

NETWORKING AND DATA MOVEMENT

NETWORKING OVERVIEW

DESIGNING YOUR VPC

NETWORKING ON AZURE

VPC IN GCP

NETWORKING OVERVIEW

NETWORKING OVERVIEW
DESIGNING YOUR VPC
NETWORKING ON AZURE
VPC IN GCP

VIRTUAL PRIVATE CLOUD (VPC)

Provision a private, isolated virtual network on the cloud.

Have complete control over your virtual networking environment.

Please note that we will first cover generic VPC and AWS, then Azure and GCP.

VPCS AND SUBNETS

A subnet defines a range of IP addresses in your VPC.

You can launch resources into a subnet that you select.

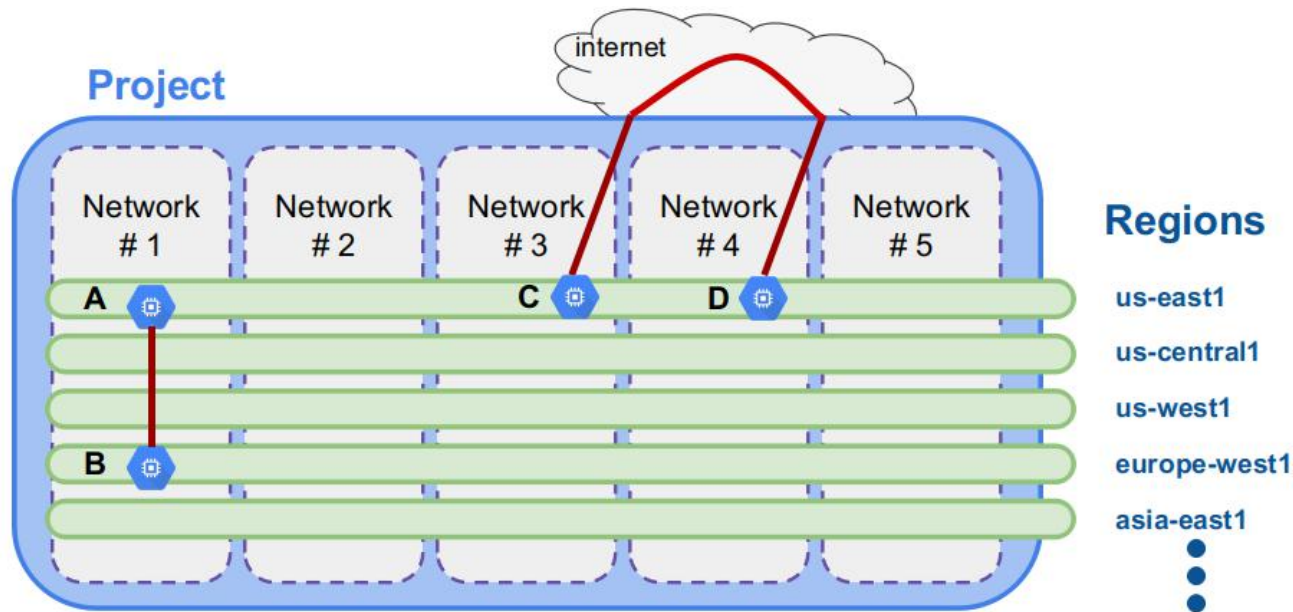
A private subnet should be used for resources that won't be accessible over the Internet.

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.

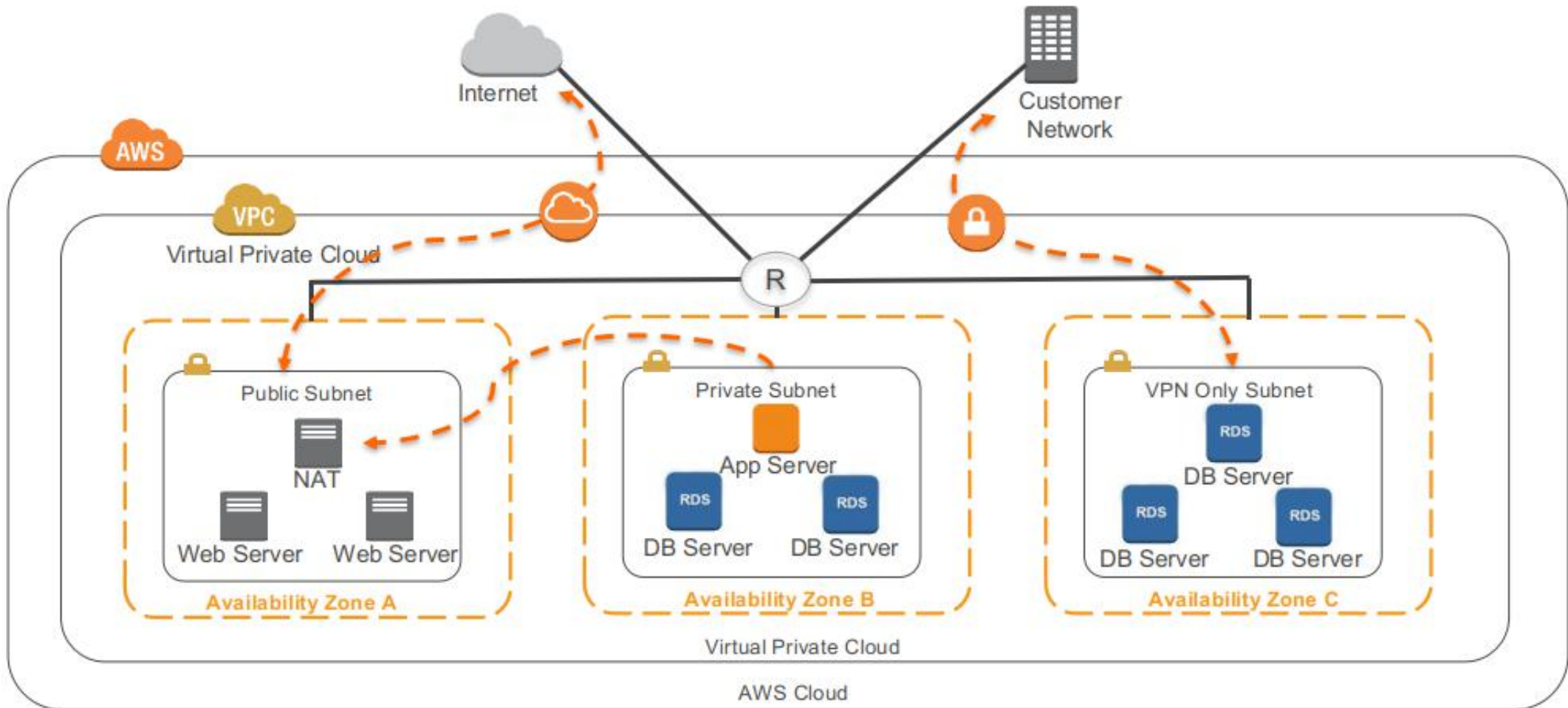
VPC AND REGIONS

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.*

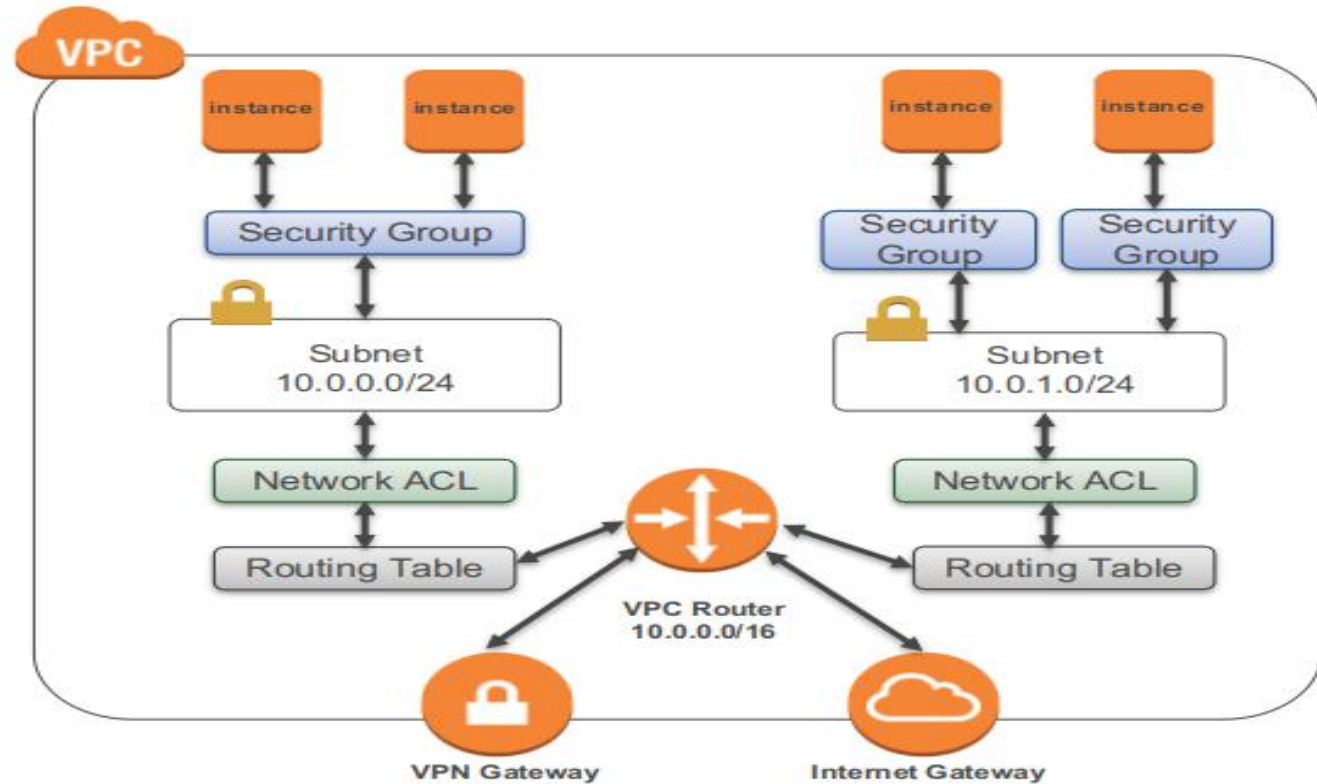
VPC EXAMPLE



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

QUIZ

What acts as an additional layer of security at the subnet level in a VPC?

- A. AAA
- B. CLA
- C. ACL
- D. SSL

DESIGNING YOUR VPC

NETWORKING OVERVIEW

DESIGNING YOUR VPC

NETWORKING ON AZURE

VPC IN GCP

REGION

Does your region meet your environment's data sovereignty and compliance requirements?

Do you meet data security laws of the country and locality in which your data is stored?

Can your researchers' data legally exist outside of the country where you are operating?

Will you be able to meet your governance requirements by placing your environment in the region where you plan to place it?

REGION

How close is the region to your university, users or data centers?

Very important for Amazon: Every 100-ms delay on Amazon.com costs 1% in sales on the website.

- Region travel is limited by speed of light which take 1/8 of a second around the world
- Add other factors - and region choice becomes important even outside of commerce

Most organizations choose an initial region closest to data centers or customers, e.g.:

New York: US East (N. Virginia)

Netherlands: EU (Ireland) or EU (Frankfurt)

Philippines: Asia Pacific (Singapore)

Two equidistant regions to choose from? Consider which has lower costs.

REGION

Does the region you're considering offer all of the services and features your environment might require?

- Not all services and features are available in all regions.
- New services typically launch in a limited number of regions

Are you choosing the most cost-effective region?

- Service costs vary by region.
- Some services (like Amazon S3) have costs when you transfer data out of their original region.
- If you want to replicate your environment across more than one region, is that the most cost-effective solution?

DISCUSSION

Research-related regions consideration

Consider how time sensitive the communications are

- If local instruments or other such local issues are involved, then distance may be a major factor.
- The example that comes to mind is an earthquake shake table where the output of data processing provides near-real time control of the table.
- With a shake table near SF CA, doing compute at TACC was problematic because of the speed of light issues all the way to Texas and back.

HOW MANY AVAILABILITY ZONES SHOULD I USE?

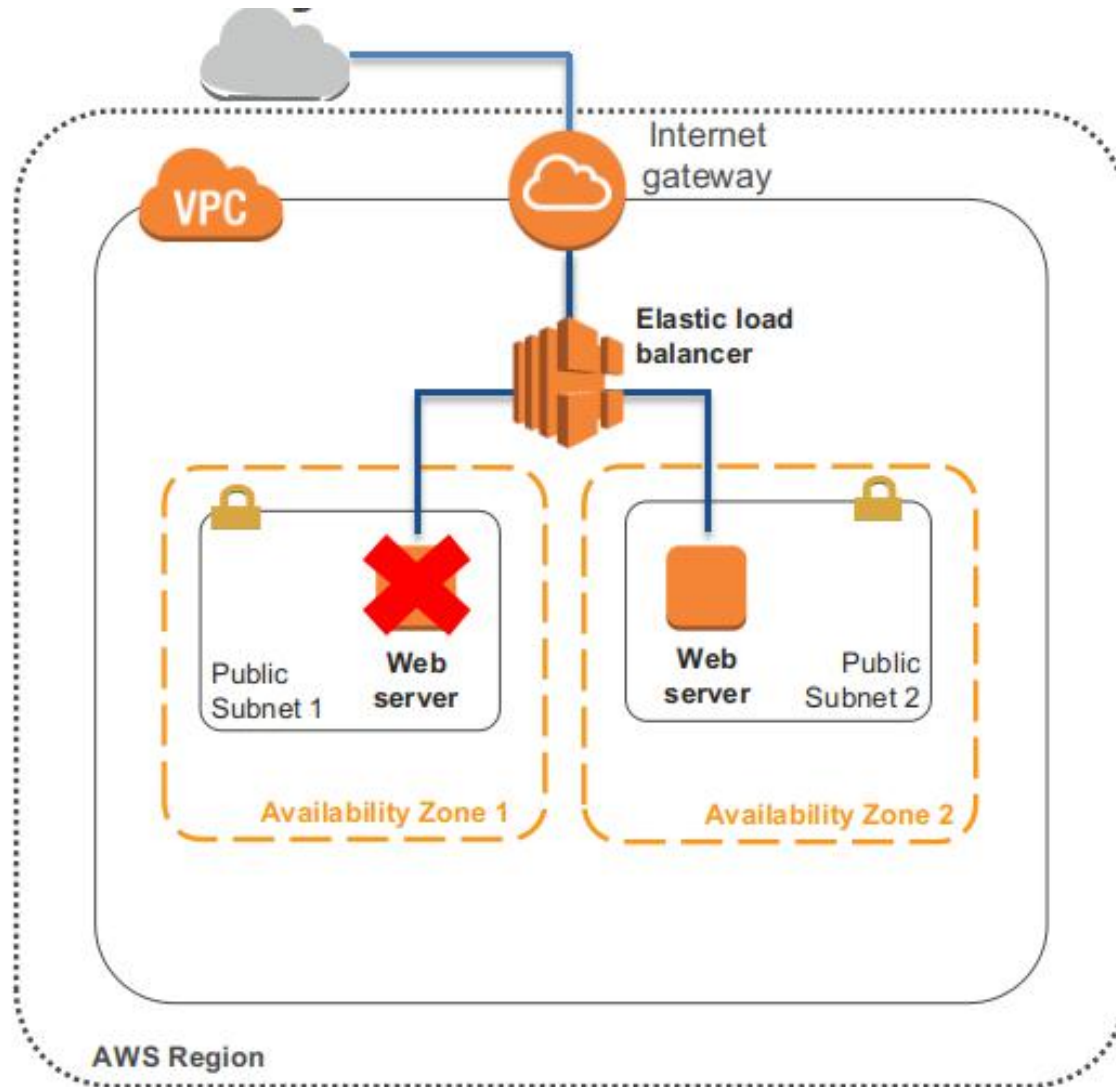
Recommendation: Start with two Availability Zones per region.

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:

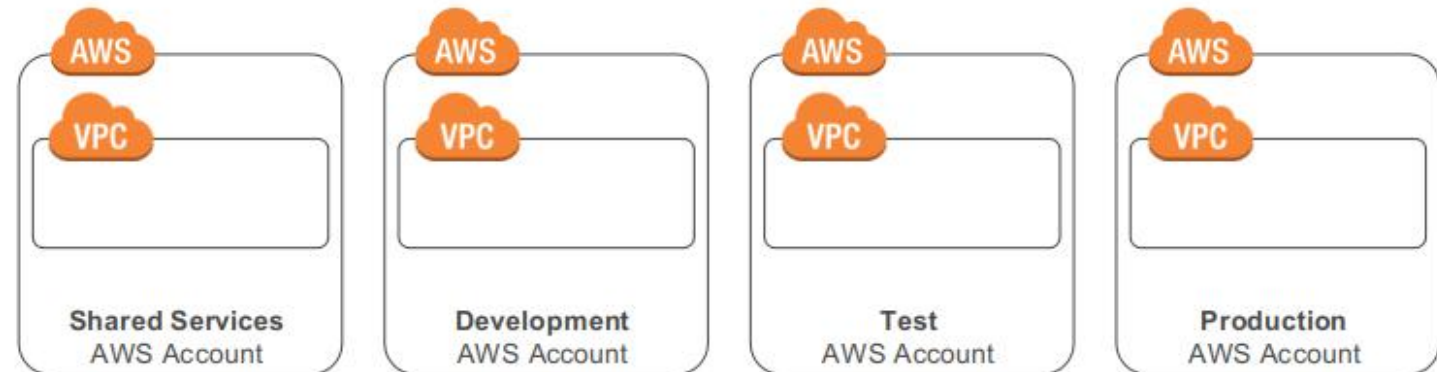
- **Multi-VPC** and **Multi-Account**

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?

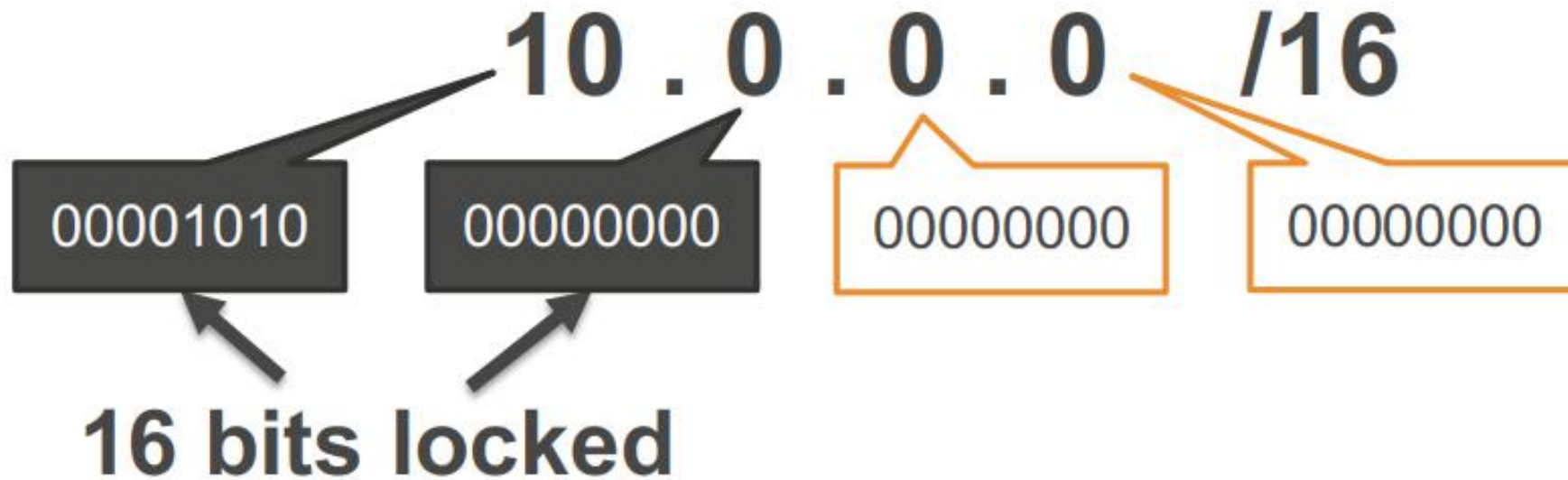
IPS AND CIDR

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:

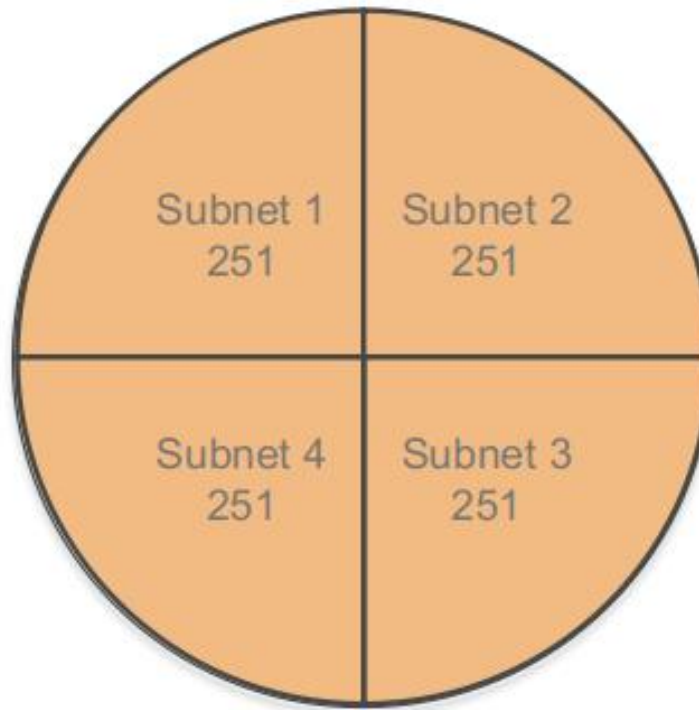
CIDR / Total IPs						
/16	/17	/18	/19	/20	/21	/22
65,536	32,768	16,384	8,192	4,096	2,048	1,024
/23	/24	/25	/26	/27	/28	
512	256	128	64	32	16	

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

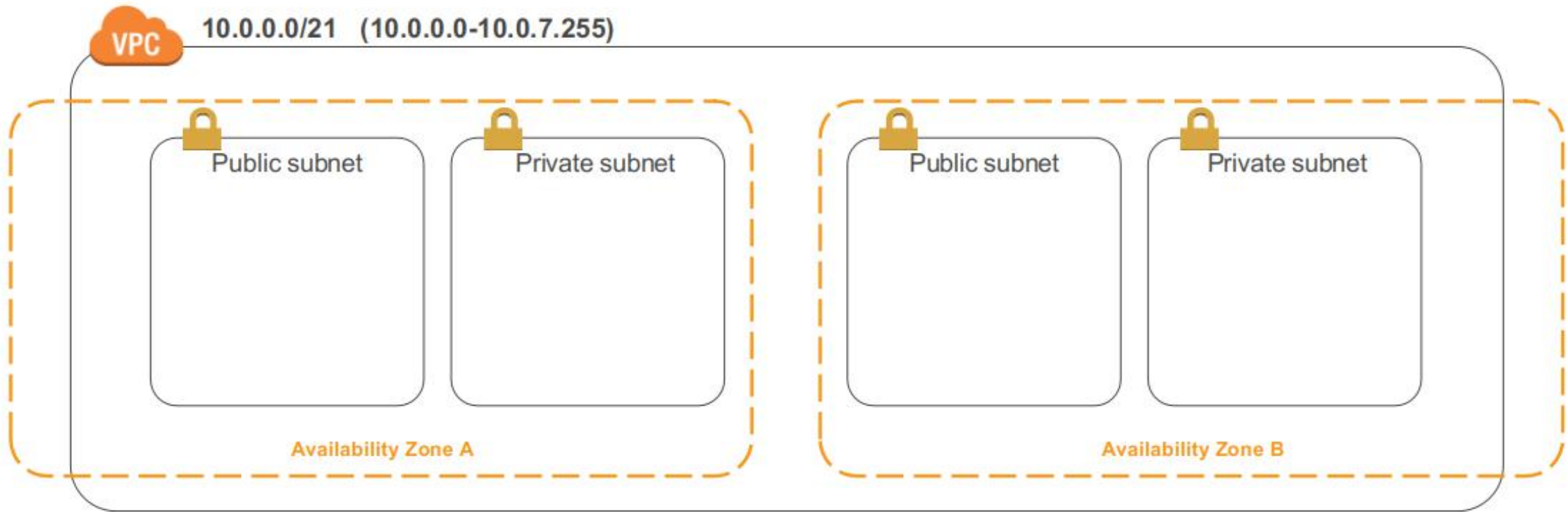
- Include a routing table entry to an **Internet gateway** to support inbound/outbound access to the public Internet.

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.

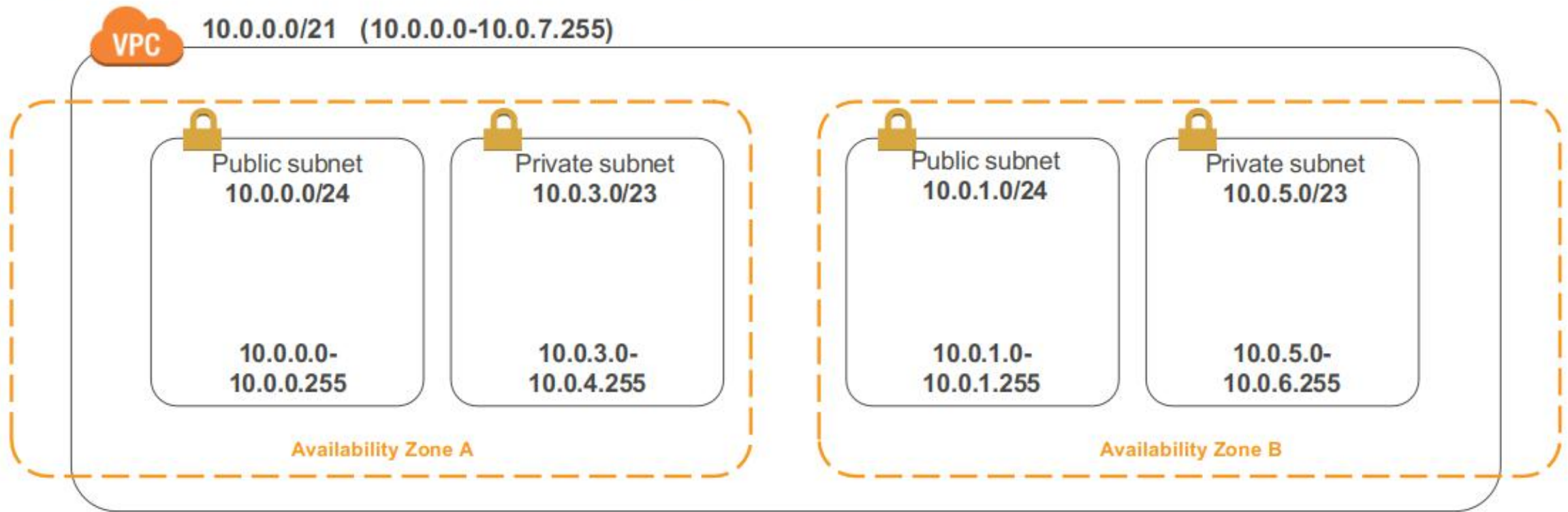
SUBNETS

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.

QUIZ

Which subnet type (public or private) should you use for these resources ?

- A. Datastore instances
 - Public or Private?
- B. Batch processing instances?
 - Public or Private?
- C. Back-end instances
 - Public or Private?
- D. Web application instances?
 - Public or private?

HOW DO YOU CONTROL YOUR VPC TRAFFIC?

Route tables

Security groups

Network ACLs

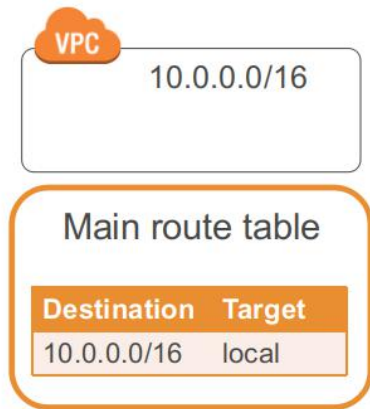
Internet gateways

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.



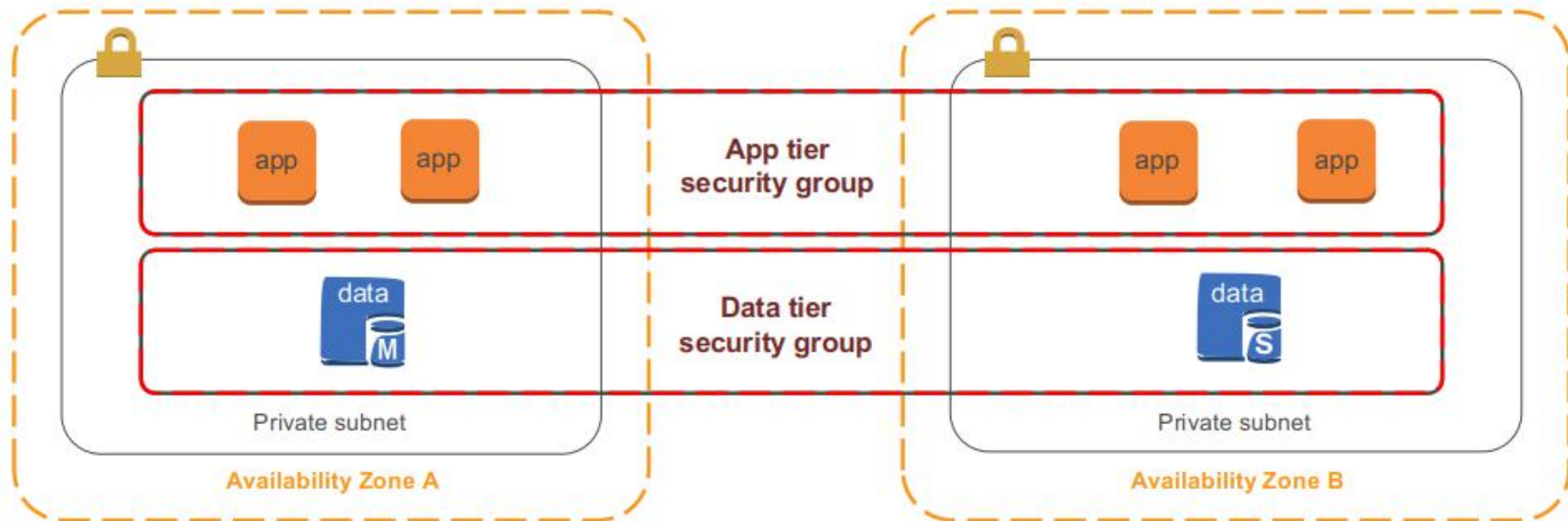
SECURING VPC TRAFFIC WITH SECURITY GROUPS

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

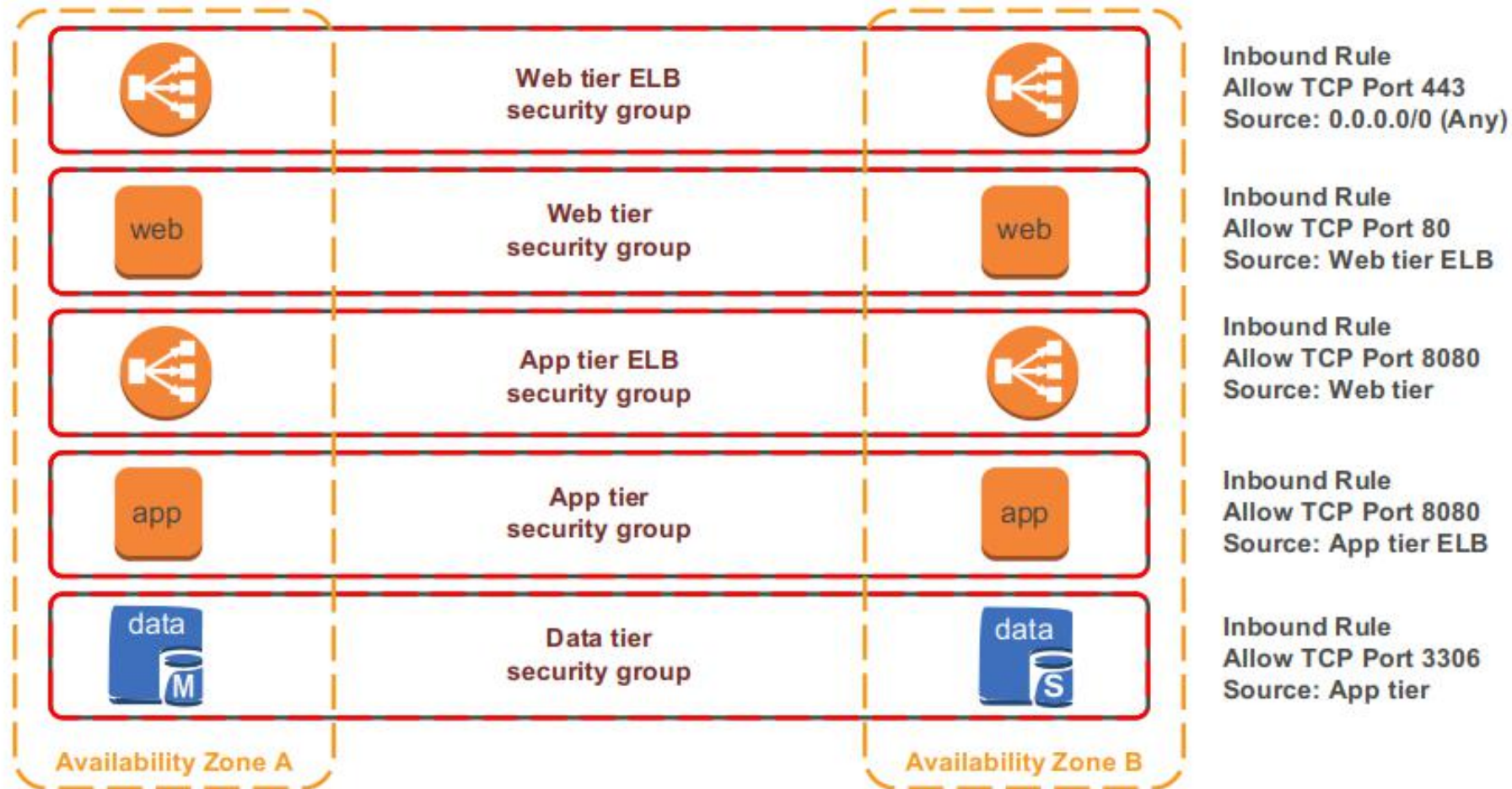
By default, all newly created security groups allow all outbound traffic to all destinations.

- 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.

QUIZ

VPC stands for:

- A. Very Private Cloud
- B. Virtual Public Cloud
- C. Virtual Private Cloud
- Very Public Cloud

QUIZ

Having just created a new VPC and launching an instance into its public subnet, you realise that you have forgotten to assign a public IP to the instance during creation. What is the simplest way to make your instance reachable from the outside world?

- A. Create an elastic IP and a new network interface. Associate the elastic IP to the new network interface, and the new network interface to your instance.
- B. Associate the private IP of your instance to the public IP of the internet gateway
- C. Create an elastic IP address and associate it with your instance
- D. Nothing - by default all instance deployed into any public subnet will automatically receive a public IP

QUIZ

True or False: A subnet can span multiple Availability Zones.

- A. True
- B. False

QUIZ

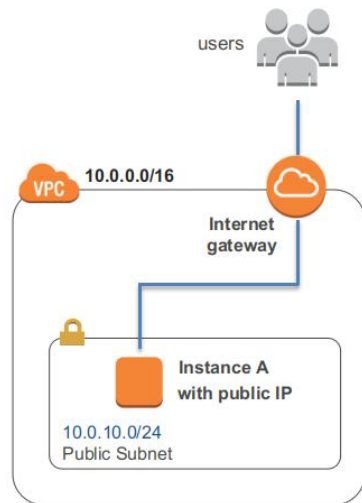
Are you permitted to conduct your own vulnerability scans on your own VPC without alerting AWS first?

- A. Yes. You can perform any scan without first alerting AWS
- B. No. You must always alert AWS before performing any kind of vulnerability scan
- C. It depends. Until recently customers were not permitted to conduct penetration testing without AWS engagement. However that has changed. There are still conditions though.

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.

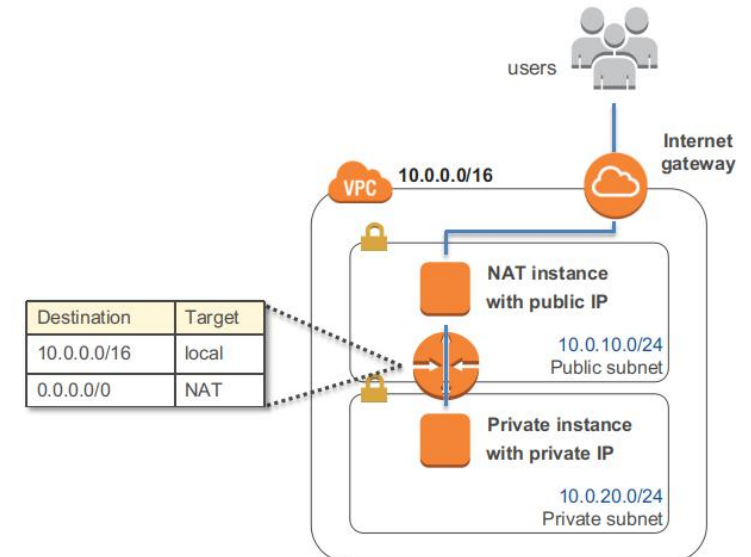
OUTBOUND TRAFFIC FROM PRIVATE INSTANCES

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



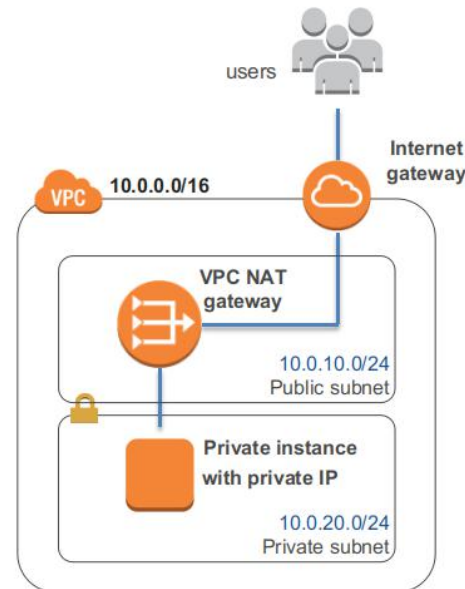
OUTBOUND TRAFFIC FROM PRIVATE INSTANCES

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:

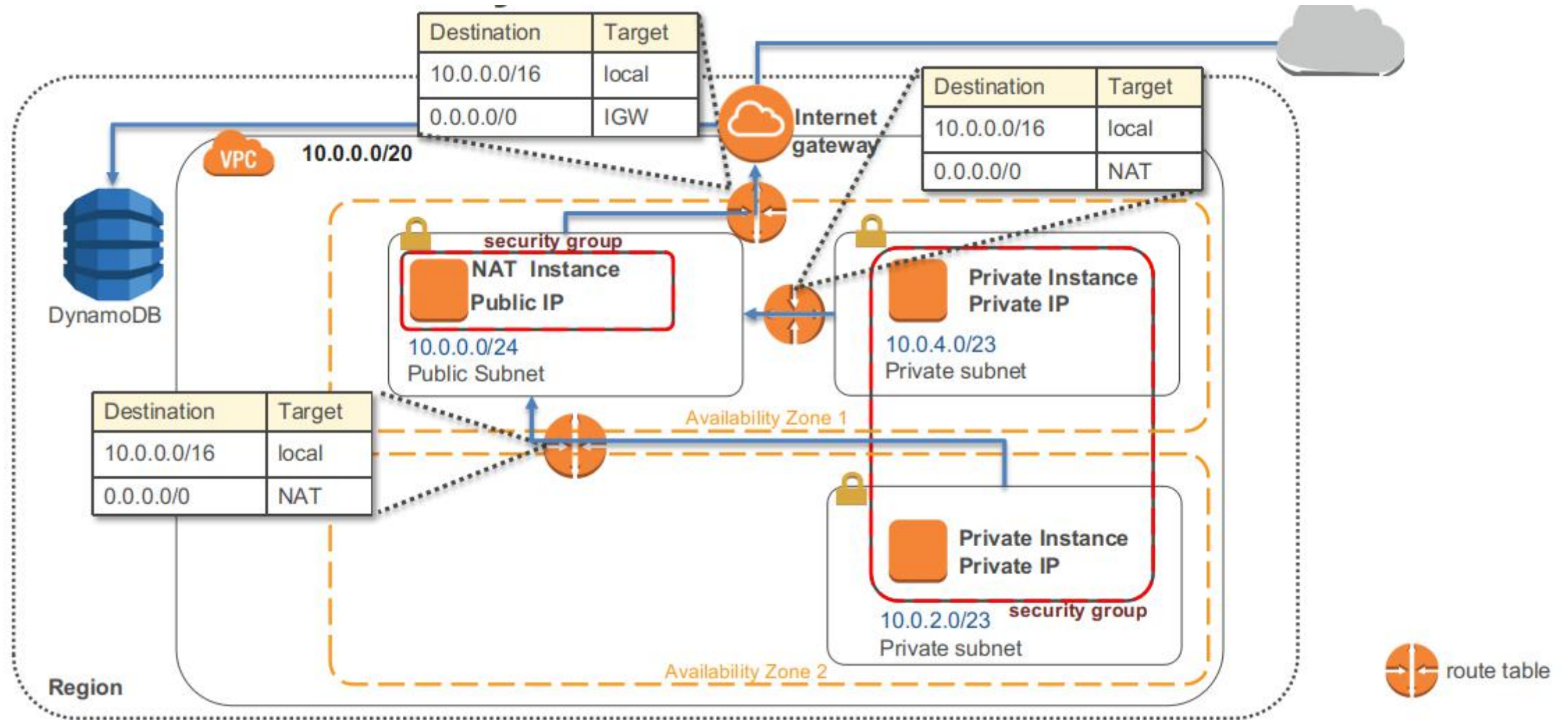
- Amazon EC2 instance set up as a NAT in a public subnet
- VPC NAT Gateway



VPC NAT Gateways vs. NAT Instances

	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:

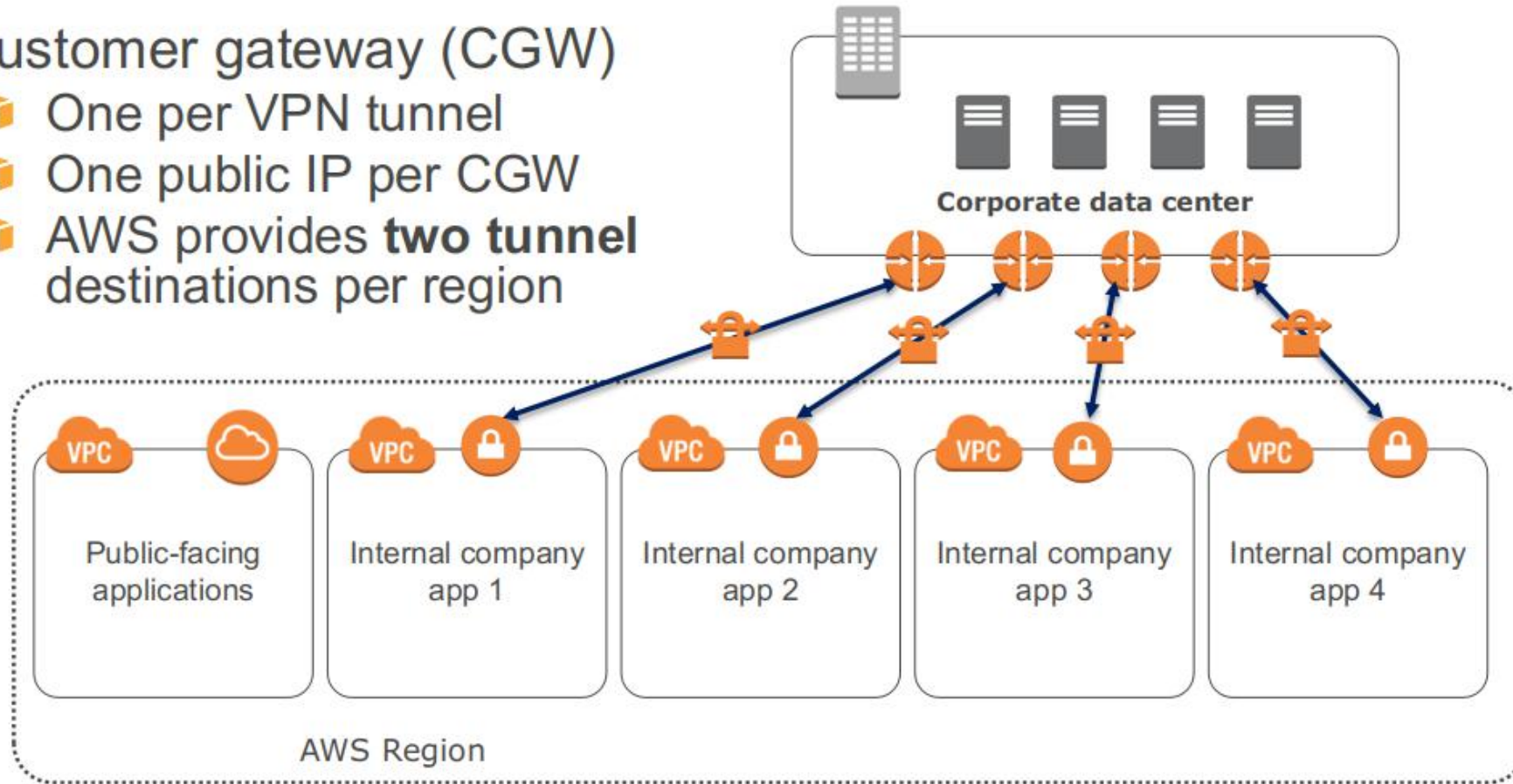
-  Troubleshoot connectivity issues.
-  Test network access rules.
-  Monitor traffic.
-  Detect and investigate security incidents.

CONNECTING VPCS TOGETHER

Not the right way

Customer gateway (CGW)

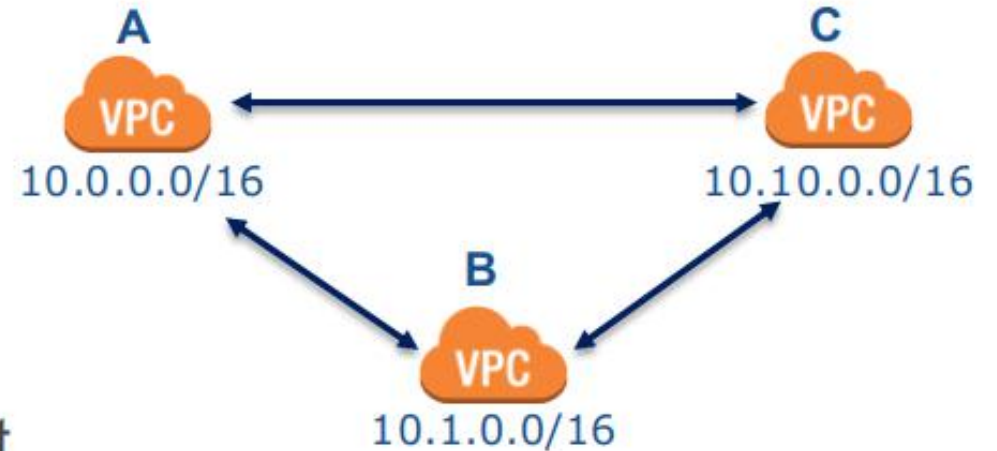
- One per VPN tunnel
- One public IP per CGW
- AWS provides **two tunnel** destinations per region



VPC PEERING

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

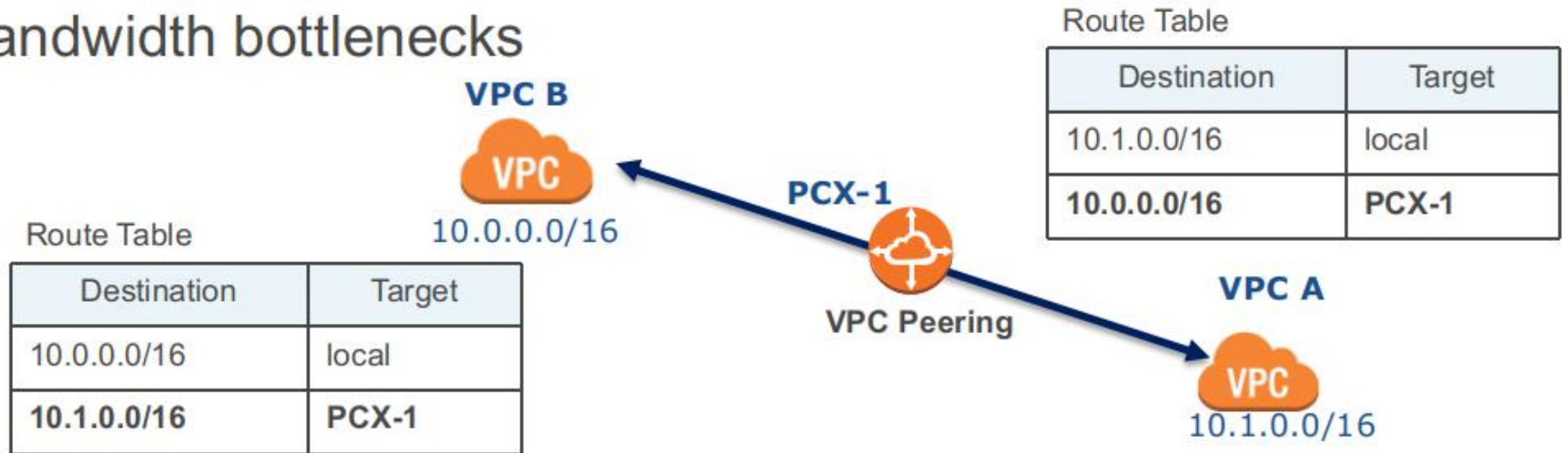
- 📦 Use private IP addresses.
- 📦 VPCs reside in the same region.
- 📦 IP space cannot overlap.
- 📦 Only one between any two VPCs.
- 📦 Transitive peering relationships are not supported



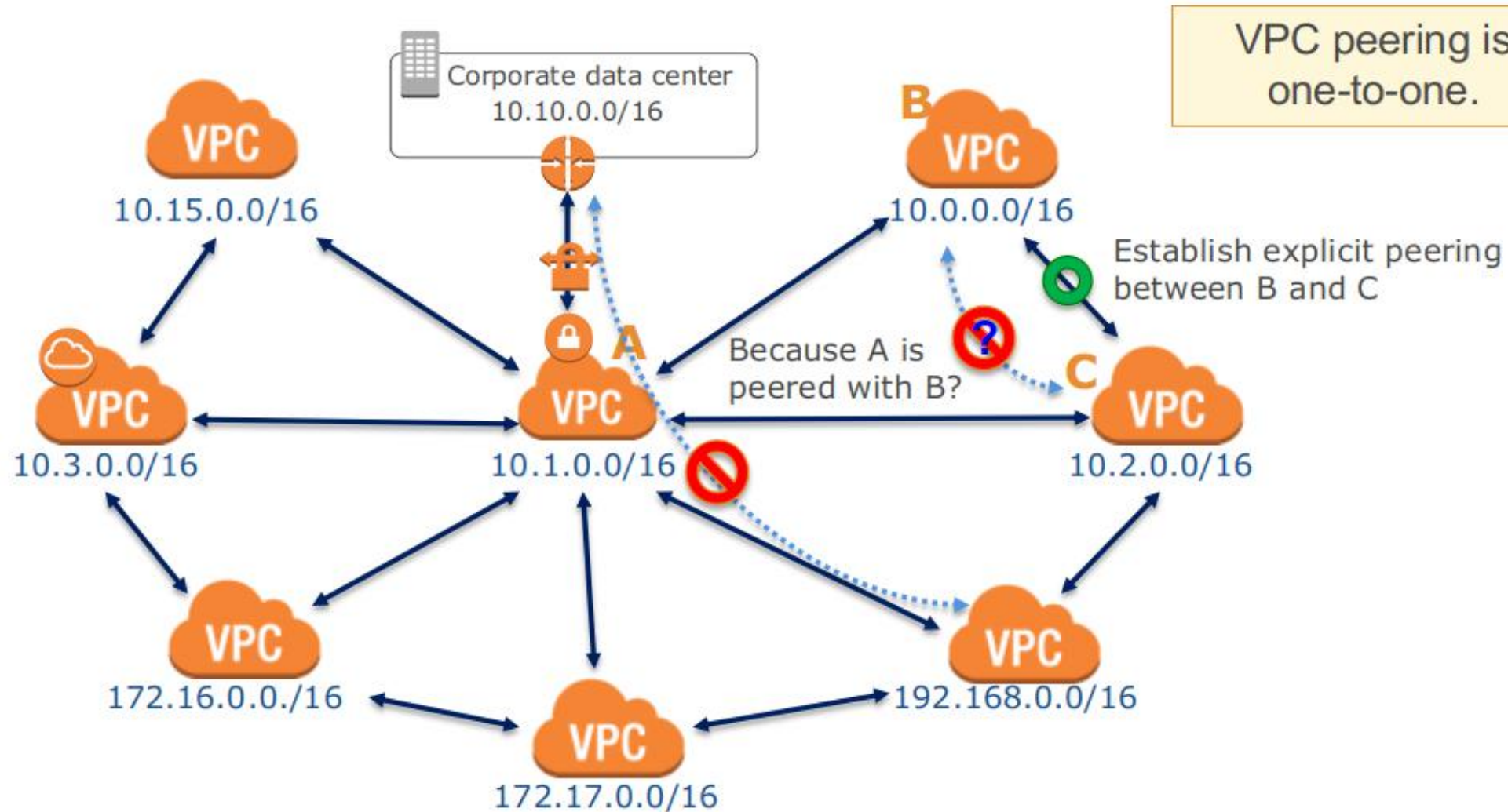
Instances in either VPC can communicate with each other as if they are within the same network.

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.

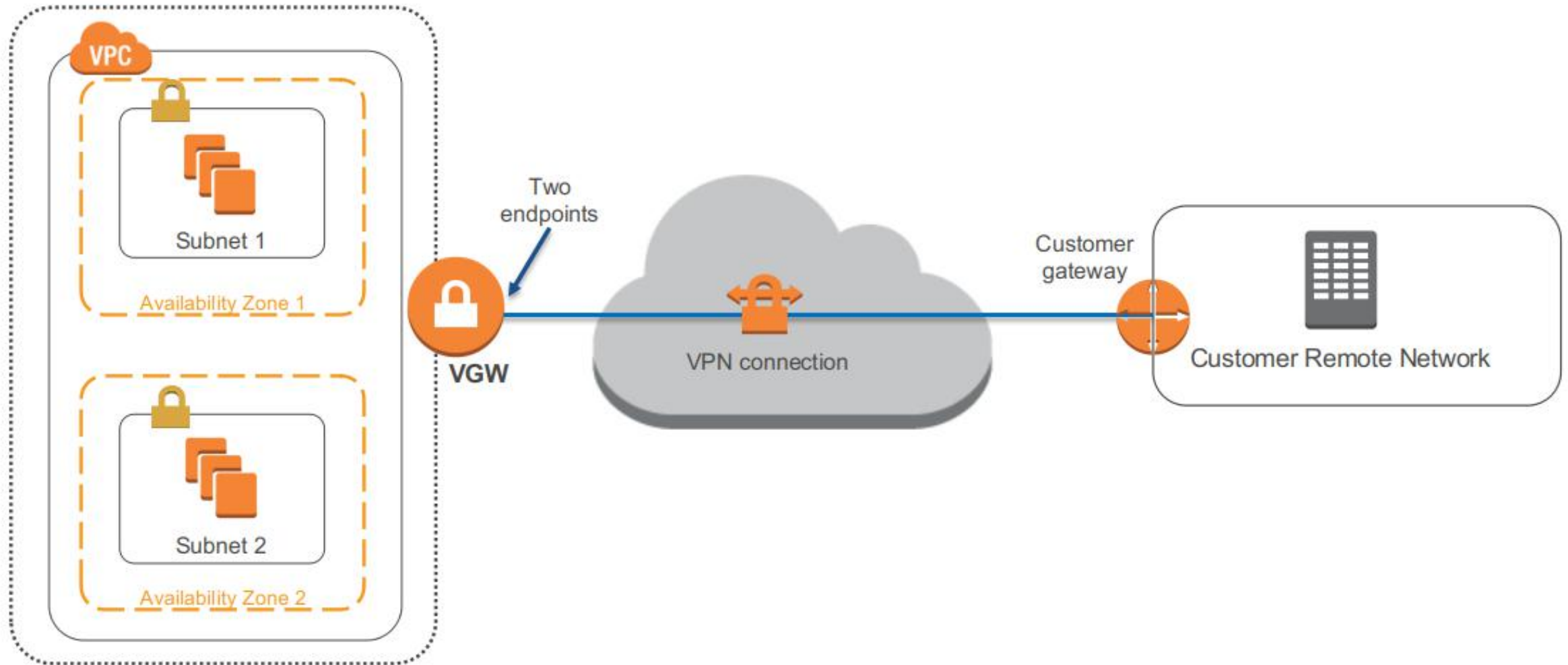
Routing controls: Routing tables control the local subnets that can route to remote subnets.

Security groups control what traffic an instance can send or receive.

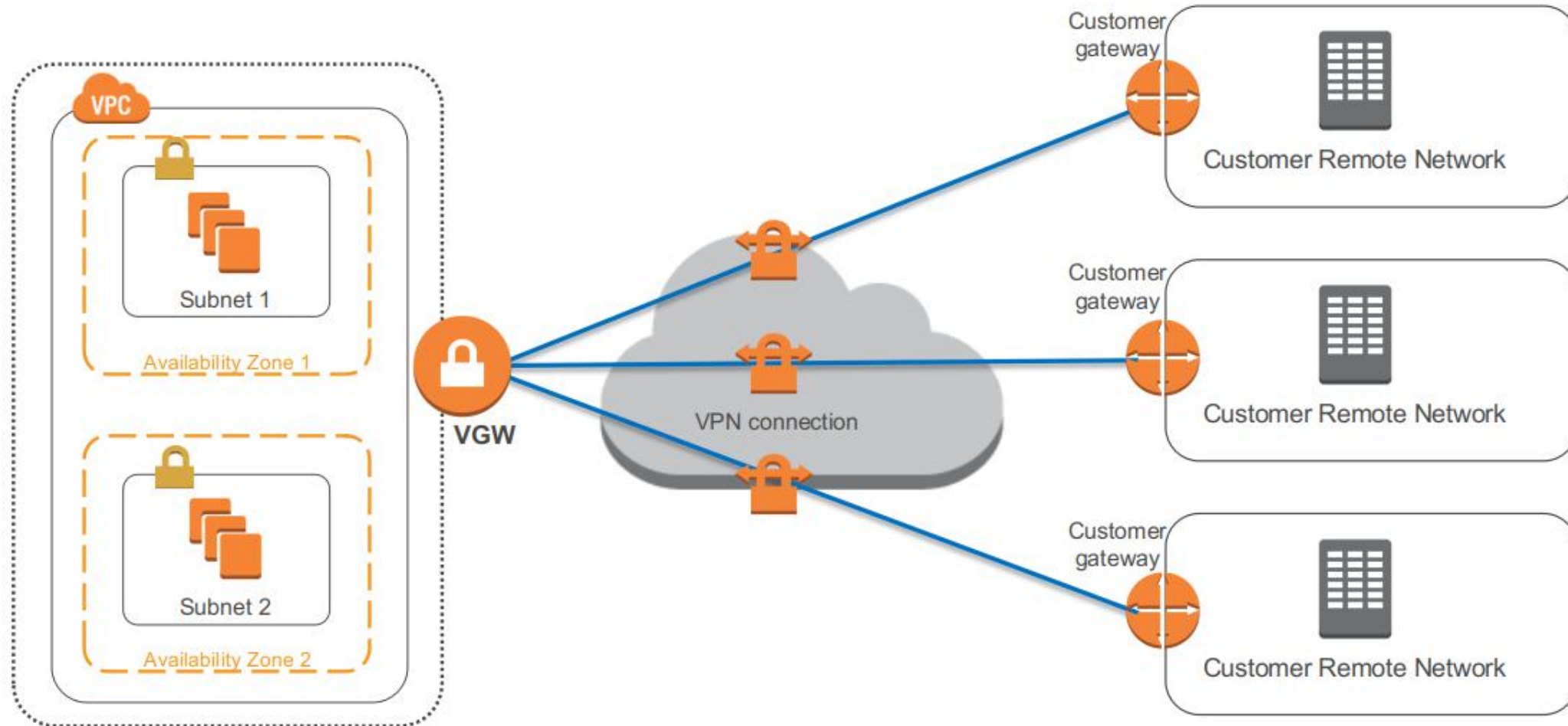
Network ACLs control what traffic a subnet can send or receive.

No edge-to-edge routing or transitive trusts: Reduces inadvertently creating unexpected network connections.

EXTENDING NETWORK TO AWS: VPN CONNECTIONS



EXTENDING 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 TO 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.

QUIZ

True or False: You can accelerate your application by adding a second internet gateway to your VPC.

- A. True
- B. False

QUIZ

When peering VPCs, you may peer your VPC only with another VPC in your same AWS account.

- A. True
- B. False

QUIZ

True or False: An application load balancer must be deployed into at least two subnets.

- A. True
- B. False

QUIZ

Which of the following is a chief advantage of using VPC endpoints to connect your VPC to services such as S3?

- A. Traffic between the VPC and the other service does not have to leave the Amazon network
- B. VPC endpoints offer a faster path through the public internet
- C. VPC endpoints require a public IP which gives faster connectivity
- D. VPC endpoints are hardware devices

QUIZ

Which of the following allows you to SSH or RDP into an EC2 instance located in a private subnet?

- A. Bastion host
- B. NAT instance
- C. NAT gateway
- D. Internet gateway

QUIZ

When I create a new security group, all outbound traffic is allowed by default.

- A. True
- B. False

QUIZ

To save administration headaches, a consultant advises that you leave all security groups in web-facing subnets open on port 22 to 0.0.0.0/0 CIDR. That way, you can connect wherever you are in the world. Is this a good security design?

- A. True
- B. False

NETWORKING ON AZURE

NETWORKING OVERVIEW
DESIGNING YOUR VPC
NETWORKING ON AZURE
VPC IN GCP

AZURE VIRTUAL NETWORKS

Virtual networks are for connecting

- VMs
- App Service Environment for Power Apps
- Azure Kubernetes Service
- Azure virtual machine scale sets.

Azure Service endpoints

- To connect to other Azure resource types
- Azure SQL databases
- Storage accounts
- This approach enables you to link multiple Azure resources to virtual networks to improve security and provide optimal routing between resources.

COMMUNICATE WITH ON-PREMISES RESOURCES

Point-to-site virtual private networks

- This approach is like a virtual private network (VPN) connection that a computer outside your organization makes back into your corporate network, except that it's working in the opposite direction. In this case, the client computer initiates an encrypted VPN connection to Azure to connect that computer to the Azure virtual network.

Site-to-site virtual private networks

- A site-to-site VPN links your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the internet.

Azure ExpressRoute

- For environments where you need greater bandwidth and even higher levels of security, Azure ExpressRoute is the best approach. ExpressRoute provides dedicated private connectivity to Azure that doesn't travel over the internet.

ROUTE NETWORK TRAFFIC

By default, Azure routes traffic between subnets on any connected virtual networks, on-premises networks, and the internet. You also can control routing and override those settings, as follows:

Route tables

- A route table allows you to define rules about how traffic should be directed. You can create custom route tables that control how packets are routed between subnets.

Border Gateway Protocol

- Border Gateway Protocol (BGP) works with Azure VPN gateways or ExpressRoute to propagate on-premises BGP routes to Azure virtual networks.

FILTER NETWORK TRAFFIC

Network security groups

- A network security group is an Azure resource that can contain multiple inbound and outbound security rules. You can define these rules to allow or block traffic, based on factors such as source and destination IP address, port, and protocol.

Network virtual appliances

- A network virtual appliance is a specialized VM that can be compared to a hardened network appliance. A network virtual appliance carries out a particular network function, such as running a firewall or performing wide area network (WAN) optimization.

CONNECT VIRTUAL NETWORKS

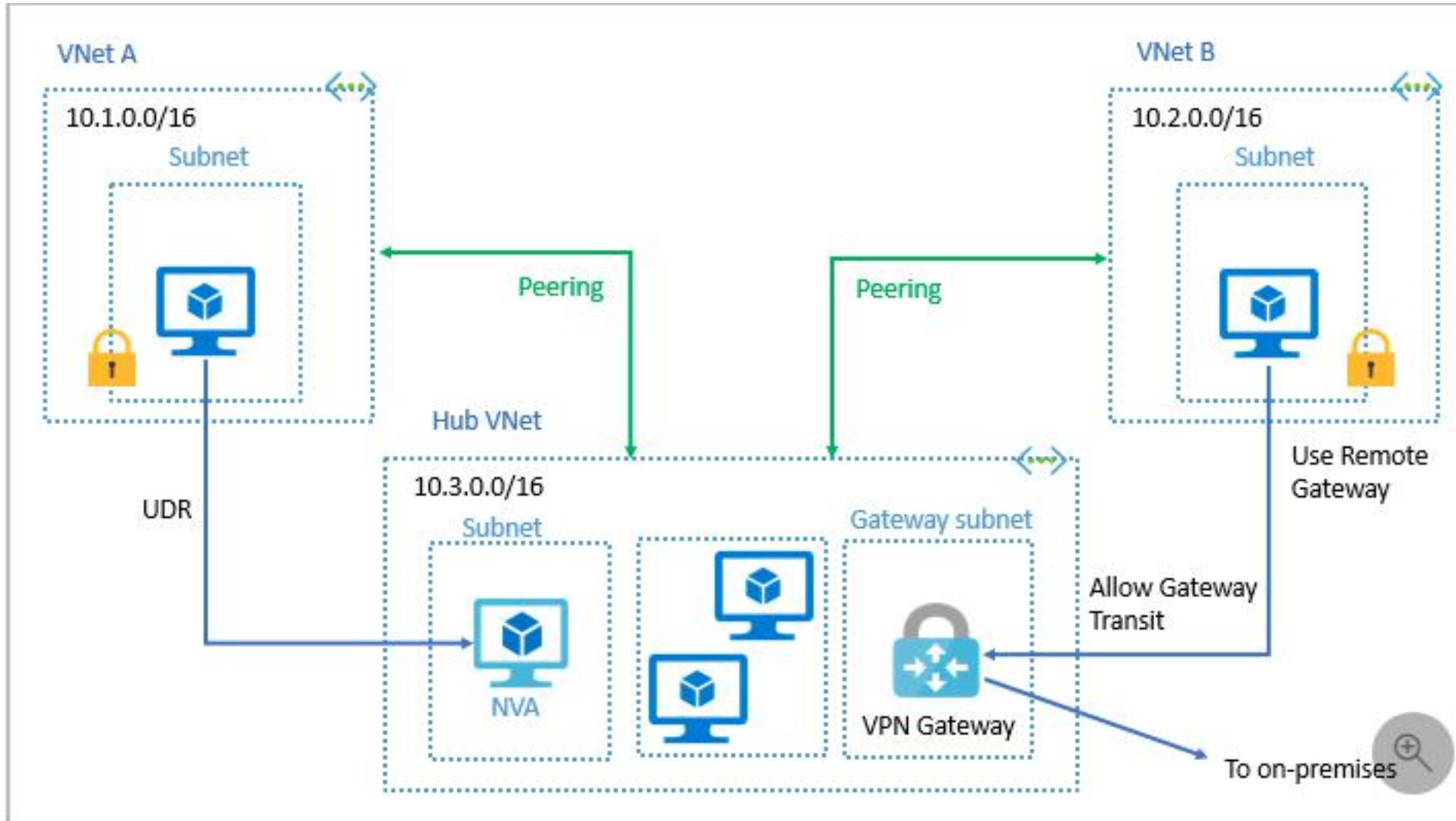
You can link virtual networks together by using virtual network peering.

- Peering enables resources in each virtual network to communicate with each other. These virtual networks can be in separate regions, which allows you to create a global interconnected network through Azure.

UDR is user-defined Routing.

- UDR is a significant update to Azure's Virtual Networks
- allows network admins to control the routing tables between subnets within a subnet as well as between VNets thereby allowing for greater control over network traffic flow.

NETWORK PEERING



CREATE A VIRTUAL NETWORK

Configure a number of basic settings

[Home](#) > [New](#) > [Virtual Network](#) >

Create virtual network

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription *	<div>Pay-As-You-Go (d418faed-fae9-4d3f-bd63-cee2db8fcea) ▼</div>
Resource group *	<div>▼</div> <div>Create new</div>

Instance details

Name *	<div></div>
Region *	<div>(US) East US ▼</div>

NETWORK CREATED

You will be able to adjust the settings later

Microsoft Azure

[Home](#) > [New](#) > [Virtual Network](#) >

Create virtual network

✓ Validation passed

Basics

IP Addresses

Security

Tags

Review + create

Basics

Subscription

Resource group

Name

Region

Pay-As-You-Go

(new) Internet2

Class

East US

IP addresses

Address space

Subnet

10.0.0.0/16

default (10.0.0.0/24)

Tags

None

Security

BastionHost

DDoS protection plan

Firewall

Disabled

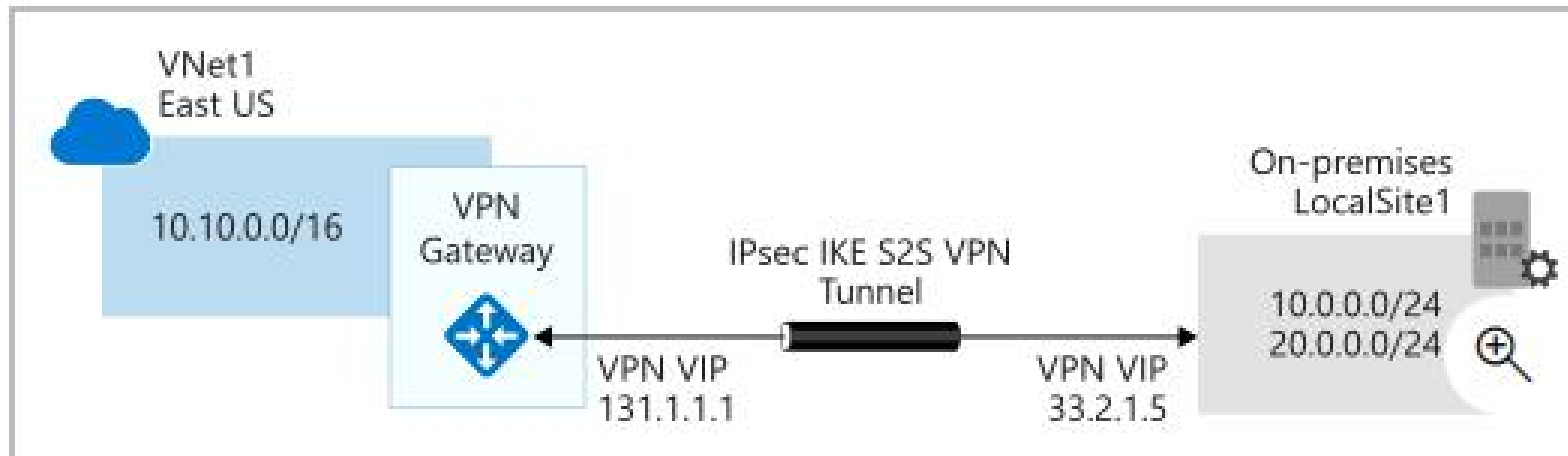
Basic

Disabled

VPN GATEWAYS

A VPN gateway is a type of virtual network gateway. Azure VPN Gateway instances are deployed in Azure Virtual Network instances and enable the following connectivity:

- Connect on-premises datacenters to virtual networks through a site-to-site connection.
- Connect individual devices to virtual networks through a point-to-site connection.
- Connect virtual networks to other virtual networks through a network-to-network connection.



QUIZ

You want to create a secure communication tunnel between branch offices. Which of the following technologies can NOT be used?

- A. Point-to-site virtual private network
- B. Implicit FTP over SSL
- C. Azure ExpressRoute
- D. Site-to-site virtual private network

QUIZ

You want to use Azure ExpressRoute to connect its on-premises network to the Microsoft cloud. Which of the following choices isn't an ExpressRoute model that you can use?

- A. Any-to-any connection
- B. Site-to-site virtual private network
- C. Point-to-point Ethernet connection
- D. CloudExchange colocation

QUIZ

Which of the following options can you use to link virtual networks?

- A. Network address translation
- B. Multi-chassis link aggregation
- C. Dynamic Host Configuration Protocol
- D. Virtual network peering

VPC IN GCP

NETWORKING OVERVIEW
DESIGNING YOUR VPC
NETWORKING ON AZURE
VPC IN GCP

ORGANIZING THINGS IN GCP

Projects, networks, and subnetworks

IP addresses

Routes and rules

Billing

PROJECTS AND NETWORKS

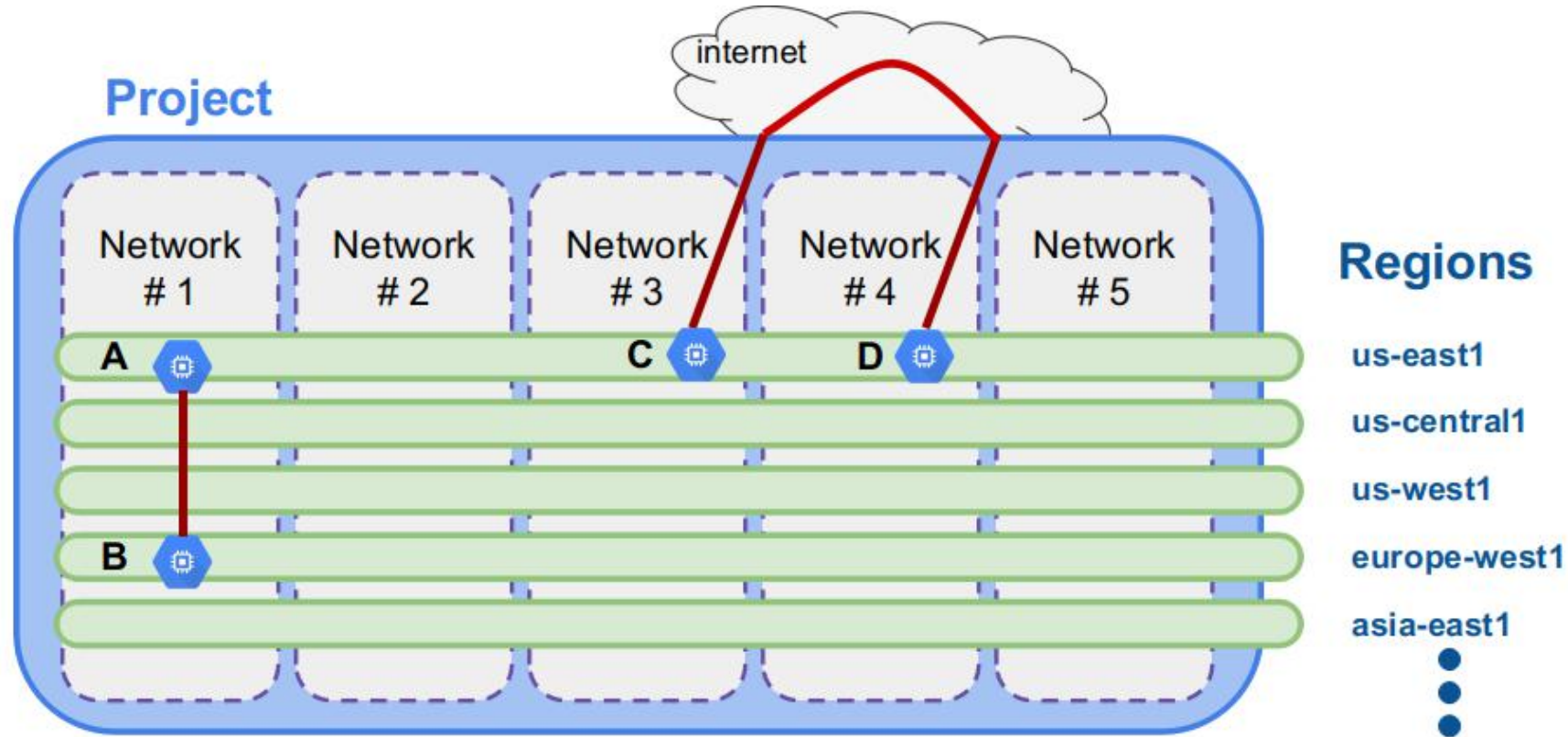
A project:

- Associates objects and services with billing.
- Contains networks (quota max 5).

A network:

- Has no IP address range.
- Is global and spans all available regions.
- Contains subnetworks.
- Can be of type default, auto mode, or custom mode.

NETWORKS ISOLATE SYSTEMS



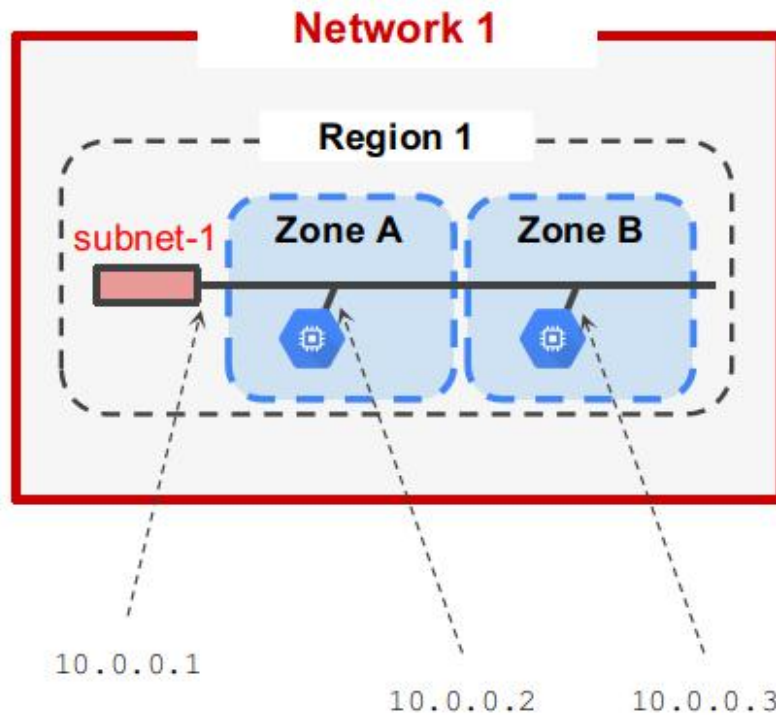
- A and B can communicate over internal IPs *even though they are in different regions.*
- C and D must communicate over external IPs *even though they are in the same region.*

SUBNETWORKS CROSS ZONES

Subnetworks can extend across zones in the same region.

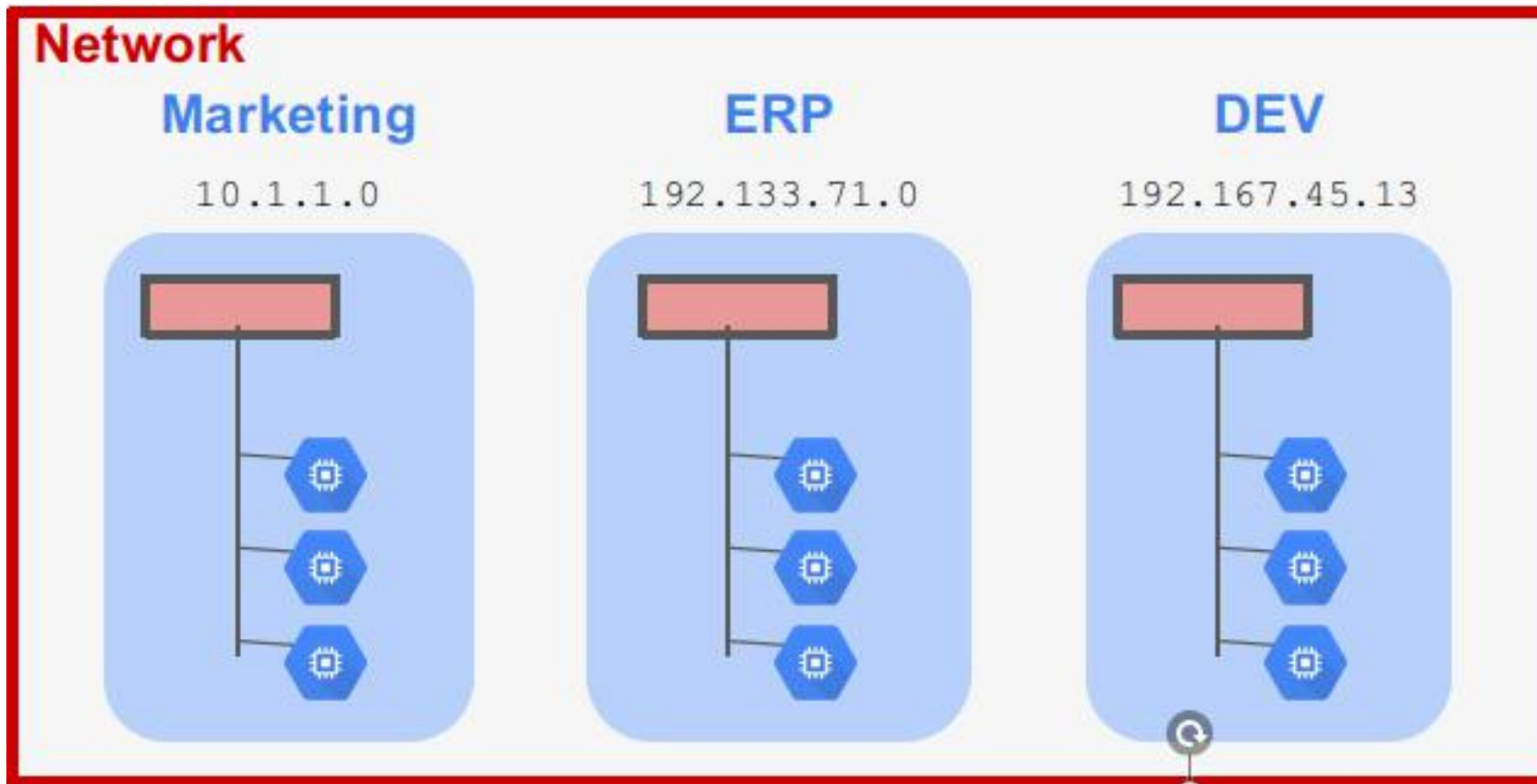
One VM and an alternate VM can be on the same subnet but in different zones.

A single firewall rule can apply to both VMs even though they are in different zones.



SUBNETWORKS ARE FOR MANAGING RESOURCES

Networks have no IP range, so subnetworks don't need to fit into an address hierarchy. Instead, subnetworks can be used to group and manage resources. They can represent departments, business functions, or systems.



IP ADDRESSES



Internal IP	External IP
Allocated from subnet range to VMs by DHCP	Assigned from pool (ephemeral)
DHCP lease is renewed every 24 hours	Reserved (static) Billed when not attached to a running VM
VM name + IP is registered with network-scoped DNS	VM doesn't know external IP; it is mapped to the internal IP

External IPs are mapped to internal IPs

DNS RESOLUTION FOR INTERNAL ADDRESSES

Each instance has a hostname that can be resolved to an internal IP address:

- The hostname is the same as the instance name.
- FQDN is [hostname].c.[project-id].internal.
 - Example: guestbook-test.c.guestbook-151617.internal

Name resolution is handled by internal DNS resolver:

- Provided as part of Compute Engine (169.254.169.254).
- Configured for use on instance via DHCP.
- Provides answer for internal and external addresses.

ROUTE - MAPPING OF IP RANGE TO A DESTINATION

Every network has:

- Routes that let instances in a network send traffic directly to each other.
- A default route that directs packets to destinations that are outside the network.

The fact that a packet has a route to a destination doesn't mean it can get there; firewall rules must also allow the packet.

QUIZ

GCP firewall rules are stateful

- A. True
- B. False

QUIZ

When you enable a project as a shared VPC, all of its existing and future networks will be shared networks

- A. True
- B. False

QUIZ

Once VPCs are peered, administration of routes, firewalls, etc can be performed centrally

- A. True
- B. False

QUIZ

GCP VPC networks are global resources

- A. True
- B. False

QUIZ

When you configure an ingress firewall rule, the subsequent egress traffic is automatically allowed

- A. True
- B. False

CONGRATS ON COMPLETION

