AWS VPC

CS516 – Cloud Computing

Computer Science Department

Maharishi International University

Maharishi International University - Fairfield, Iowa

Content

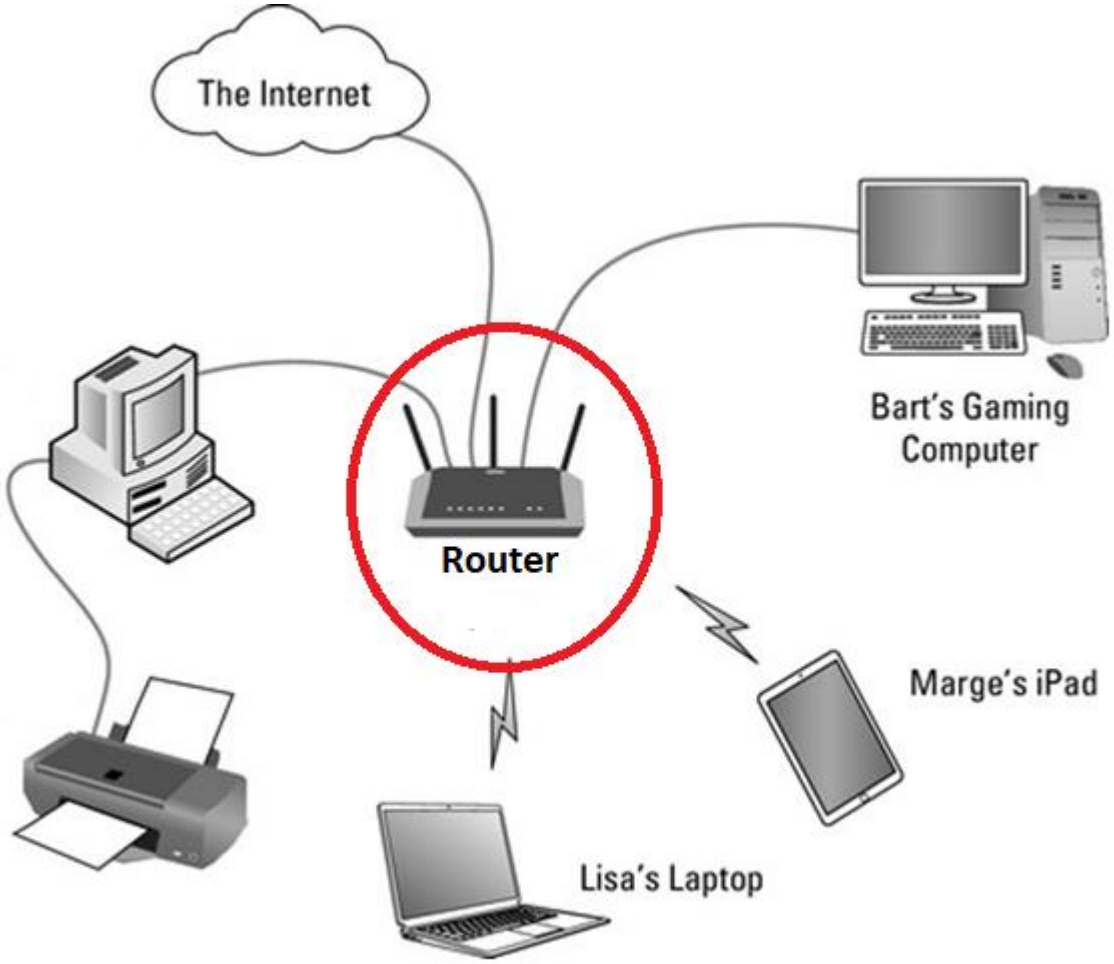
- Networking & internet
- Private & public subnets
- CIDR
- AWS Global Infrastructure
- VPC
  - Internet Gateways (IGW)
  - Route Tables (RT)
  - Network Access Control Lists (NACL)
  - NAT gateway

Networking

A computer network is a set of computers sharing resources located on or provided by network nodes.

Router routes traffic between devices and the internet.

If you understand how networking works at home, then the same ideas apply in organizations and the cloud.



Internet

Internet is a global network of networks (autonomous systems) for communication that consists of **private** and **public** sub network (**subnet**).

The computers use common **protocols** (such as TCP/IP) to communicate with each other.

An Internet Protocol (**IP**) address is a 32-bit numerical label such as 192.0.2.1. An IP address serves two main functions:

1. host or **network interface** identification
2. location addressing.

IPv4 vs IPv6

There are 2 types of IP addresses:

1. IPv4
2. IPv6

The people who designed the internet thought 4.3 billion IP (2 to the power 32) addresses are enough. But it get exhausted in the 90s. Then they designed IPv6. There are trillions of IPs (2 to the power 128) in IPv6.

It is the reason why IPv4 addresses are dynamic.

Subnet

A subnet is a sub-section of a network. Generally, it includes all the computers in a specific location like zip code for addressing houses.

The subnet is a pool of IP addresses.

It is a way to divide the network logically into multiple sub-groups. Designing subnets is all up to you or your organization. You can create a subnet at your home per room or per floor etc. For example:

- IP address of the devices in the living room will be in **192.168.0.0 to 192.168.0.10**
- IP address of the devices in the kitchen will be in **192.168.0.11 to 192.168.0.20**
- IP address of the devices in the bedroom will be in **192.168.0.21 to 192.168.0.30**

There is a shorter way to represent IP ranges called **CIDR**.

Private and public subnets

As we run out of IPv4, we needed a quick solution. That was to allocate and use private IPs (such as 192.168.x.y) within a single network. These private IPs are used simultaneously by millions of organizations and home networking. Hence, it is saving a number of IPv4 addresses available.

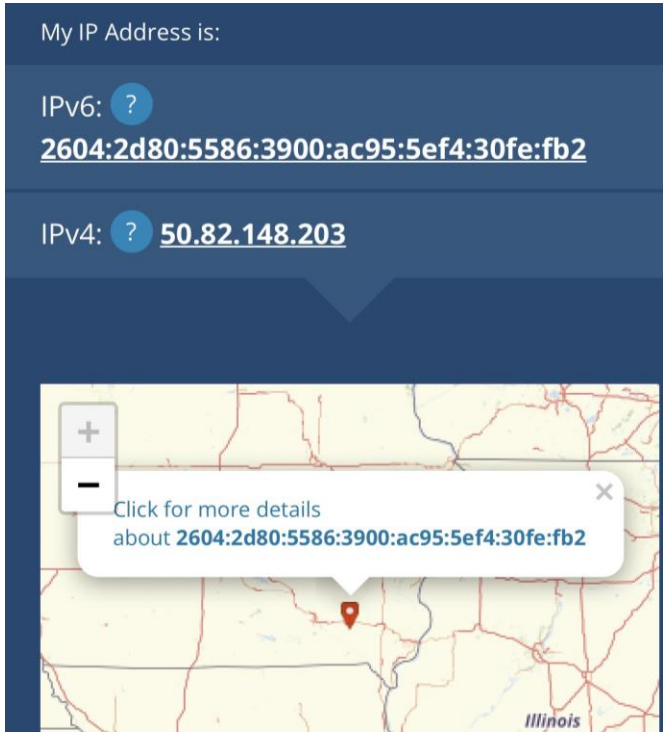
A private subnet is a **secure** place where you can run your back-end app and database. Because the internet can't directly access it. The only way to access from the internet to your apps in a private subnet is through your server in your public subnet.

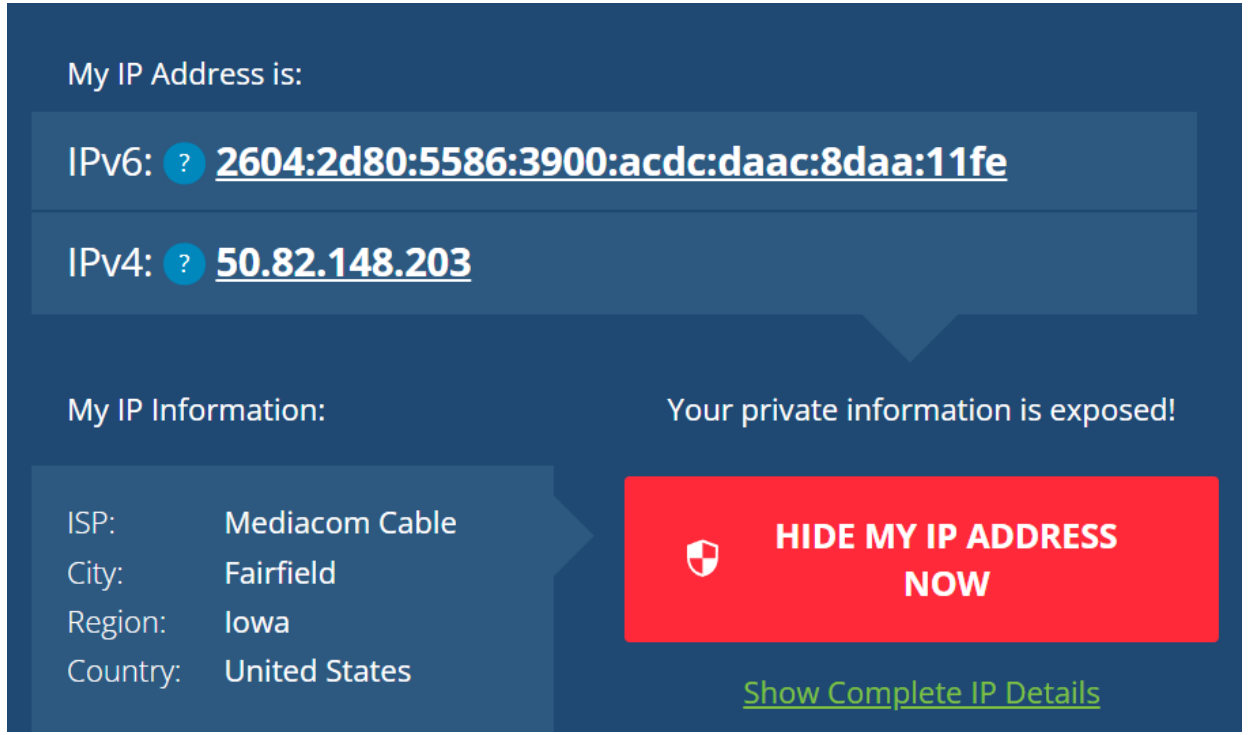
The internet can directly access your **public subnet**. Servers get created in public subnet receive public IP automatically. You must design and define what public IP your server will receive by creating subnet.

Network Access Translation

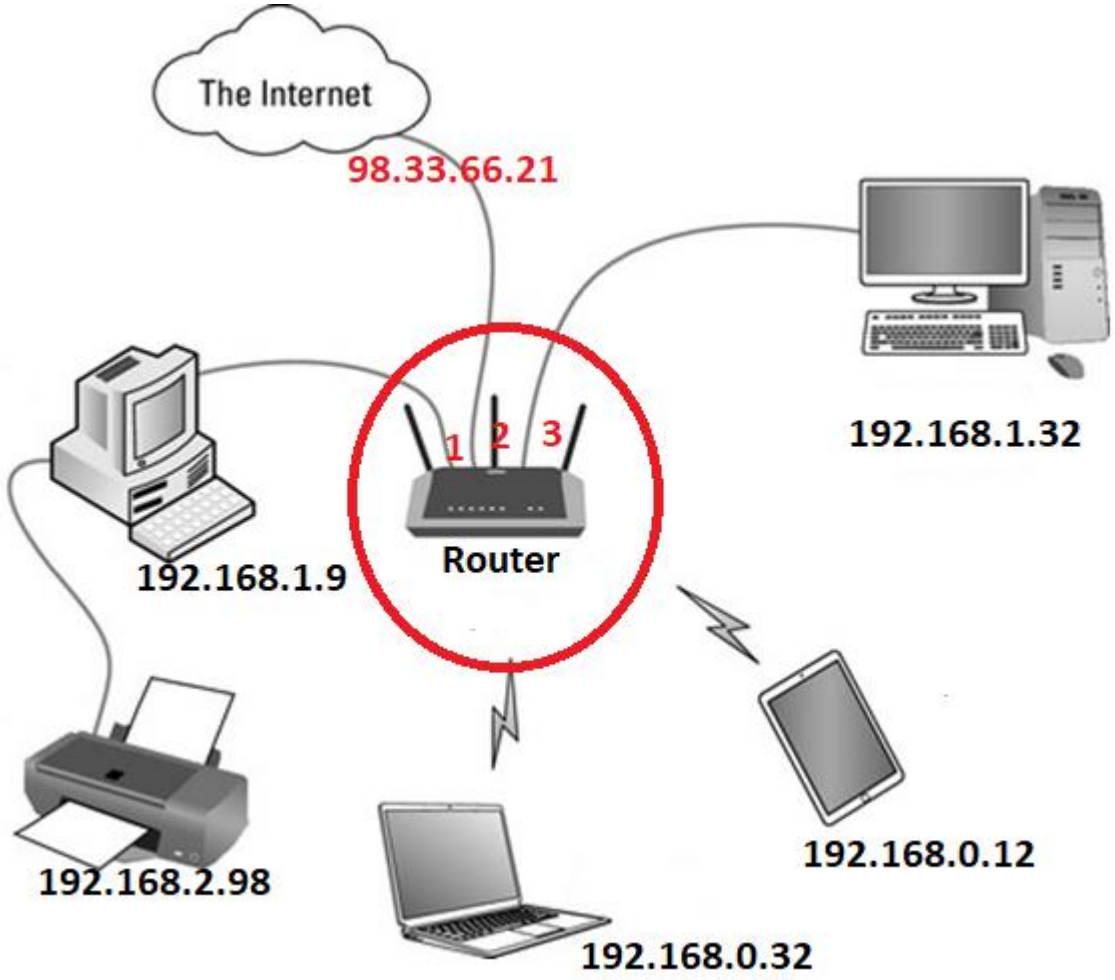
Network Address Translation is a method of mapping private IP addresses into a public IP address.

Your router at home has these feature in it. Here is an example that my phone and computer have the same public IPv4.





How NAT works



NAT sends responses from the internet to the right machine based on port.

Port	IP
1	192.168.1.9
2	192.168.0.12
3	192.168.1.32
4	192.168.0.32
5	192.168.2.98

Classless Inter-Domain Routing - CIDR

CIDR is a method for allocating IP addresses within a network.

CIDR IP addresses are composed of two sets of numbers:

1. The network address is written as a prefix.
2. The suffix which indicates how many bits are in the entire address.

For example: 10.0.0.0/24

CIDR to IPv4 Conversion: https://www.ipaddressguide.com/cidr

CIDR ranges for the private network

CIDR	CIDR Range	Number of hosts
10.0.0.0/8	10.0.0.0–10.255.255.255	16777216
172.16.0.0/12	172.16.0.0–172.31.255.255	1048576
192.168.0.0/16	192.168.0.0–192.168.255.255	65536
100.64.0.0/10	100.64.0.0–100.127.255.255	4194304
198.18.0.0/15	198.18.0.0–198.19.255.255	131072
192.0.0.0/24	192.0.0.0–192.0.0.255	256

CIDR to IP Range

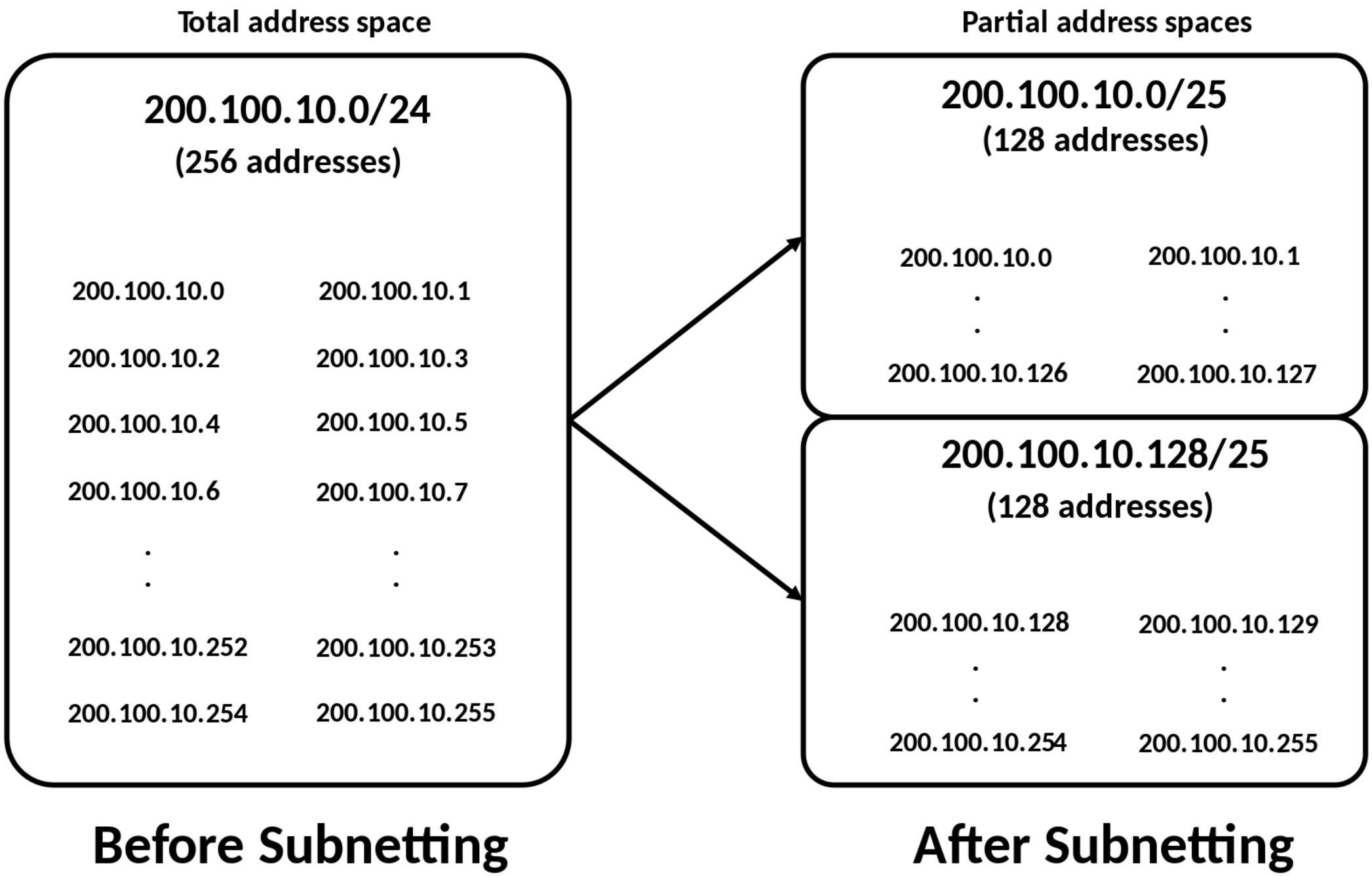
Result

CIDR Range	10.0.0.0/24
Netmask	255.255.255.0
Wildcard Bits	0.0.0.255
First IP	10.0.0.0
First IP (Decimal)	167772160
Last IP	10.0.0.255
Last IP (Decimal)	167772415
Total Host	256

CIDR

10.0.0.0/24

Calculate


Total address space
200.100.10.0/24
(256 addresses)
200.100.10.0
200.100.10.1
200.100.10.2
200.100.10.3
200.100.10.4
200.100.10.5
200.100.10.6
200.100.10.7
200.100.10.252
200.100.10.253
200.100.10.254
200.100.10.255
Partial address spaces
200.100.10.0/25
(128 addresses)
200.100.10.0
200.100.10.1
200.100.10.126
200.100.10.127
200.100.10.128/25
(128 addresses)
200.100.10.128
200.100.10.129
200.100.10.254
200.100.10.255
Before Subnetting
After Subnetting

AWS Global Infrastructure Map

https://aws.amazon.com/about-aws/global-infrastructure/

AWS Global Infrastructure

Regions - A physical location around the world where AWS *clusters* data centers. Usually comprised of multiple AZs.

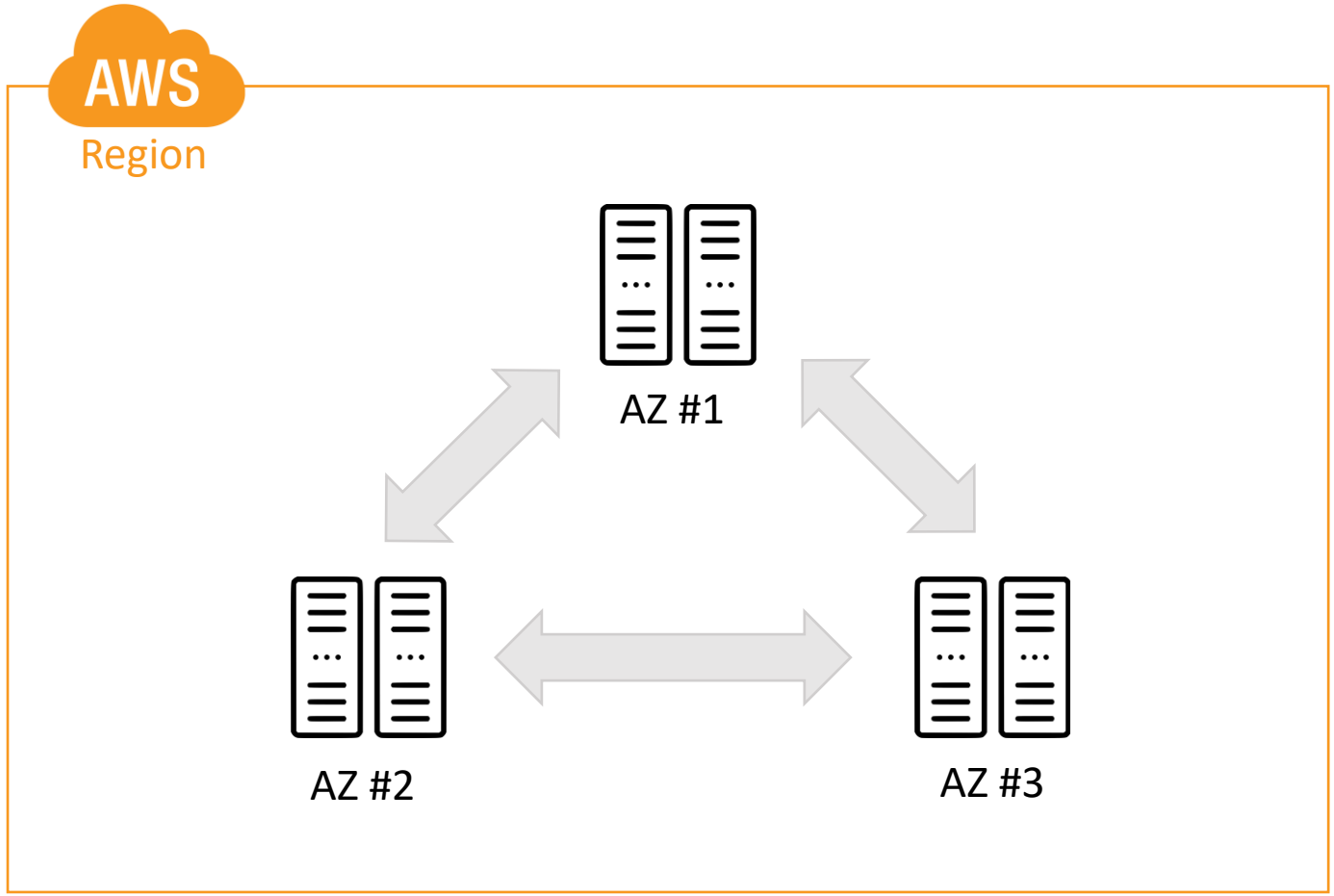
Availability Zones - Geographical isolated data centers within a region.

Data Centers - Where the physical hardware that runs AWS services is located.

Read More about: [AWS Global Infrastructure]

AWS Region/AZ

Each Region has multiple, isolated locations known as *Availability Zones*.



High Availability is creating an architecture in such a way that the system is always available (or has the least amount of downtime as possible).
Fault Tolerant is the ability of your system to withstand failures in one or more of its components and still remain available.

Availability Zones provide redundancy for AWS resources in that region, highly available, fault tolerant, and more scalability.
AZs have low latency, high-bandwidth network connection, and supports synchronous **replication** between AZs. All traffic is **encrypted**.

Read More about: [Regions and Zones]

Regions and AZs

Sl No	CodeName	Location	No. of AZ	List of Azs
1	ap-northeast-1	Asia Pacific (Tokyo)	3	ap-northeast-1a, ap-northeast-1b, ap-northeast-1c
2	ap-southeast-1	Asia Pacific (Singapore)	2	ap-southeast-1a, ap-southeast-1b
3	ap-southeast-2	Asia Pacific (Sydney)	2	ap-southeast-2a, ap-southeast-2b
4	eu-central-1	EU (Frankfurt)	2	eu-central-1a, eu-central-1b
5	eu-west-1	EU (Ireland)	3	eu-west-1a, eu-west-1b, eu-west-1c
6	sa-east-1	South America (Sao Paulo)	2	sa-east-1a, sa-east-1b
7	us-east-1	US East (N. Virginia)	5	us-east-1a, us-east-1b us-east-1c, us-east-1d us-east-1e
8	us-west-1	US West (N. California)	3	us-west-1a, us-west-1b, us-west-1c
9	us-west-2	US West (Oregon)	3	us-west-2a, us-west-2b, us-west-2c
10	?	China (Beijing) Region *	2	?
11	us-gov-west	Gov Cloud(the Northwestern US) Region	2	us-gov-west-1, us-gov-west-2

Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud is an isolated virtual network where your AWS resources run. You have complete control over your virtual networking environment, including selection of your own **IP address range**, creation of **subnets** and configuration of other VPC components such as **route tables** and **network gateways**.

In a private (secure) sub-section of VPC, you can place AWS resources, like back-end servers and databases.

VPC is a regional service and is associated to a single region like most of other AWS services. You cannot span a VPC across regions. If you work on a global application, you deploy regional services in each region.

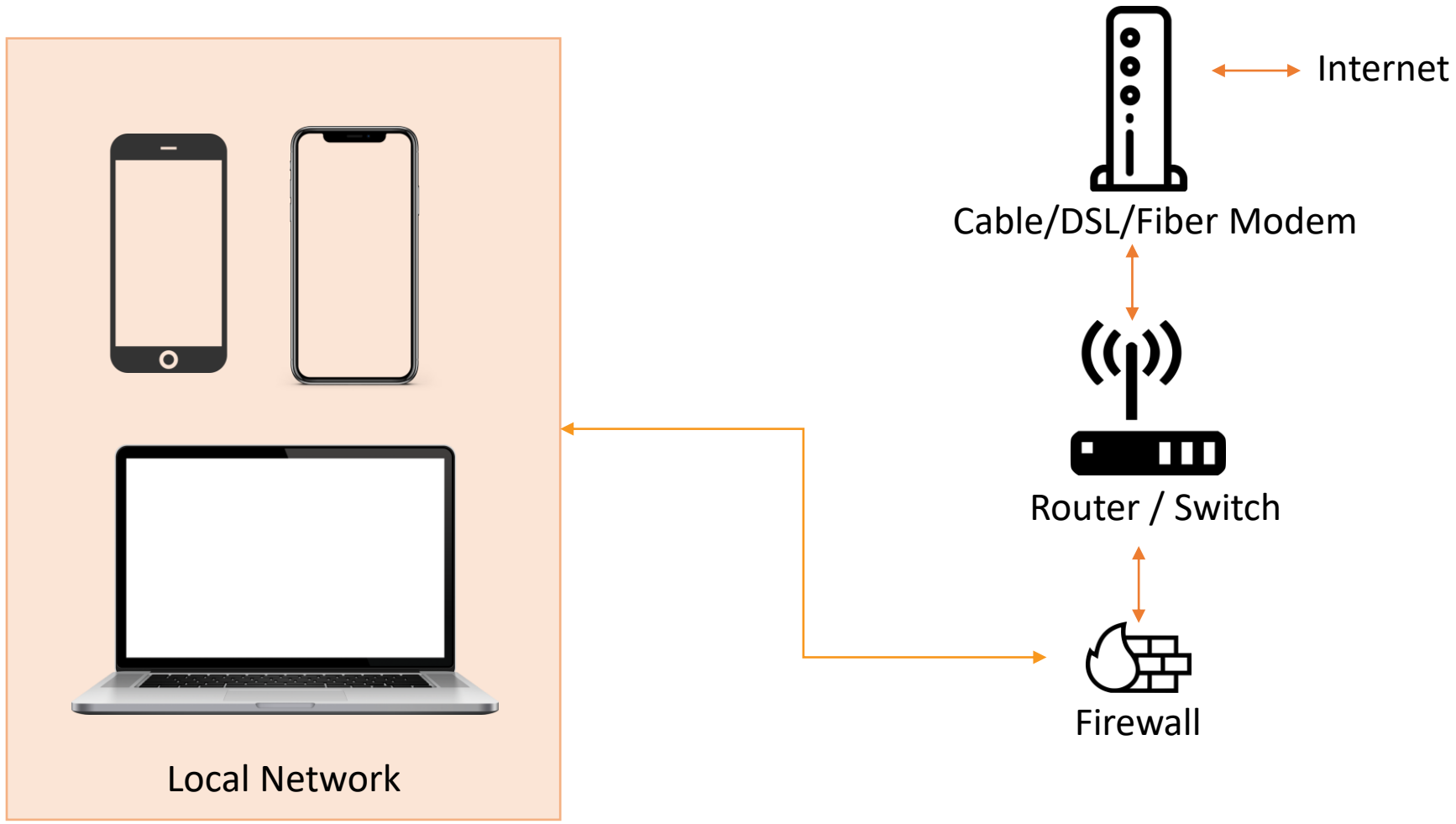
Default VPC

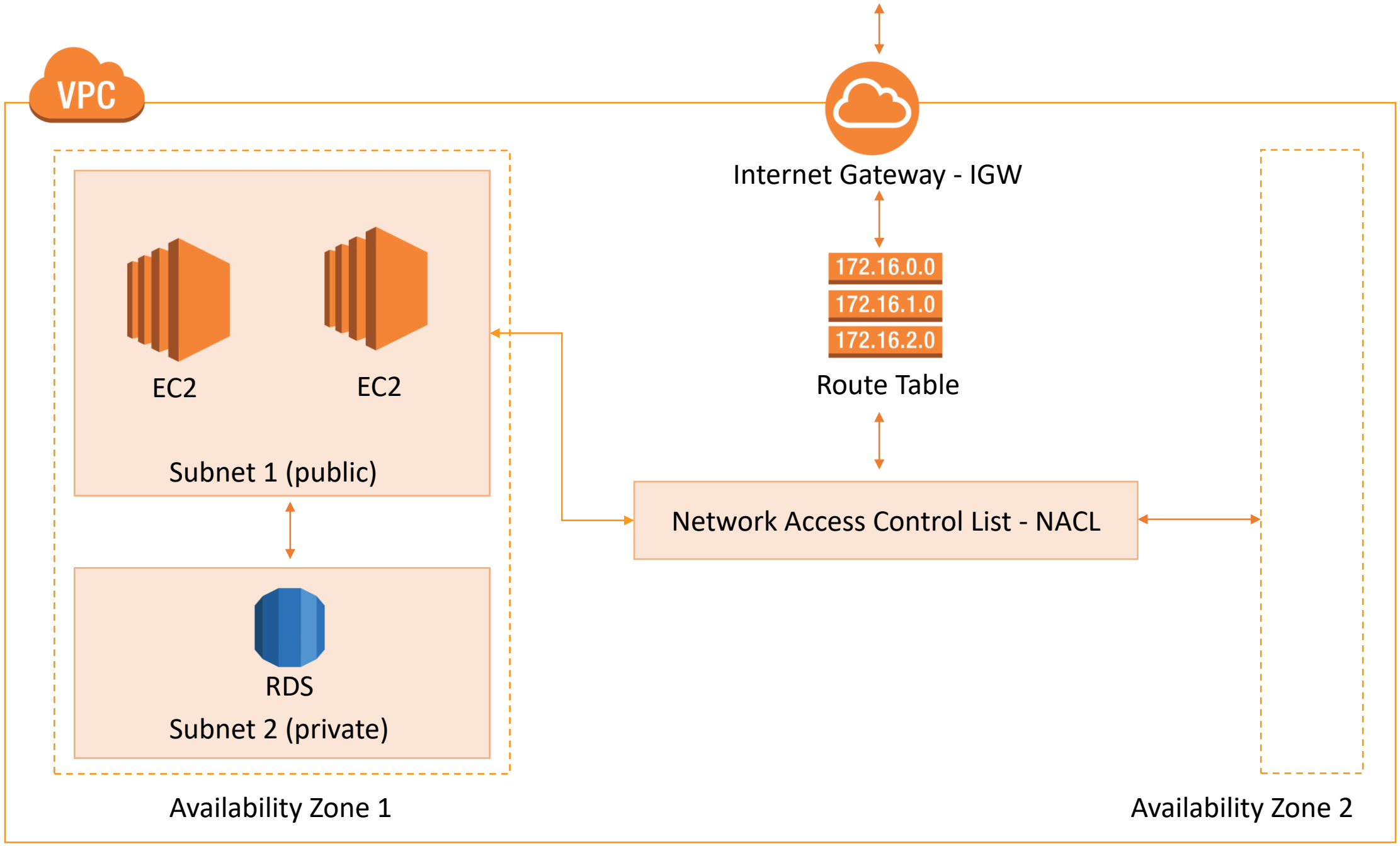
When you create an AWS account a default VPC is created for you. It includes the standard components that are needed to make it functional:

- Internet Gateway (IGW)
- A Route table (with predefined routes to the default subnets)
- A Network Access Control List - NACL (with predefined rules for access)
- Subnets to provision AWS resources (such as EC2 instances)

You can select your own IP address range, create subnets and configure route tables and network gateways.

Your Home Network




VPC
Internet Gateway - IGW
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
EC2
EC2
Subnet 1 (public)
Network Access Control List - NACL
RDS
Subnet 2 (private)
Availability Zone 1
Availability Zone 2

Internet Gateways - IGW

A combination of hardware and software that provides your private network with a route to the Internet.

One IP for all resources in your network (VPC).

A horizontally scaled redundant and highly available VPC component that **allows communication between instances in your VPC and the Internet**.

- Your default VPC already has an IGW attached.
- Only 1 IGW can be attached to a VPC at a time.
- An IGW cannot be detached from a VPC while there are active AWS resources in the VPC.

Name	Name	ID	State	VPC
		igw-12dcdb6a	attached	vpc-af9b48d5

Read more about [Internet Gateways]

Route Tables

A route table contains a set of rules, called routes, that are used to **determine where network traffic is directed**.

- To define access between subnets, we use Route Tables
- To define access to the internet, we use Route Tables

Read more about Route Tables

Route Tables

- Your default VPC already has a main route table.
- Unlike IGW, you can have multiple active route tables in a VPC.
- You cannot delete a route table if it has dependencies (associated subnets)

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	igw-12dcdb6a	Active	No

Any subnet associated with this RT will be public and have access to the internet

Route Tables

Route Table ID	Explicitly Associat	Main	VPC
rtb-0ace9175	0 Subnets	Yes	vpc-af9b48d5

All subnets are **implicitly** associated with the Main RT.

rtb-093ba3a40a1ec618d | EssentialsRT

Summary | Routes | **Subnet Associations** | Route Propagation | Tags

Edit

Subnet	IPv4 CIDR	IPv6 CIDR

You do not have any subnet associations.

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-060c6688b4428dfa4	172.31.0.0/20	-
subnet-009d1d5ecaeab29f9	172.31.16.0/20	-
subnet-05333ae15bef423dc	172.31.32.0/20	-

Subnet in VPC

After creating a VPC, you can add one or more subnets in each AZ. Each subnet **must reside entirely within one AZ** and **cannot span zones**.

- Subnets **must** be associated with a Route Table.
- A **Public subnet** has a route to the Internet.
- A **Private subnet** does not have a route to the Internet.
- A subnet is located in **one** specific Availability Zone.

Creating subnets in VPC

CIDR range for the VPC – **10.0.0.0/16** – 65,536 IPs – It is an estimation of total resources in your network.

Subnets	CIDR	AZ	Available IPs	Total number of IPs
public-subnet-1a	10.0.0.0/24	us-east-1a	10.0.0.0 – 10.0.0.255	256
public-subnet-1b	10.0.1.0/24	us-east-1b	10.0.1.0 – 10.0.1.255	256
public-subnet-1c	10.0.2.0/24	us-east-1c	10.0.2.0 – 10.0.2.255	256
private-subnet-1a	10.0.3.0/24	us-east-1a	10.0.3.0 – 10.0.3.255	256
private-subnet-1b	10.0.4.0/24	us-east-1b	10.0.4.0 – 10.0.4.255	256
private-subnet-1c	10.0.5.0/24	us-east-1c	10.0.5.0 – 10.0.5.255	256

Note: The first (network) and the last (broadcast) IPs cannot be used. When you create resources on AWS, some of them implicitly gets an IP from the subnet.

VPC Security Layers

The VPC has two layers of security:

- Security Groups (SG) can be allowed to modify permission any **resource** that it is attached to. *(Instance level)*
- Network Access Control Lists (NACL) are applicable for the whole **subnet** that they are attached to. *(Subnet level)*

NACLs are **stateless** so you must define both the inbound and outbound traffic while SG is **stateful**.

You can write deny rules on NACL but you can’t write deny rules on SG. SGs have only allow rules and deny all by default.

Network Access Control Lists - NACL

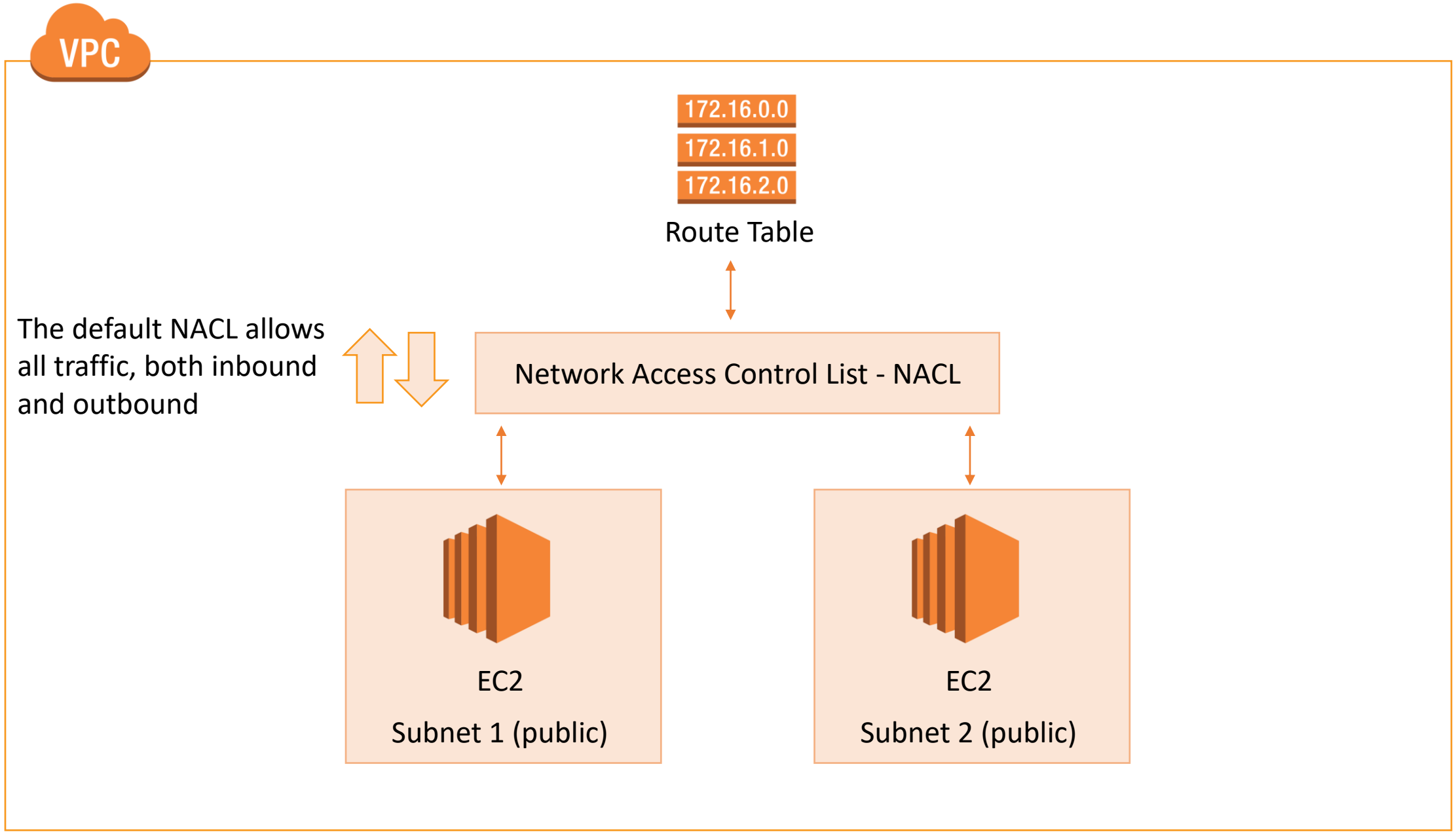
Acts as a **firewall between subnets**. A network access control list (NACL) is an **optional layer of security** for your VPC that acts as a **firewall** for controlling traffic in and out of one or more **subnets**.

- Your default VPC already has an NACL in place and associated with all default subnets.

Network ACL ID	Associated With	Default	VPC
acl-2b9fa451	6 Subnets	Yes	vpc-af9b48d5

In N. Virginia region, we have 6 AZs, AWS created a subnet replicated in all AZs.

Read more about [Network ACLs]


VPC
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
The default NACL allows all traffic, both inbound and outbound
Network Access Control List - NACL
EC2
Subnet 1 (public)
EC2
Subnet 2 (public)

NACL Rules

- Rules are evaluated from lowest to highest based on rule #. The first rule found that applies to the traffic type is immediately applied, regardless of any rules that come after it.
- A subnet can only be associated with one NACL at a time.
- A NACL allows or denies traffic from entering a subnet. Once inside the subnet, other AWS resources may have additional security layers such as Security Groups.

NACL Rules

- The **default NACL allows all traffic** to the default subnets.
- Any **new NACL you create denies all traffic** by default.

Inbound

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

All traffic is allowed

Inbound

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
90	SSH (22)	TCP (6)	22	0.0.0.0/0	DENY
100	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

All traffic is denied

Only Allow SSH

Inbound

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Only allow SSH

Outbound

Rule #	Type	Protocol	Port Range	Destination	Allow / Den
100	Custom TCP Rule	TCP (6)	1024-65535	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Allow SSH response

Only Allow HTTP

Inbound

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Only allow HTTP

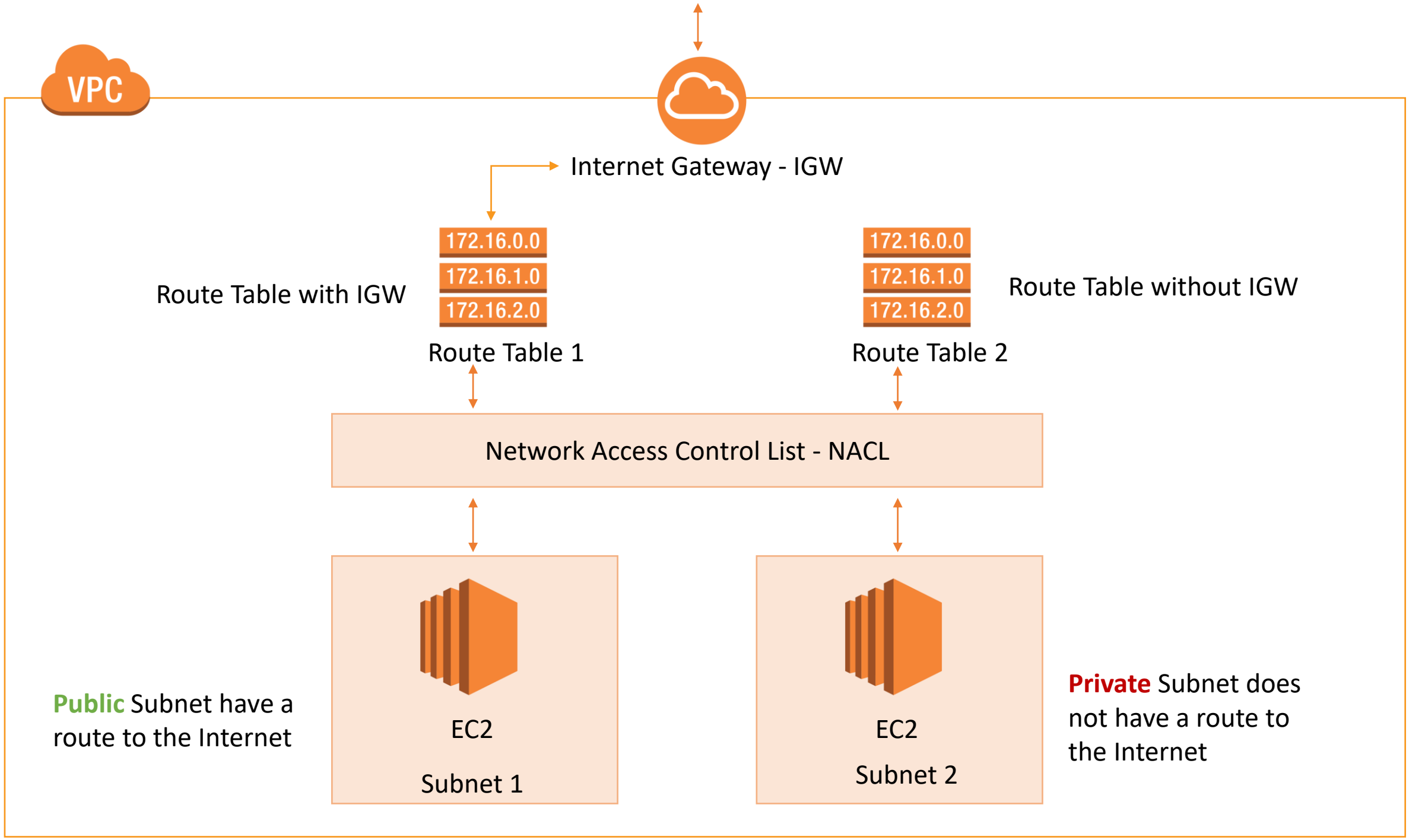
Outbound

Rule #	Type	Protocol	Port Range	Destination	Allow / Den
100	HTTP (80)	TCP (6)	1024-65535	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Allow HTTP response

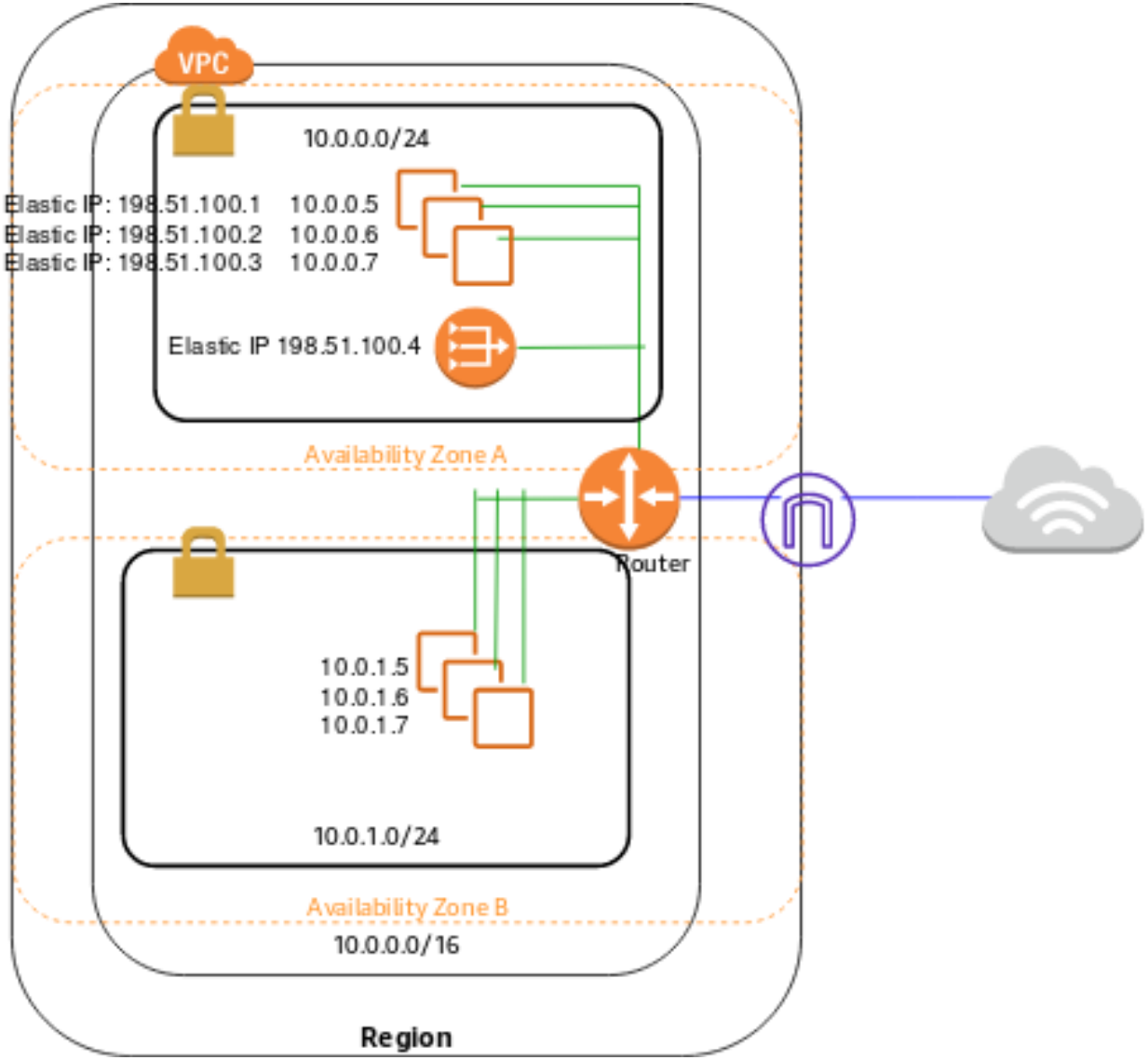
Notes

- The outbound traffic will use ephemeral ports 1024-65535 for the return web traffic and not port 80.
- An ephemeral port is a short-lived transport protocol port for Internet Protocol (IP) communications.


VPC
Internet Gateway - IGW
Route Table with IGW
172.16.0.0
172.16.1.0
172.16.2.0
Route Table 1
172.16.0.0
172.16.1.0
172.16.2.0
Route Table 2
Route Table without IGW
Network Access Control List - NACL
EC2
Subnet 1
EC2
Subnet 2
Public Subnet have a route to the Internet
Private Subnet does not have a route to the Internet

NAT gateways

You can use a network address translation (NAT) gateway to **enable instances in a private subnet to connect to the internet** or other AWS services, but prevent the internet from initiating a connection with those instances.



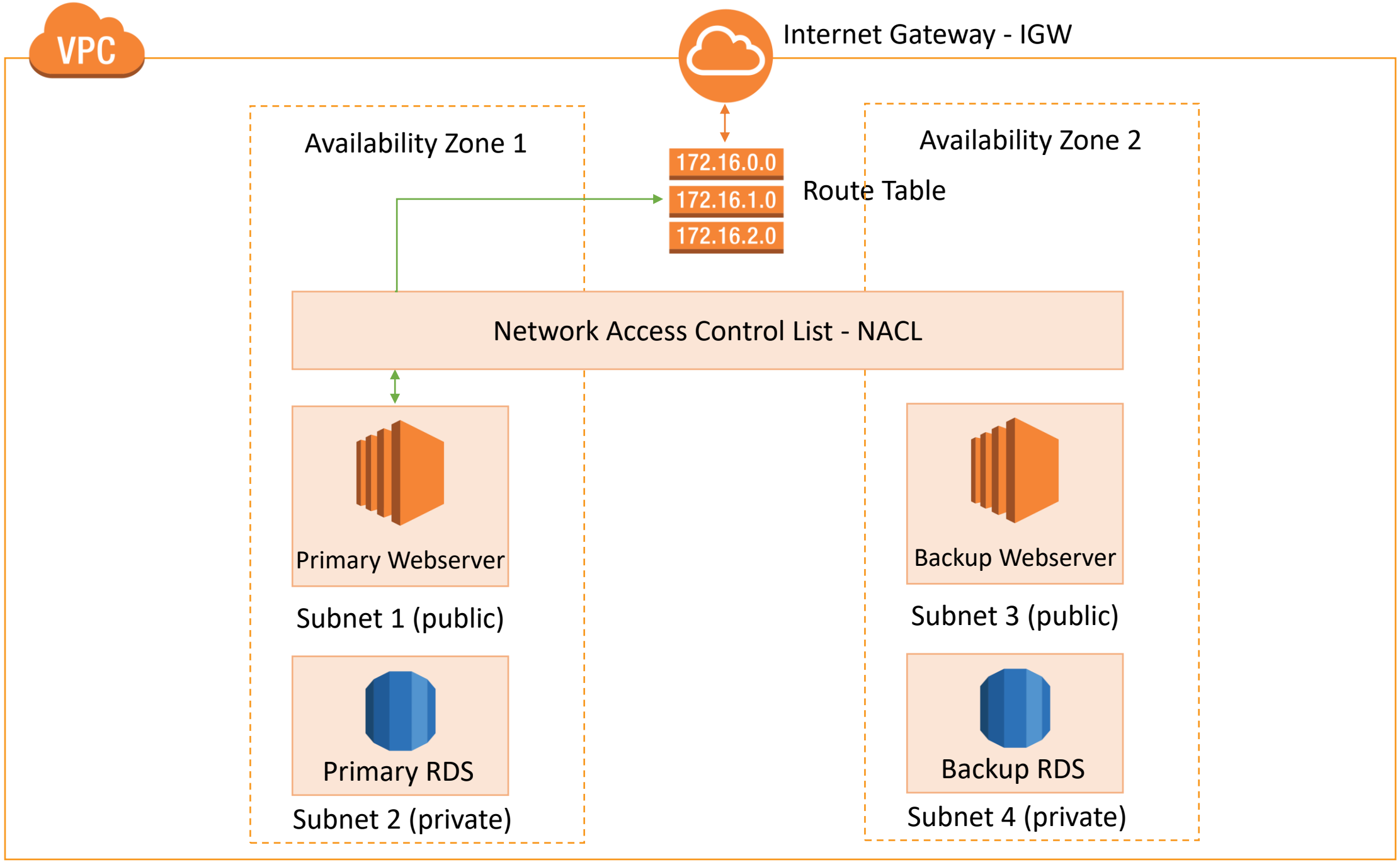
NAT gateways

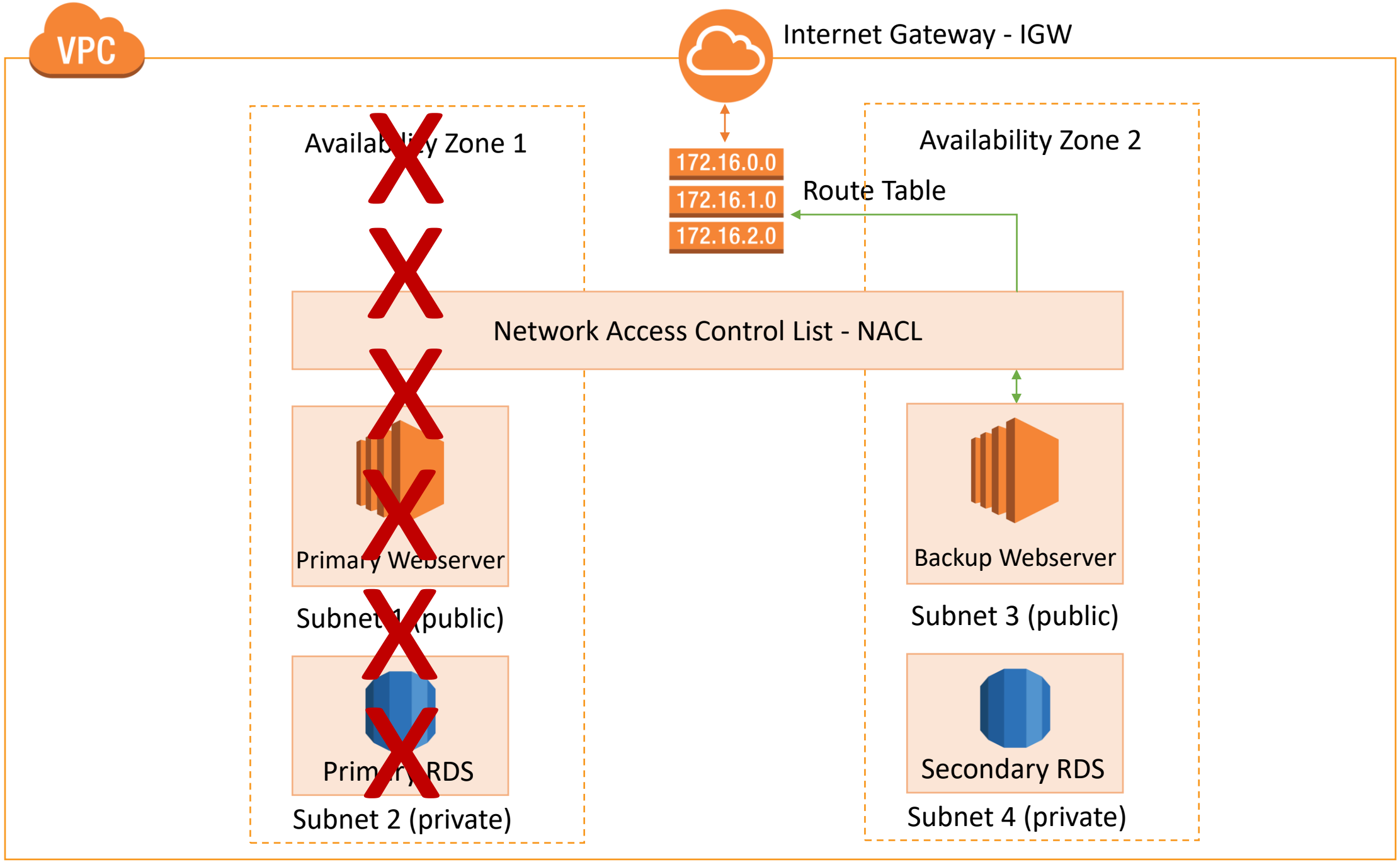
We need to create a custom Route Table for private subnets.

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

Keep the main table as below. We must create the NAT gateway in public subnet.

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*internet-gateway-id*


VPC
Internet Gateway - IGW
Availability Zone 1
Availability Zone 2
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
Network Access Control List - NACL
Primary Webserver
Subnet 1 (public)
Backup Webserver
Subnet 3 (public)
Primary RDS
Subnet 2 (private)
Backup RDS
Subnet 4 (private)


VPC
Internet Gateway - IGW
Availability Zone 1
Availability Zone 2
172.16.0.0
172.16.1.0
172.16.2.0
Route Table
Network Access Control List - NACL
Primary Webserver
Subnet 1 (public)
Backup Webserver
Subnet 3 (public)
Primary RDS
Subnet 2 (private)
Secondary RDS
Subnet 4 (private)