

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

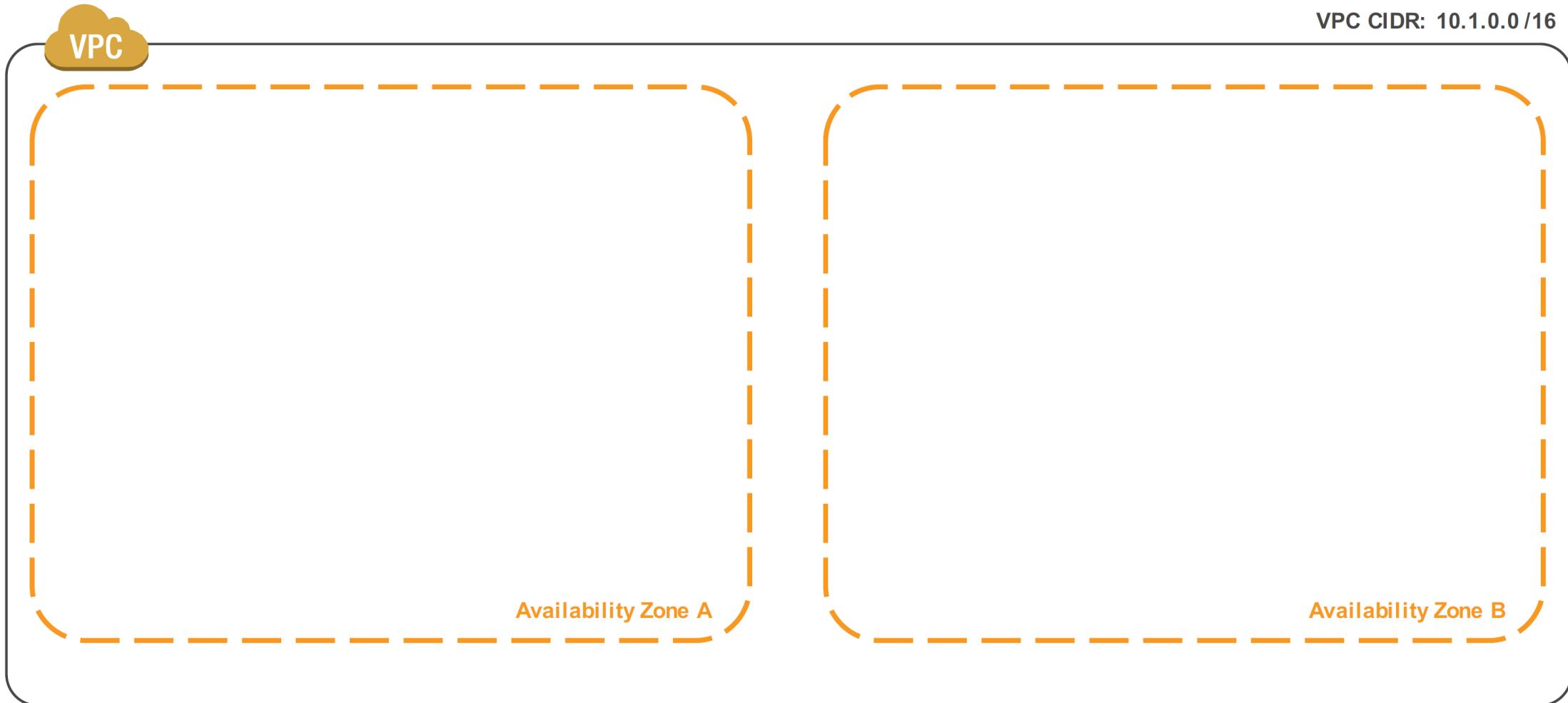


Virtual Private Gateway - The Amazon end of a VPN connection

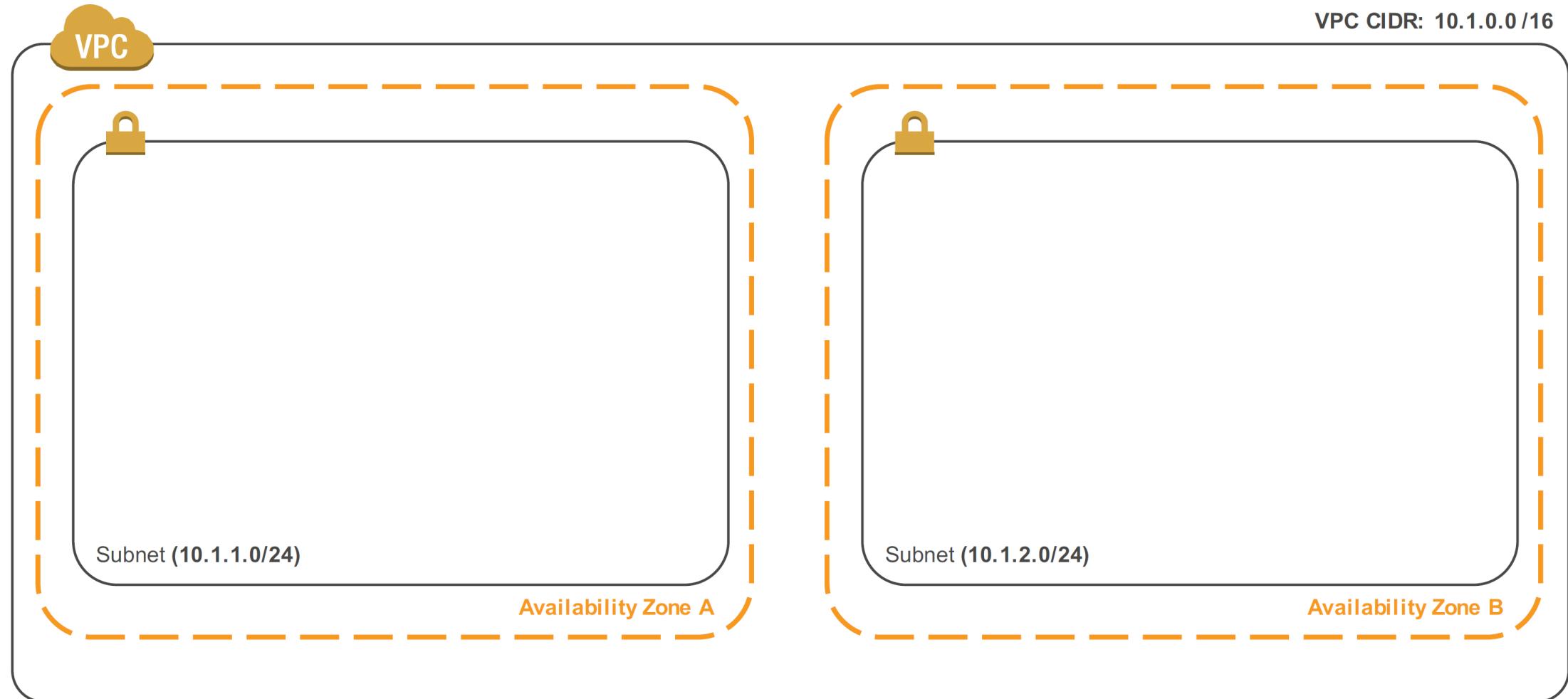


Customer Gateway - The router at the customer end of a VPN connection

VPCs span an entire region



Subnets sit in a single VPC in a single AZ

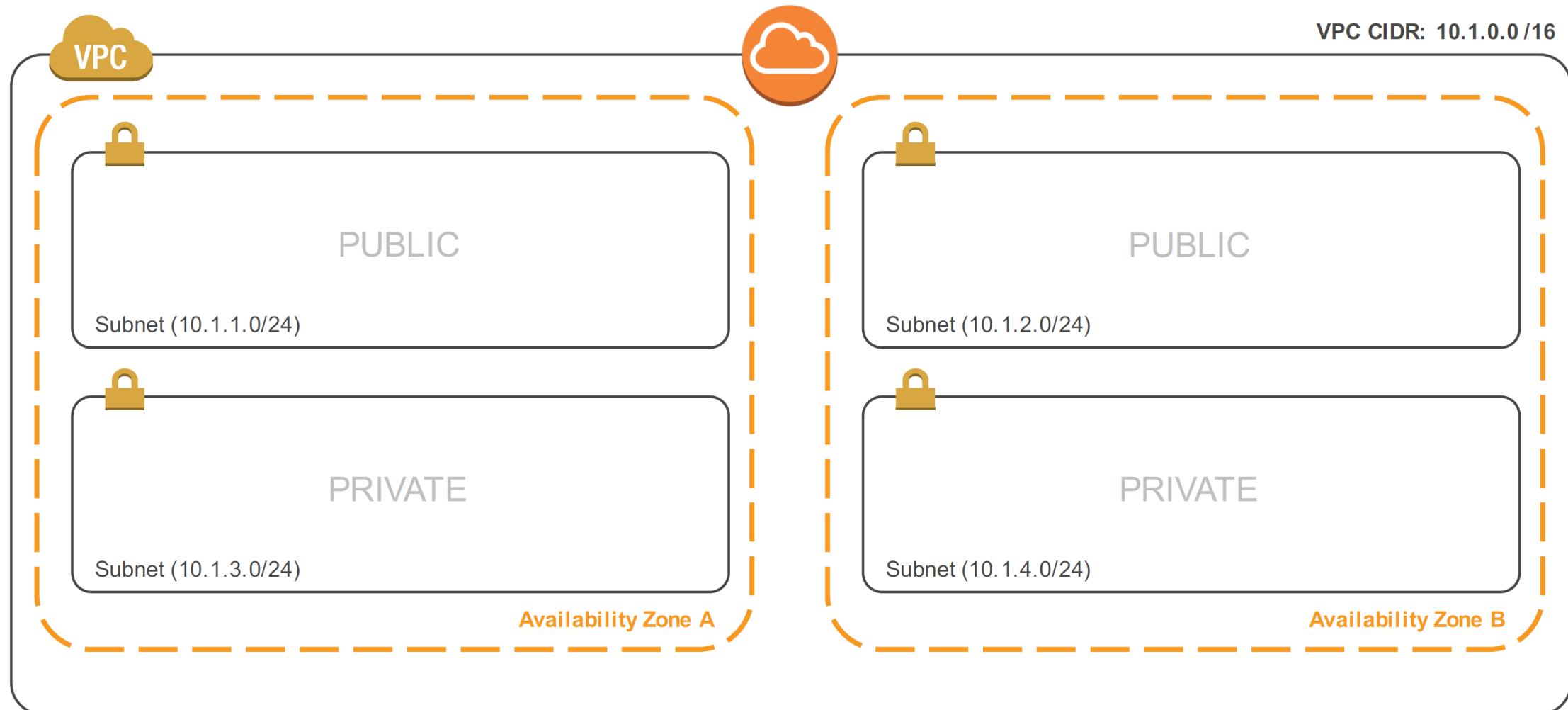


Plan your VPC IP space before creating it

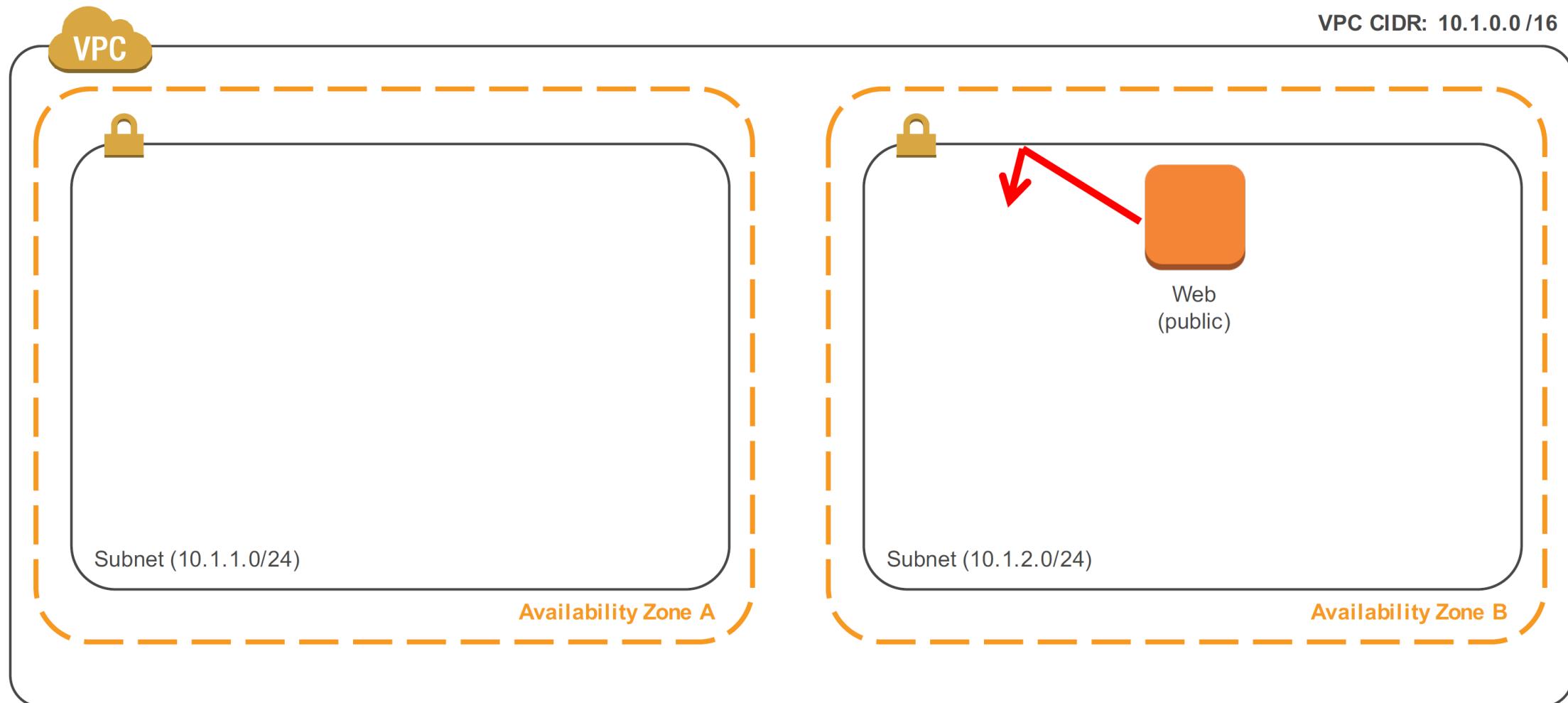


- Consider future AWS region expansion
- Consider future connectivity to your internal networks
- Consider subnet design
- VPC can be /16 down to /28
- CIDR cannot be modified after creation

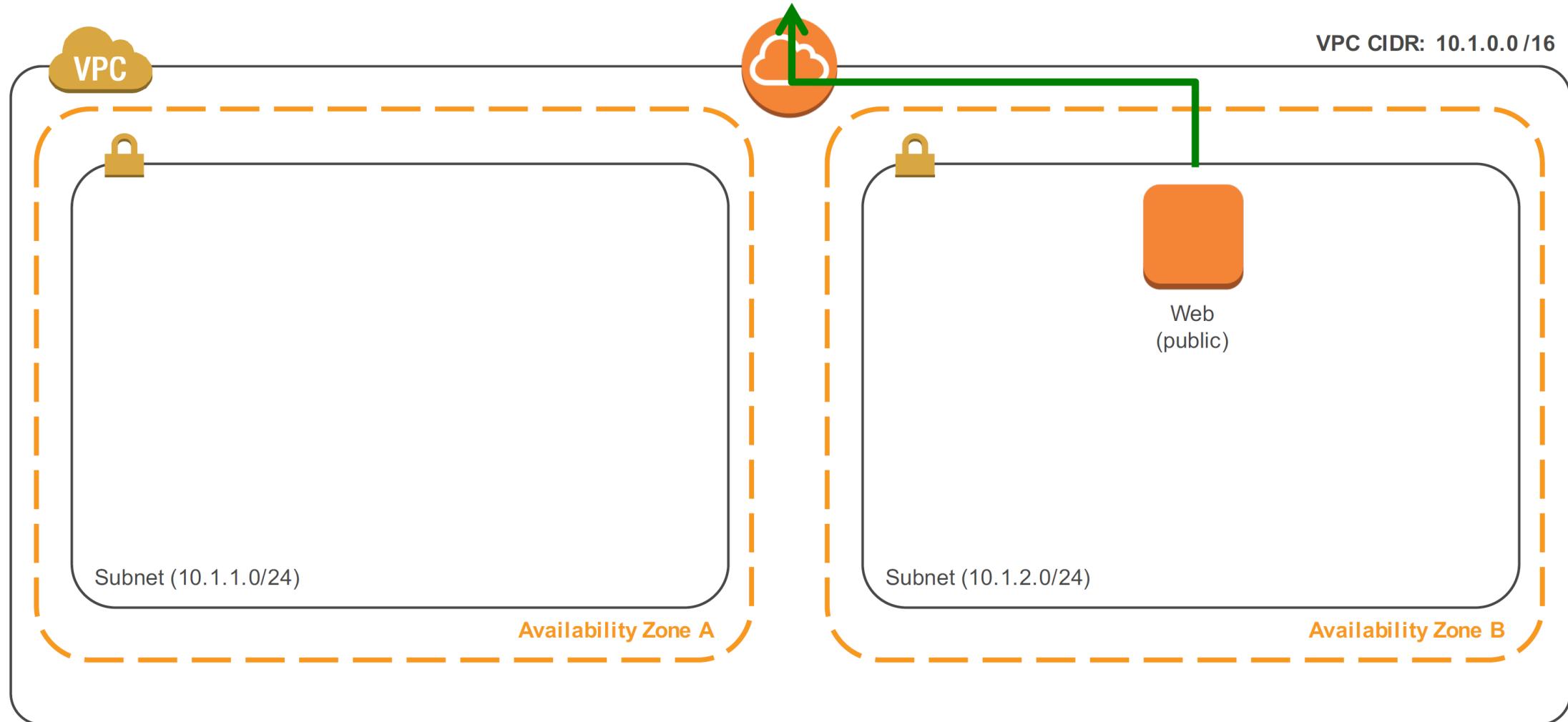
Public / Private Subnets



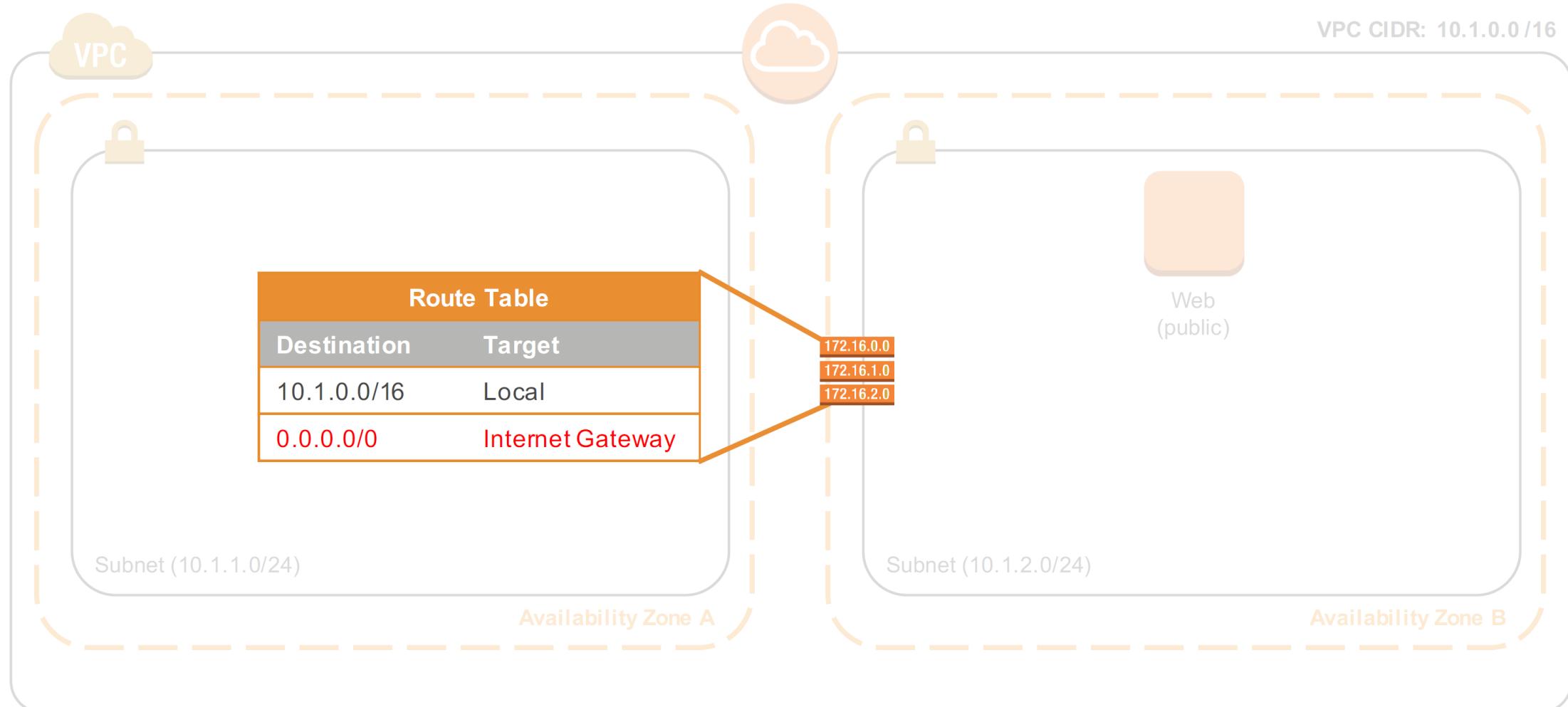
Public Subnet Routing



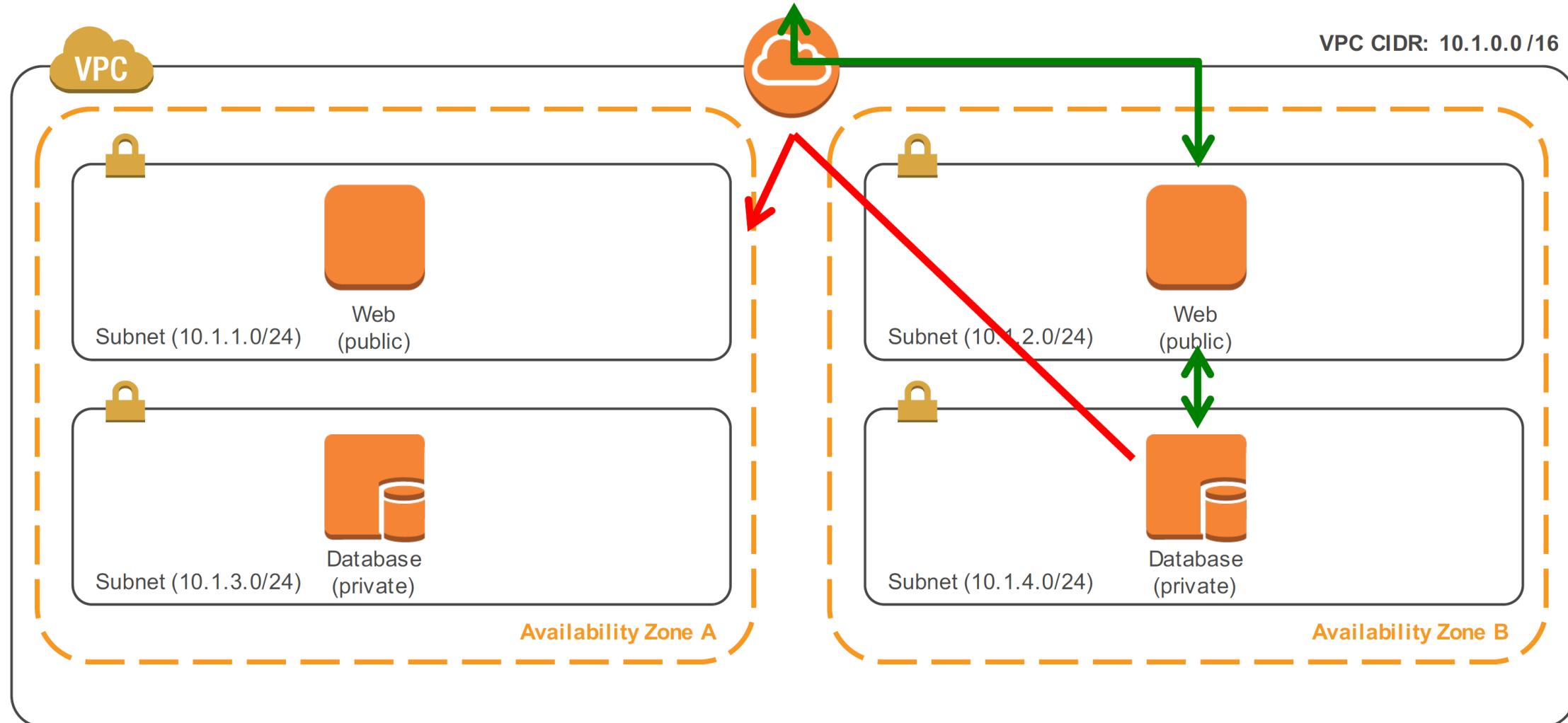
Public Subnet Routing – Internet Gateway



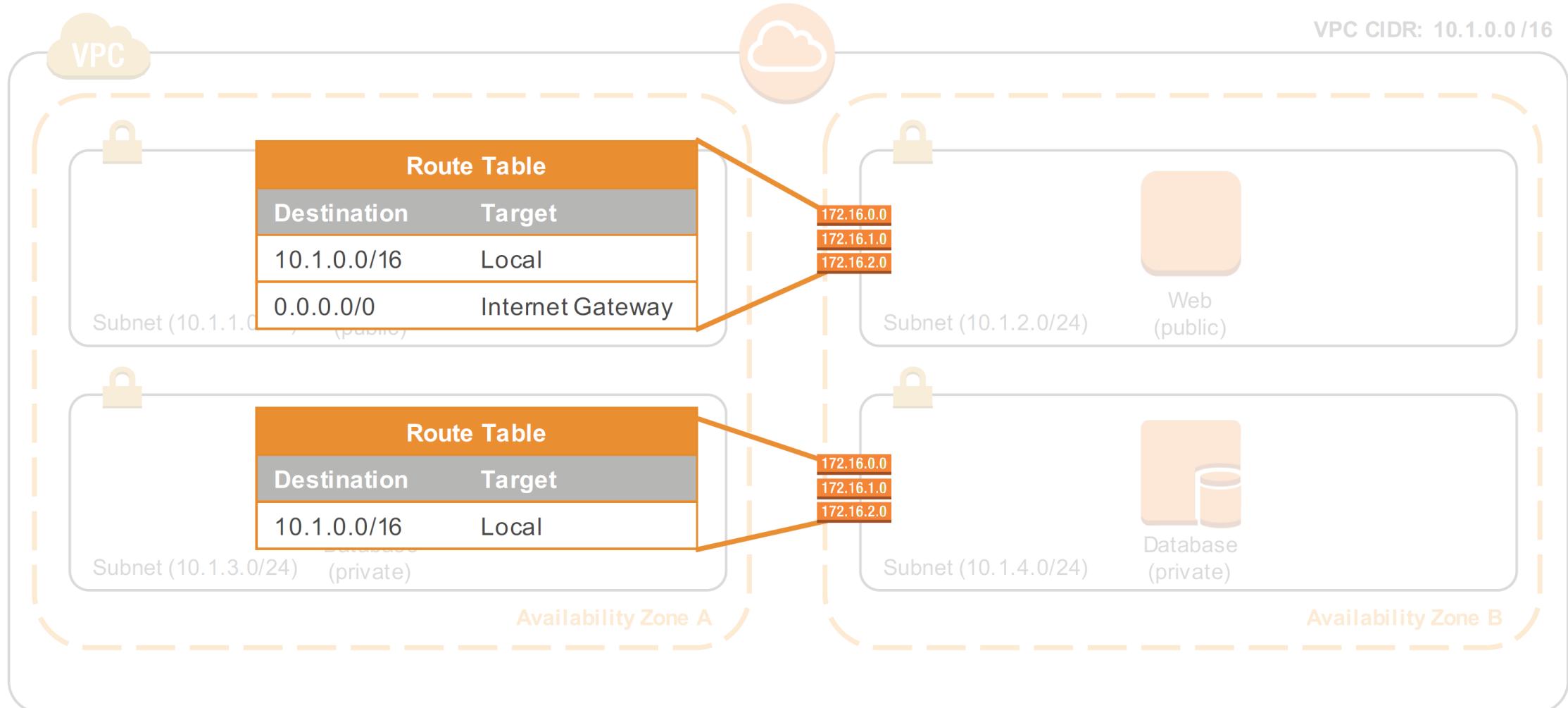
Public Subnet Routing – Internet Gateway



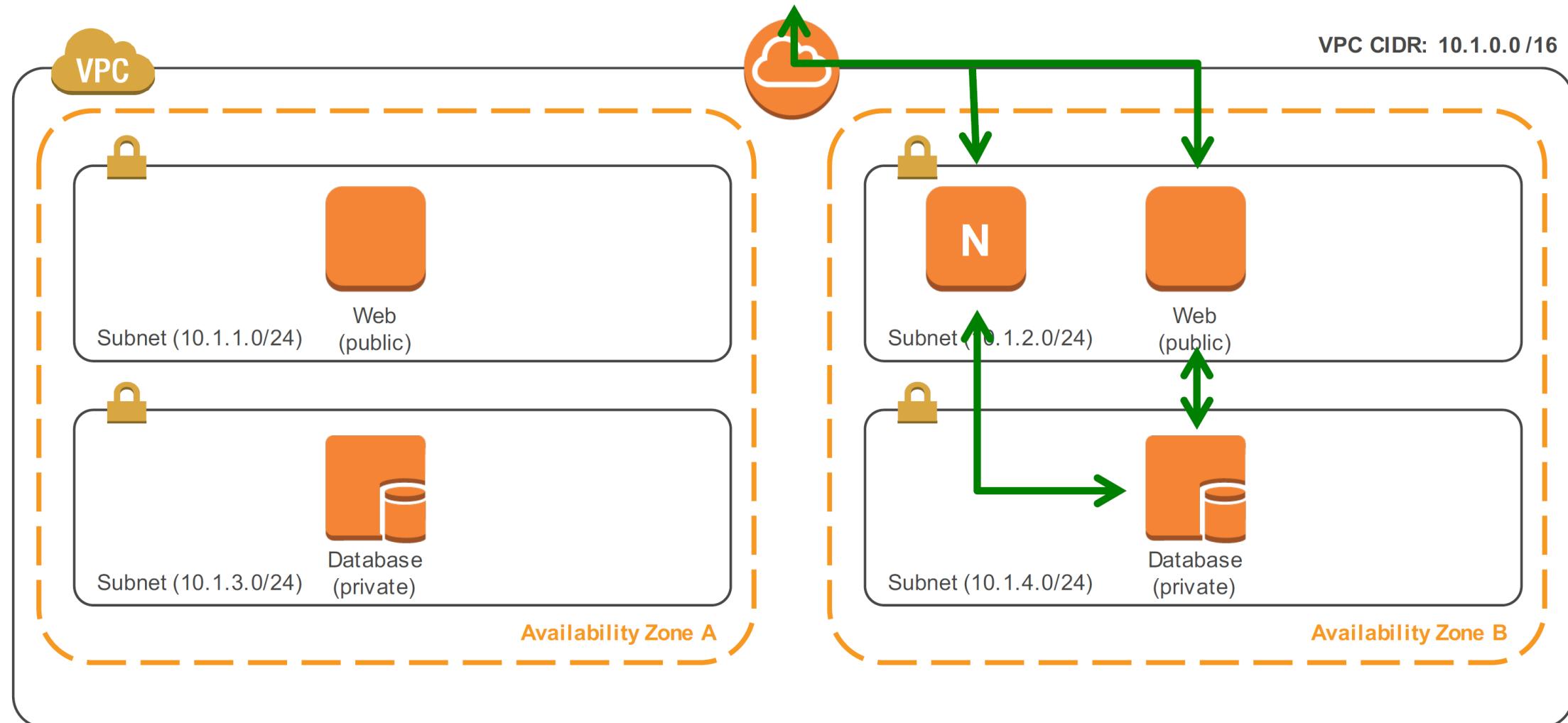
Private Subnet Routing



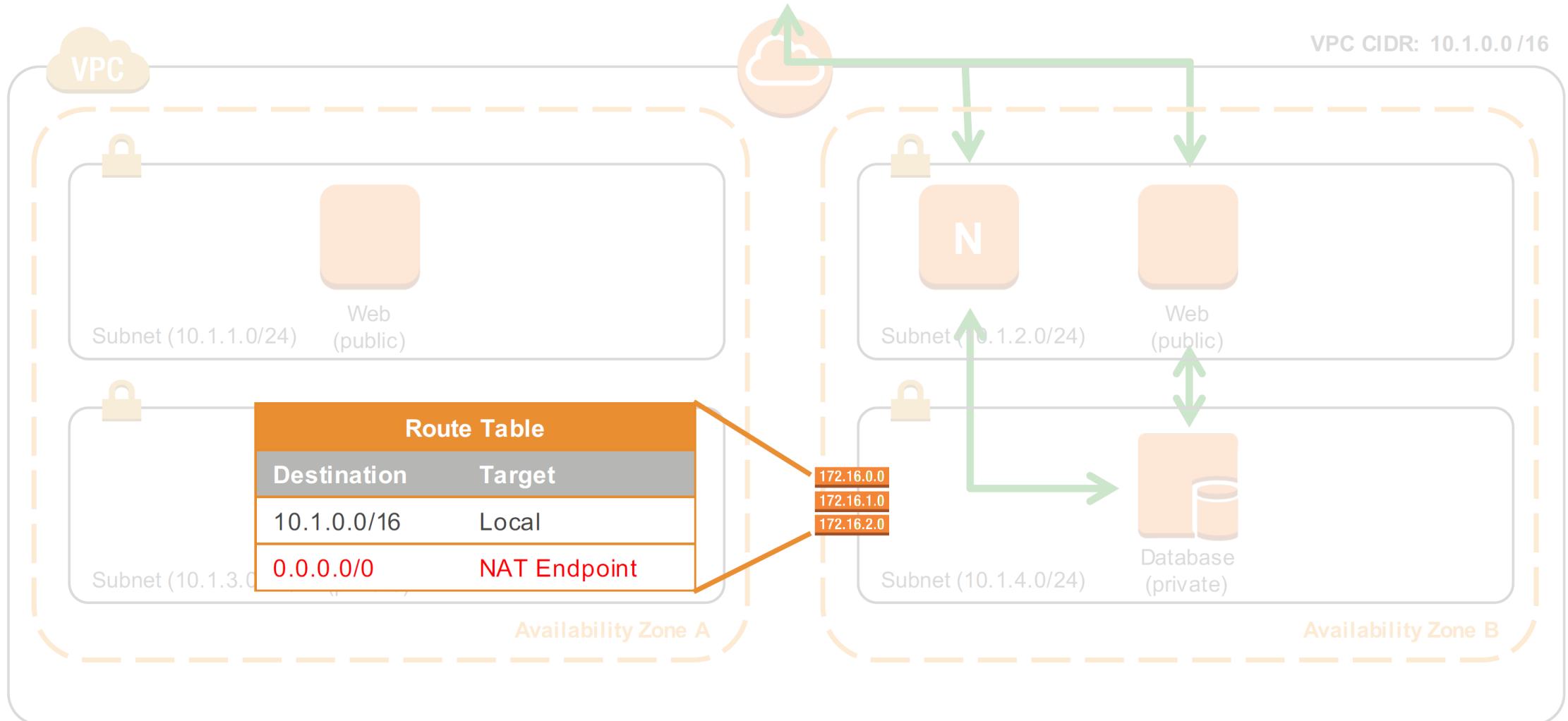
Private Subnet Routing



Private Subnet Routing – NAT Gateway



Private Subnet Routing - NATGateway



Network ACLs = Stateless Firewall Rules

Can be applied on a subnet basis

The screenshot shows the AWS Network ACLs interface. At the top, there's a search bar with placeholder text "Search Network ACLs and the X". Below it is a table with columns: Name, Network ACL ID, Associated VPC, Subnets, and Status. One row is selected, showing "acl-5cc5b539", "vpc-327d1857 (172.31.0)", "3 Subnets", and "Yes". A yellow arrow points from the "Can be applied on a subnet basis" text to this row. To the right of the table, another yellow box contains the text "English translation: Allow all traffic in". Below the table, under the heading "acl-5cc5b539", is a detailed view of the rules. It has a table with columns: Rule #, Type, Protocol, Port Range, Source, and Allow / Deny. Two rows are listed: Rule #100 with Type "ALL Traffic", Protocol "ALL", Port Range "ALL", Source "0.0.0.0/0", and Allow/Deny "ALLOW"; and a wildcard rule "*" with the same parameters, Allow/Deny "DENY". This table is also highlighted with a black border.

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

Security Groups = Stateful Firewall Rules

Create Security Group Delete Security Group

Filter VPC security groups X « < 1 to 3

<input type="checkbox"/>	Name tag	Group ID	Group Name	VPC	Description
<input checked="" type="checkbox"/>	MyWebServers	sg-82ba7ee6	MyWebServers	vpc-327d1857	Allows all traffic from the Internet
<input type="checkbox"/>	MyBackends	sg-8fba7eeb	MyBackends	vpc-327d1857	Allows only traffic from MyWebServers
<input type="checkbox"/>		sg-07996163	default		

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

sg-82ba7ee6 | MyWebServers

Summary Edit

Type Protocol

HTTP (80) TCP (6) 80 0.0.0.0/0

Security Group Mutual Trust

Create Security Group Delete Security Group

Filter VPC security groups « < 1 to 3 of »

<input type="checkbox"/>	Name tag	Group ID	Group Name	VPC	Description
<input type="checkbox"/>	MyWebServers	sg-82ba7ee6	MyWebServers	vpc-327d1857	Allows all traffic from the Internet
<input checked="" type="checkbox"/>	MyBackends	sg-8fba7eeb	MyBackends		
<input type="checkbox"/>		sg-07996163	default		

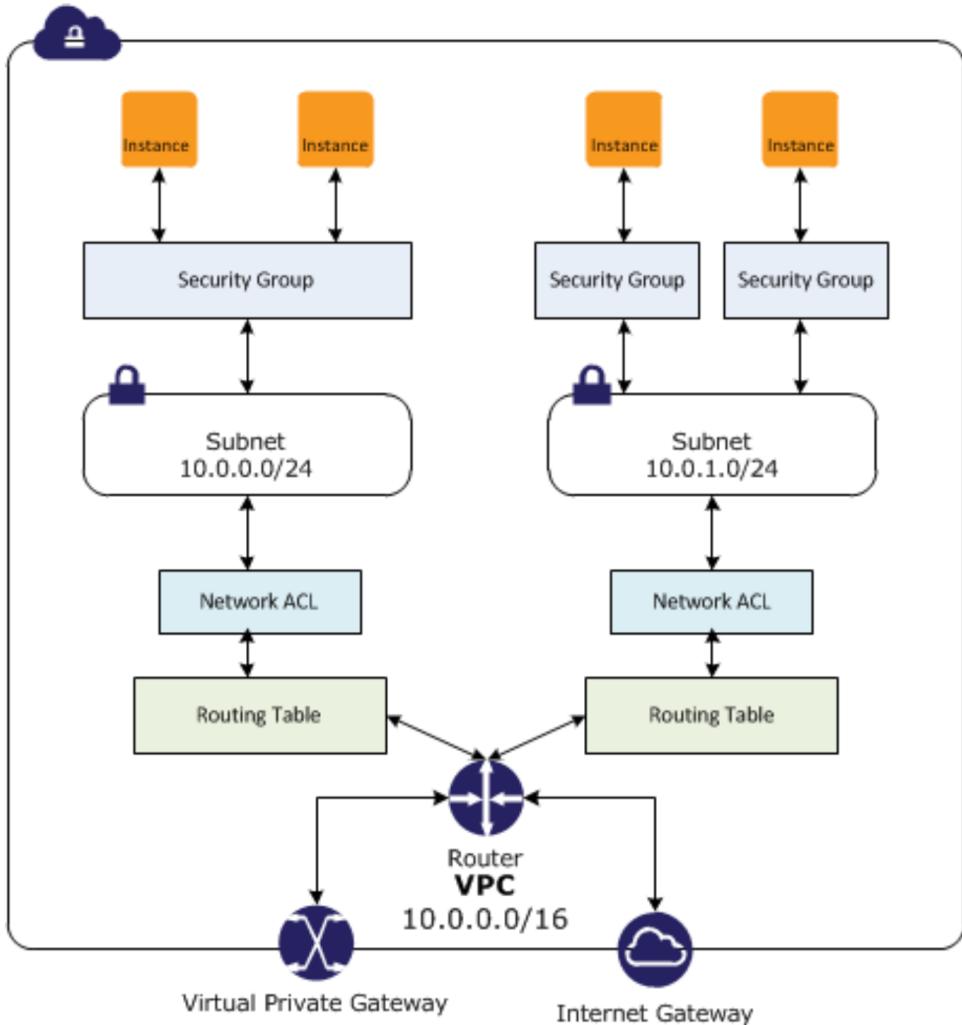
In English: Only instances in the MyWebServers Security Group can reach instances in this Security Group

sg-8fba7eeb | MyBackends

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP (6)	2345	sg-82ba7ee6

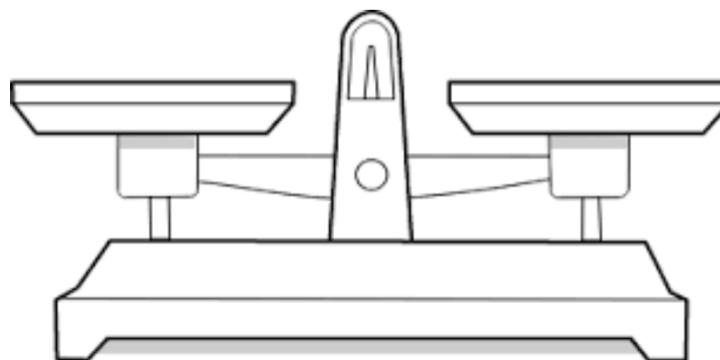
Custom TCP Rule TCP (6) 2345 sg-82ba7ee6

Security Balancing Act



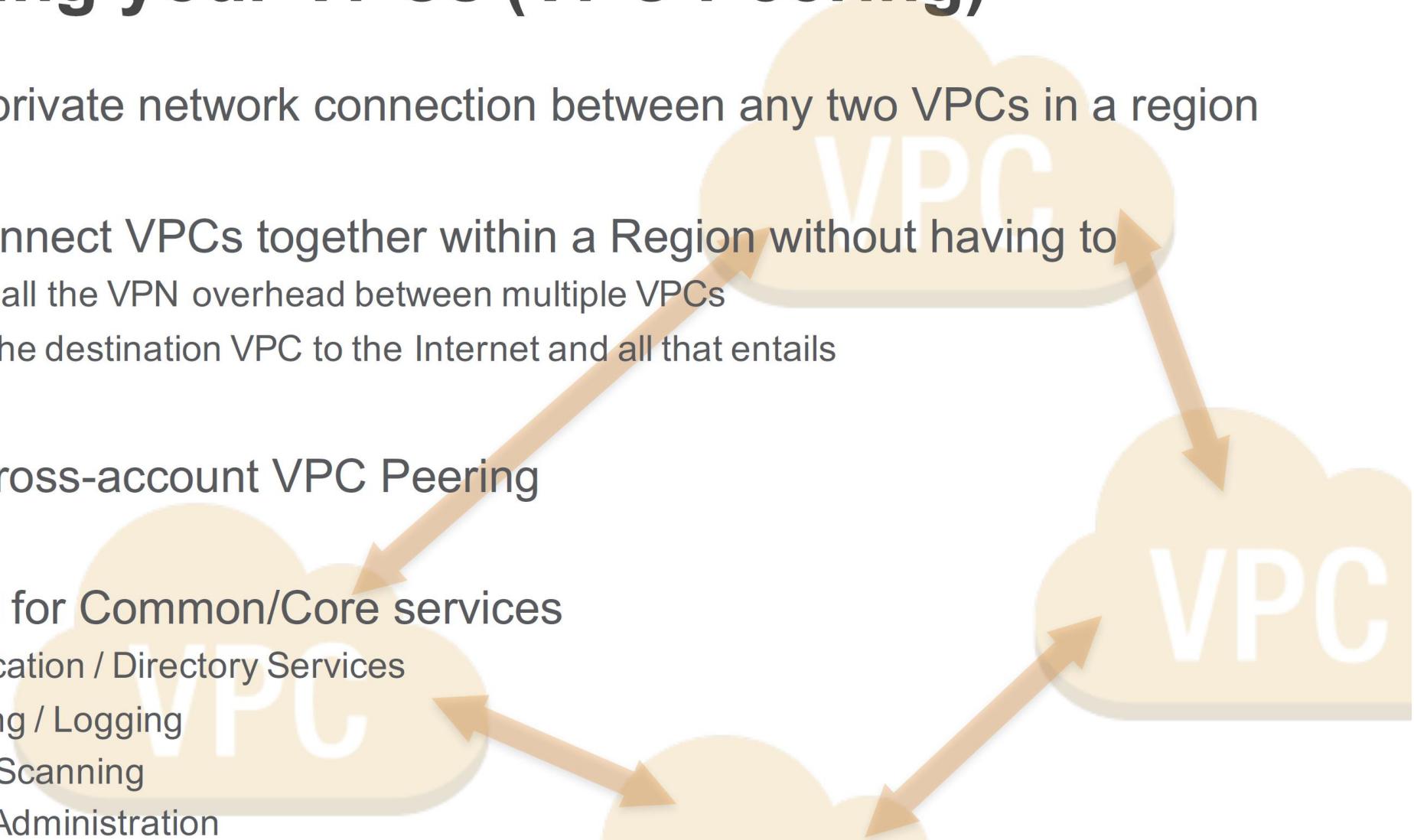
Comparison between Security Groups and Network ACLs

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



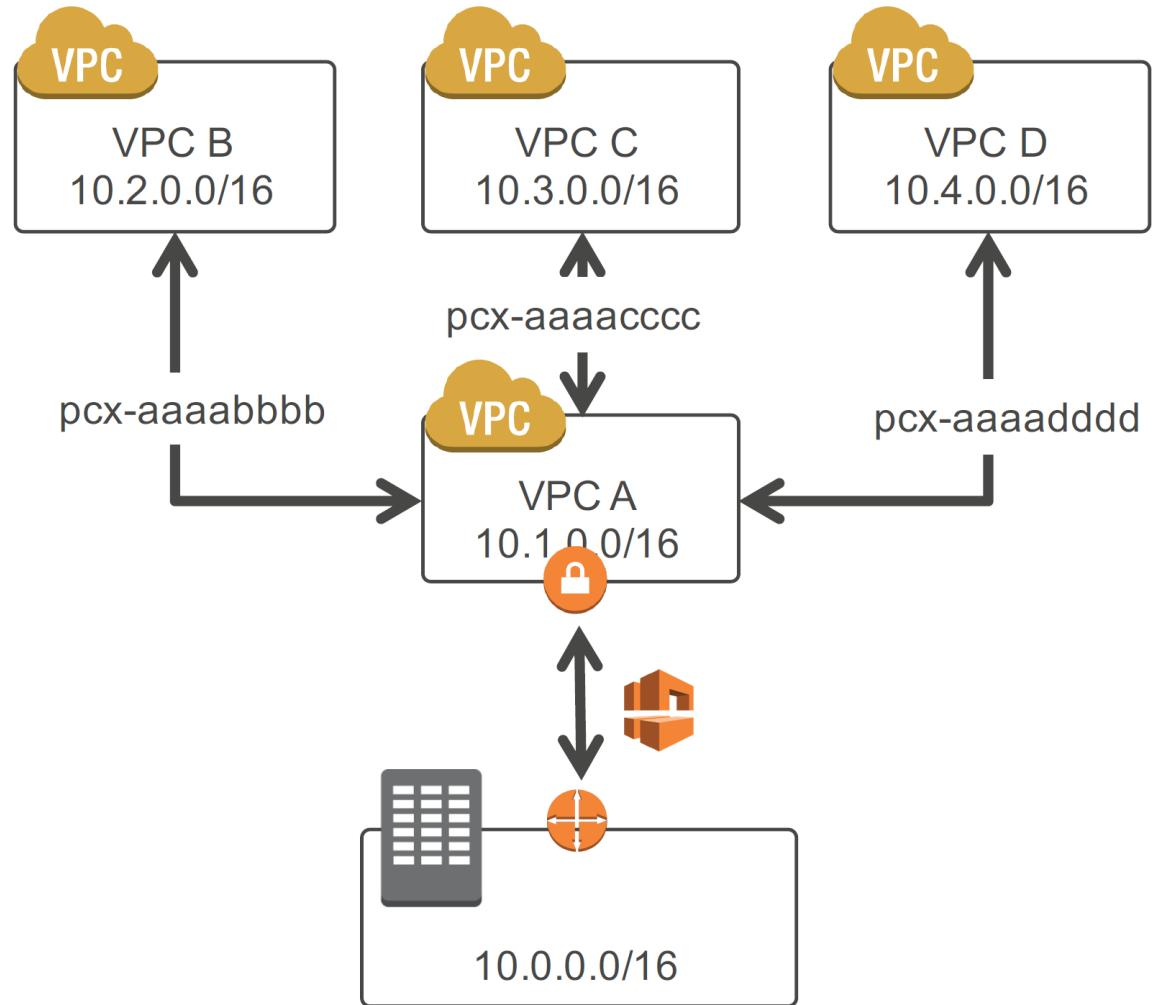
Connecting your VPCs (VPC Peering)

- 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

Amazon VPC

Create an Amazon VPC and specify its **private IP address range** from any range you choose.

Divide your VPC's private IP address range into multiple **subnets**.

Bridge your Amazon VPC to your own IT infrastructure via an encrypted **VPN connection**.



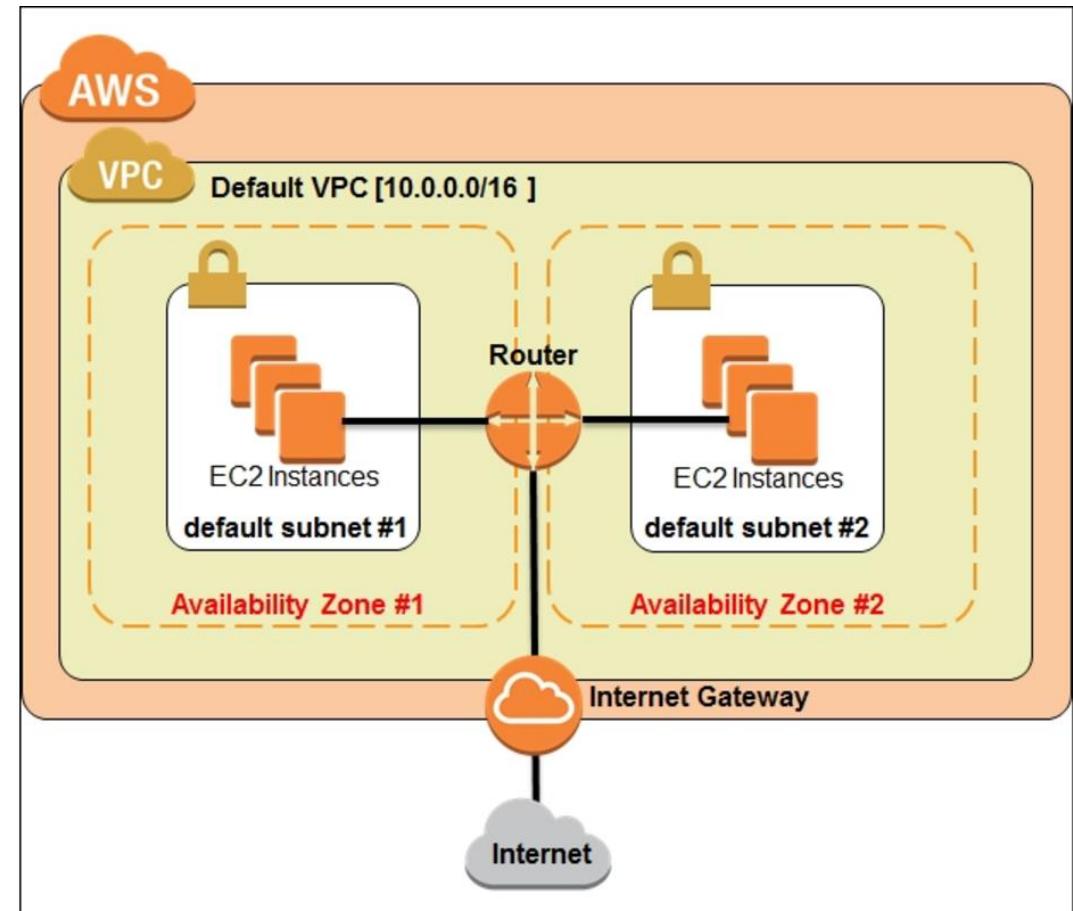
Control inbound and outbound access to subnets by using **Network Access Control Lists**.

Attach an Amazon **Elastic IP address**—a type of static, public IP address—to any instance in your VPC to ensure continuity of access to the instance from the Internet.

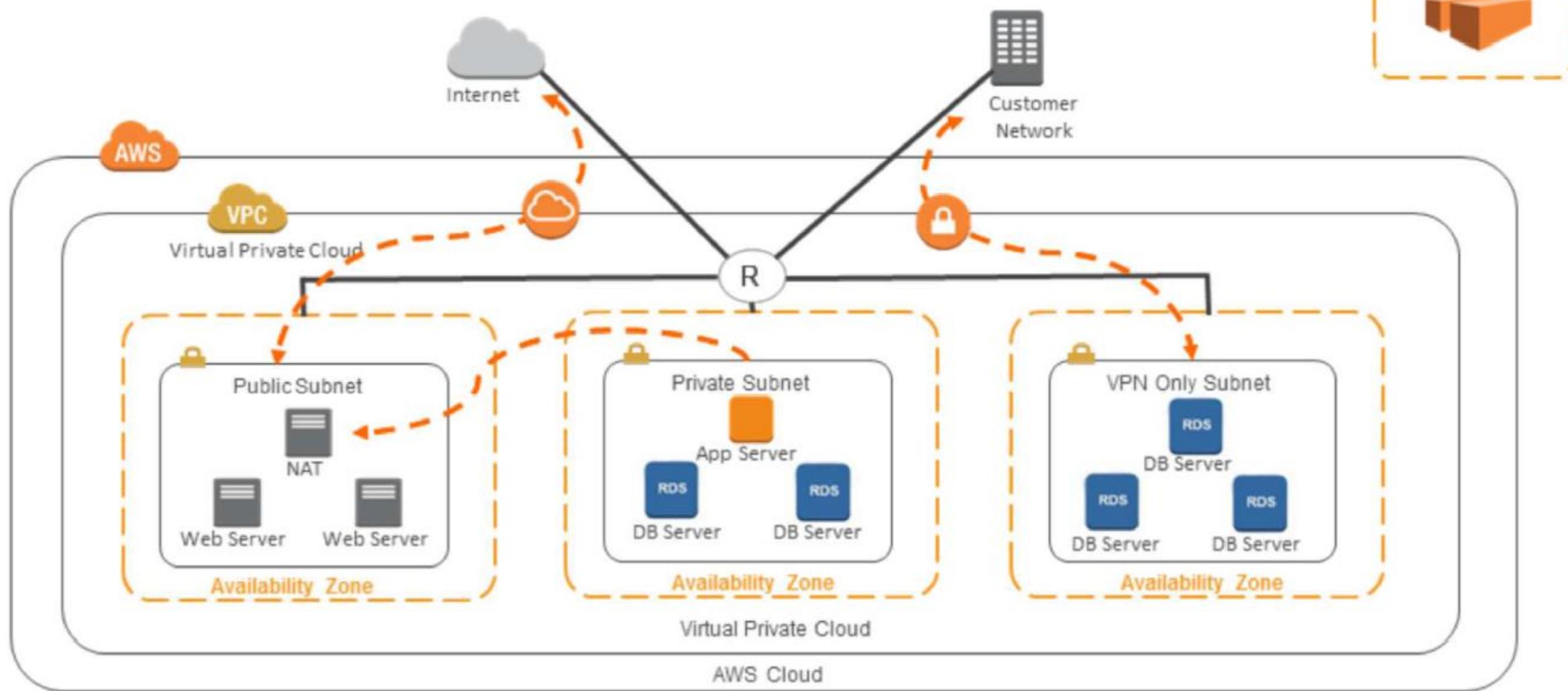


Default VPC Key Concepts

- 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 Linux instance inside your private subject
- Make sure your you can connect to your private instance via the NAT Instance

