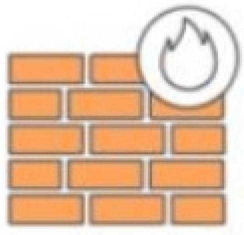


Inbound rule
Allow HTTPS port 443
Source: 0.0.0.0/0 (any)

Inbound rule
Allow HTTP port 80
Source: Web tier

Inbound rule
Allow TCP port 3306
Source: App tier

Network Access Control List (ACLs)

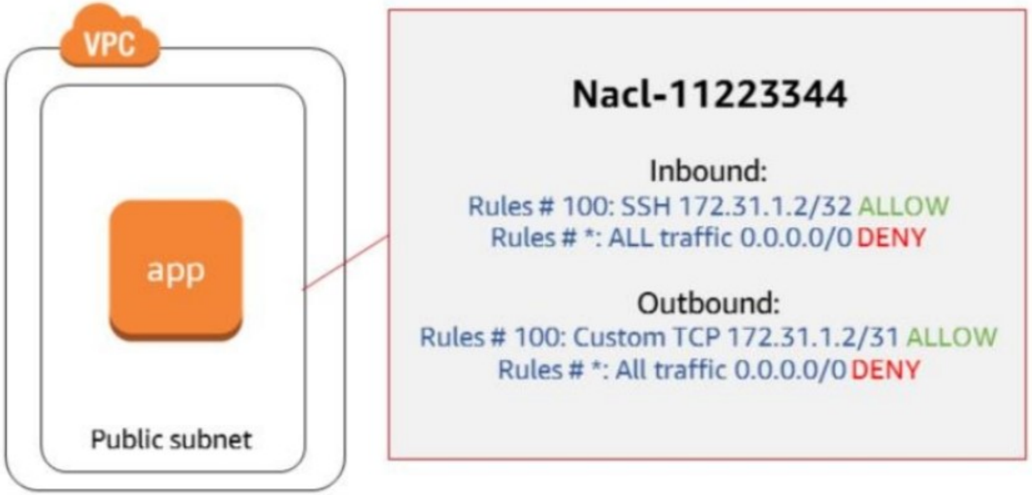


- **Firewalls** at the subnet boundary
- Will **allow all inbound and outbound traffic** by default
- Are **stateless**, requiring **explicit** rules for both inbound and outbound traffic

Network Access Control List (ACLs)

Recommended for
specific network security requirements
only

- **Firewalls** at the subnet boundary
- Will **allow all inbound and outbound traffic** by default
- Are **stateless**, requiring **explicit** rules for both inbound and outbound traffic



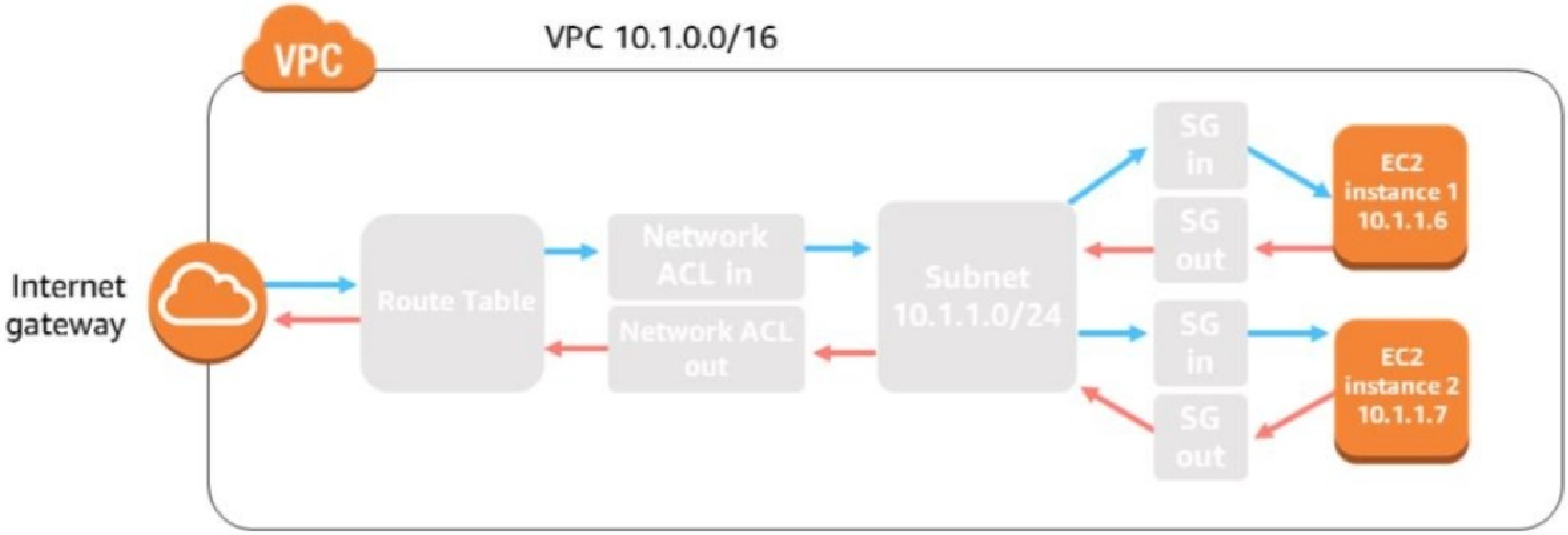
Nacl-11223344

Inbound:
Rules # 100: SSH 172.31.1.2/32 ALLOW
Rules # *: ALL traffic 0.0.0.0/0 DENY

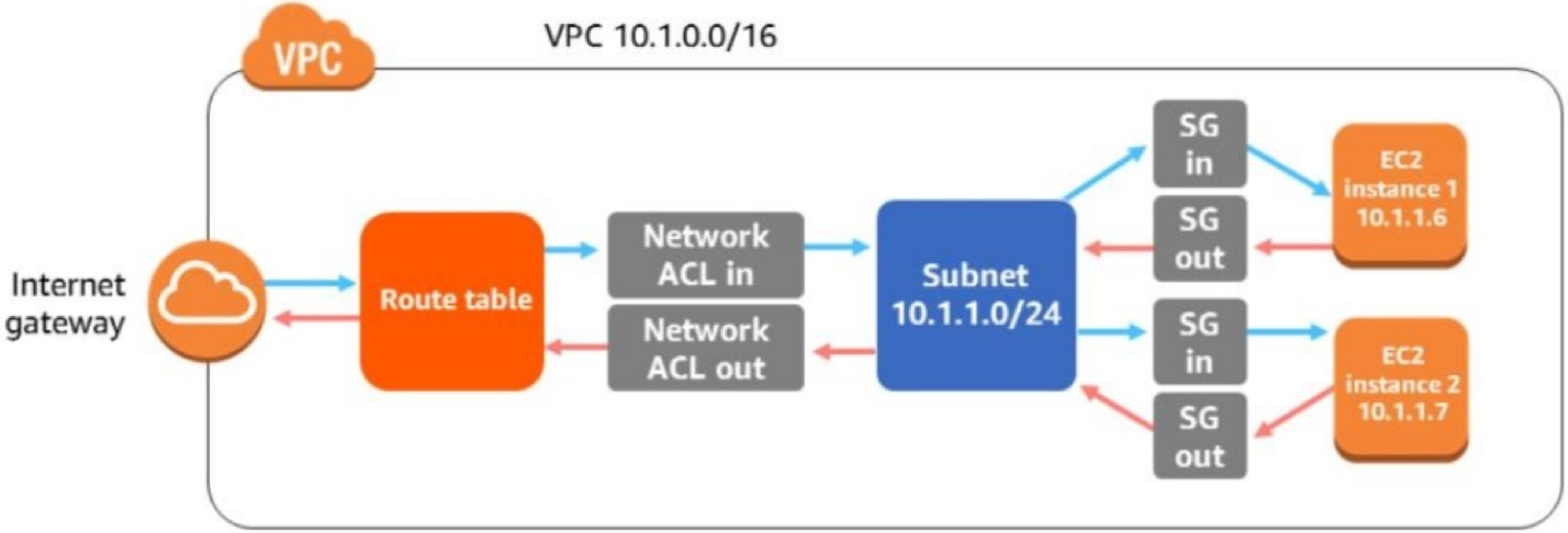
Outbound:
Rules # 100: Custom TCP 172.31.1.2/31 ALLOW
Rules # *: All traffic 0.0.0.0/0 DENY

Review

Structure You infrastructure with Multiple Layers of Defense



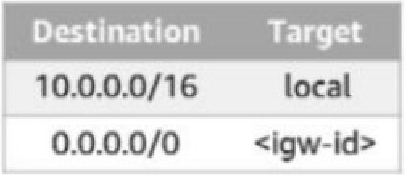
Structure You infrastructure with Multiple Layers of Defense



Directing Traffic To Your VPC

To **enable internet access** for instances in a VPC subnet, you must:

Attach an internet gateway to your VPC



Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>

Point your route tables to the internet gateway

Make sure your instances have public IP or Elastic IP addresses

Ensure that your network ACLs and SGs allow relevant traffic to flow

Knowledge Check

Where are VPCs deployed?

- Regions
- Availability Zones
- Subnets
- CIDR Blocks

Knowledge Check

Where are VPCs deployed?

- Regions
- Availability Zones
- Subnets
- CIDR Blocks

Knowledge Check

Security groups allow all traffic in by default. You must set rules to specifically block unwanted traffic.

- True
- False

Knowledge Check

Security groups allow all traffic in by default. You must set rules to specifically block unwanted traffic.

- True
- False

Lab: Creating Virtual Private Cloud

Lab: Creating Virtual Private Cloud

"I need a private network in the cloud"

Technologies used:

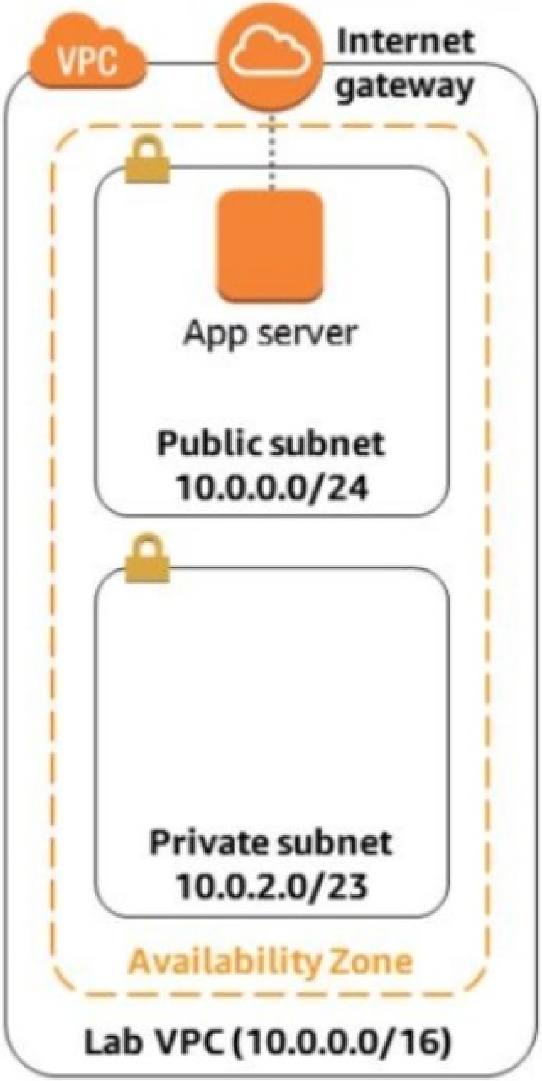
- Amazon VPC
- VPC Peering
- Testing uses Amazon EC2 and Amazon RDS

Lab: Creating Virtual Private Cloud

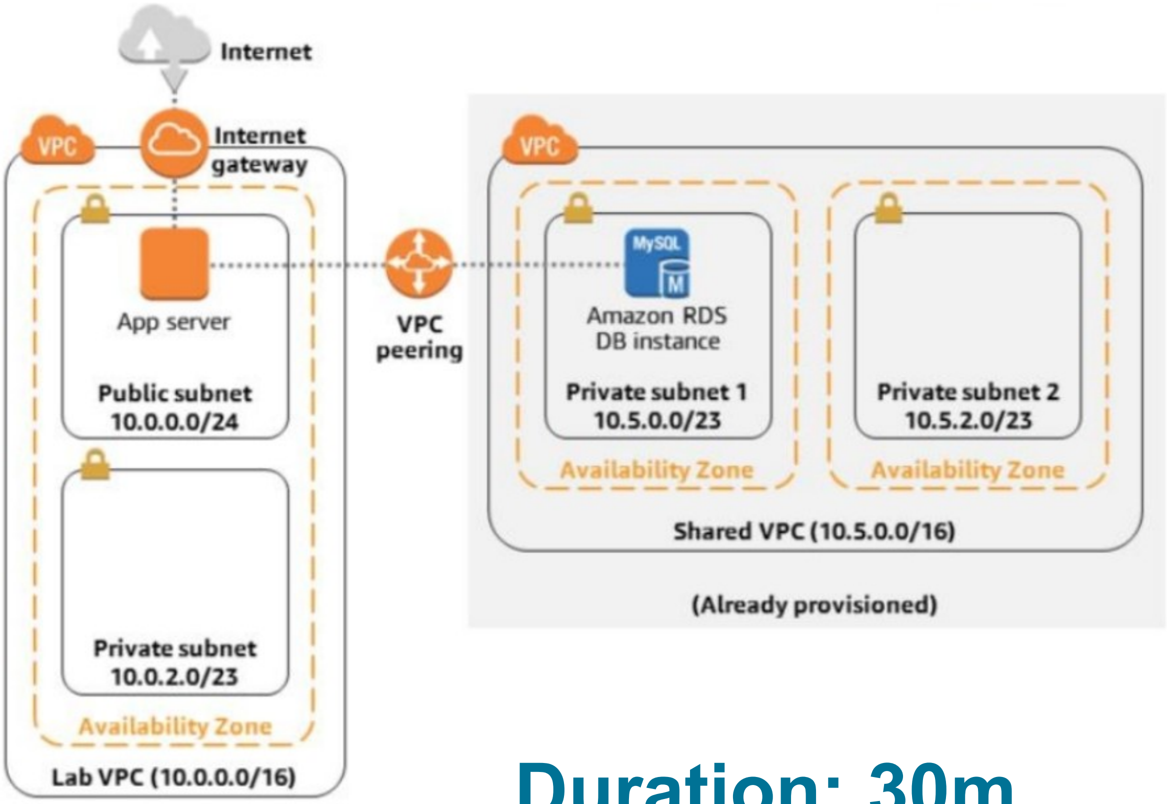
You will create a VPC with:

- An internet gateway
- A public subnet
- A private subnet
- Route tables for each subnet

Then test the public subnet by launching an connecting to it.



Lab: Creating Virtual Private Cloud



Optional Challenge:

- Create a VPC peering connection
- Configure route tables
- Test by connecting application to database

Duration: 30m

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

People matter, results count.

About Capgemini

With more than 145,000 people in 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2014 global revenues of EUR 10.5 billion.
Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Rightshore® is a trademark belonging to Capgemini

www.capgemini.com