



[Mithun Technologies](#)  
[devopstrainingblr@gmail.com](mailto:devopstrainingblr@gmail.com)  
**+91-9980923226**

# AWS VPC

# VPC (Virtual Private Cloud)

- VPC is a private sub-section of AWS that you control, in which you place AWS resources.
- You have full control over who has access to the AWS resources that you place inside our VPC.
- VPC lets you provision a logically isolated section of the AWS cloud where you launch AWS resources in a virtual network.
- In the VPC we can control our virtual networking environment, IP address, creation of subnets, route tables & gateways.
- When we create an AWS account, a default "VPC" is created for you.

## What's in the VPC tool box?



**VPC** -User-defined address space up to /16 (65,536 addresses)



**Subnets** -200 user-defined subnets up to /16



**Route Tables** – Define how traffic should be routed from/to each subnet



**Access Control Lists** – Stateless network filtering between subnets



**Internet Gateway** –A **logical** device enabling traffic to be routed to/from the public internet



**NAT** – Provide NetworkAddress Translation to private instances for 10Gbps traffic



## VPC Fundamentals

- If a subnet has a route to an AWS Internet Gateway it is called a **public subnet**
- If there is no route from a subnet to an AWS Internet Gateway it is a **private subnet**.  
If an instance in a private subnet wants to access the internet it needs to use a **NAT** in a public subnet
- Each subnet must reside entirely **within one Availability Zone**.
- Instances in a VPC communicate based on Route Table, VPC Security Groups and Access Control Lists
- **VPC Security Groups** control both inbound and outbound access between instances (EC2 Security Groups can only define inbound rules). A **firewall at the instance level**.
- **VPC Access Control Lists (ACLs)** control access between subnets – **firewall at the subnet level**, an extra level of security over VPC Security Groups
- Subnet **Route Table** specifies subnet IP routing.

### Subnet

- Subnet is a sub-section of network, generally includes all the computers in a specific location.
- When we create a VPC, it spans on all of the Availability Zones in the region.
- You can add one or more subnets in each Availability Zone.
- Each subnet must reside entirely within one Availability zone.
- The default VPC already has a subnet created by default.
- Subnets Must be associated with a route table
- A PUBLIC subnet has a route to the Internet
- A PRIVATE subnet doesn't have a route to the Internet



## Internet Gateway

- Our Default VPC already has an IGW attached.
- Only 1 IGW can be attached to a VPC at any time.
- An IGW cannot be detached from a VPC while there are active resources in the VPC.
- Without IGW the resources can talk to each other but not to the internet.



## Route Table

- RT contains a set of rules, called routes that are used to determine where the network traffic is directed
- The Default VPC already has a main route table
- Unlike an IGW, you can have multiple active route tables in a VPC
- You cannot delete a route table if it has "dependencies"

## NACL - Network Access Control Lists

- NACL is an optional layer of security for your VPC that acts as a firewall for controlling traffic in & out of one or more subnets
- Your default VPC already has a NACL in place & associated with the default subnets
- If a subnet has a route to an AWS Internet Gateway it is called a public subnet

## CIDR

- Classless Inter-Domain Routing (CIDR ) is a method for allocating IP addresses and IP routing, CIDR range 0-32
- When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block, for example, 10.0.0.0/16. This is the primary CIDR block for your VPC.
- When you create a subnet, you specify the CIDR block for the subnet, which is a subset of the VPC CIDR block. Each subnet must reside entirely within one Availability Zone and cannot span zones

## VPC and Subnet Sizing for IPv4

- When you create a VPC, you must specify an IPv4 CIDR block for the VPC. The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses).
- For example, if you create a VPC with CIDR block 10.0.0.0/24, it supports 256 IP addresses. You can break this CIDR block into two subnets, each supporting 128 IP addresses. One subnet uses CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other uses CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255).
- The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:
  - 10.0.0.0: Network address.
  - 10.0.0.1: Reserved by AWS for the VPC router.
  - 10.0.0.2: Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two.
  - 10.0.0.3: Reserved by AWS for future use.
  - 10.0.0.255: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

## Calculate No of IP Address:

Ex:

10.0.0.0/24

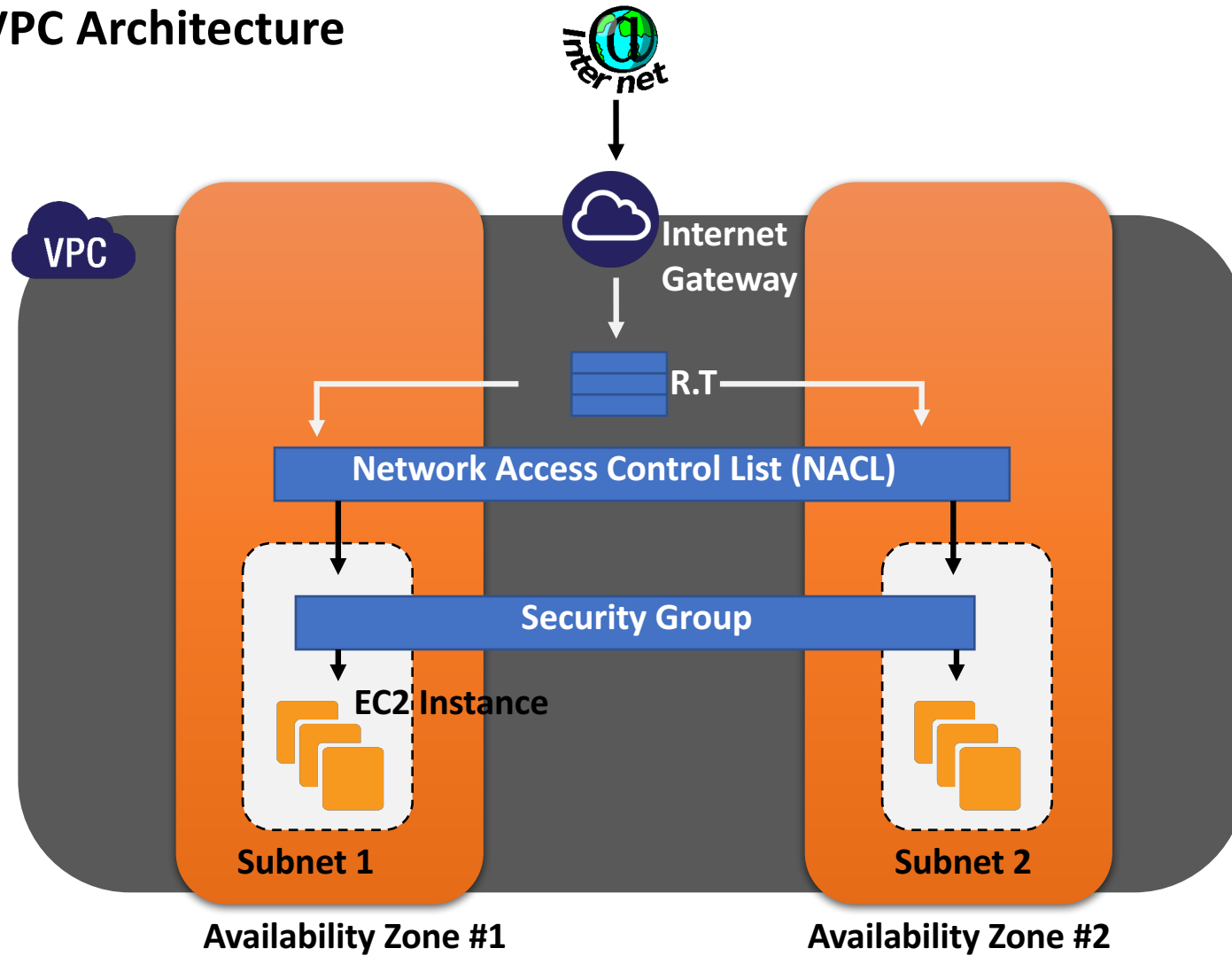
$$32-24=8$$

Hosts = 2 = 256 = 0-255 (First 4 & last 1 IP will be reserved by AWS)

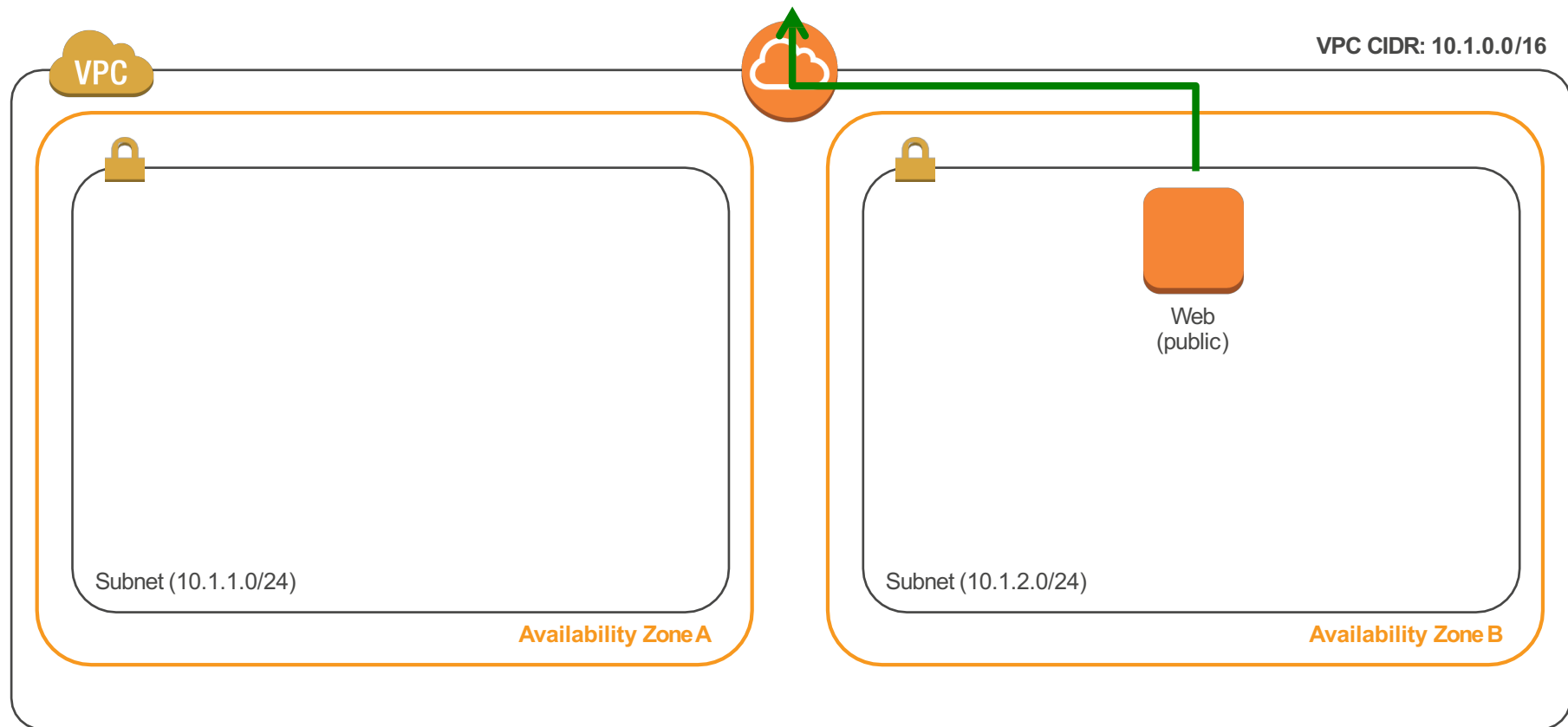
- 256-5 = 251 will be IP address will be available for your use.



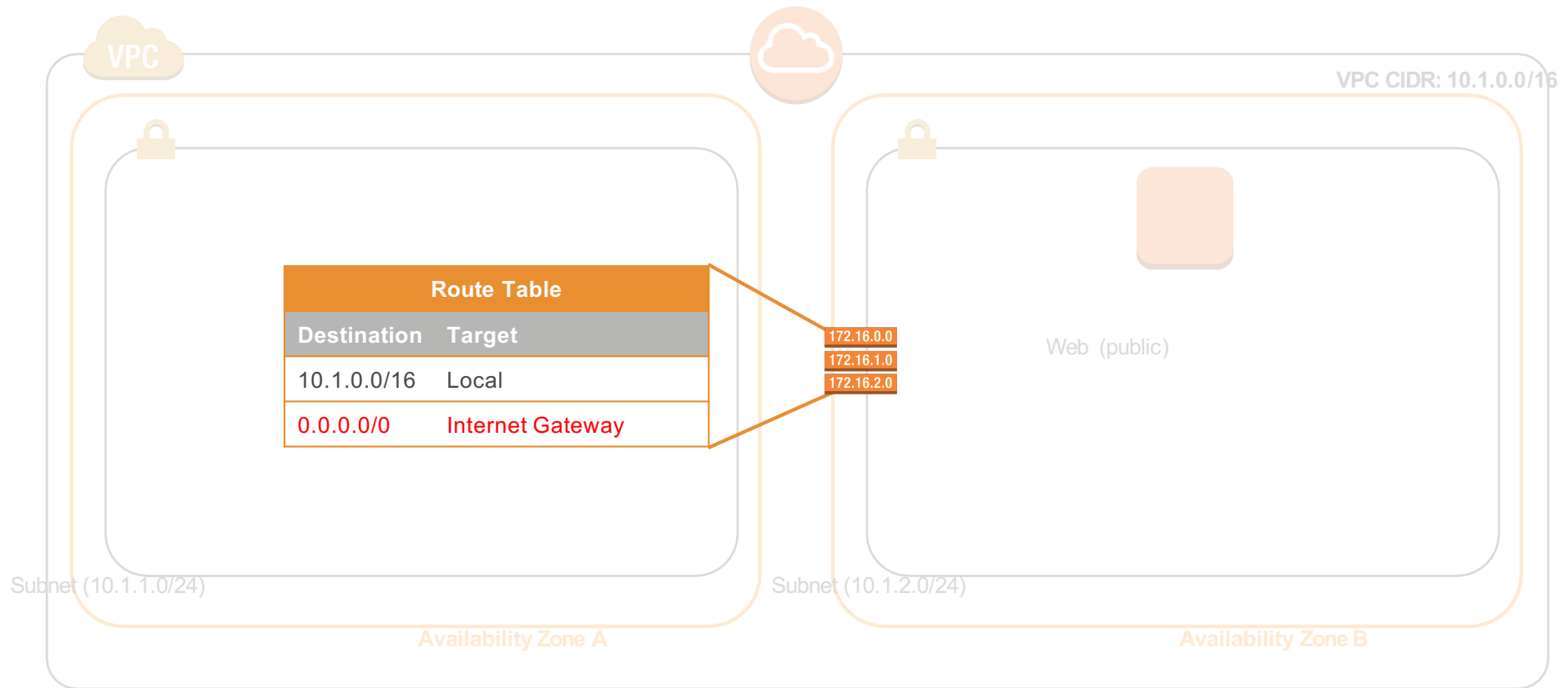
## VPC Architecture



# Public Subnet Routing – Internet Gateway

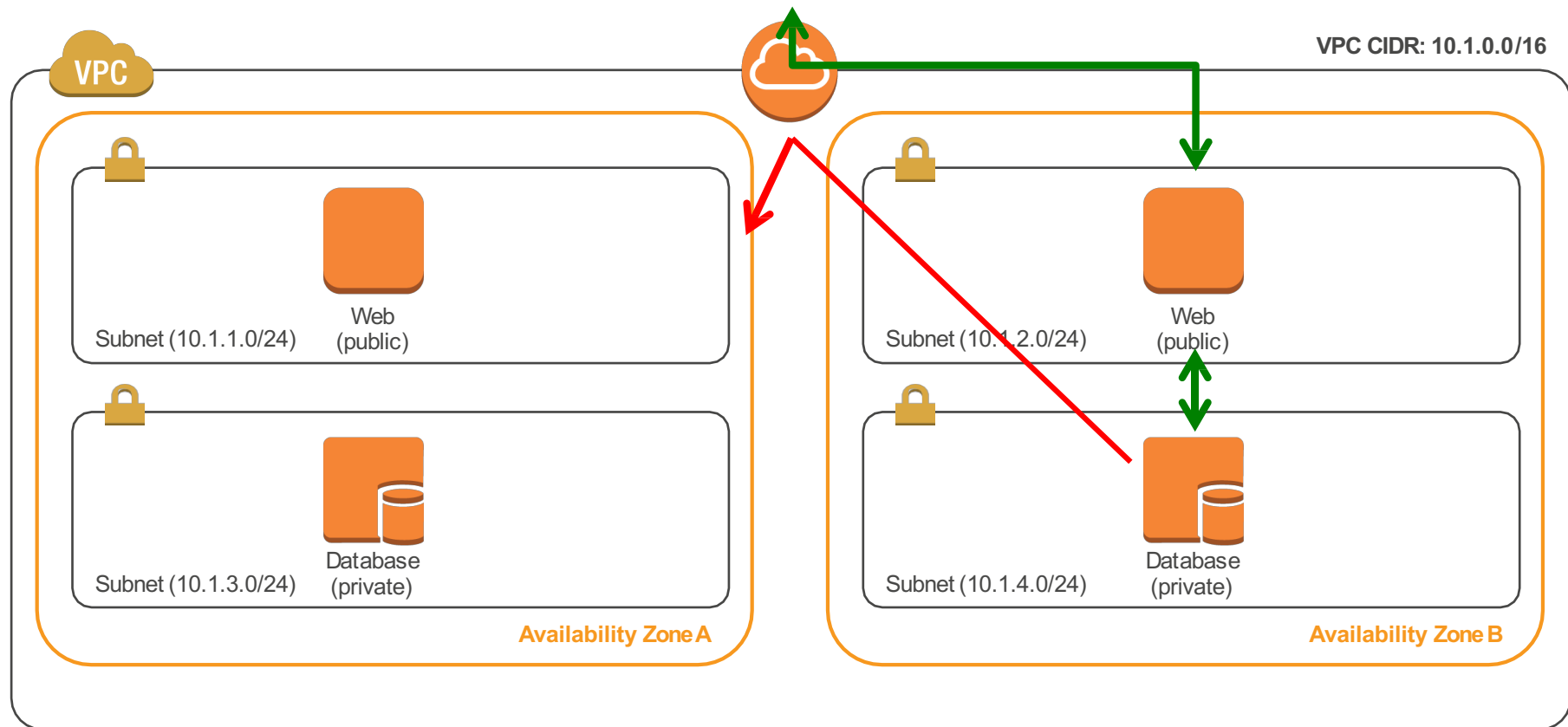


# Public Subnet Routing – Internet Gateway

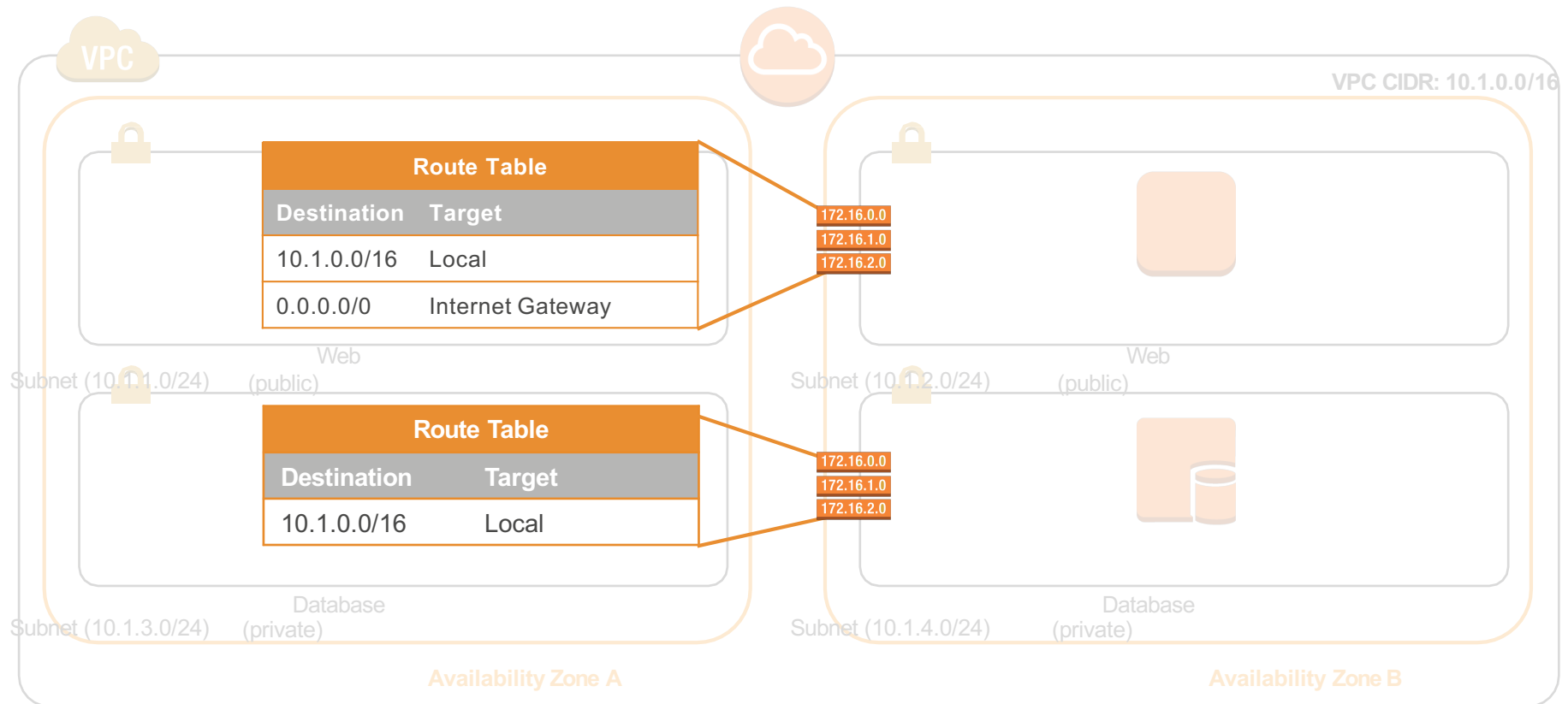




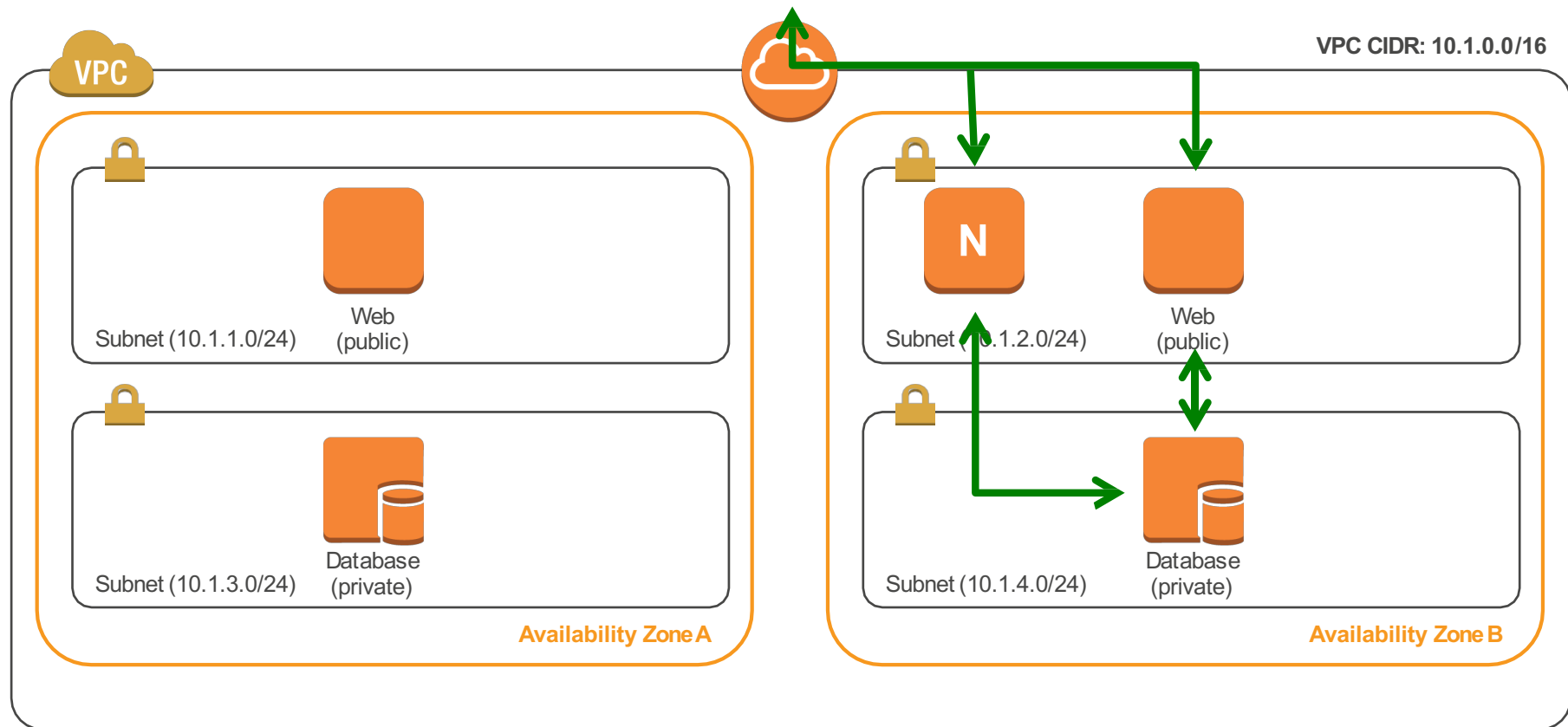
# Private Subnet Routing



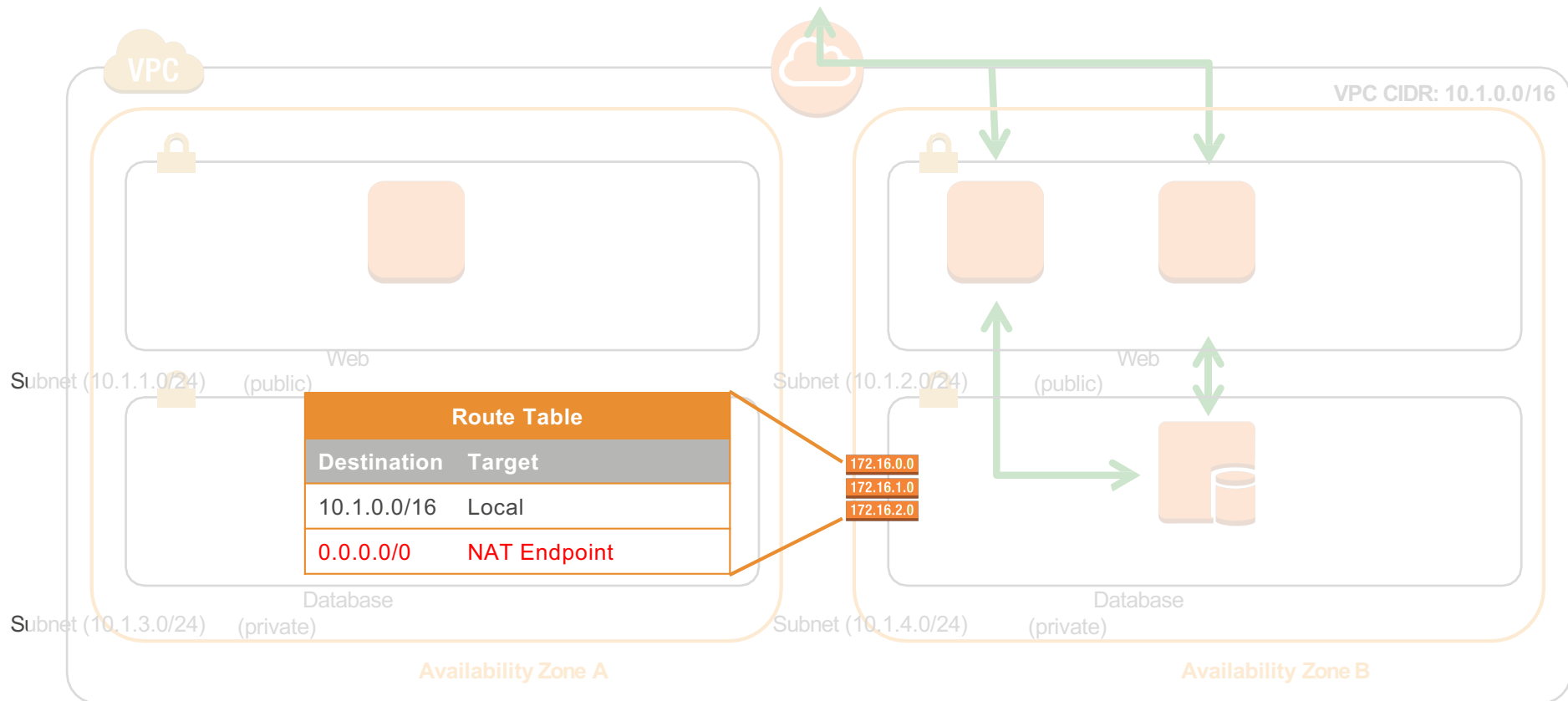
# Private Subnet Routing



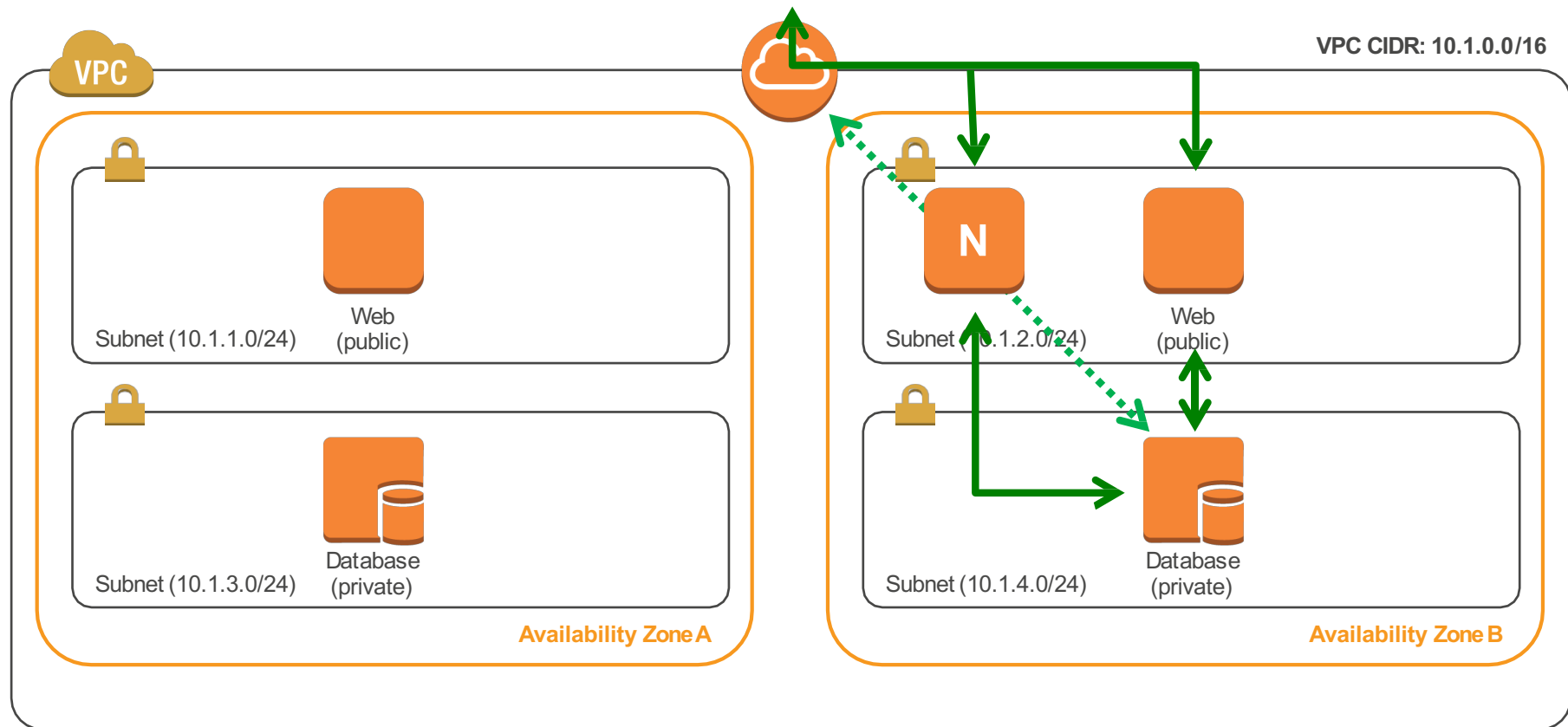
# Private Subnet Routing – NAT Gateway



# Private Subnet Routing -NATGateway



# Private Subnet Routing



# Questions ?

[Mithun Technologies](#)  
[devopstrainingblr@gmail.com](mailto:devopstrainingblr@gmail.com)  
**+91-9980923226**

