AWS VPC

Mithun Technologies
devopstrainingblr@gmail.com
+91-9980923226

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 Network Address Translation to private instances for 10Gbps traffic

Mithun Technologies

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 an 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

Mithun Technologies

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

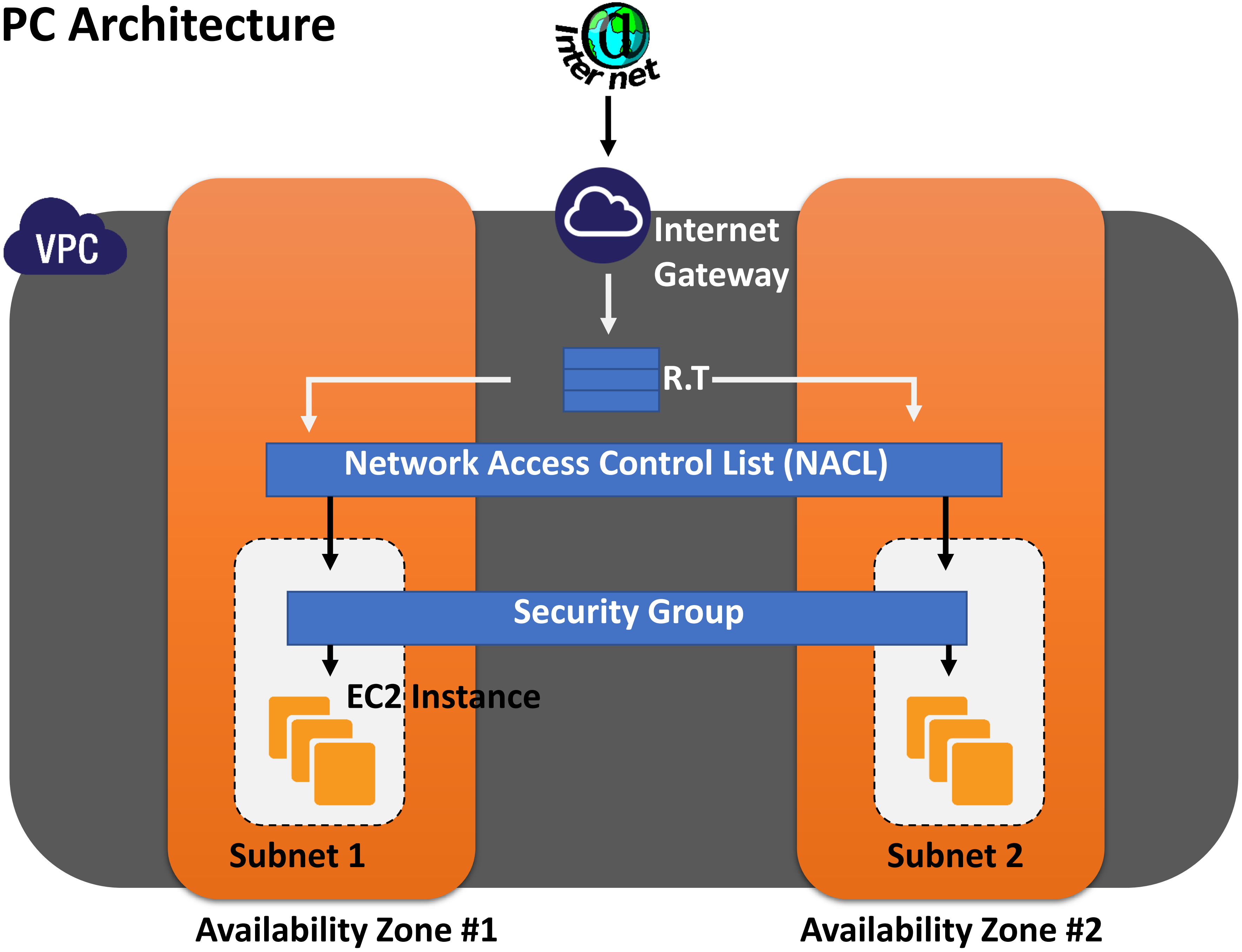
Hosts = 2 = 256 =0-255 (First 4 & last 1 IP will be reserved by AWS)

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

What is an RFC1918 address?

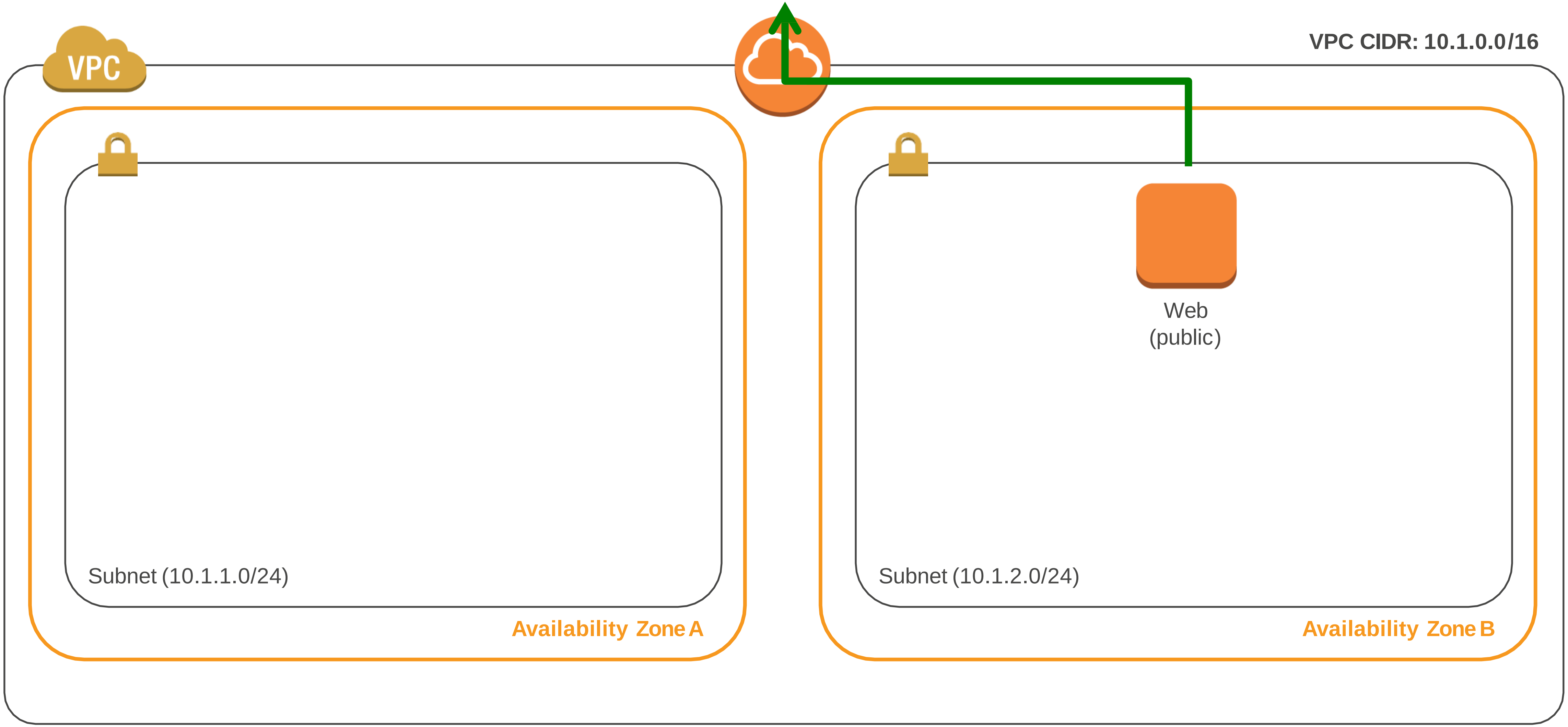
- An RFC1918 address is an IP address that is assigned by an enterprise organization to an internal host. These IP addresses are used in private networks, which are not available, or reachable, from the Internet.
- In fact, one of the basic requirements of the Internet is that each host has a unique IP address. RFC1918 removes this requirement. RFC1918 IP addresses can be used on multiple networks, as long as they're private and isolated from each other. To implement this solution every Internet router must be configured to discard IP packets with these addresses. IP packets carrying private addresses can only flow on internal, private networks.
- RFC1918 Motivations
- This RFC was drafted in 1996 when it became clear to Internet operators that the IPv4 address space, consisting of 4,294,967,296 unique addresses, was not sufficient to address every single computer in the world. By that time, the Internet was rapidly growing beyond initial expectations. Soon, no IPv4 addresses would be available to use, limiting the Internet's growth. As a solution, RFC1918 was drafted to enable private organizations to use these addresses internally. Private addresses can be used without asking permission to the Internet Assigned Numbers Authority (IANA), which governs the IP addresses assignment.
- The only drawback of RFC1918 is that computers configured with private addresses cannot be reached from the Internet. With this new standard, computers were basically divided between public and private hosts. Hosts configured with private addresses are basically "clients": they can connect to Internet servers, or other internal hosts, but can't be reached from the Internet.
- RFC1918 Subnets
- The RFC1918 address space includes the following networks:
- 10.0.0.0 – 10.255.255.255 (10/8 prefix)
- 172.16.0.0 – 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 – 192.168.255.255 (192.168/16 prefix)
- **NAT, Network Address Translation**
- Network Address Translation (NAT) is a technology that makes RFC1918 a feasible solution to the IPv4 address exhaustion problem. NAT enables an internal host to communicate with an Internet server. A NAT device, generally a network router or a firewall, sits between the Internet and a private network. The Internet interface is configured with a public IP address while the private interface is connected to the internal network and configured with an RFC1918 address.
- When the NAT device receives a packet from an internal host, it rewrites the packet using its own public IP address as source before sending it to the Internet. This process is also called "masquerading" because it seems as if the conversation was (falsely) originated by the NAT device itself.

VPC Architecture

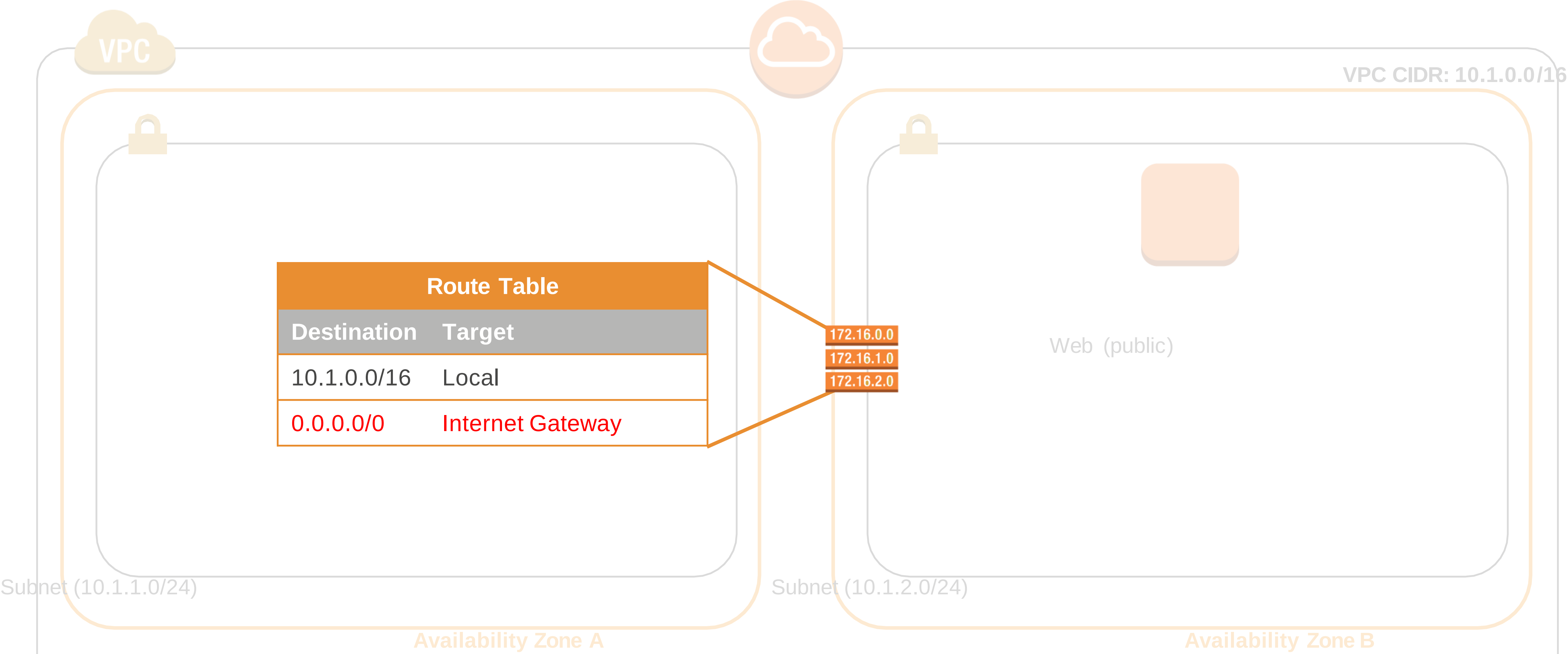


Mithun Technologies

Public Subnet Routing – Internet Gateway

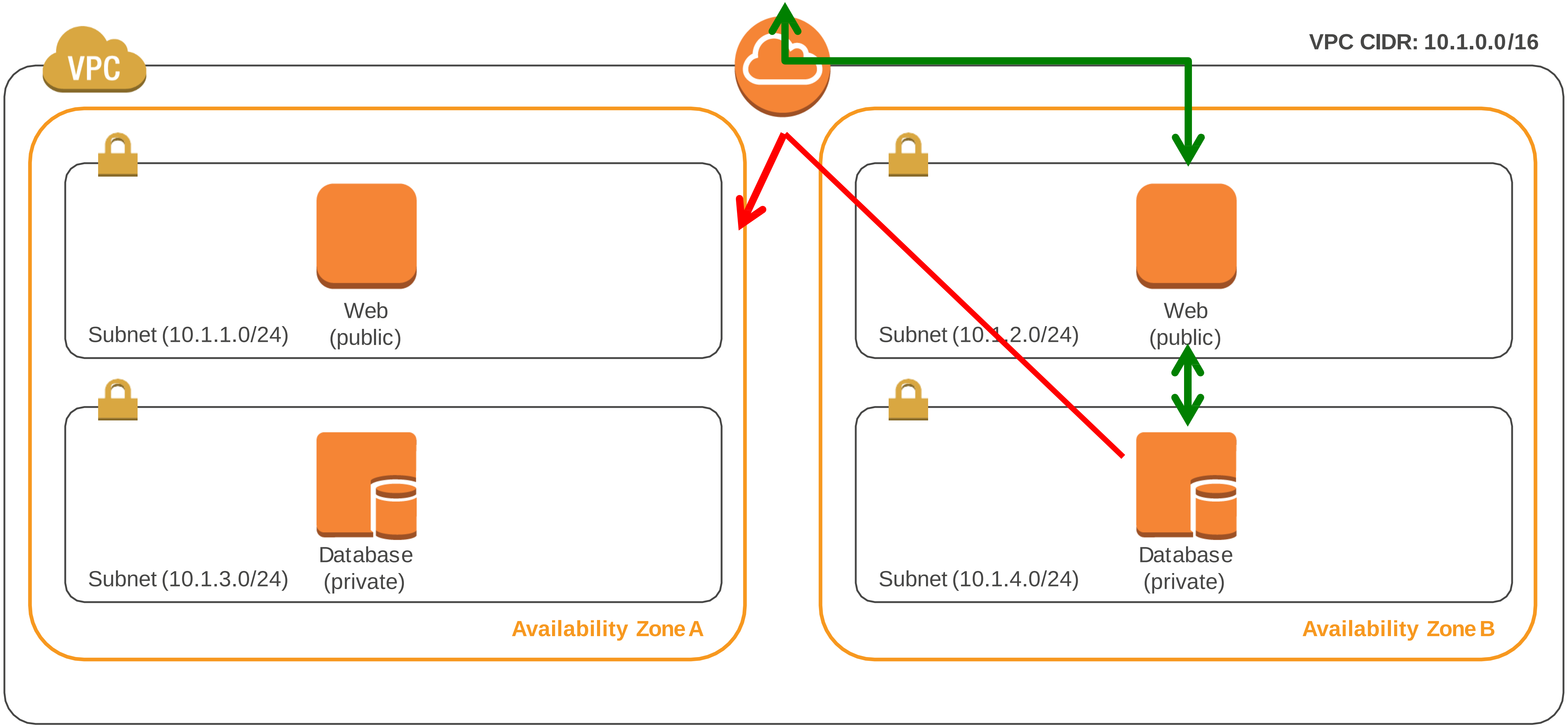


Public Subnet Routing – Internet Gateway

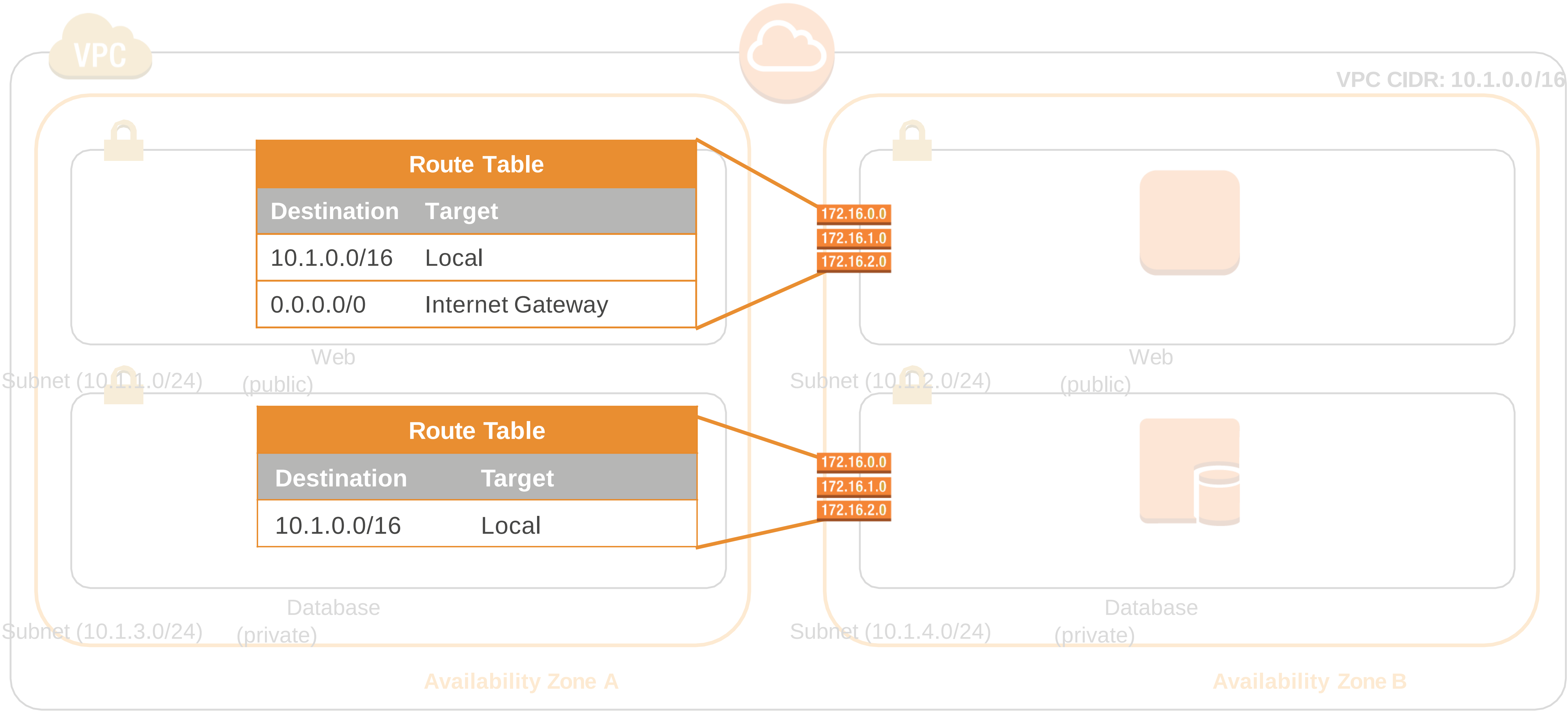


Route Table	
Destination	**Target**
10.1.0.0/16	Local
0.0.0.0/0	Internet Gateway

Private Subnet Routing



Private Subnet Routing



Route Table

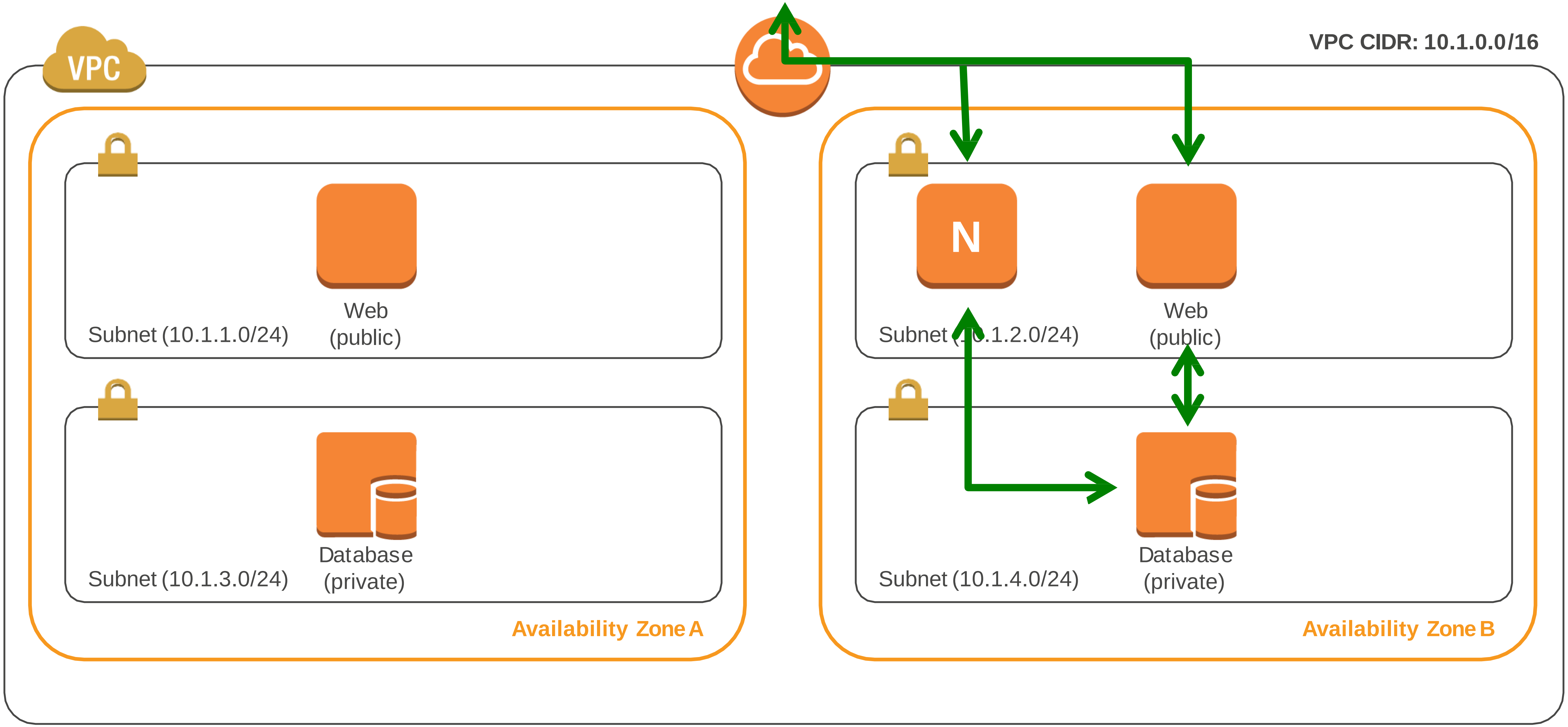
Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	Internet Gateway

Route Table

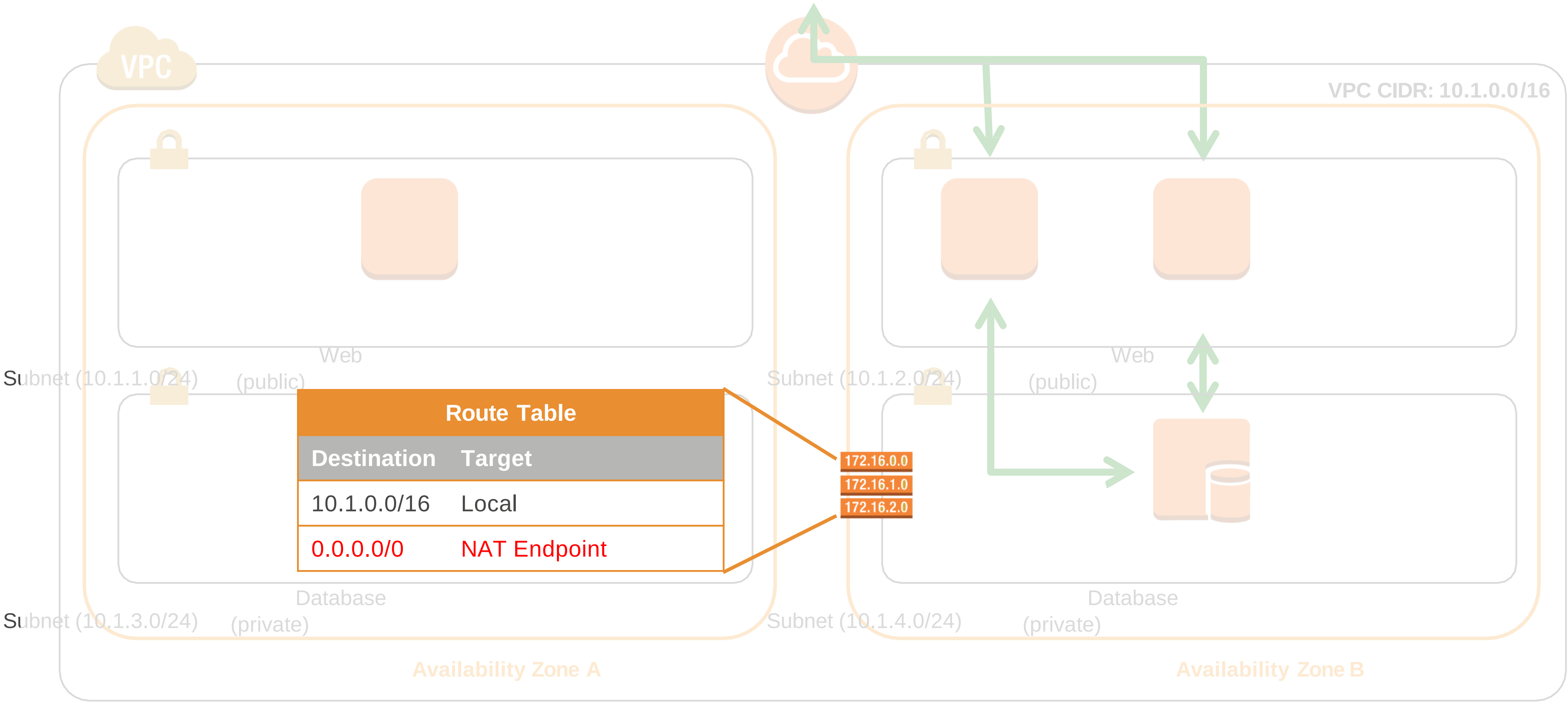
Destination	Target
10.1.0.0/16	Local

Mithun Technologies

Private Subnet Routing – NAT Gateway



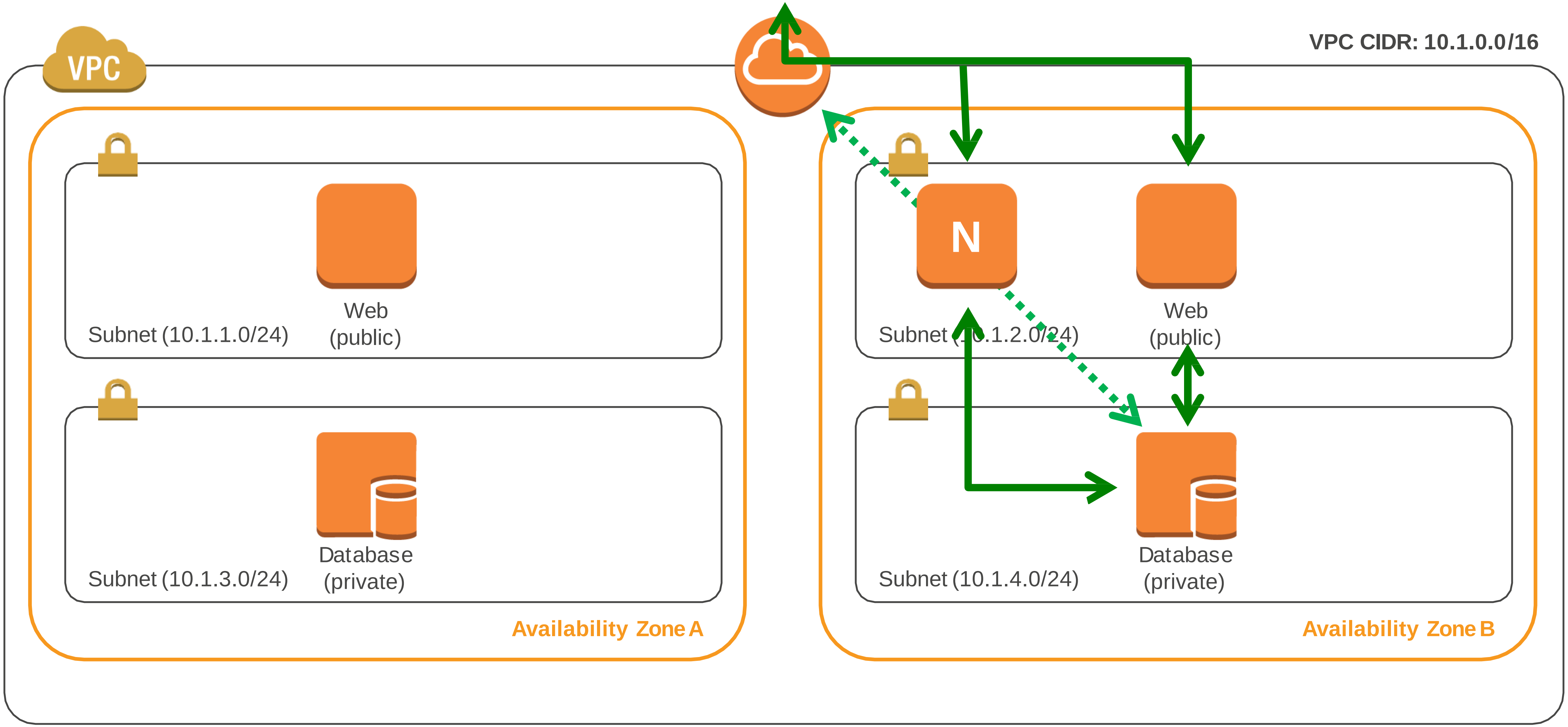
Private Subnet Routing -NATGateway



Route Table	
Destination	**Target**
10.1.0.0/16	Local
0.0.0.0/0	NAT Endpoint

Mithun Technologies

Private Subnet Routing



Questions ?

Mithun Technologies
devopstrainingblr@gmail.com
+91-9980923226