

Cloud Networking



WORKFORCE DEVELOPMENT

Content Usage Parameters

Content refers to material including instructor guides, student guides, lab guides, lab or hands-on activities, computer programs, etc. designed for use in a training program

1

Content is subject to copyright protection

2

Content may only be leveraged by students enrolled in the training program

3

Students agree not to reproduce, make derivative works of, distribute, publicly perform and publicly display content in any form or medium outside of the training program

4

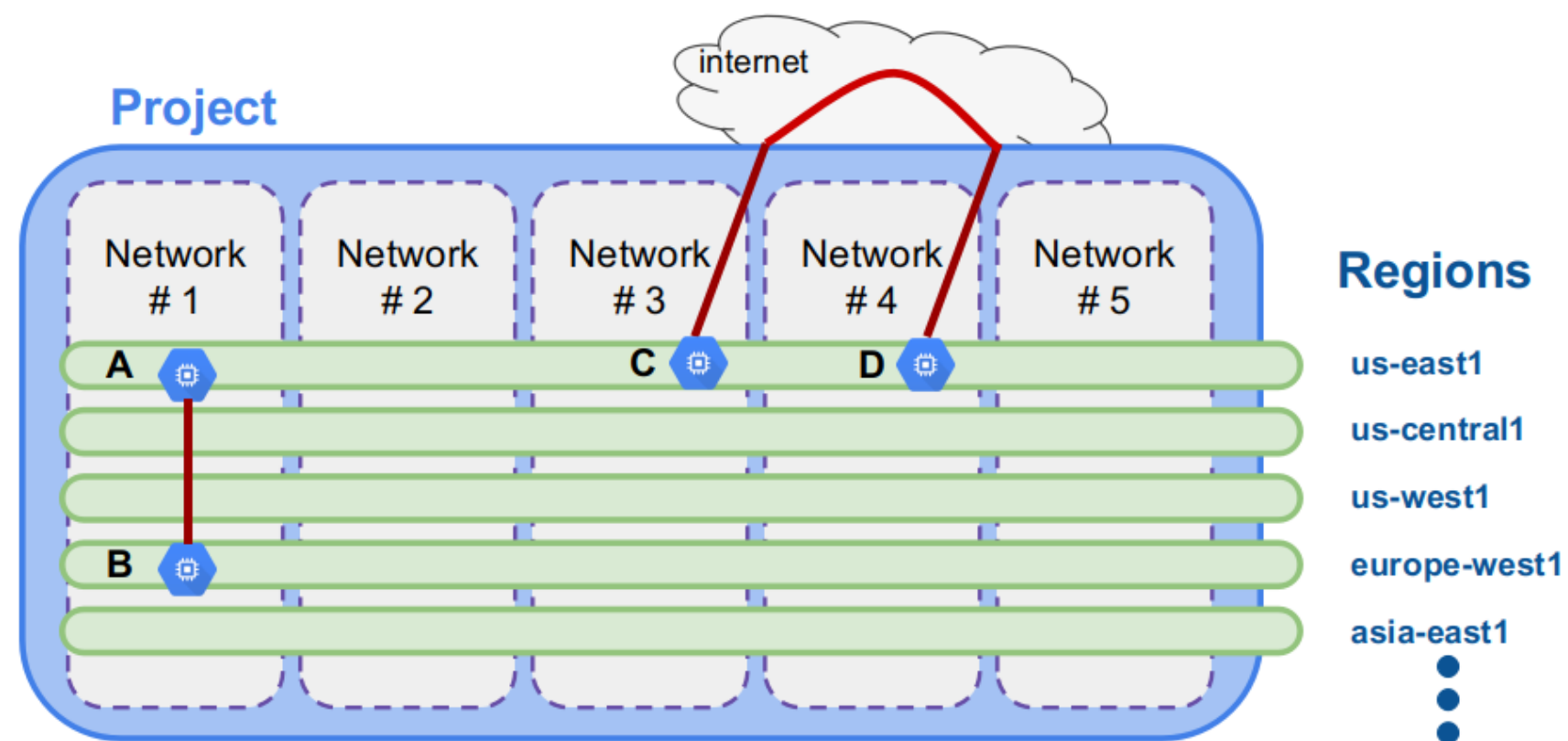
Content is intended as reference material only to supplement the instructor-led training

VPCS AND SUBNETS

- A **subnet** defines a range of IP addresses in your VPC.
- You can launch resources into a subnet that you select.
- A **private subnet** should be used for resources that won't be accessible over the Internet.
- A **public subnet** should be used for resources that will be accessed over the Internet.
- A **VPC endpoint** enables private connections between your VPC and supported AWS services and VPC endpoint services powered by AWS PrivateLink.

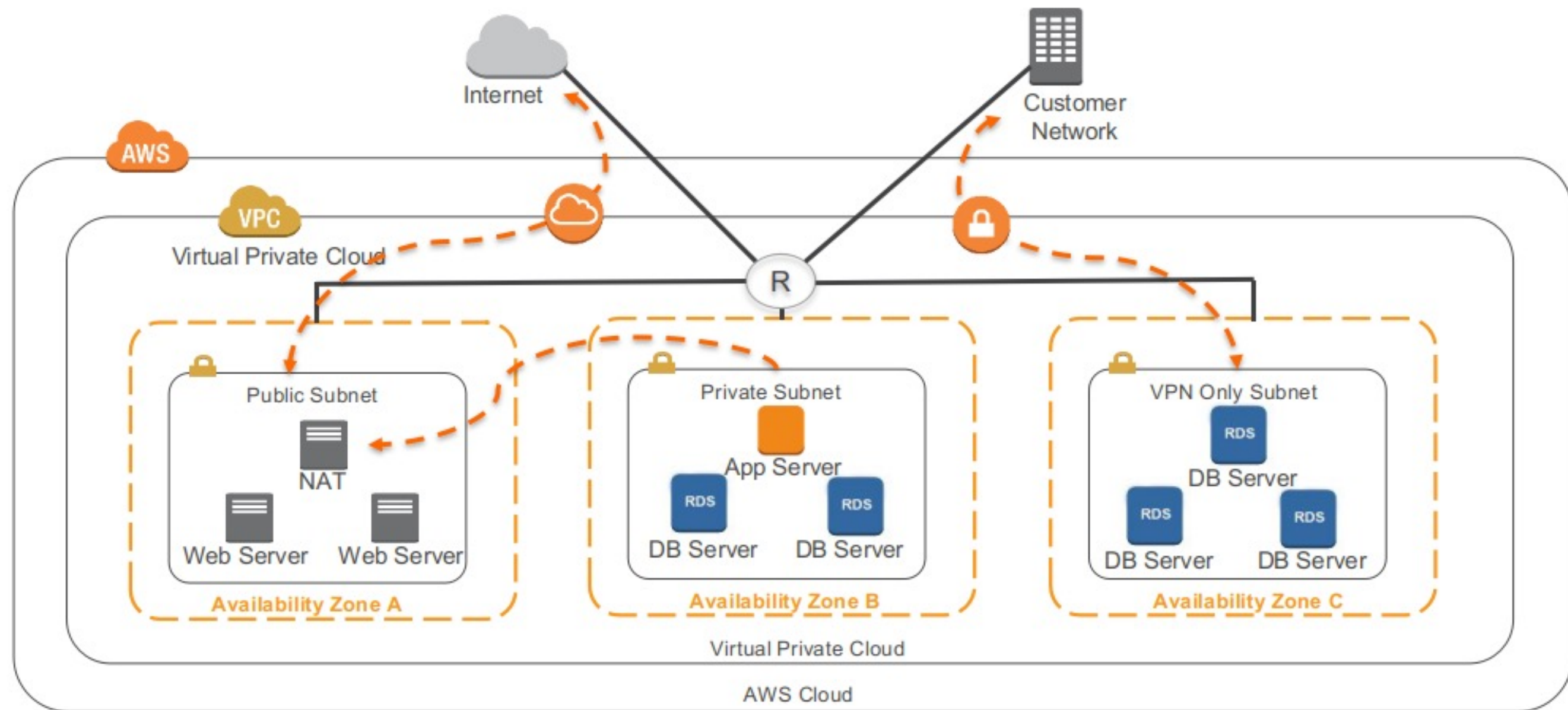
VPC AND REGIONS

- VPCs are for building your private clouds. Depending on cloud implementation, they can span regions, but we will not cover such architectures because they are unlikely



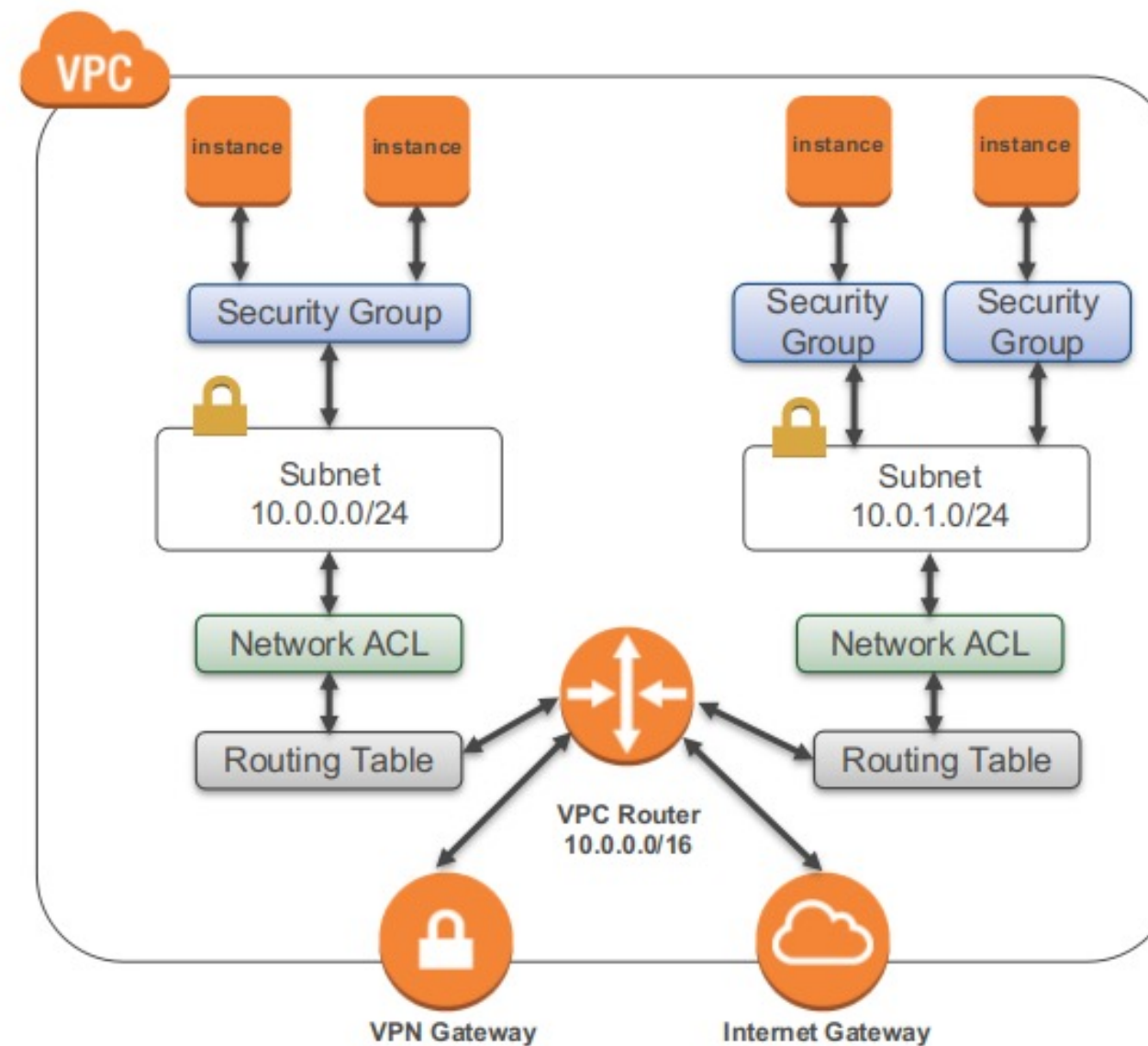
- A and B can communicate over internal IPs even though they are in different regions.
- C and D must communicate over external IPs even though they are in the same region.

VPC EXAMPLE



SECURITY IN YOUR VPC

- Security groups
- Network access control lists (ACLs)



VPN CONNECTIONS

VPN Connectivity option	Description
AWS Hardware VPN	You can create an IPsec, hardware VPN connection between your VPC and your remote network.
AWS Direct Connect	AWS Direct Connect provides a dedicated private connection from a remote network to your VPC.
AWS VPN CloudHub	You can create multiple AWS hardware VPN connections via your VPC to enable communications between various remote networks.
Software VPN	You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a software VPN appliance.

- Other clouds give similar options

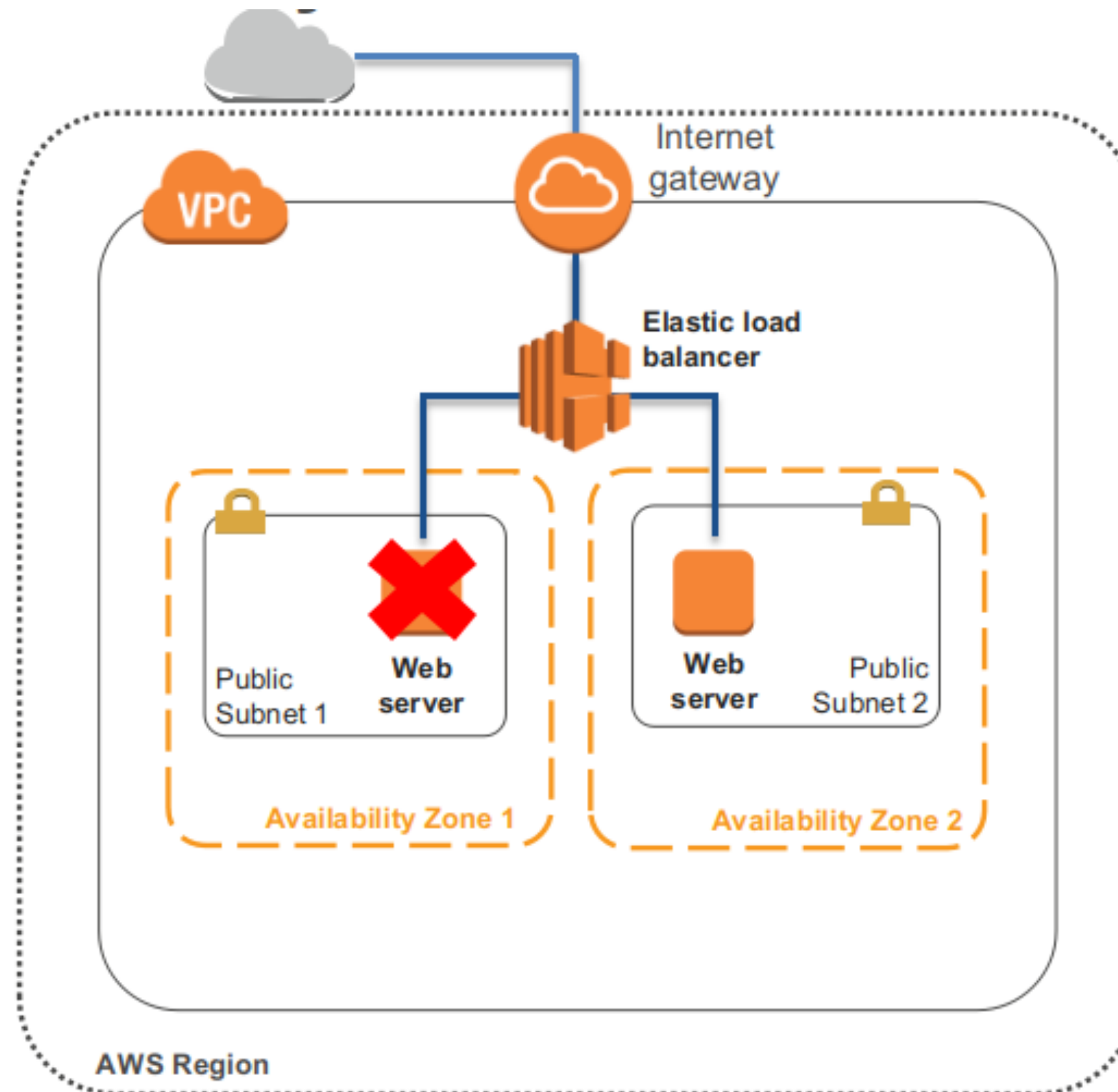
NETWORKING IN YOUR VPC

- You can use the following components to configure networking in your VPC:
 - IP Addresses
 - Elastic Network Interfaces
 - Route Tables
 - Internet Gateways
 - Network Address Translation (NAT)
 - Dynamic Host Configuration Protocol (DHCP) Options Sets
 - Domain Name System (DNS)
 - VPC Peering
 - VPC Endpoints
 - VPC Flow Logs

HOW MANY AVAILABILITY ZONES SHOULD I USE?

- **Recommendation:** Start with two Availability Zones per region.
- **Best practice:** If resources in one Availability Zone are unreachable, your application shouldn't fail.
- Most applications can support two Availability Zones.
- Using more than two Availability Zones for HA is not usually cost-effective.

EXAMPLE OF USING TWO AVAILABILITY ZONES



OTHER REASONS TO USE TWO AVAILABILITY ZONES

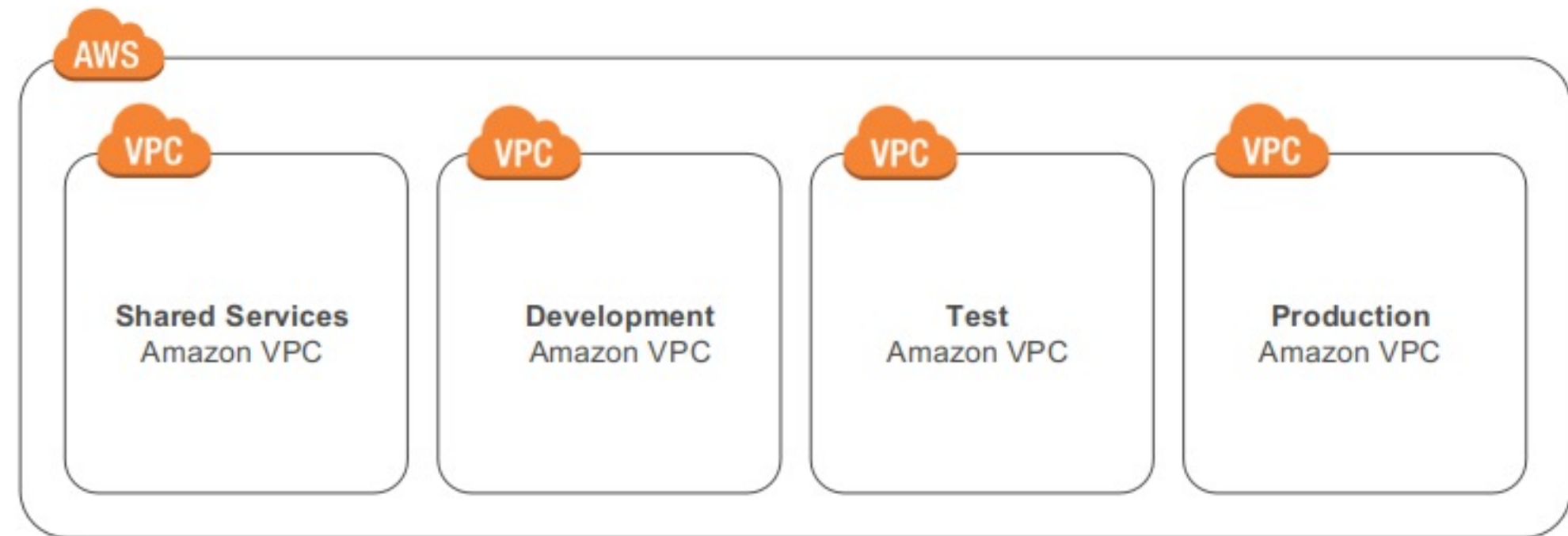
- How many Availability Zones would be recommended for each scenario?
 - Applications heavily use preemptible (spot) Instances **for cost control** :
 - Two Availability Zones or more for more **price options**
 - Applications have data sources such as MySQL, MS SQL Server, and Oracle:
 - Two Availability Zones to support active/passive
 - Applications have data sources such as Cassandra or MongoDB:
 - Two Availability Zones or more for extremely high availability

USING ONE VPC

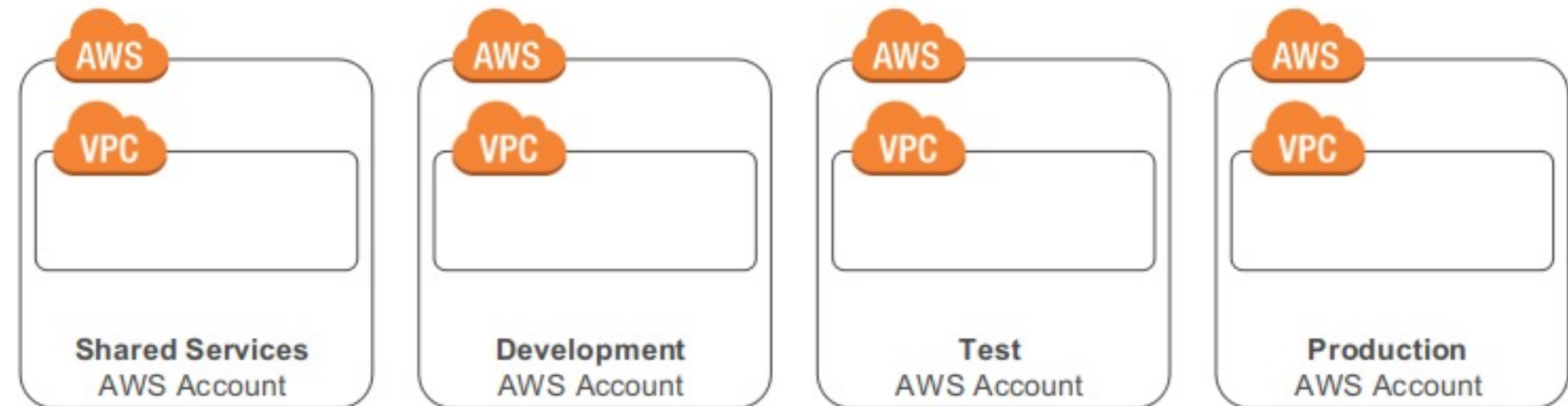
- There are limited use cases where one VPC could be appropriate:
 - High-performance computing
 - Identity management
 - Small, single applications managed by one person or very small team
- For most use cases, there are two primary patterns for organizing your infrastructure:
 - **Multi-VPC** and **Multi-Account**

AWS INFRASTRUCTURE PATTERNS

VPC pattern



Account pattern



VPC PATTERNS

- How do you know which pattern to use?
 - The primary factors for determining this are the **complexity** of your organization and your **workload isolation** requirements:
- Single IT team? **Multi-VPC**
- Large organization with many IT teams? **Multi-account**
 - Rare for research
- High workload isolation required? **Multi-account**

MULTI-VPC PATTERN

- Features:
 - Uses **one account**
 - Uses **two or more VPCs** to organize application environments
- Best suited for:
 - **Single team or single organizations**
- Why?
 - Limited teams make **maintaining standards** and **managing access** far easier.
- Exception:
 - **Governance and compliance** standards may require workload isolation regardless of organizational complexity.

MULTI-ACCOUNT PATTERN

- Features:
 - Uses **two or more accounts** to organize application environments
 - Uses **one VPC** per AWS account
- Best suited for (though not likely for university researchers):
 - **Large organizations** and **organizations with multiple IT teams** , such as Enterprise-level corporations or government agencies
 - **Medium-sized organizations** that anticipate rapid growth
- Why?
 - **Managing access** and **standards** can be more challenging in more complex organizations.

OTHER IMPORTANT CONSIDERATIONS FOR AWS

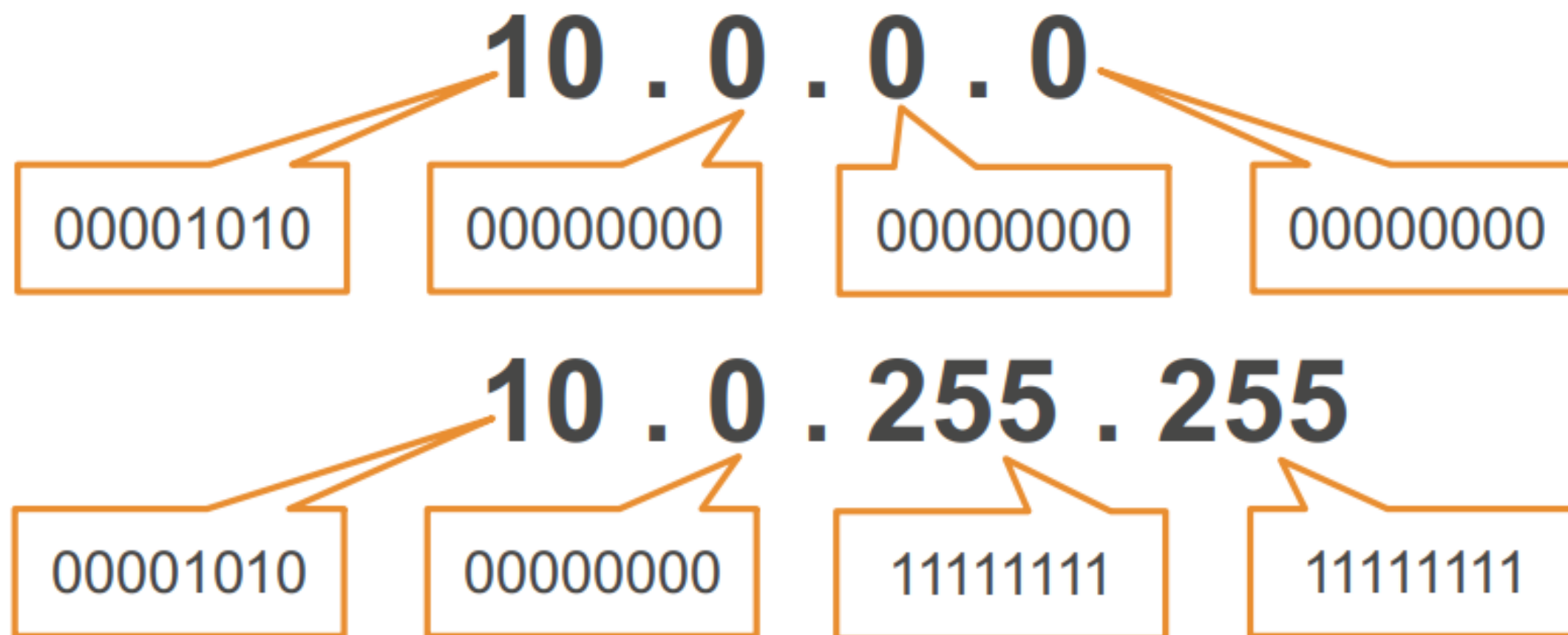
- The majority of AWS services **do not actually sit within a VPC** .
 - For these services, a VPC **cannot provide any isolation** outside of connectivity.
 - Communication between resources based in a VPC and resources outside of that VPC traverses the **public AWS network** by default.
 - Amazon S3 offers **VPC endpoints** to connect without traversing the public Internet:
 - Endpoints are supported within the same region only.
 - Support for endpoints with other services will be added in the future.

VPCS AND IP ADDRESSES

- When you create your VPC, you specify its set of IP addresses with CIDR notation.
- Classless Inter-Domain Routing (CIDR) notation is a simplified way to show a specific range of IP addresses.
- Example: 10.0.0.0/16 = all IPs from 10.0.0.0 to 10.0.255.255
- How does that work? What does the 16 define?

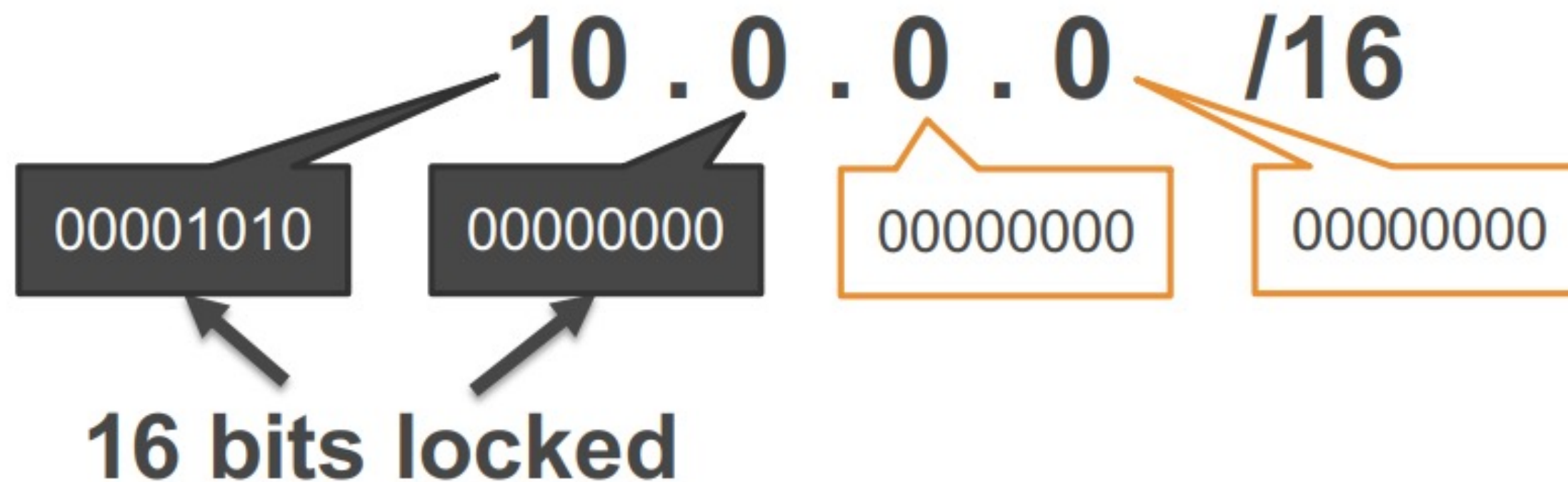
IPS AND CIDR

Every set of 3 digits in an IP address represents a set of 8 binary values (8 bits).

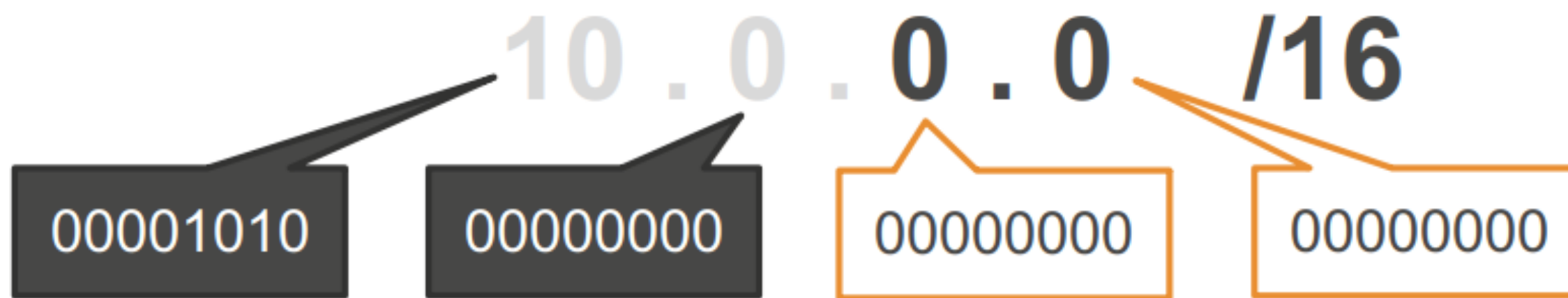


IPS AND CIDR

The 16 in the CIDR notation example represents how many of those bits are "locked down" and cannot change.



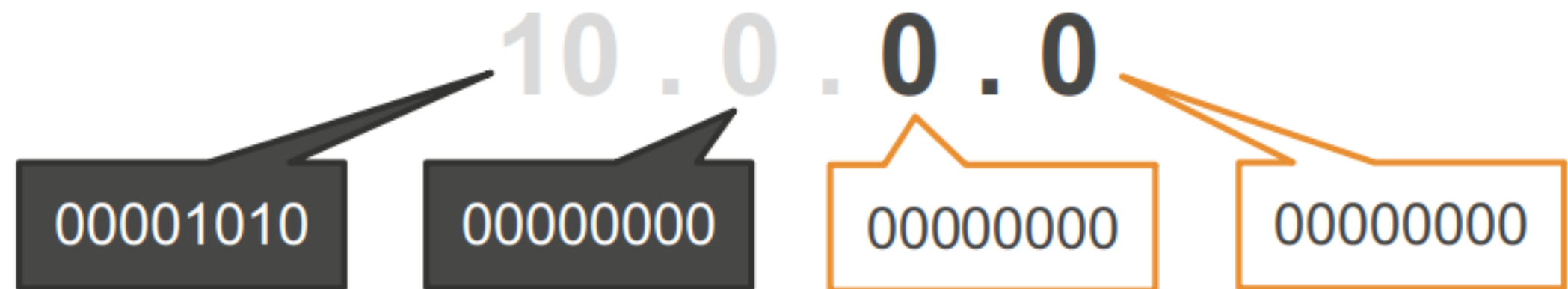
IPS AND CIDR



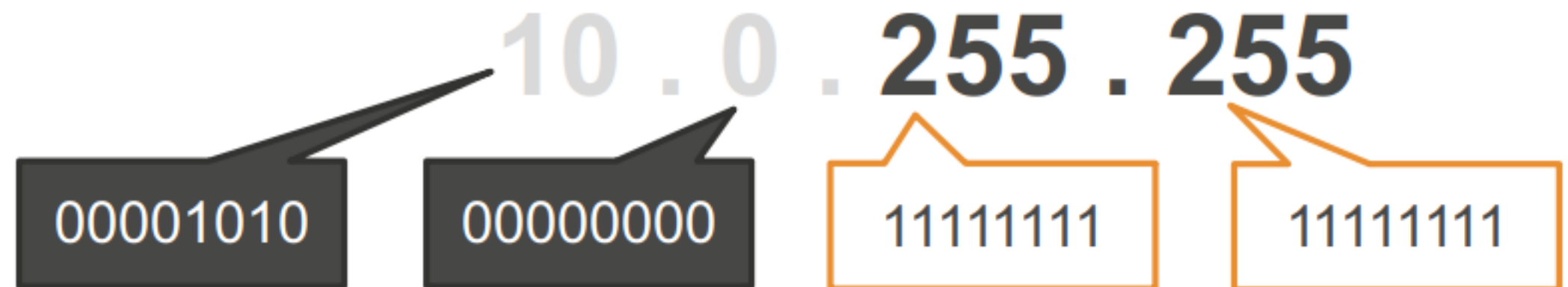
The unlocked bits can change between 1 and 0, allowing the full range of possible values.

CIDR EXAMPLE: 10.0.0.0/16

**Lowest
possible IP**



**Highest
possible IP**



VPCS AND IP ADDRESSES

VPCs can use CIDR ranges between **/16 and /28**.

For every one step a CIDR range increases, the total number of IPs is cut in half:

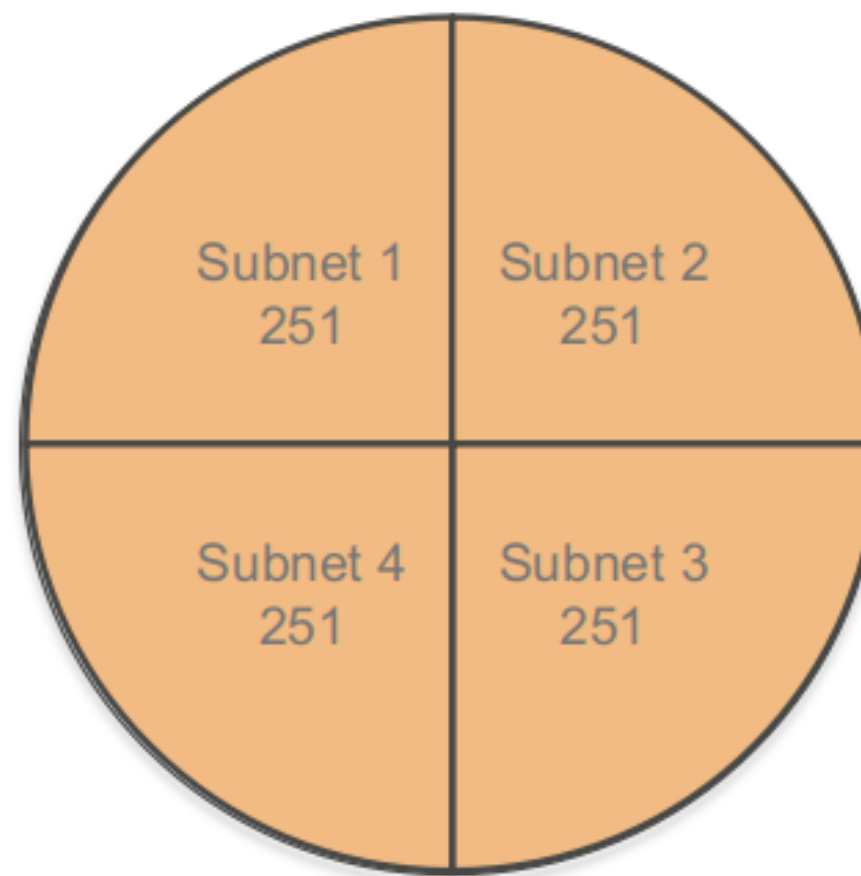
CIDR / Total IPs						
/16	/17	/18	/19	/20	/21	/22
65,536	32,768	16,384	8,192	4,096	2,048	1,024
/23	/24	/25	/26	/27	/28	
512	256	128	64	32	16	

WHAT ARE SUBNETS?

Subnets are **segments** or **partitions** of a network, divided by **CIDR range**.

Example:

A VPC with **CIDR /22** includes 1,024 total IPs



Note: In the cloud, some of the first and last IP addresses may be reserved for the cloud use.

HOW TO USE SUBNETS

Recommendation: Use subnets to define Internet accessibility.

Public subnets

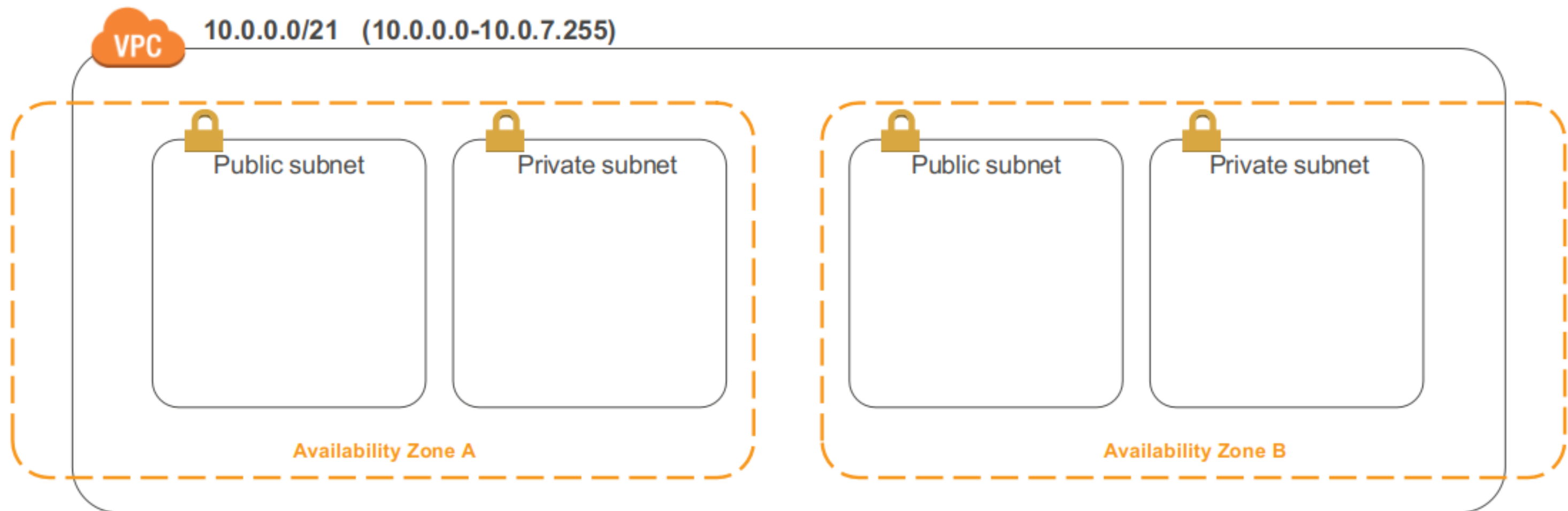
- ❏ Include a routing table entry to an **Internet gateway** to support inbound/outbound access to the public Internet.

Private subnets

- ❏ Do not have a routing table entry to an Internet gateway and are **not directly accessible** from the public Internet.
- ❏ Typically use a "jump box" (NAT/proxy/bastion host) to support restricted, **outbound-only** public Internet access.

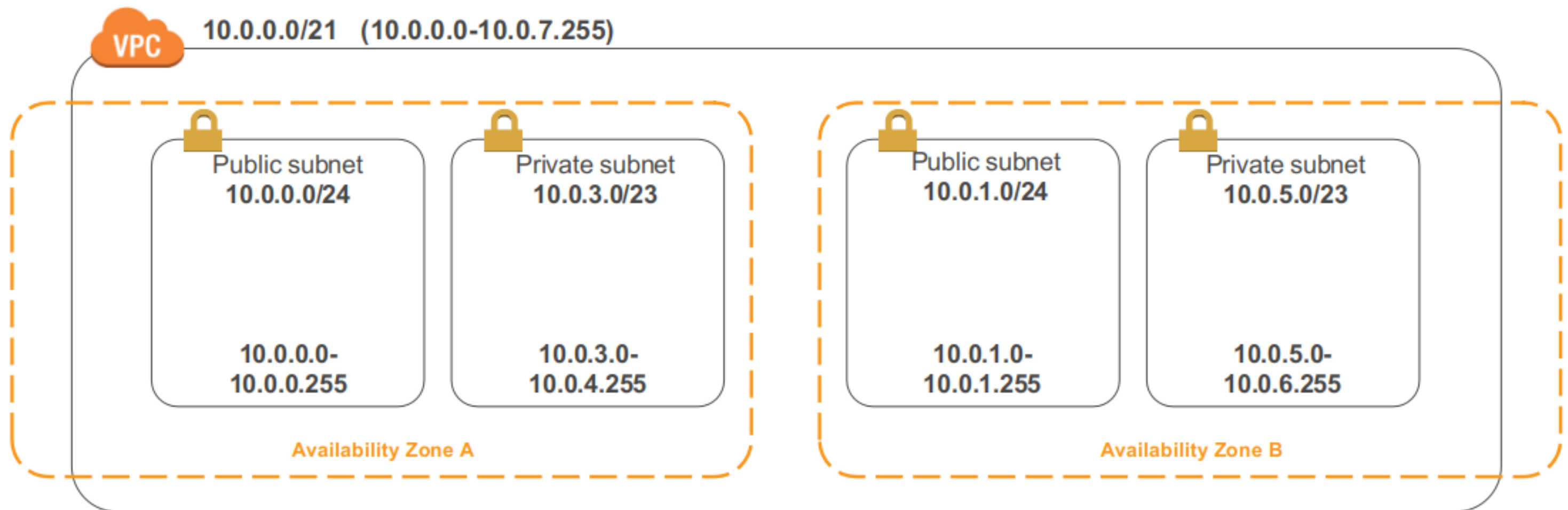
SUBNETS

Recommendation: Start with one public and one private subnet per Availability Zone.



SUBNETS

Recommendation: Allocate substantially more IPs for private subnets than for public subnets.



SUBNET SIZES

- Recommendation: Consider larger subnets over smaller ones (/24 and larger).
- Simplifies workload placement:
 - Choosing where to place a workload among 10 small subnets is more complicated than with one large subnet.
- Less likely to waste or run out of IPs:
 - If your subnet runs out of available IPs, you can't add more to that subnet.
 - Ex.: If you have 251 IPs in a subnet that's using only 25 of them, you can't share the unused 226 IPs with another subnet that's running out.

ROUTE TABLES: DIRECTING TRAFFIC BETWEEN VPC RESOURCES

- Route tables:
 - Determine where network traffic is routed
 - Main and custom route tables
 - VPC route table
 - Local route
 - Only one route table per subnet
- **Best practice:** For better security, use custom route tables for each subnet.

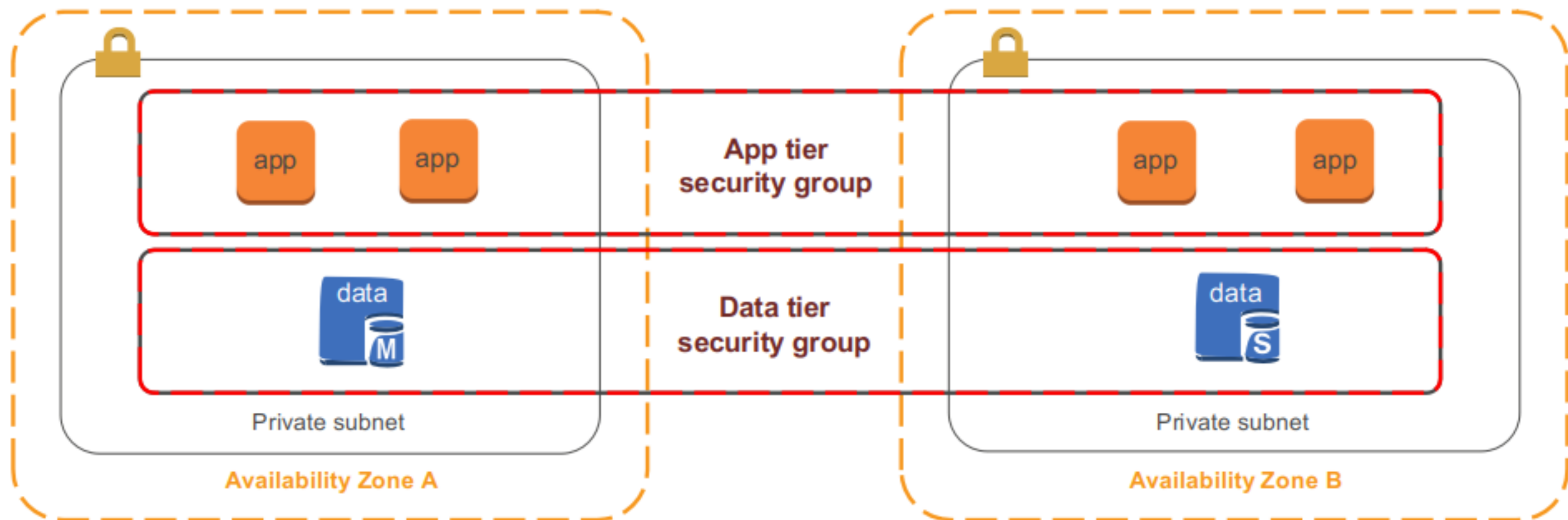


SECURING VPC TRAFFIC WITH SECURITY GROUPS

- **Security groups:**
 - Are virtual firewalls that control inbound and outbound traffic for one or more instances.
 - Deny all incoming traffic by default and use allow rules that can filter based on TCP, UDP, and ICMP protocols.
 - Are stateful, which means that if your inbound request is allowed, the outbound response does not have to be inspected/tracked, and vice versa.
 - Can define a source/target as either a CIDR block or another security group to handle situations like autoscaling.

SECURITY GROUPS

Use security groups to control traffic into, out of, and between resources.

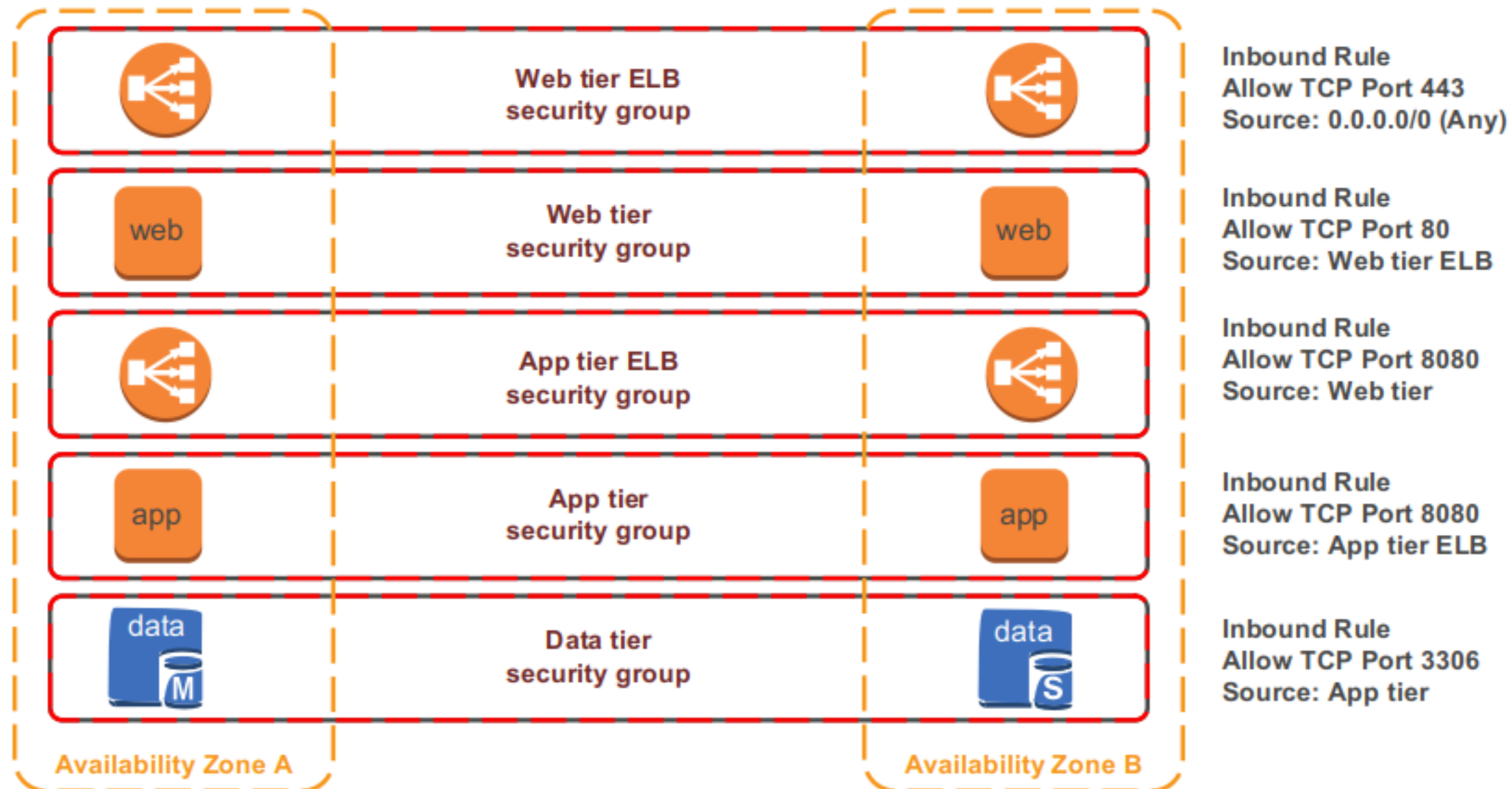


HOW SECURITY GROUPS ARE CONFIGURED

- By default, all newly created security groups allow all outbound traffic to all destinations.
 - Modifying the default outbound rule on security groups increases complexity and is not recommended unless required for compliance.
- Most organizations create security groups with inbound rules for each functional tier (web/app/data/etc.) within an application.

SECURITY GROUP CHAINING DIAGRAM

- Security group rules per application tier

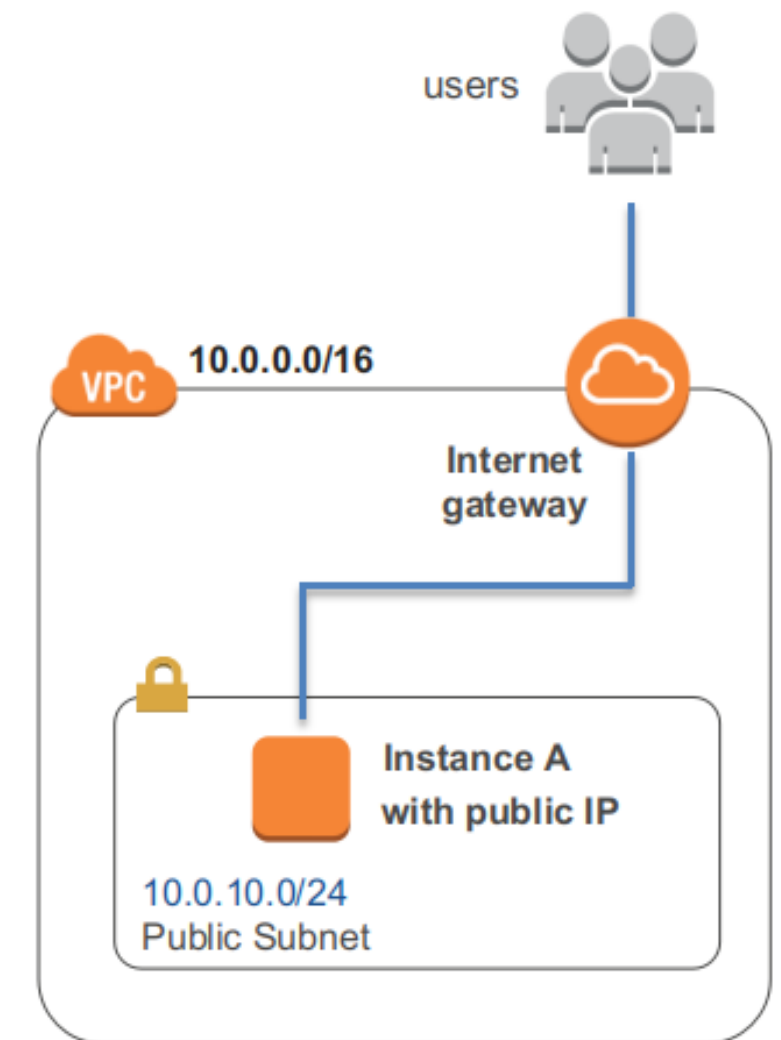


NETWORK ACLS

- Are optional virtual firewalls that control traffic in and out of a subnet.
- Allow all incoming/outgoing traffic by default and use stateless rules to allow or deny traffic.
 - "Stateless rules" inspect all inbound and outbound traffic and do not keep track of connections.
- Enforce rules only at the boundary of the subnet, not at the instance-level, like security groups.

DIRECTING TRAFFIC TO YOUR VPC

- Internet gateways:
 - Allow communication between instances in your VPC and the Internet.
 - Are a managed service: horizontally scaled, redundant, and highly available by default.
 - Provide a target in your VPC route tables for Internet-routable traffic.

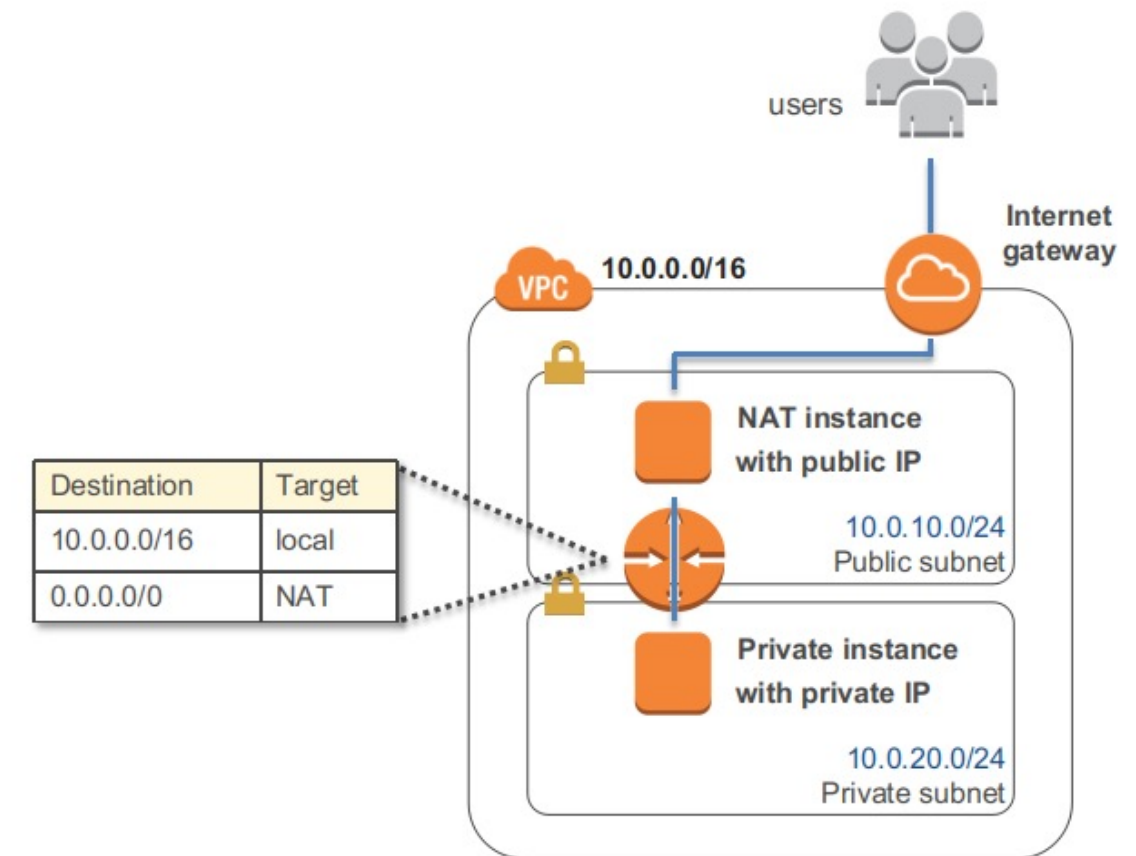


DIRECTING TRAFFIC TO YOUR VPC

- To enable access to or from the Internet for instances in a VPC subnet, you must:
 - Attach an Internet gateway to your VPC.
 - Ensure that your subnet's route table points to the Internet gateway.
 - Ensure that instances in your subnet have public IP addresses or Elastic IP addresses.
 - Ensure that your NACLs and security groups allow the relevant traffic to flow to and from your instance.

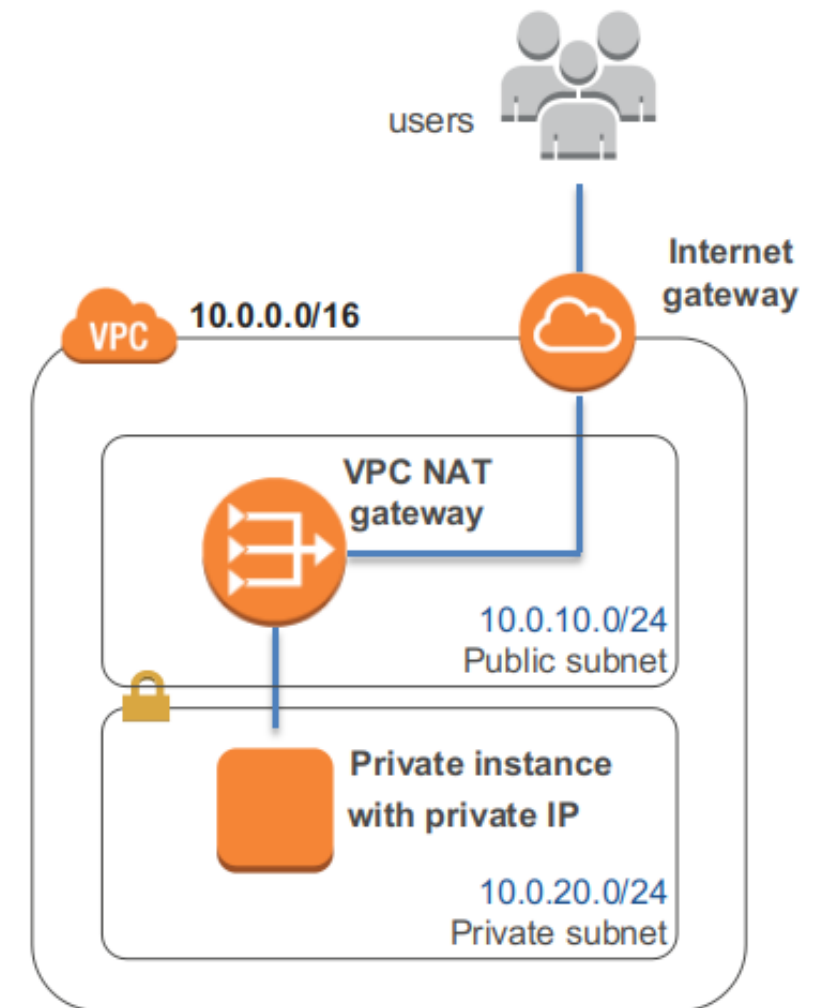
WHAT ABOUT OUTBOUND TRAFFIC FROM PRIVATE INSTANCES?

- Network Address Translation services:
 - Enable instances in the private subnet to initiate outbound traffic to the Internet or other AWS services.
 - Prevent private instances from receiving inbound traffic from the Internet.
- Two primary options:
 - Amazon EC2 instance set up as a NAT in a public subnet



WHAT ABOUT OUTBOUND TRAFFIC FROM PRIVATE INSTANCES?

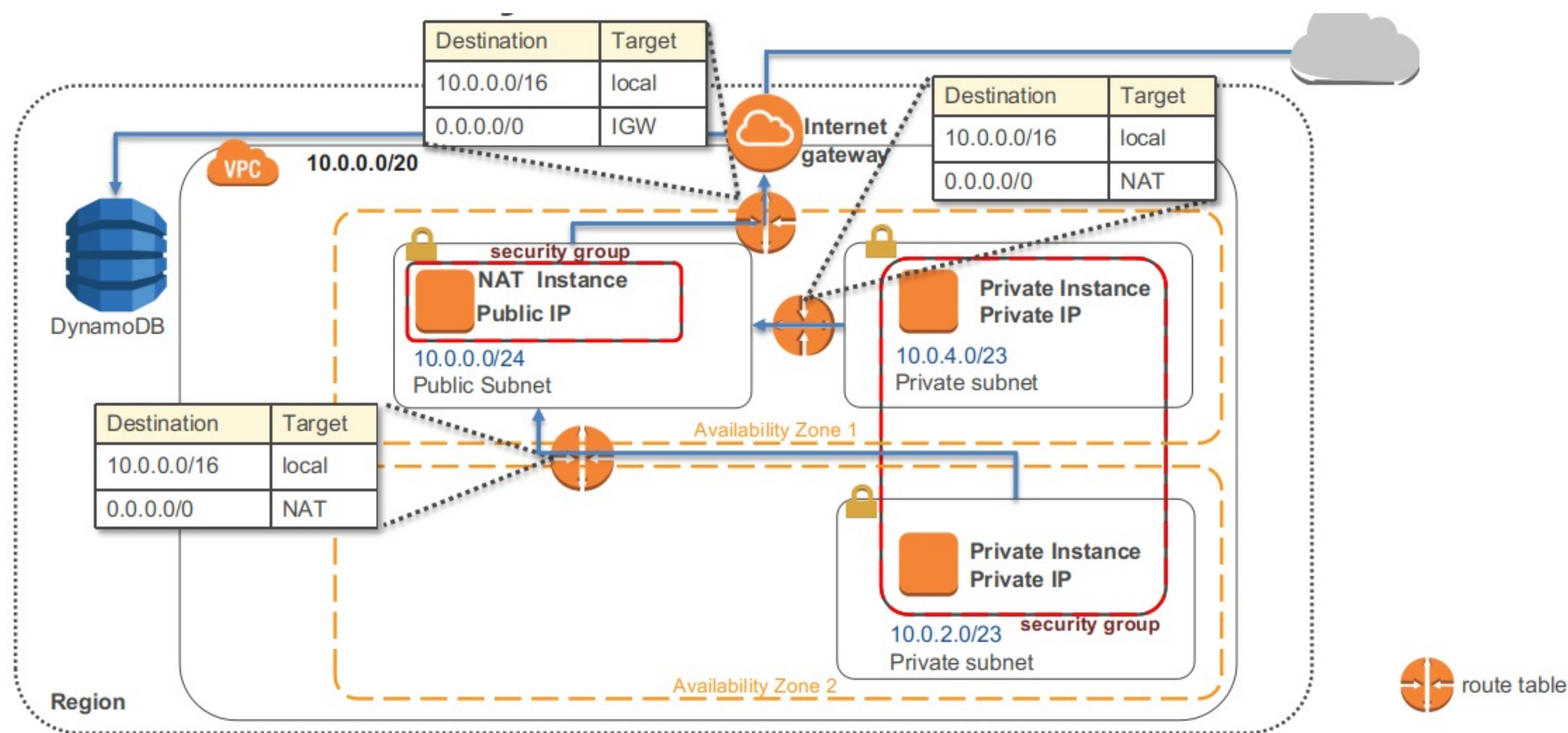
- Network Address Translation services:
 - Enable instances in the private subnet to initiate outbound traffic to the Internet or other AWS services.
 - Prevent private instances from receiving inbound traffic from the Internet.
- Two primary options:
 - Amazon EC2 instance set up as a NAT in a public subnet
 - VPC NAT Gateway



VPC NAT GATEWAYS VS. NAT INSTANCES ON AMAZON EC2

	VPC NAT gateway	NAT instance
Availability	Highly available by default	Use script to manage failover
Bandwidth	Bursts to 10 Gbps	Based on bandwidth of instance type
Maintenance	Managed by AWS	Managed by you
Security	NACLs	Security groups and NACLs
Port forwarding	Not supported	Supported





SUBNETS, GATEWAYS, AND ROUTES



AMAZON VPC FLOW LOGS

- Captures traffic flow details in your VPC.
- Accepted and rejected traffic
- Can be enabled for VPCs, subnets, and ENIs.
- Logs published to CloudWatch Logs.

Use cases:

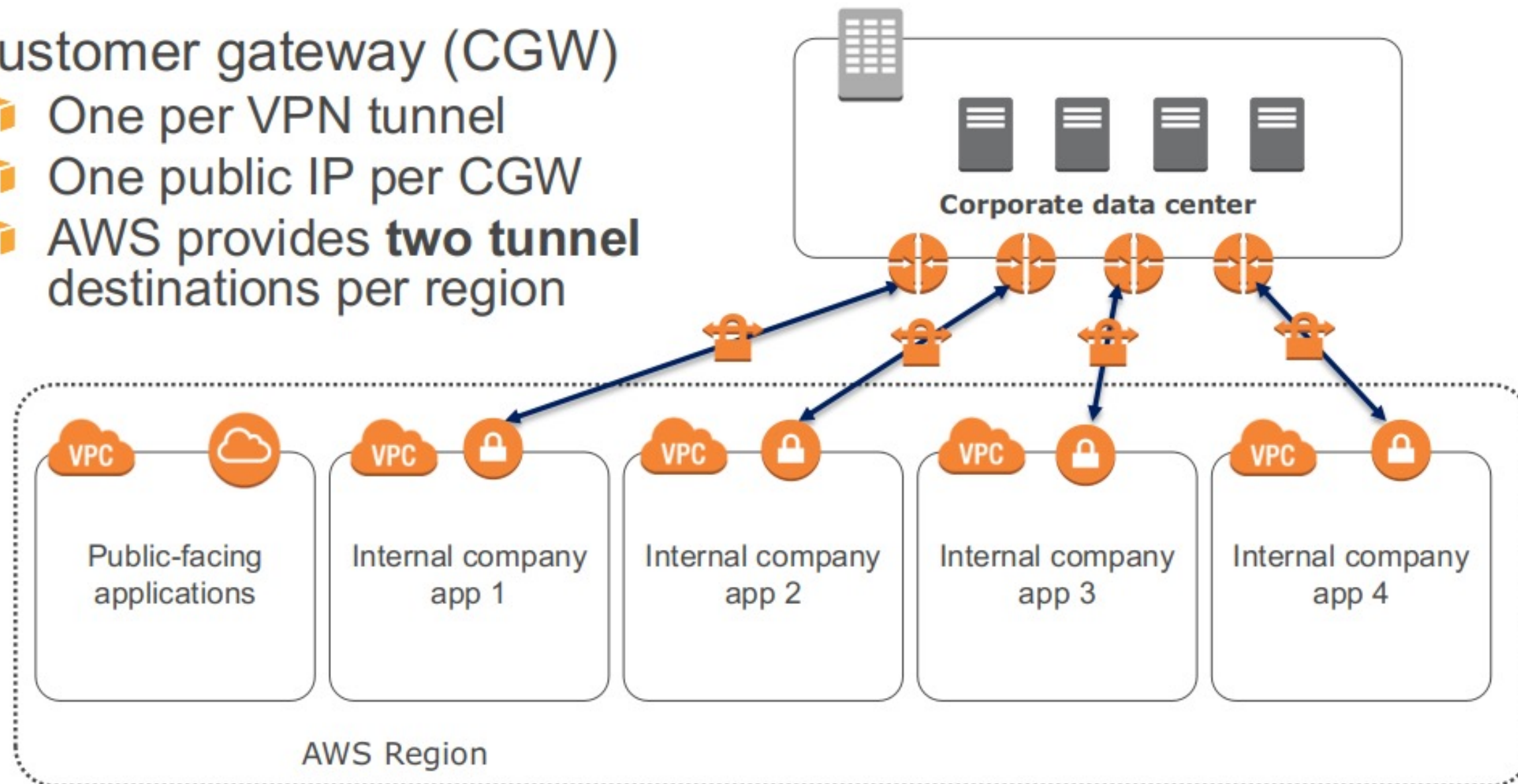
-  Troubleshoot connectivity issues.
-  Test network access rules.
-  Monitor traffic.
-  Detect and investigate security incidents.

CONNECTING VPCS TOGETHER

- Not the right way

Customer gateway (CGW)

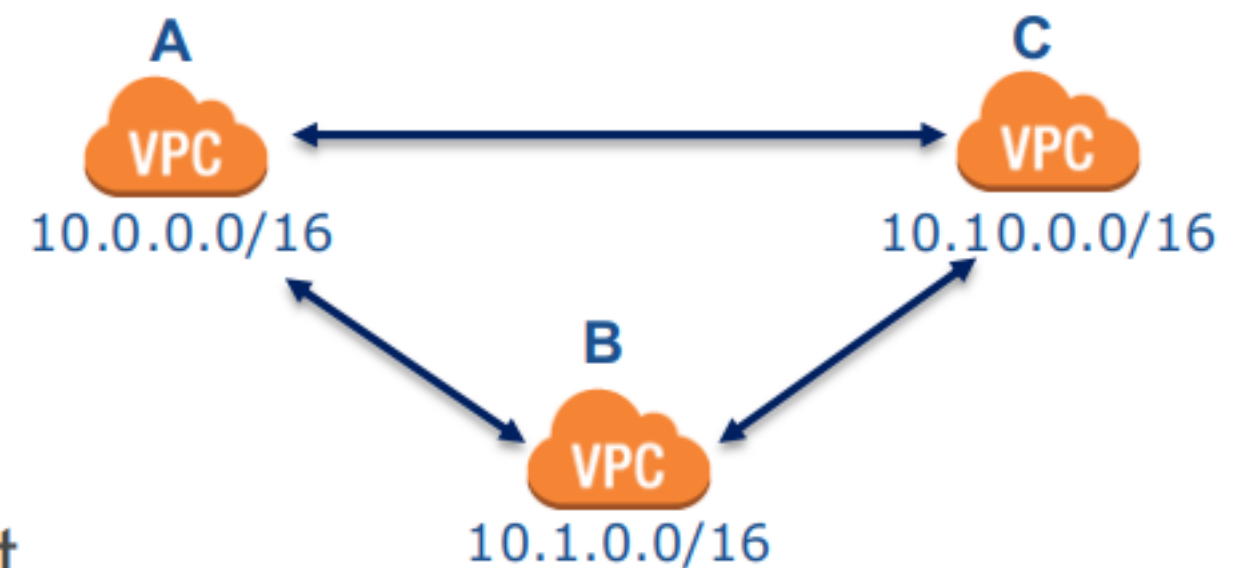
- One per VPN tunnel
- One public IP per CGW
- AWS provides **two tunnel** destinations per region



VPC PEERING

VPC peering connection allows you to route traffic between the peer VPCs.

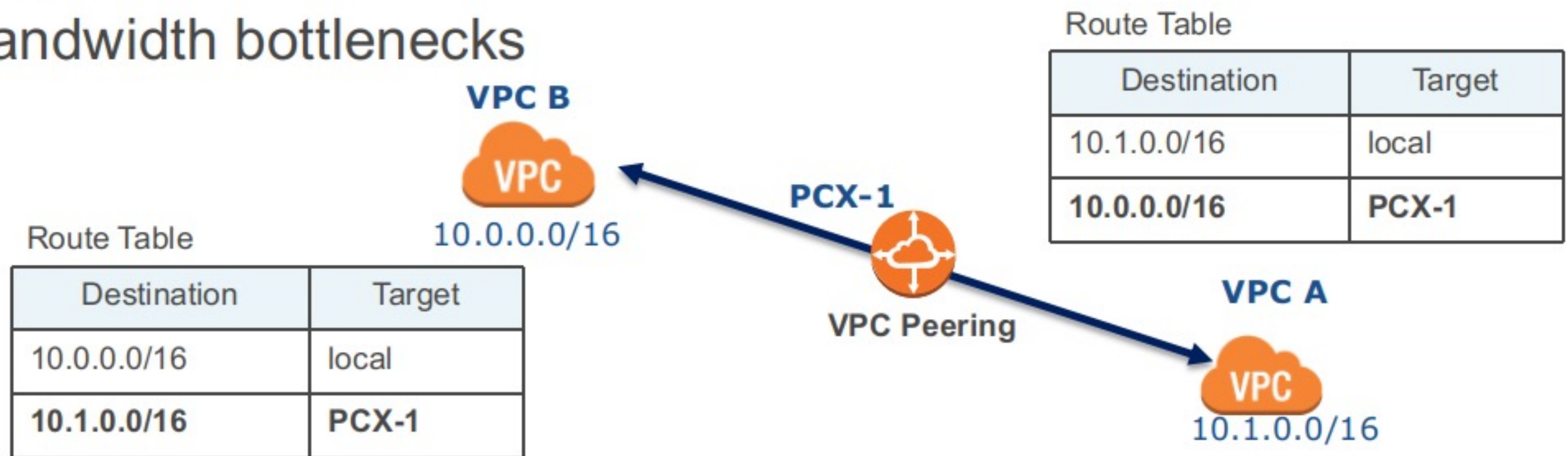
- ❏ Use private IP addresses.
- ❏ VPCs reside in the same region.
- ❏ IP space cannot overlap.
- ❏ Only one between any two VPCs.
- ❏ Transitive peering relationships are not supported



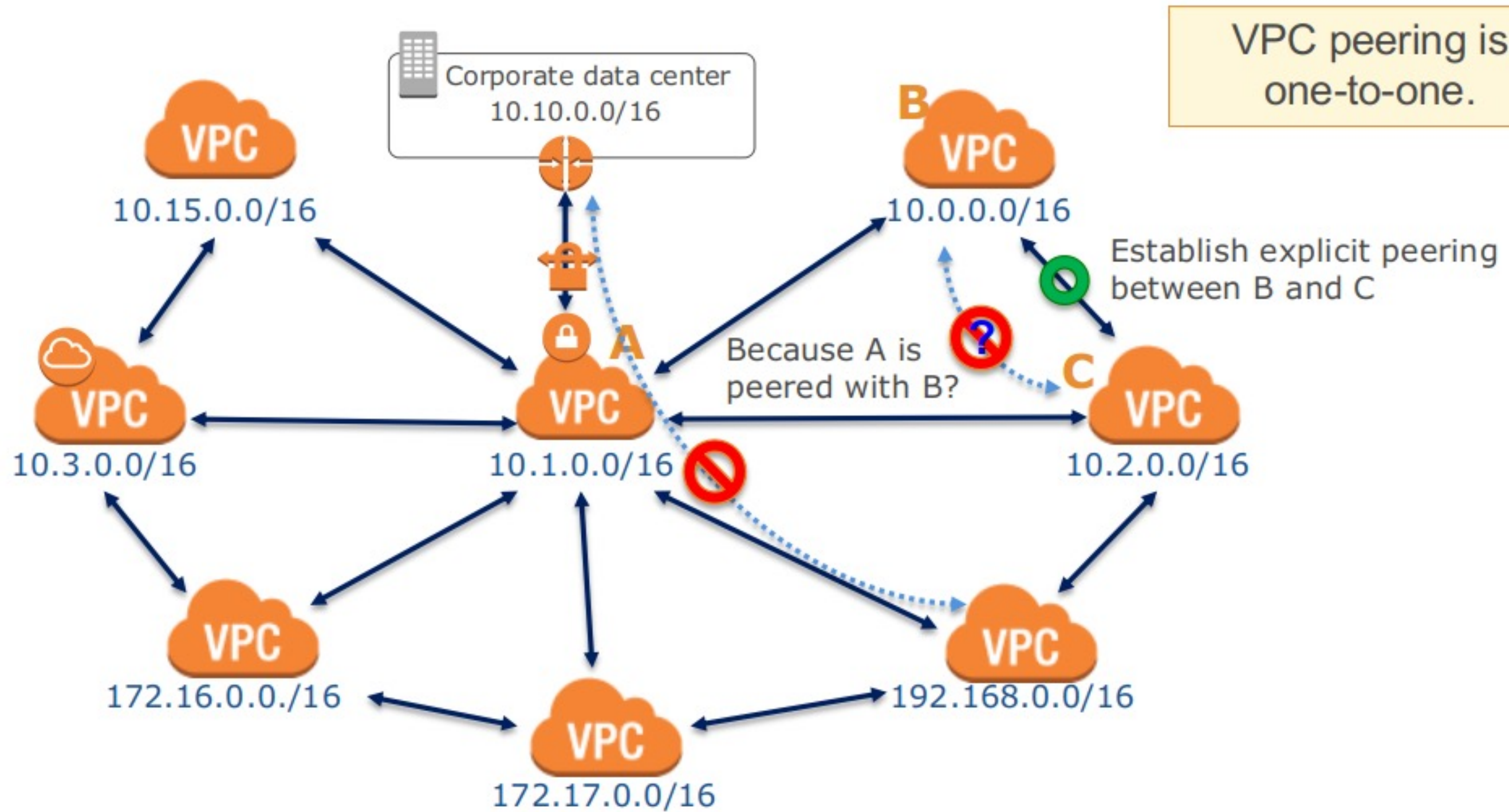
Instances in either VPC can communicate with each other as if they are within the same network.

HOW DOES VPC PEERING WORK?

- ❏ No Internet gateway or virtual gateway required
- ❏ No single point of failure
- ❏ No bandwidth bottlenecks



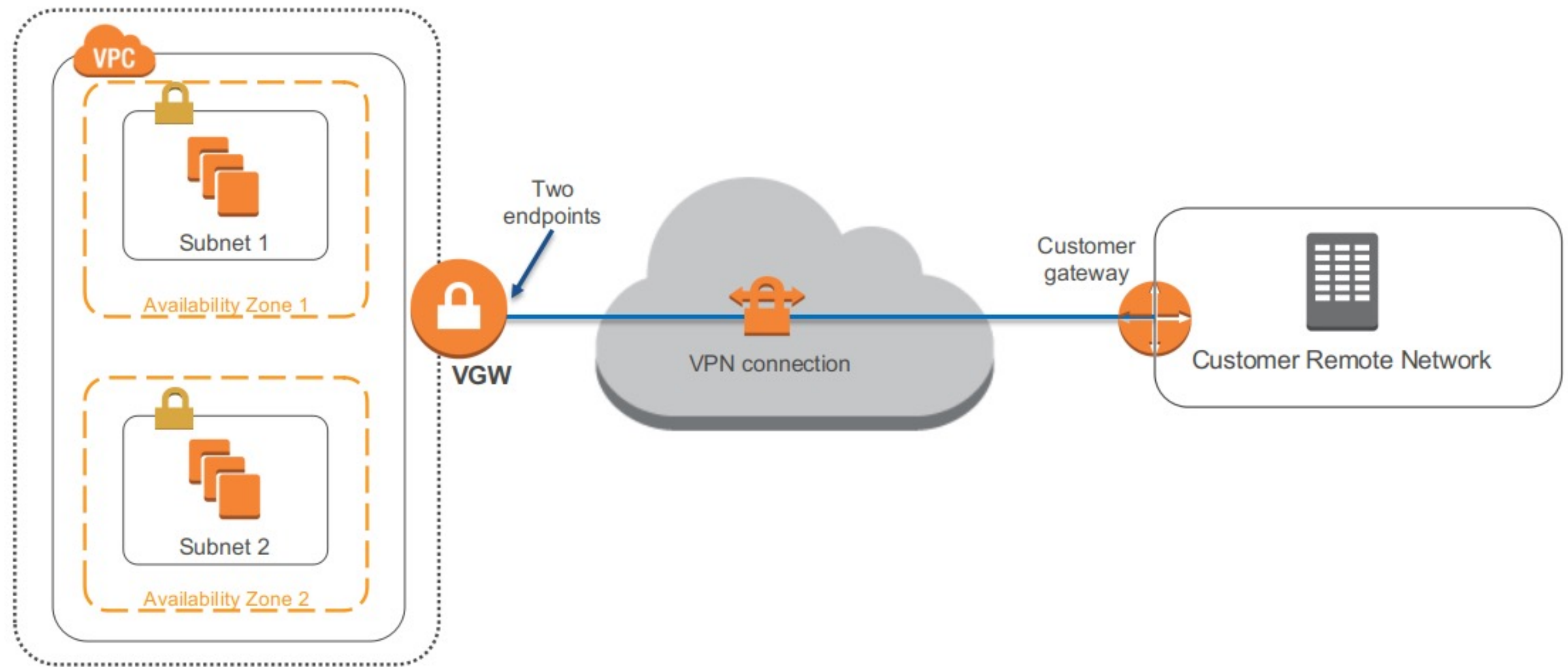
RULES OF VPC PEERING



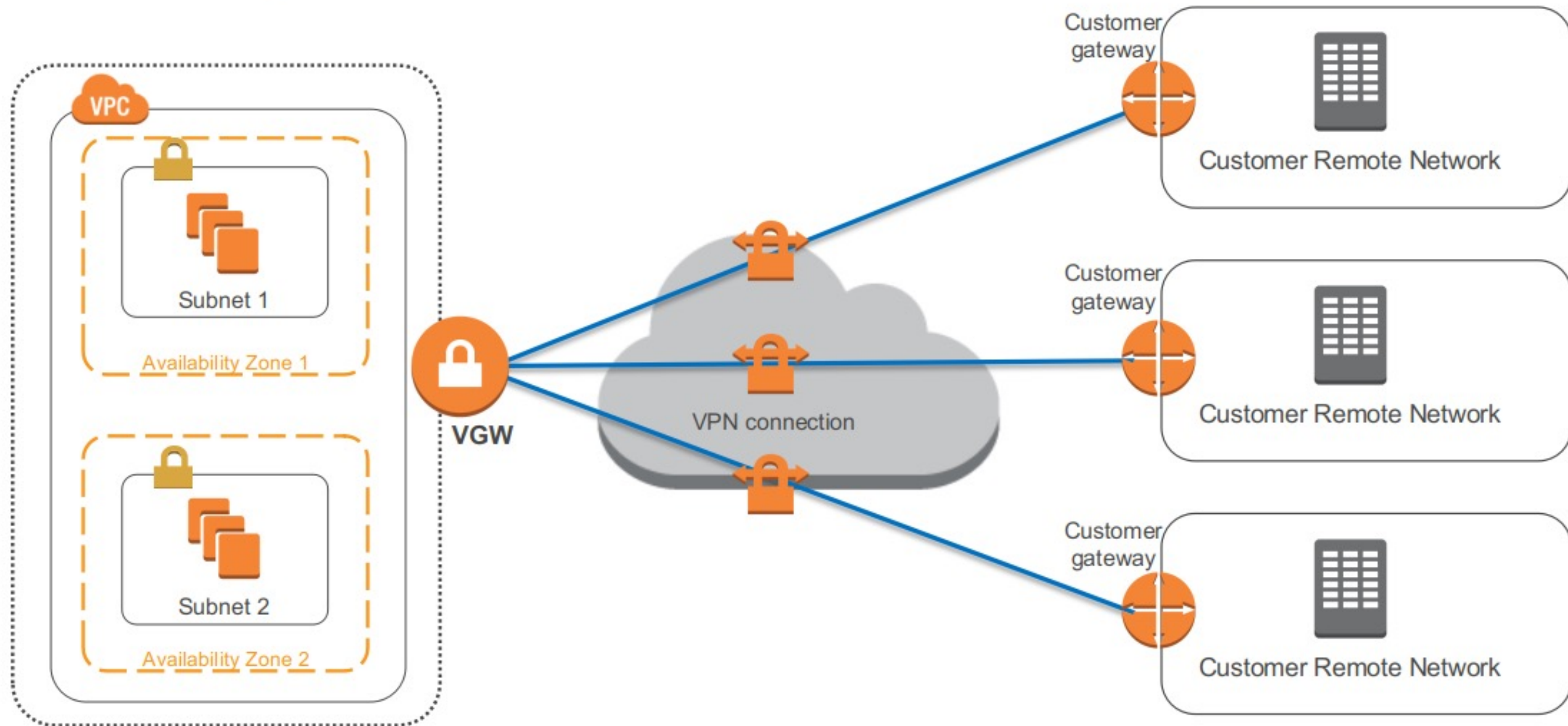
VPC PEERING SECURITY

- Two-way handshake to establish a peering connection.
- Routing controls: Routing tables control the local subnets that can route to remote subnets.
- Security groups control what traffic an instance can send or receive.
- Network ACLs control what traffic a subnet can send or receive.
- No edge-to-edge routing or transitive trusts: Reduces inadvertently creating unexpected network connections.

EXTENDING ON-PREMISES NETWORK TO AWS: VPN CONNECTIONS



EXTENDING ON-PREMISES NETWORK TO AWS: MULTIPLE VPN



AWS DIRECT CONNECT

- AWS Direct Connect provides you with a private network connection between AWS and your data center.
- It is a network service alternative to using the Internet to access AWS cloud services.
- Benefits:
 - Reduced network transfer costs
 - Note of caution. Treated as credit against compute costs, this helps if you have data AND an application, but not if you just host a big data set. We heard of cases in which the promised savings did not materialize.
 - Improved application performance with predictable metrics
 - Transferring large data sets
 - Security and compliance
 - Hybrid cloud architectures
 - Private data center expansion
 - Alternative to Internet-based IPSec VPN connections (IPSec VPN connections can be used as a failover)

DEFAULT VPCS

- Details about default VPCs:
 - Each region in your account has a default VPC.
 - Default CIDR is 172.31.0.0/16.
 - If you create a VPC-based resource (Amazon EC2, Amazon RDS, Elastic Load Balancing, etc.) but don't specify a custom VPC, it will be placed in your default VPC in that region.
 - Includes a default subnet, IGW, main route table connecting default subnet to the IGW, default security group, and default NACL.
 - Configurable the same as other VPCs; e.g., adding more subnets.

DEFAULT SUBNET

- Default subnets in default VPCs:
 - Created within each Availability Zone for each default VPC.
 - Public subnet with a CIDR block of /20 (4,096 IPs).
 - You can convert it (and any public subnet) into a private subnet by removing its route to the IGW.
 - When a new Availability Zone is added to a region, your default VPC in that region gets a subnet placed in the new Availability Zone (unless you've made modifications to that VPC).

WHEN SHOULD I USE DEFAULT VPCS AND SUBNETS?

- **Recommendation** : Use default VPCs and their subnets only for experimenting in your AWS account.
 - Default VPCs are a quick start solution.
 - They provide an easy way to test launching instances of your VPC-based resources, without having to set up a new VPC.
 - For real-world applications, create your own VPCs and subnets.
 - You'll have greater control/knowledge of their configurations.
 - You can delete them and create new ones easily.

VPC BEST PRACTICES

- Choose CIDR blocks wisely. Plan ahead.
- Use large subnets instead of a higher number of small subnets.
- Keep subnets simple and divide by Internet accessibility (public/private).
- Use Multi-AZ deployments in VPC for high availability.
- Use security groups to control traffic between resources.
- Use VPC Flow Logs to track and monitor your VPC traffic.
- Check the health of your VPN link via API calls or the AWS Management Console.