# AWS VPC

# What is a Virtual Private Cloud?

- Your own logically isolated section of the Amazon Web Services (AWS) Cloud
- By default, your VPC has no access to the internet nor are instances addressable from the internet
- You have complete control over your virtual networking environment
- Proven and well-understood networking concepts:
  - User defined IP address range
  - Subnets
  - Route Tables
  - Access Control Lists
  - Network Gateways
- A way to gain **agility** as well as additional security

# 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

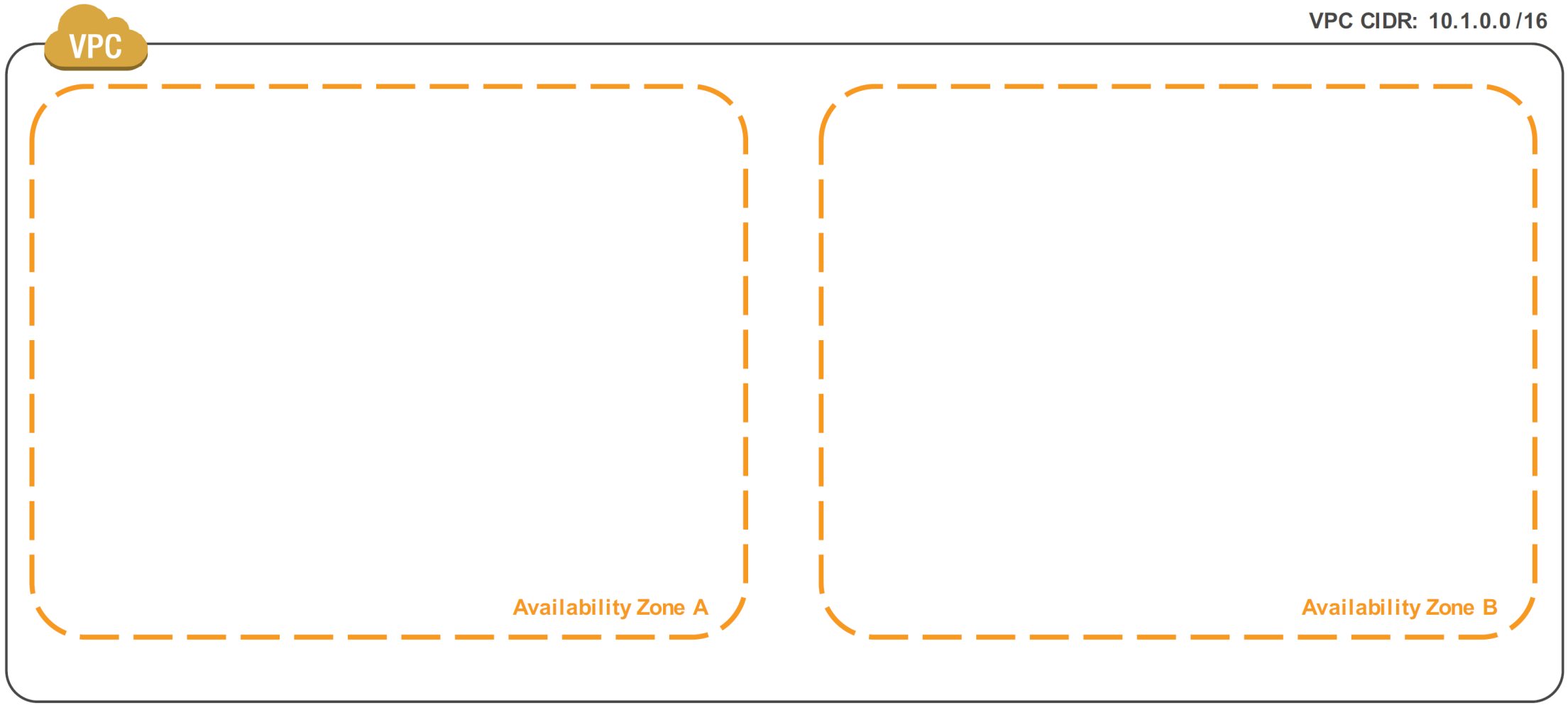
**Internet Gateway** – A **logical** device enabling traffic to be routed to/from the public internet

**Managed NAT** – Provide Network Address Translation to private instances for 10Gbps traffic

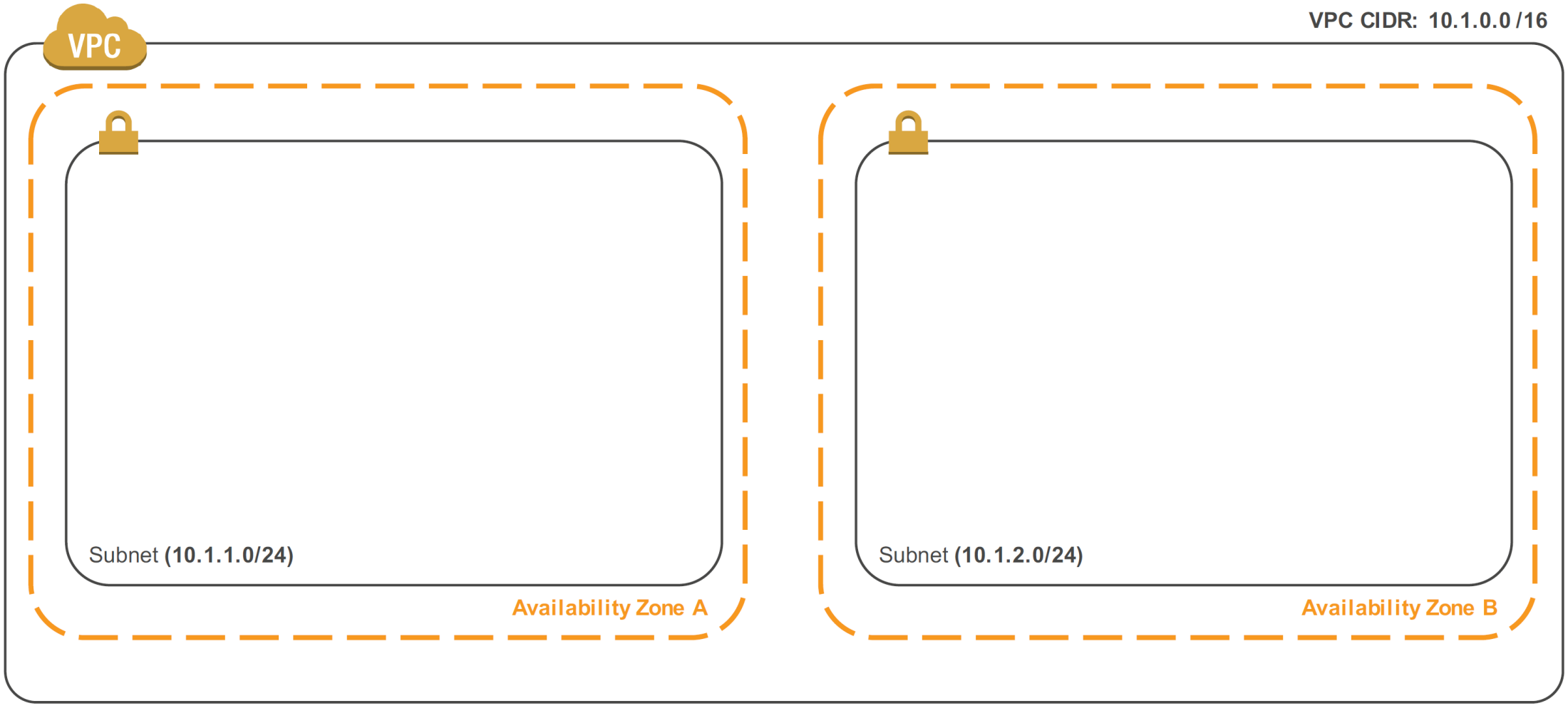
**Virtual Private Gateway** - The Amazon end of a VPN connection

**Customer Gateway** - The router at the customer end of a VPN connection

# VPCs span an entire region



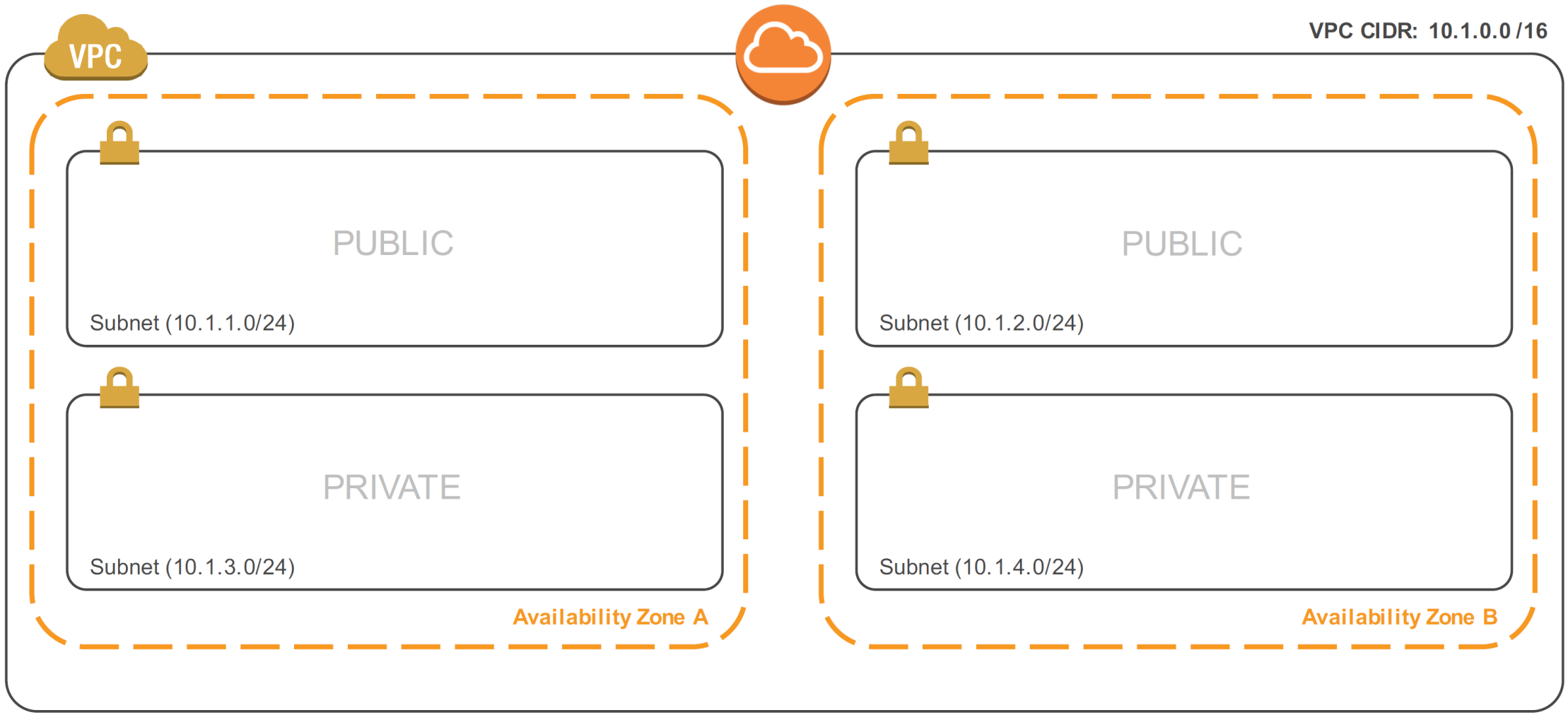
# Subnets sit in a single VPC in a single AZ



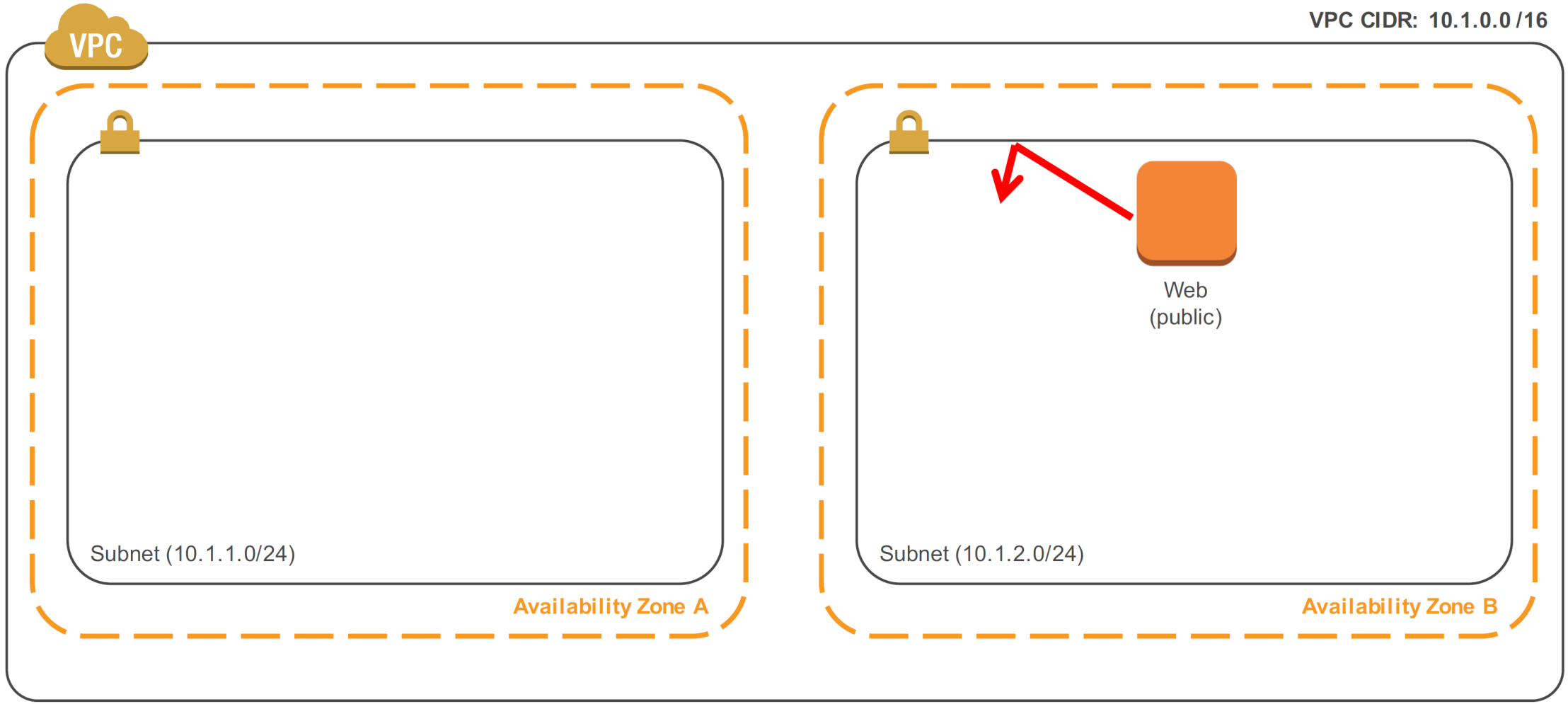
# Plan your VPC IP space before creating it

- Consider future AWS region expansion
- Consider future connectivity to your internal networks
- Consider subnet design
- VPC can be /16 down to /28
- CIDR cannot be modified after creation

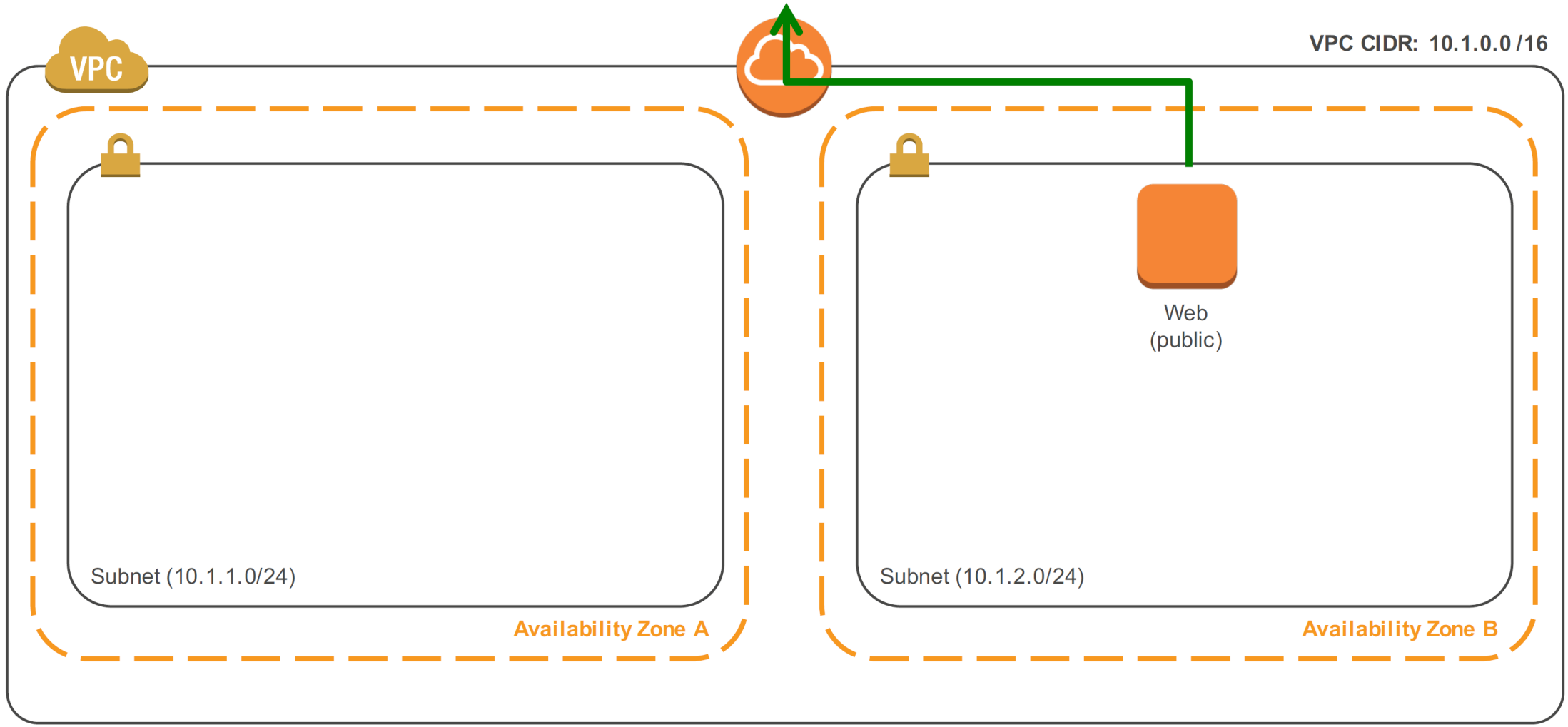
# Public / Private Subnets



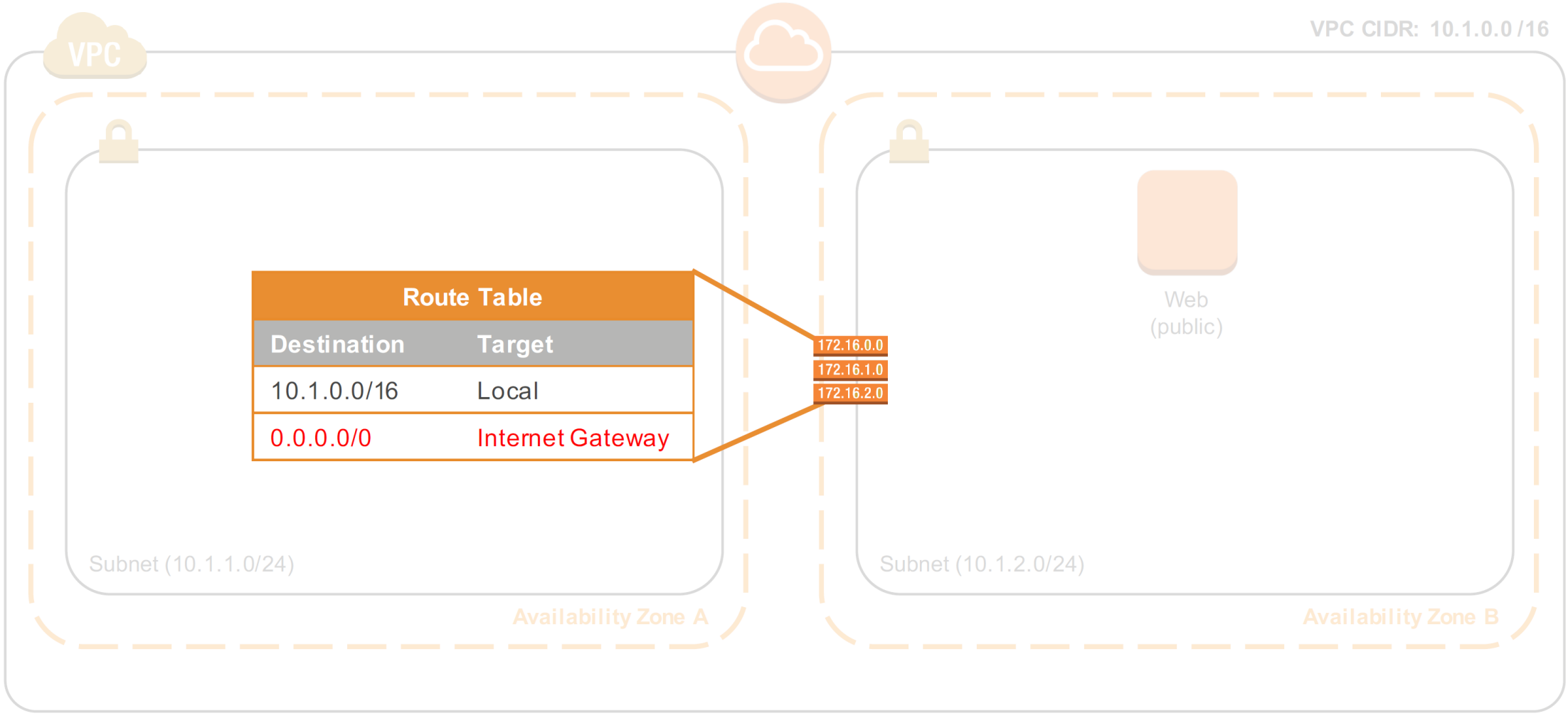
# Public Subnet Routing



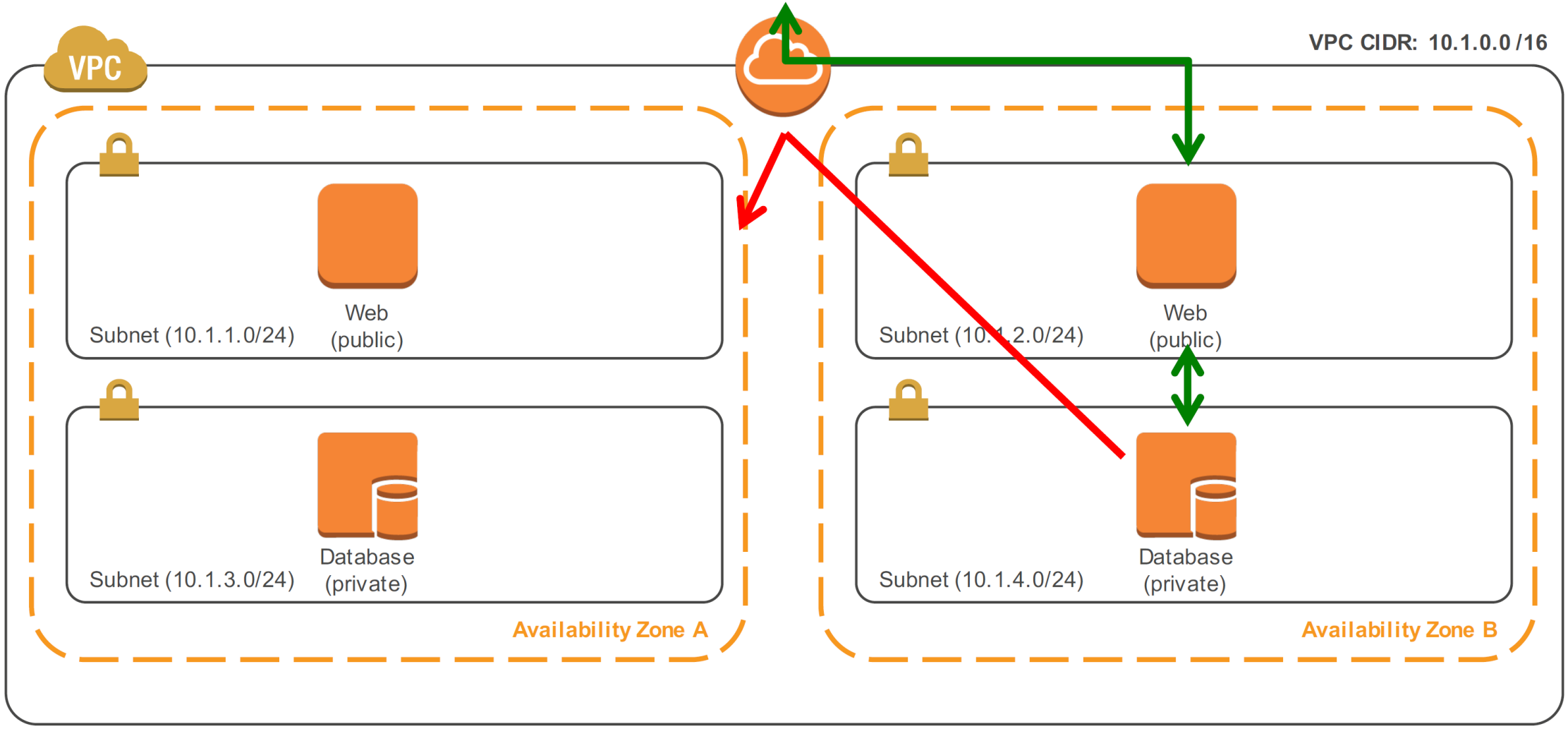
# Public Subnet Routing – Internet Gateway



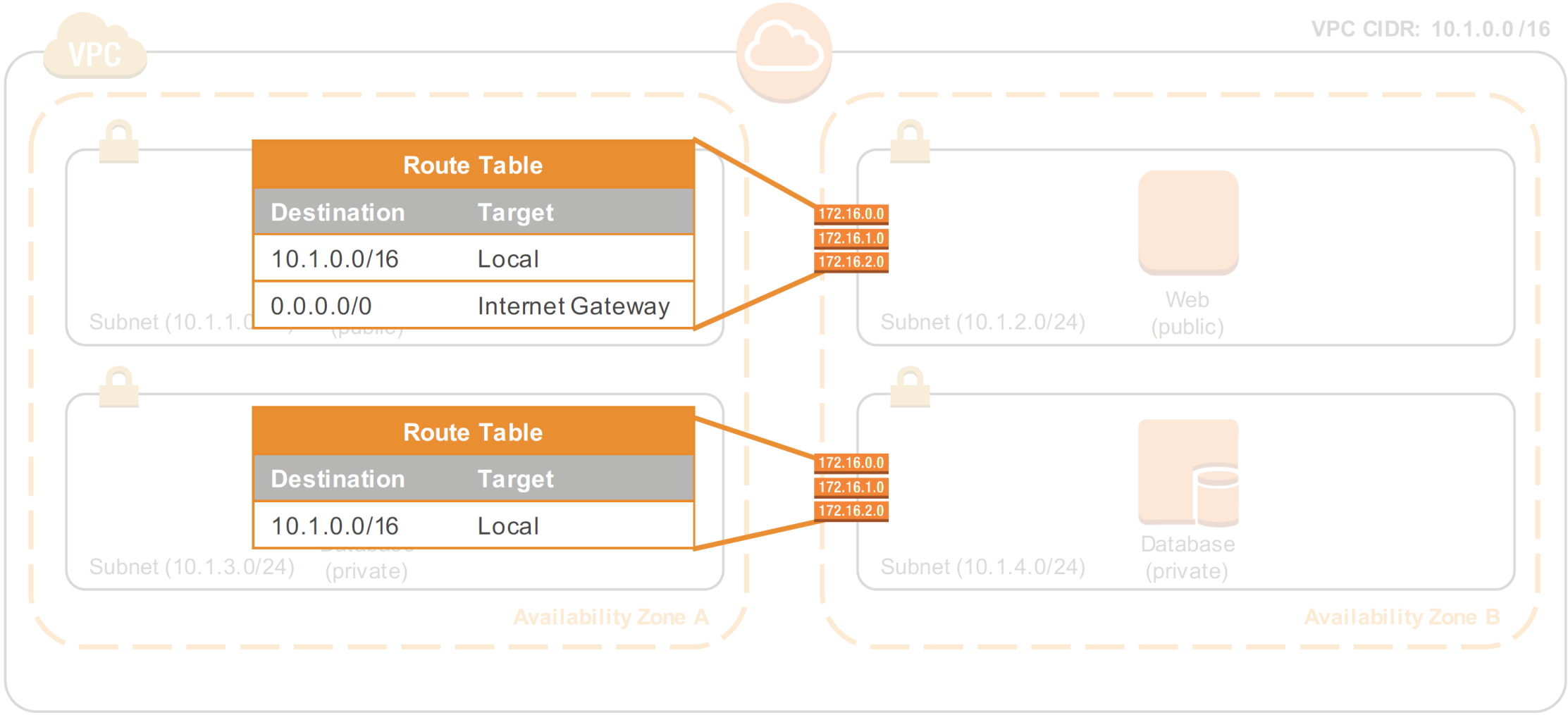
# Public Subnet Routing – Internet Gateway



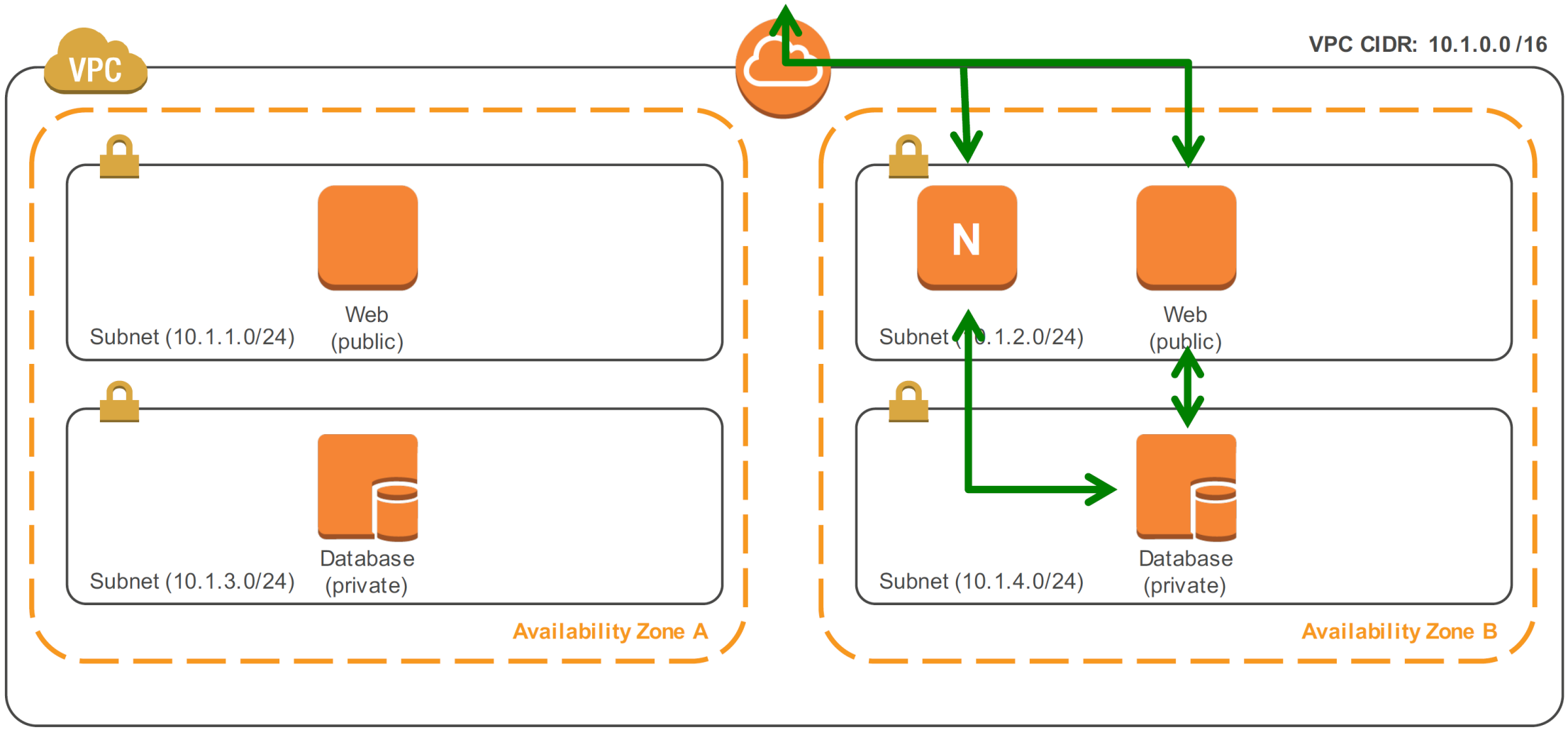
# Private Subnet Routing



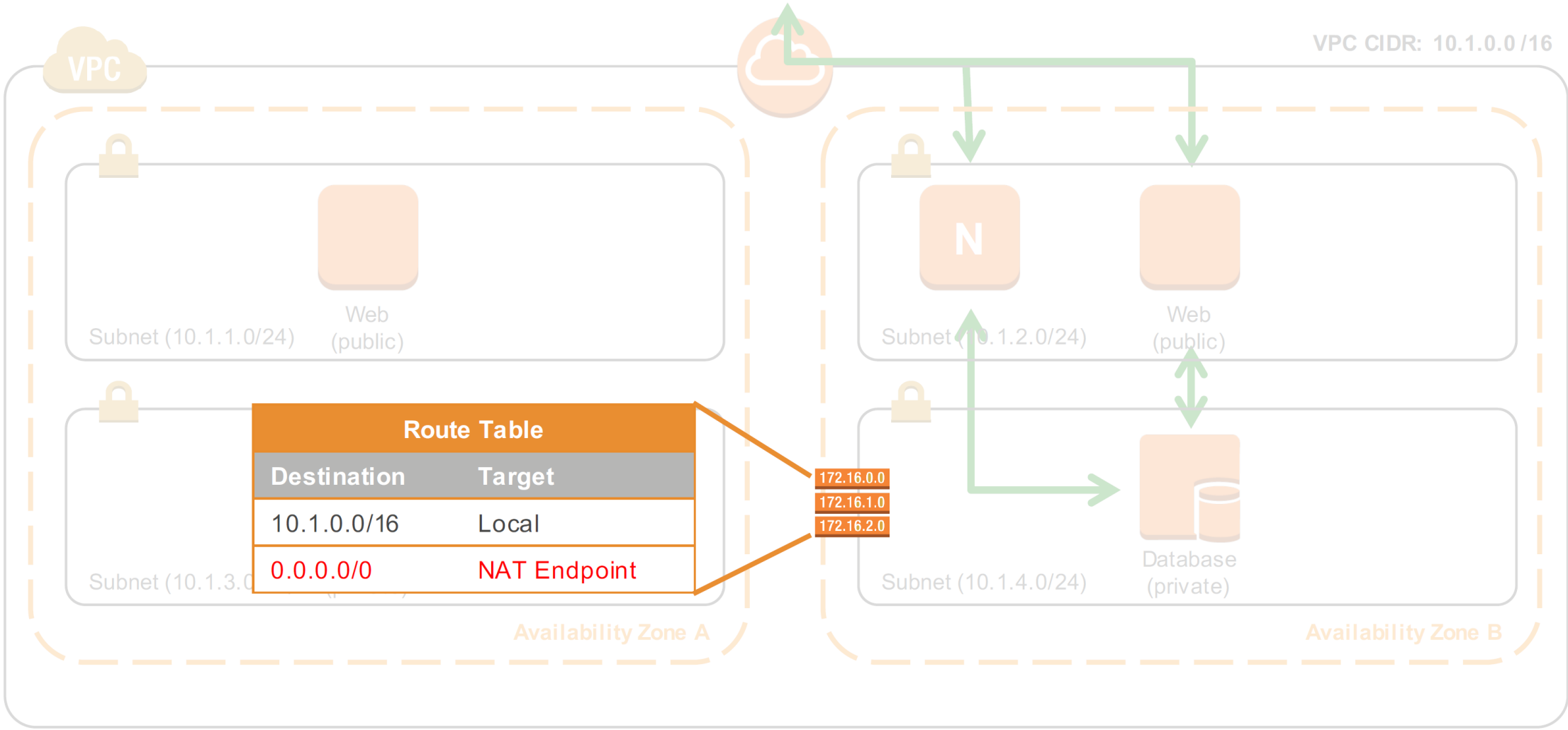
# Private Subnet Routing



# Private Subnet Routing – NAT Gateway



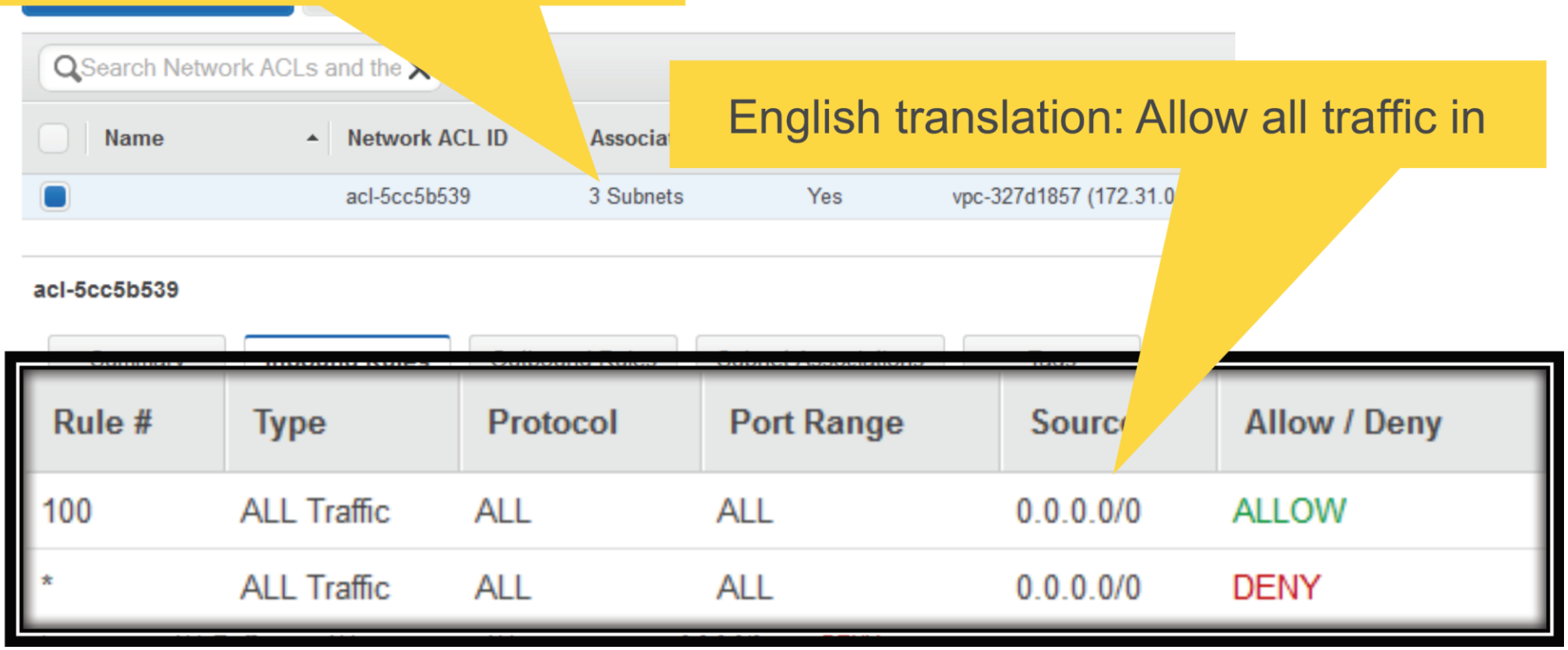
# Private Subnet Routing - NATGateway



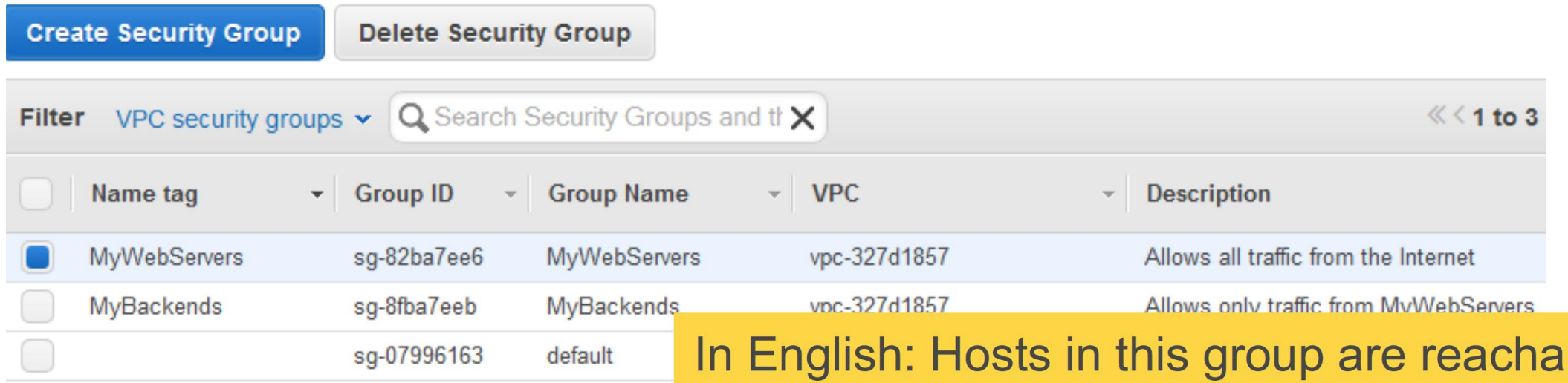
# Network ACLs = Stateless Firewall Rules

Can be applied on a subnet basis

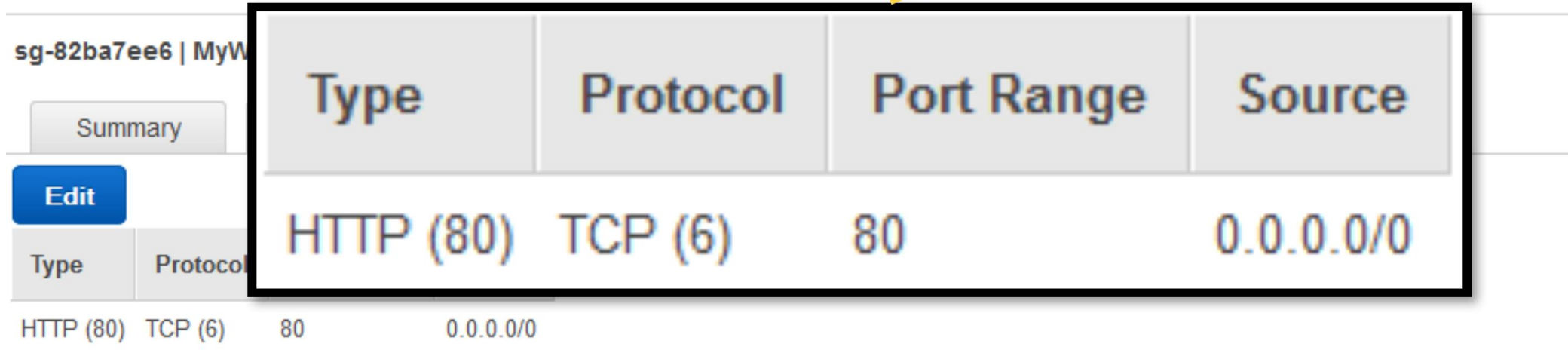
English translation: Allow all traffic in



# Security Groups = Stateful Firewall Rules

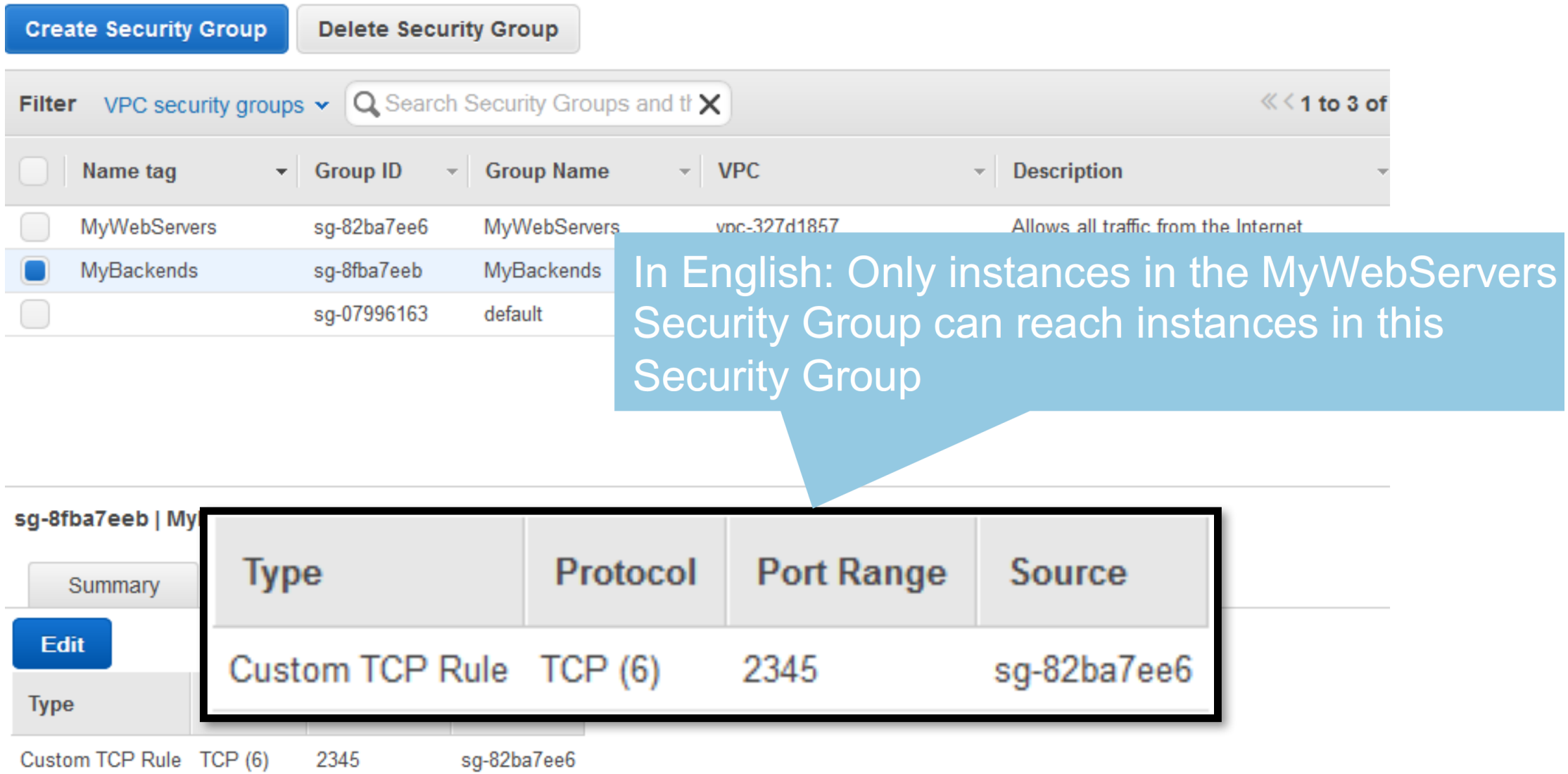



In English: Hosts in this group are reachable from the Internet on port 80 (HTTP)

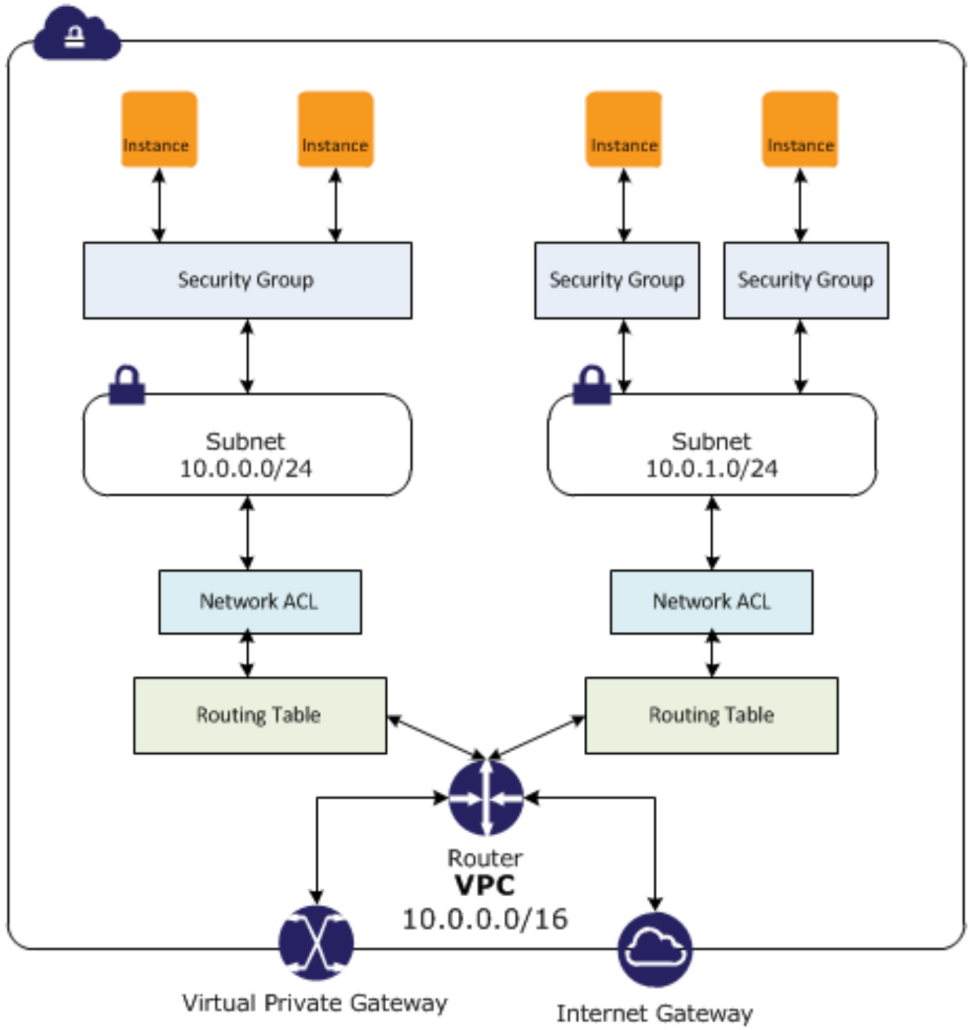



| Type | Protocol | Port Range | Source |
|---|---|---|---|
| HTTP (80) | TCP (6) | 80 | 0.0.0.0/0 |

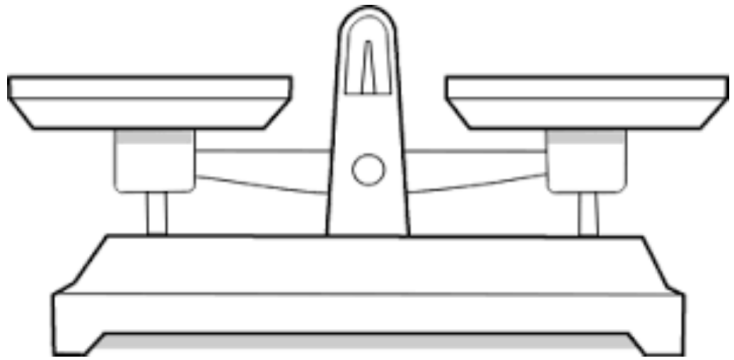
# Security Group Mutual Trust



# Security Balancing Act

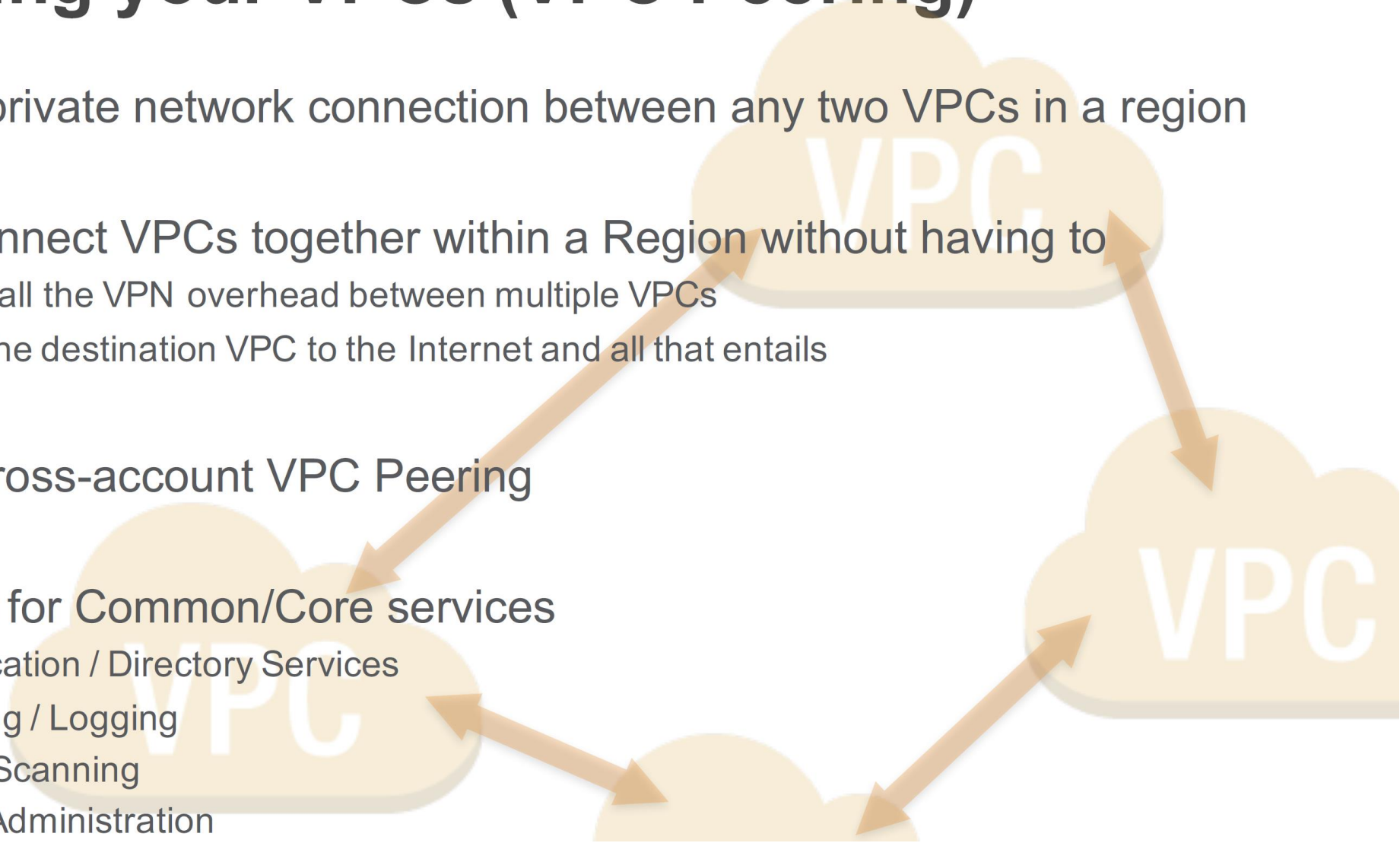



| Comparison between Security Groups and Network ACLs | | |
|---|---|---|
| **Area of Security** | **Security Group** | **Network ACL** |
| Operational Level | Instance level | Subnet level |
| Supports ALLOW rules… | …only | …and DENY rules |
| State Type | Stateful | Stateless |
| Evaluation method | All rules evaluated | Stop on first match |
| Applicability to Instances | Only if SG explicitly added to instance | Automatically to all instances in subnet |
| Source / Destination | IP CIDR and other Security Groups | IP CIDR only |



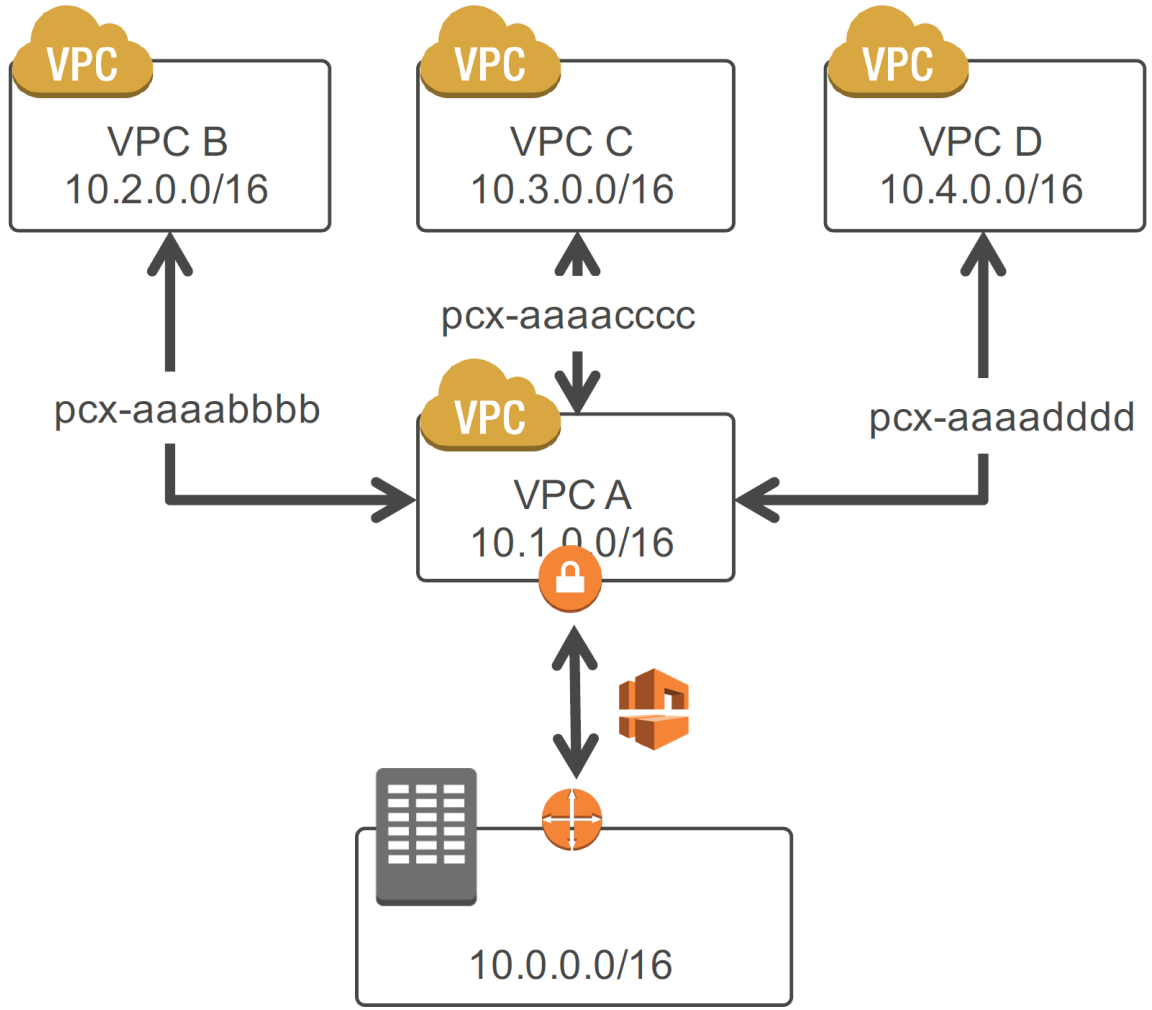
# Connecting your VPCs (VPC Peering)

- Creates a private network connection between any two VPCs in a region
- You can connect VPCs together within a Region without having to
  - Maintain all the VPN overhead between multiple VPCs
  - Expose the destination VPC to the Internet and all that entails
- Including cross-account VPC Peering
- Often used for Common/Core services
  - Authentication / Directory Services
  - Monitoring / Logging
  - Security Scanning
  - Remote Administration

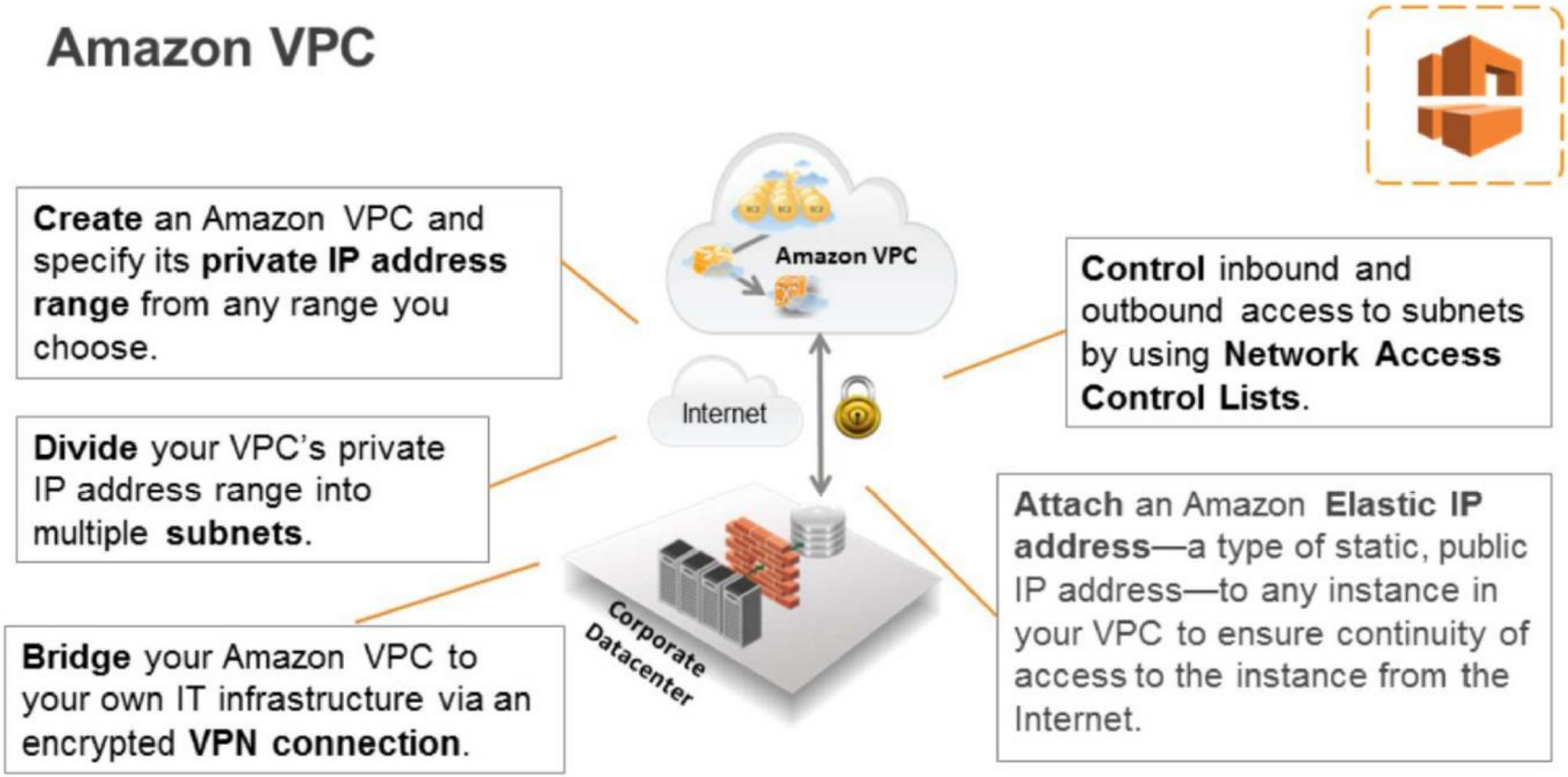


# Common Design – Shared Services VPC

- Move shared services such as Active Directory, Logging, Monitoring and Service Buses to a shared services VPC (A)
- None of the other VPCs can send traffic directly to each other – they must go through VPC A (= app isolation)
- Only VPC A has direct network access to your data center via Direct Connect
- Routing Tables define which subnets are allowed to route over a peer connection
- Security Groups and NACLs still apply, and Security Groups in VPC A can be defined to mutually trust the Security Groups in the other VPCs



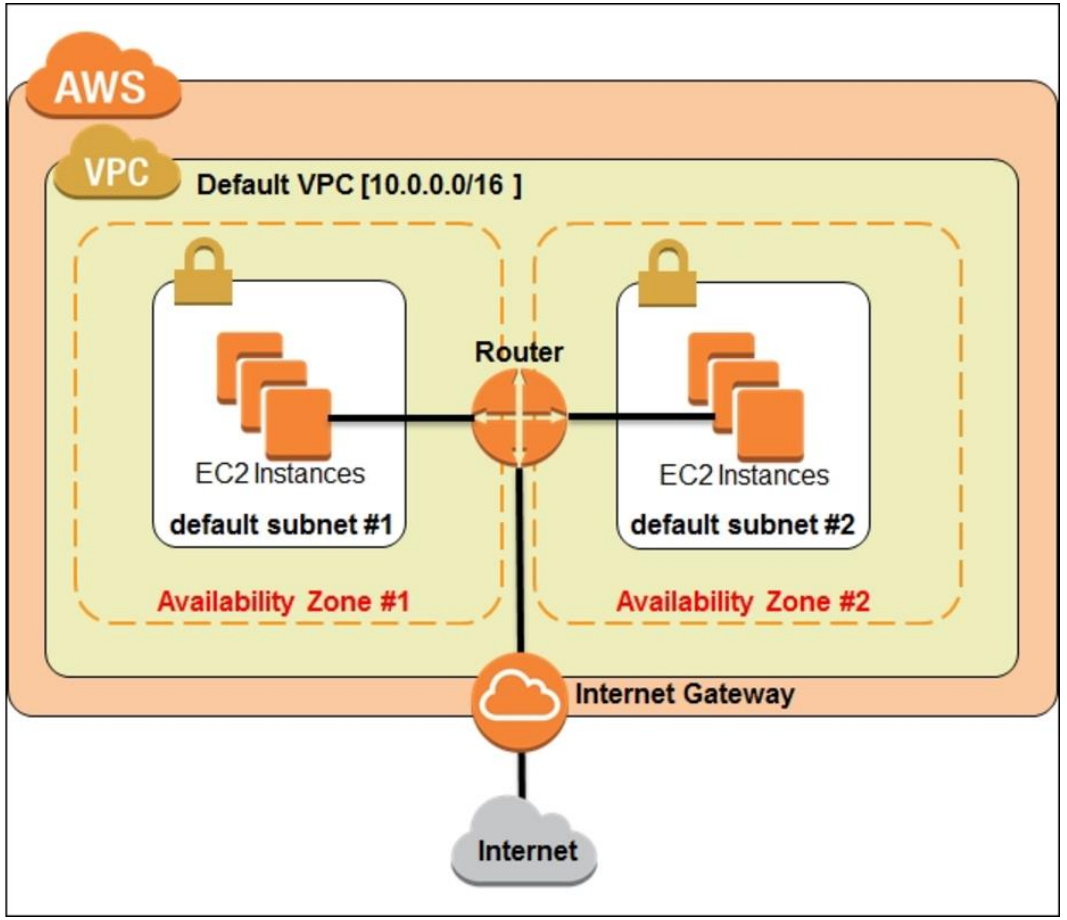
# VPC and an Enterprise Data Center



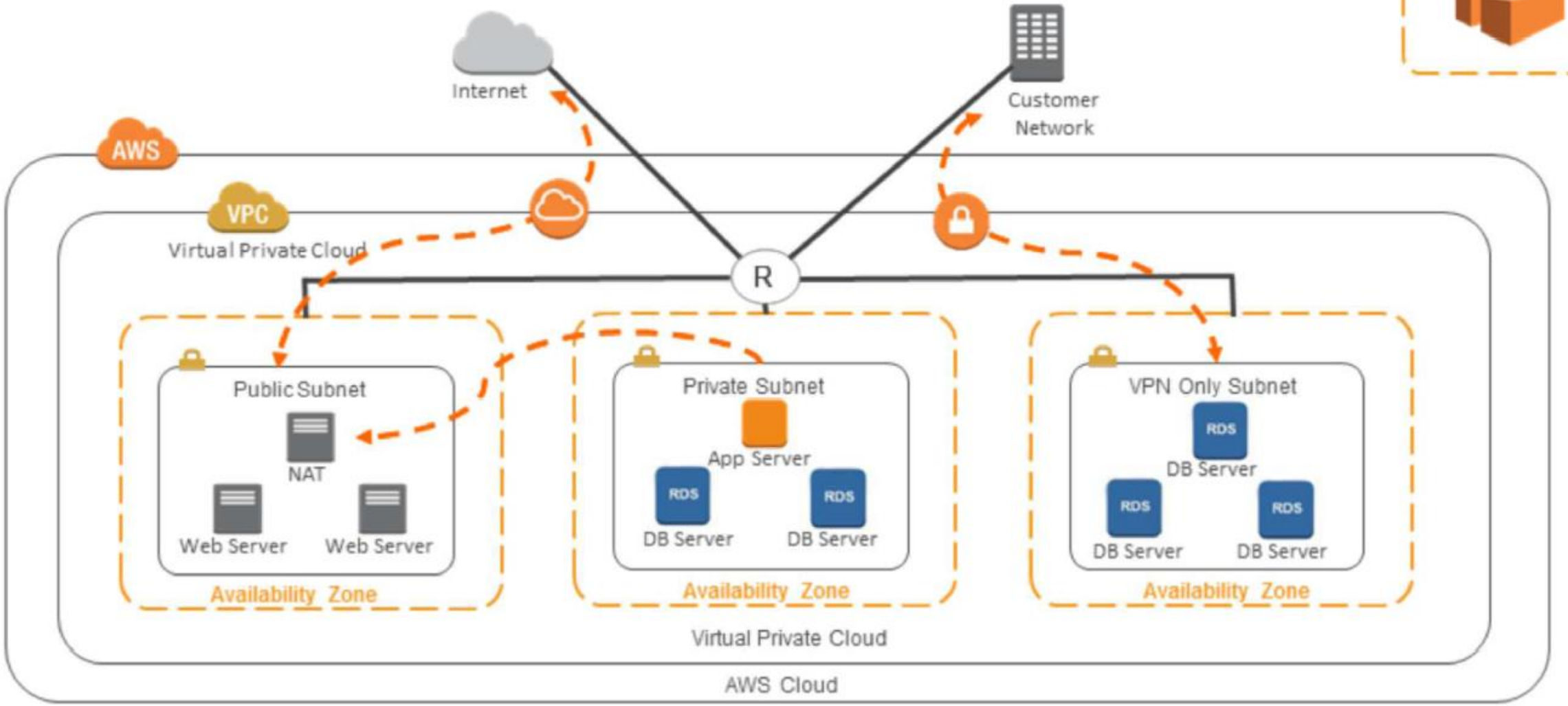
# Default VPC Key Concepts

- Subnets ~ a range of valid IP addresses that you specify
  - Private
  - Public

- The default VPC is always created with a CIDR block of /16, which means it supports 65,536 IP addresses in it.
- A default subnet is created in each AZ of your selected region. Instances launched in these default subnets have both a public and a private IP address by default as well.
- An Internet Gateway is provided to the default VPC for instances to have Internet connectivity.
- A few necessary route tables, security groups, and ACLs are also created by default that enable the instance traffic to pass through to the Internet.



# Amazon VPC Example



# To be seen

- VPC
  - https://www.youtube.com/watch?v=jcyZmj6Ywh4 (6:32)
- IAM
  - https://www.youtube.com/watch?v=Z4U5ymvEvKc

# Homework VPC

- http://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/ExerciseOverview.html

# Assignment

- Create a new VPC (LabVPC), with 2 subnets, an internet gateway to allow traffic from the internet.
- Manually create a routing tables and associate them to your subnets
- Manually create a NAT EC2 instance inside your public subnet, and an Lunix instance inside your private subject
- Make sure your you can connect to your private instance via the NAT Instance