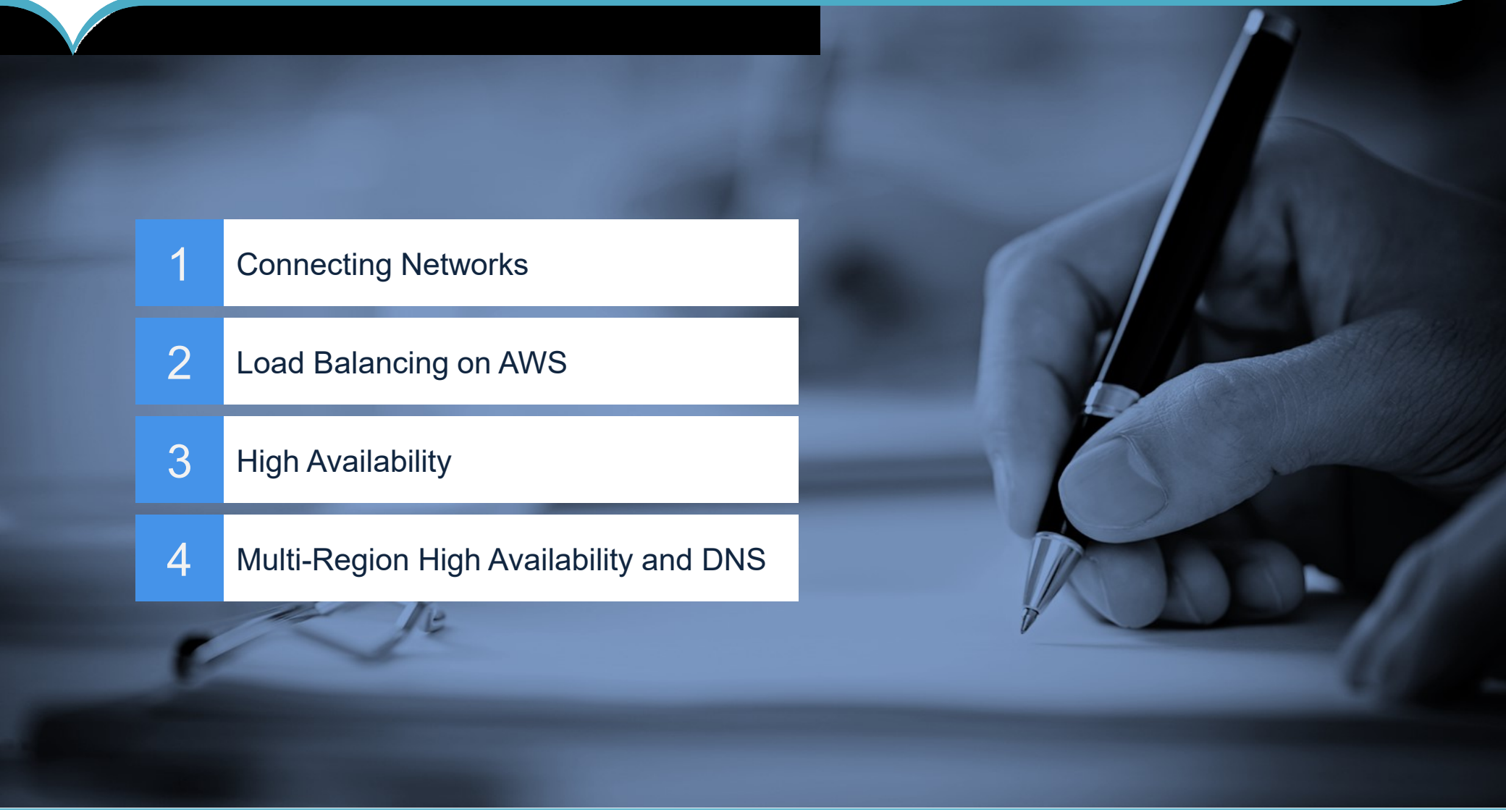
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Networking in AWS Part 2

2019

People matter, results count.

Agenda



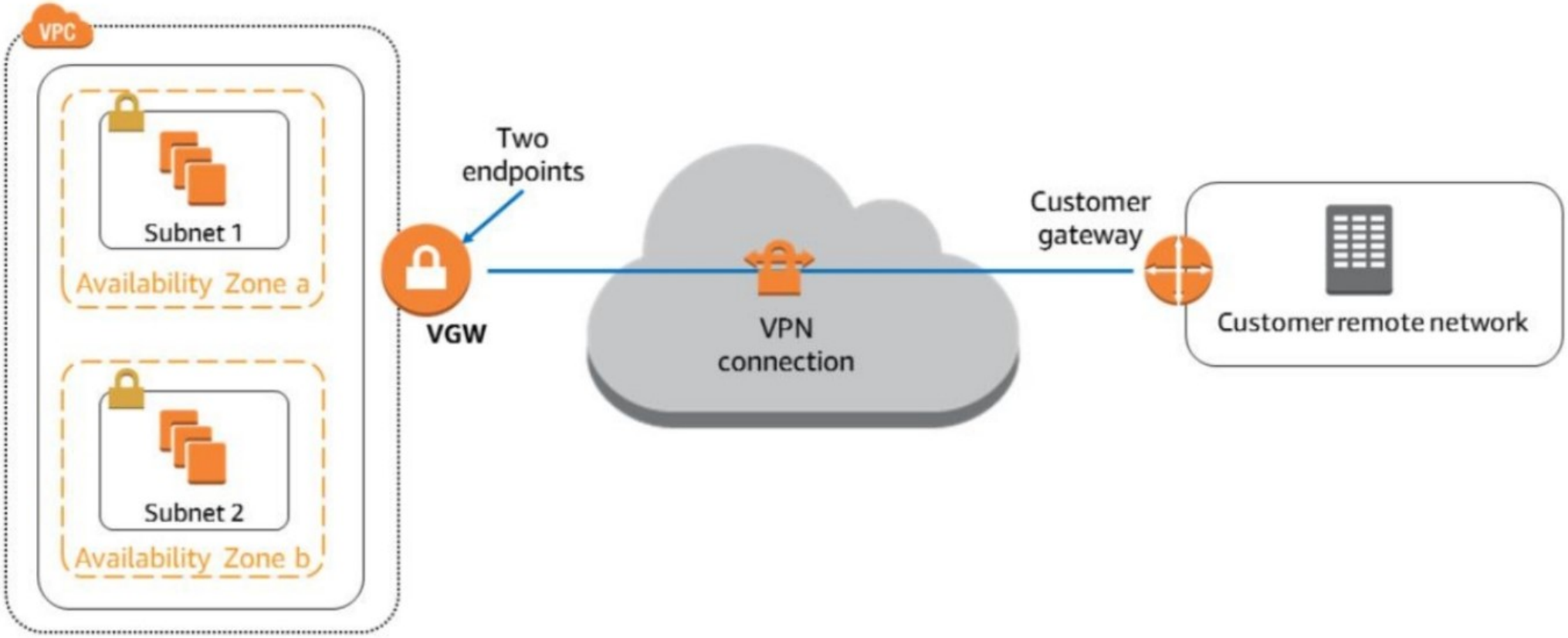
1. Connecting Networks
2. Load Balancing on AWS
3. High Availability
4. Multi-Region High Availability and DNS

Connecting Networks

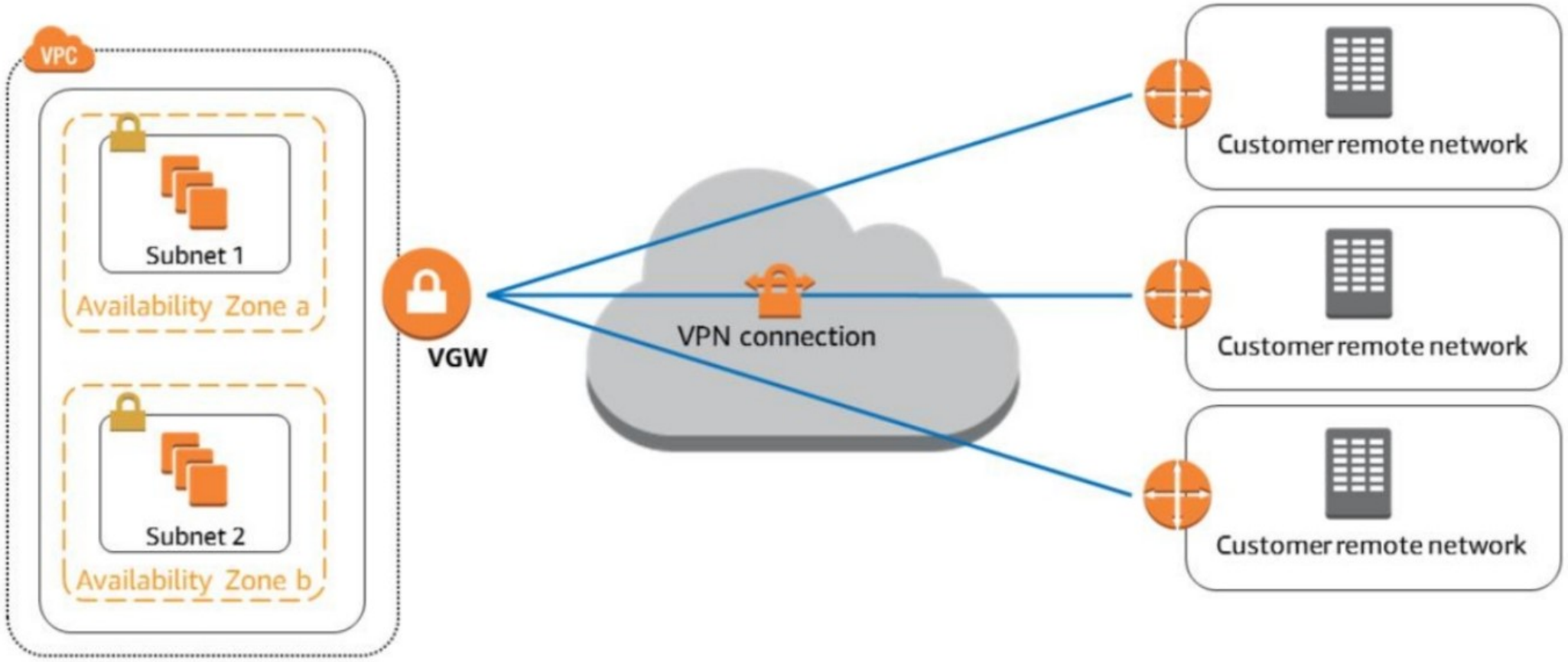
Virtual Private Gateway (VPG)

Enables you to establish private connections (VPNs) between an Amazon VPC and another network

Extending On-Premises Network to AWS: VPN Connections



Extending On-Premises Network to AWS: Multiple VPN



AWS Direct Connect (DX)

AWS Direct Connect(DX) provides you with a **dedicated, private network connection** of either 1 or 10 Gbps

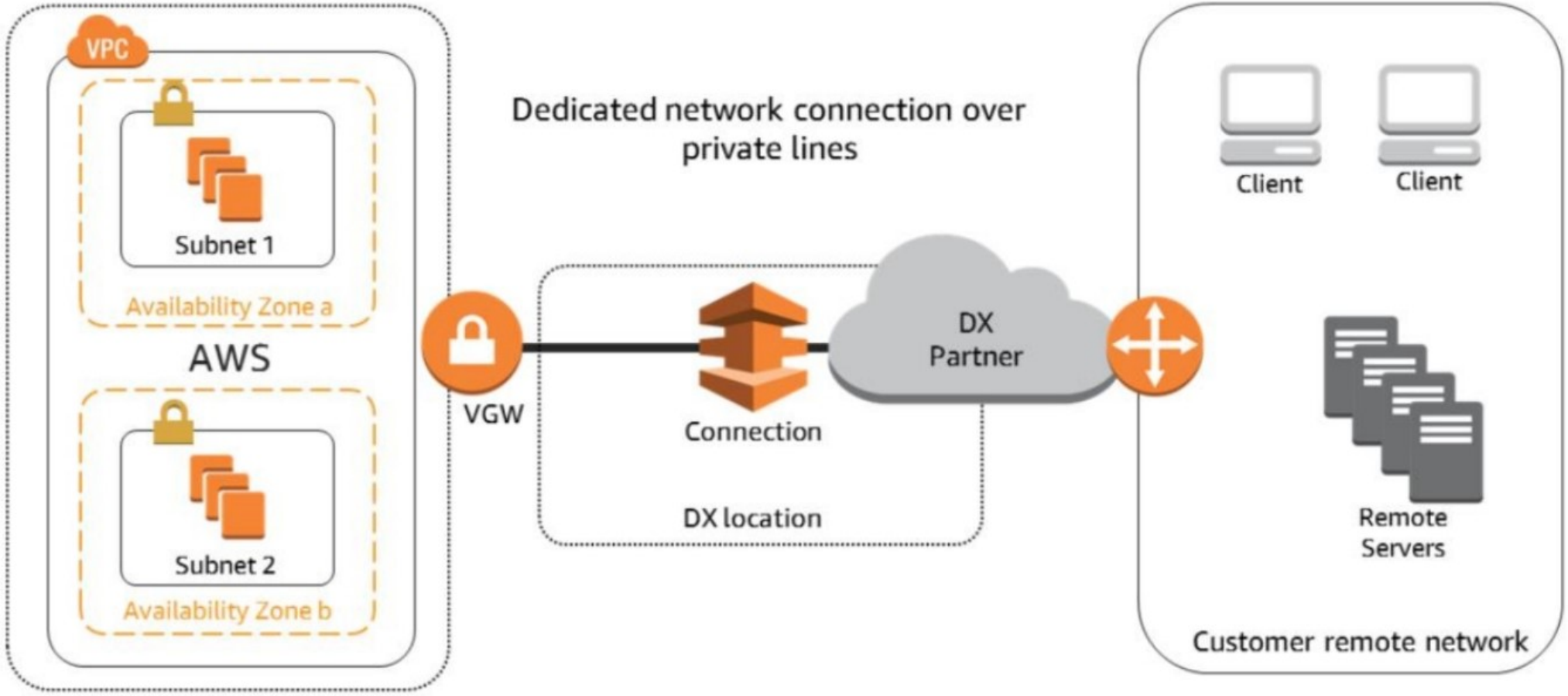
Reduces data transfer costs

Improve application performance with predictable metrics

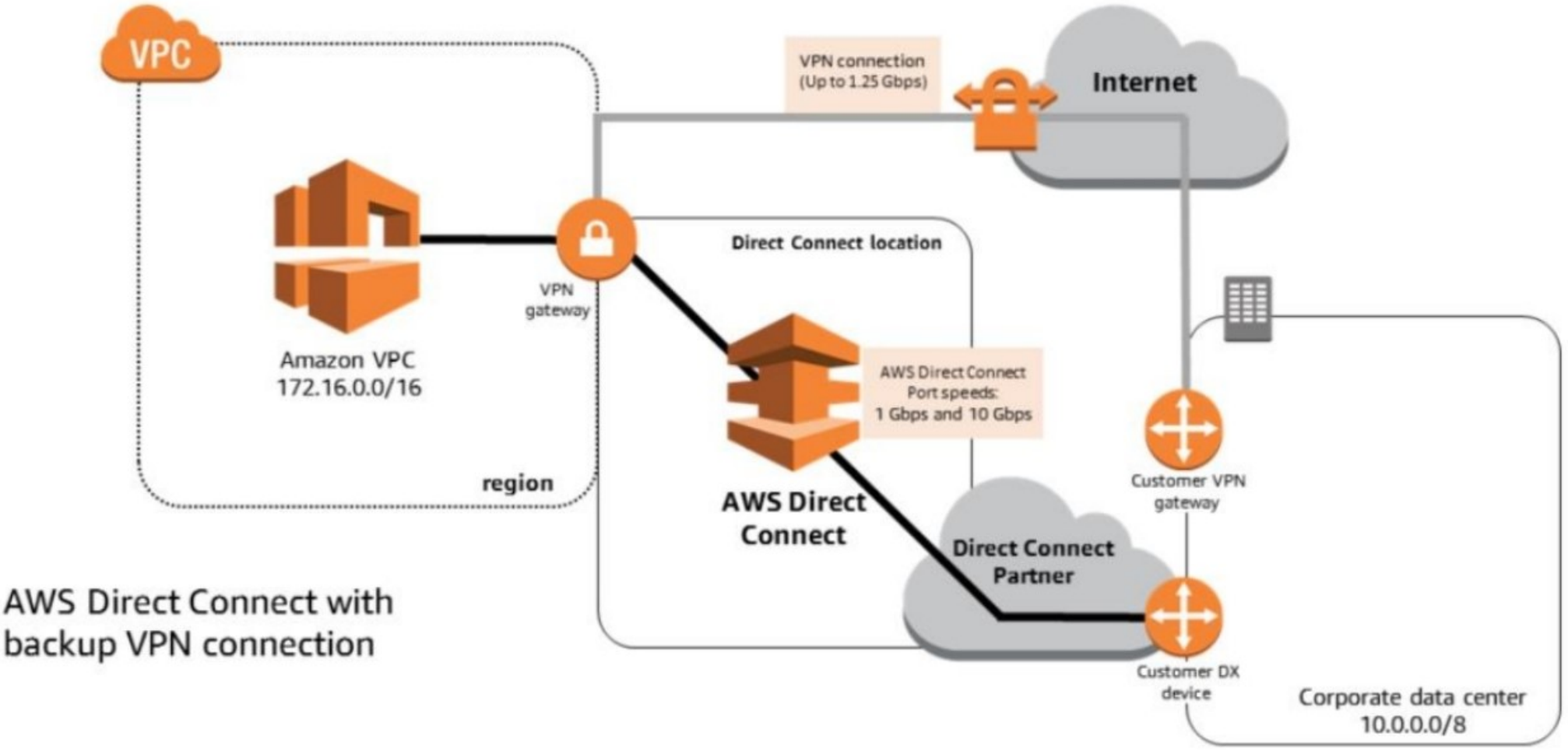
DX Use Cases

- Hybrid Cloud architectures
- Continually transferring large data sets
- Network performance predictability
- security and compliance

Extending On-Premises Network to AWS using DX



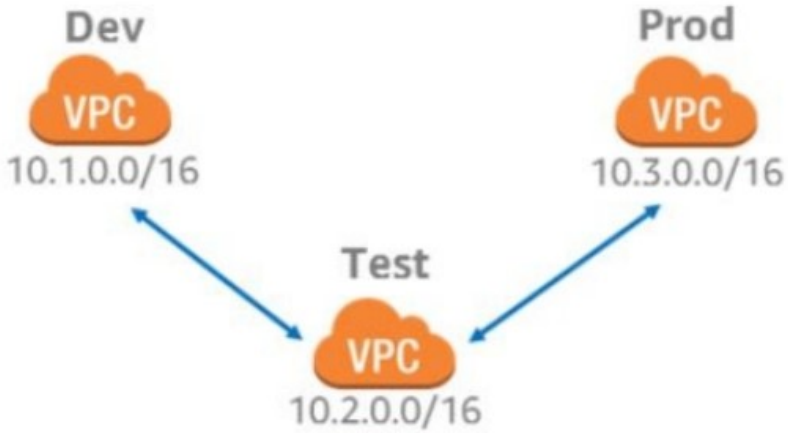
AWS Direct Connect Resiliency for Critical Workloads



Connecting VPCs

- Isolating some of your workloads is generally a good practice.
- But you may need to transfer data between two or more VPCs.

Connecting VPCs – VPC Peering

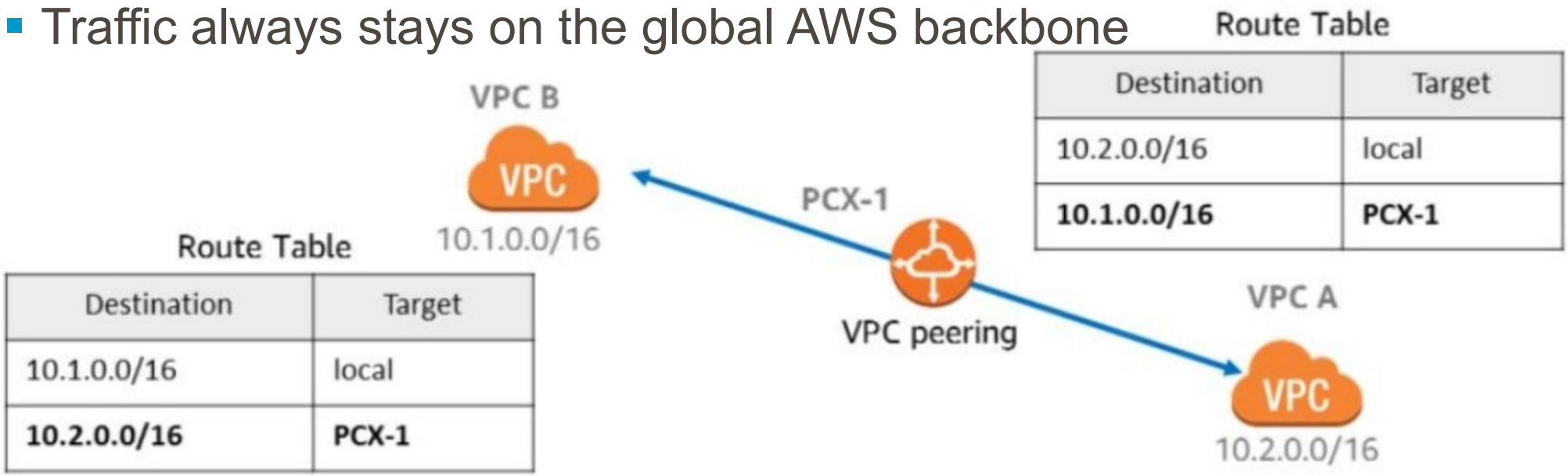


Instances can communicate across a peering connection as if they were in the same network.

- Use private IP address
- Intra and inter-region support
- IP spaces cannot overlap
- Only one peering resource between any two VPCs
- Transitive peering relationships are not supported
- Can be established between different AWS accounts

VPC Peering

- No internet gateway or virtual gateway required
- Highly available connections; not a single point of failure
- No bandwidth bottlenecks
- Traffic always stays on the global AWS backbone



Route Table

Destination	Target
10.1.0.0/16	local
10.2.0.0/16	**PCX-1**

Route Table

Destination	Target
10.2.0.0/16	local
10.1.0.0/16	**PCX-1**

Peering Multiple VPCs

General Best Practices

- When connecting multiple VPCs, there are some universal network-design principles to consider:

Destination	Target
10.1.0.0/16	local
10.2.0.0/16	**PCX-1**

No overlapping CIDR blocks

Only connect essential VPCs

Make sure your solution can scale

Connecting VPCs – Transit Gateway

- Connects up to 5,000 VPCs and on-premises environments with a single gateway
- Acts as a hub for all traffic to flow through between your networks
- Fully managed, highly available, flexible routing service

Transit Gateway in Action - Connected

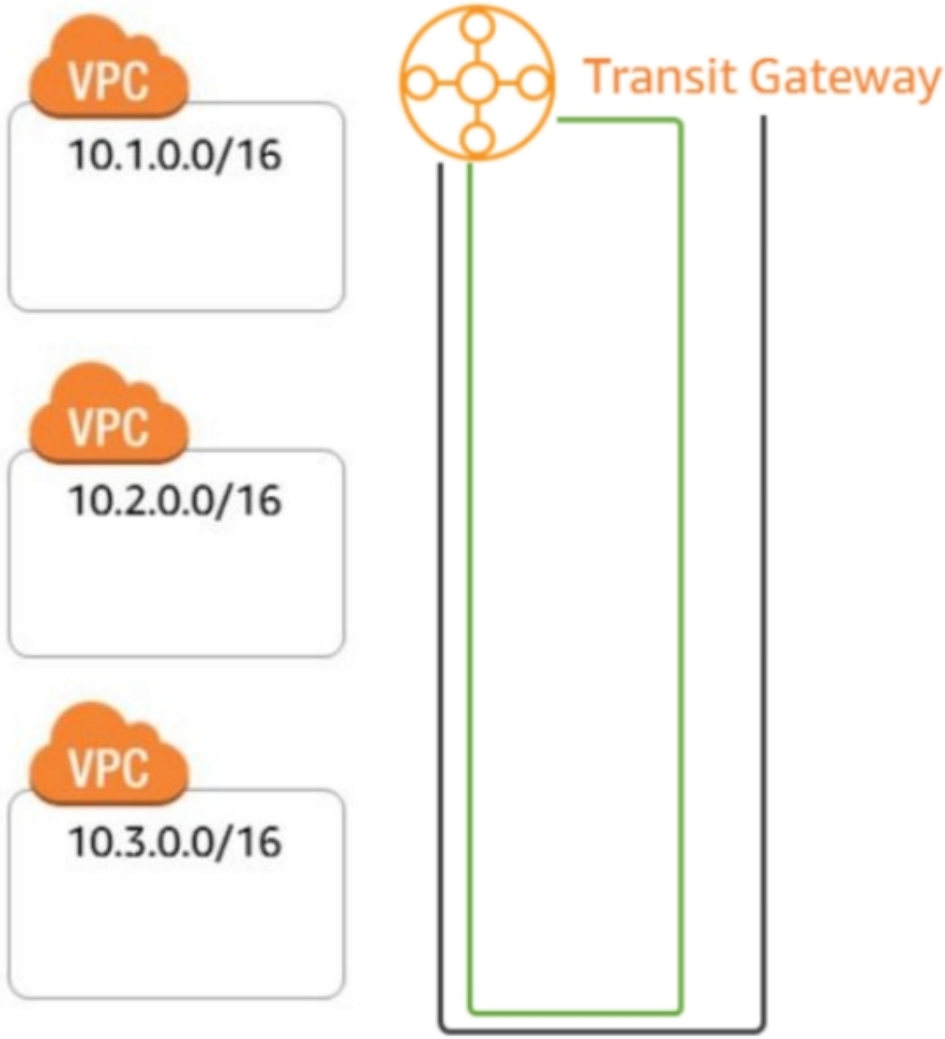
Scenario: We want all three VPCs to be able to be fully connected.

How do we do this using Transit Gateway?

Transit Gateway in Action - Connected

Scenario: We want all three VPCs to be able to be fully connected.

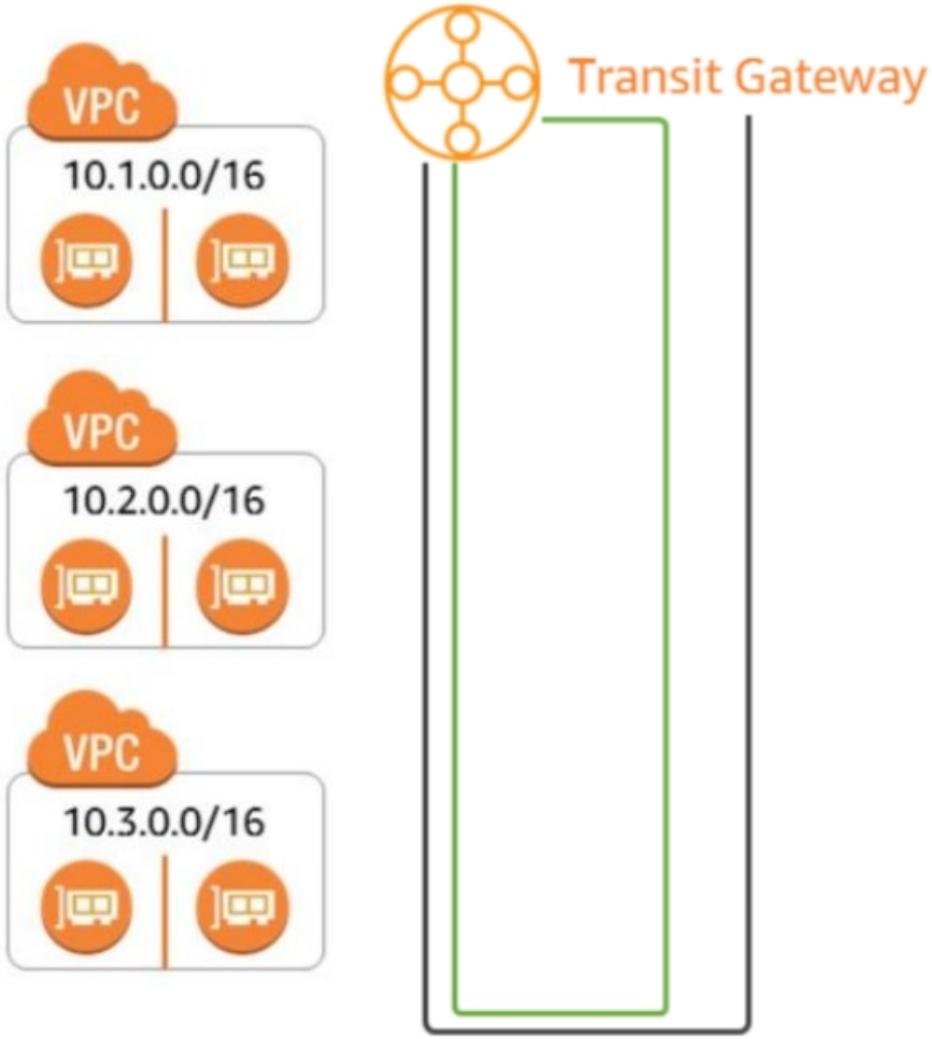
How do we do this using Transit Gateway?



Transit Gateway in Action - Connected

Scenario: We want all three VPCs to be able to be fully connected.

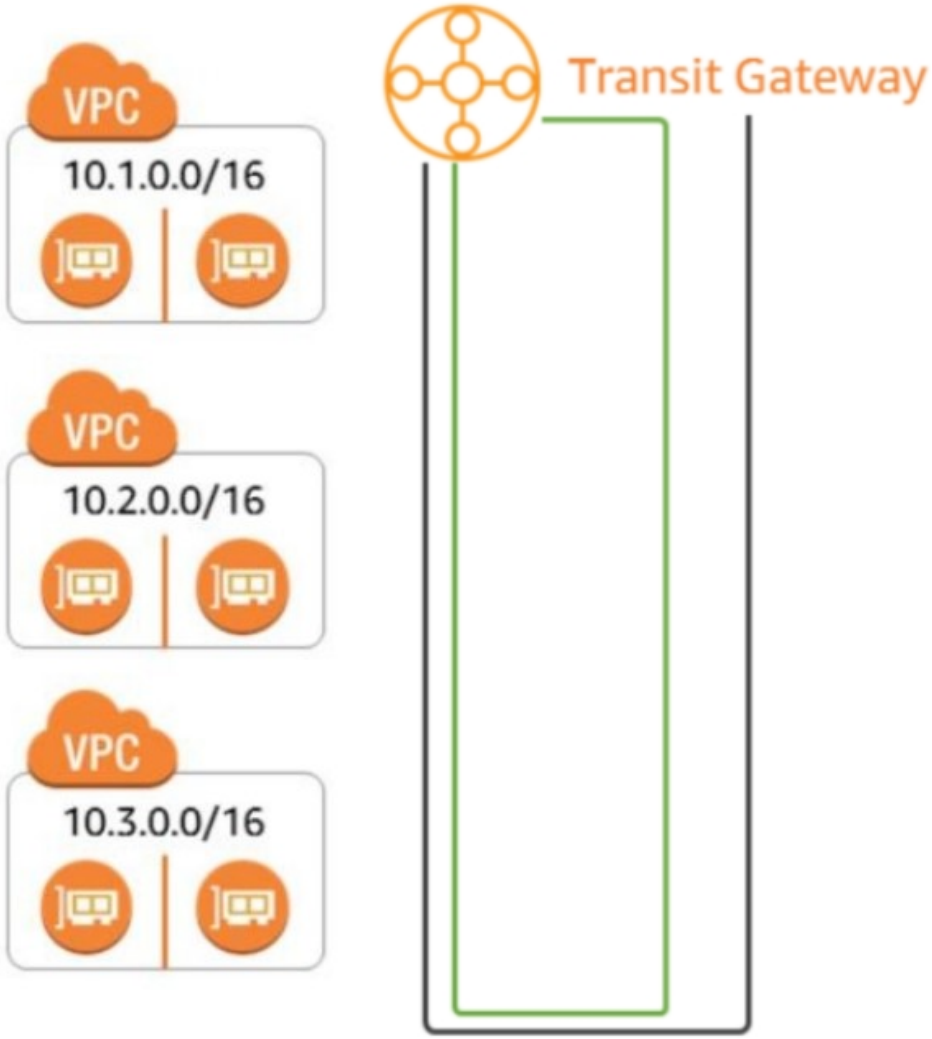
How do we do this using Transit Gateway?



Transit Gateway in Action - Connected

Scenario: We want all three VPCs to be able to be fully connected.

How do we do this using Transit Gateway?



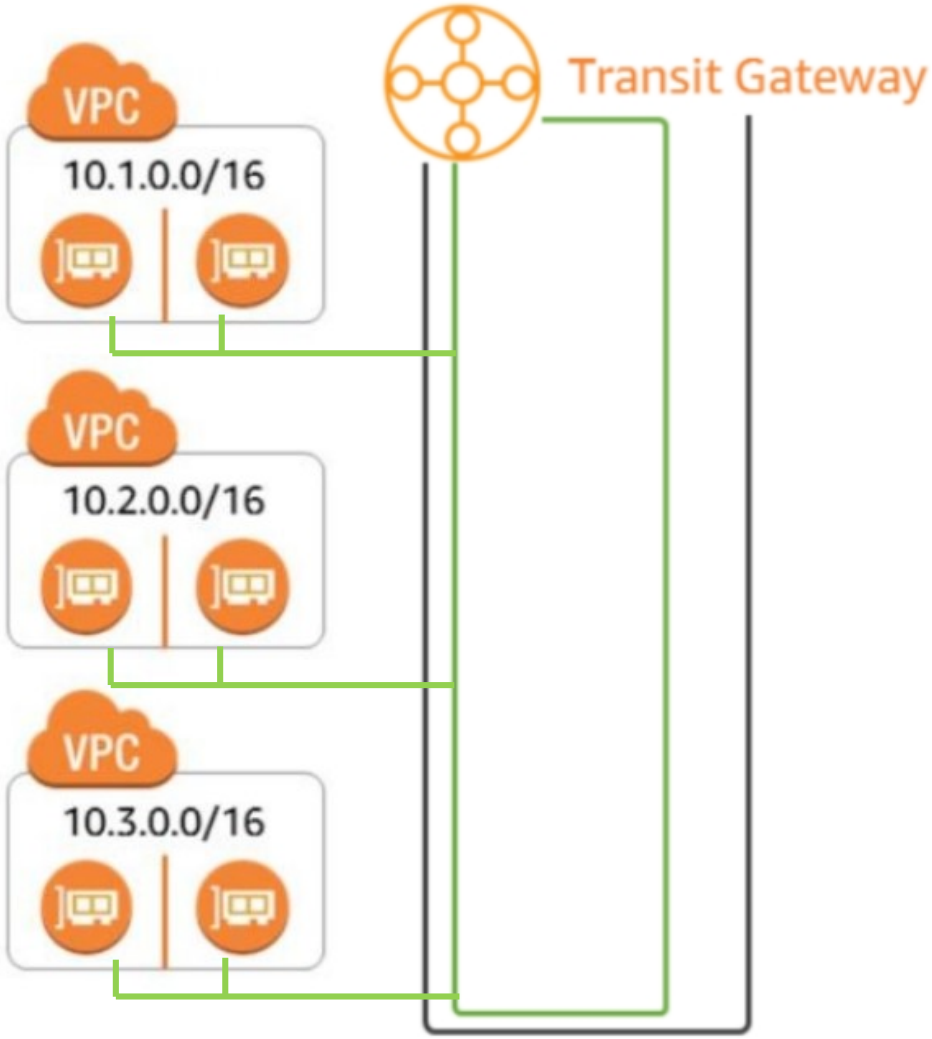
Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Transit Gateway in Action - Connected

Scenario: We want all three VPCs to be able to be fully connected.

How do we do this using Transit Gateway?



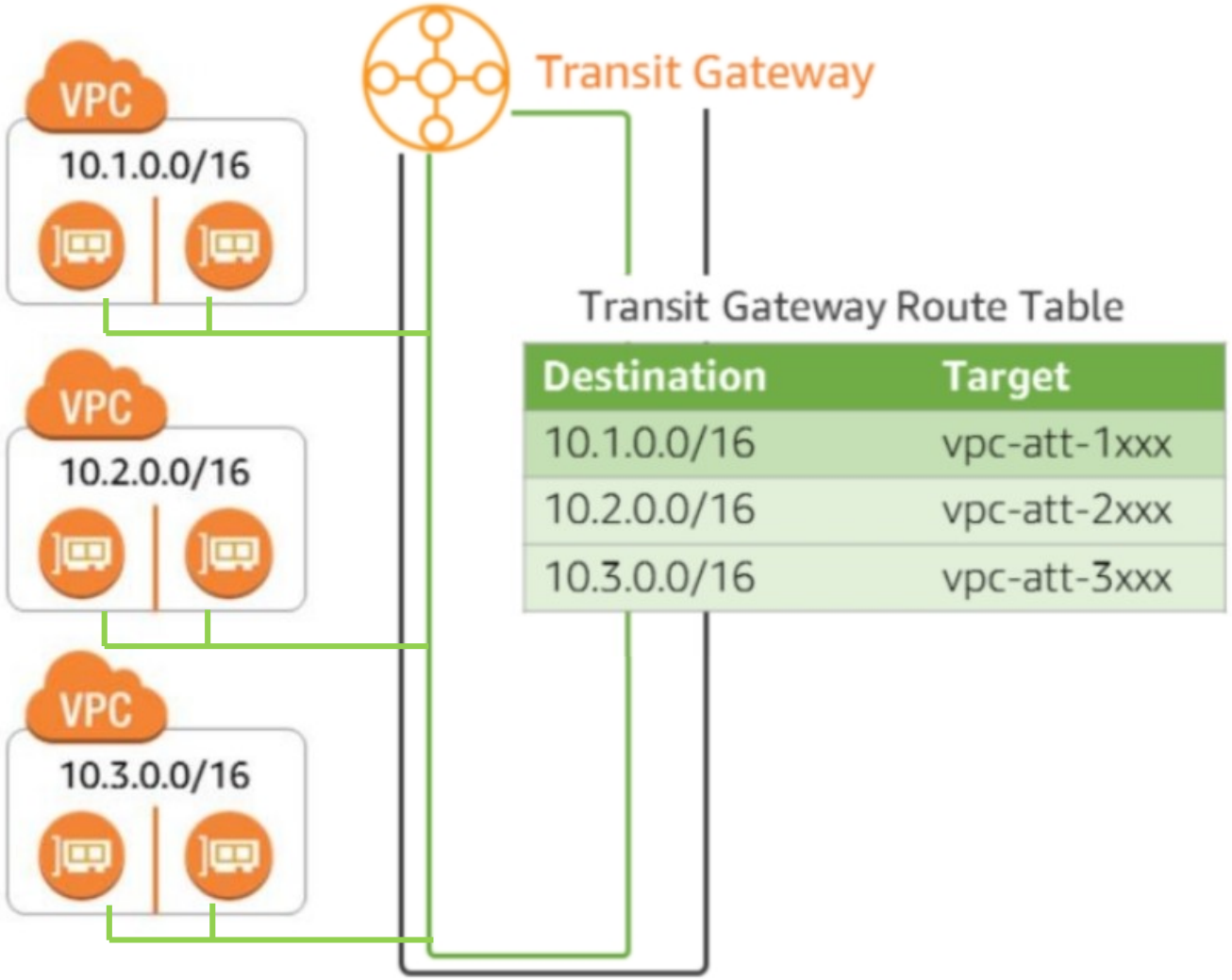
Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Transit Gateway in Action - Connected

Scenario: We want all three VPCs to be able to be fully connected.

How do we do this using Transit Gateway?

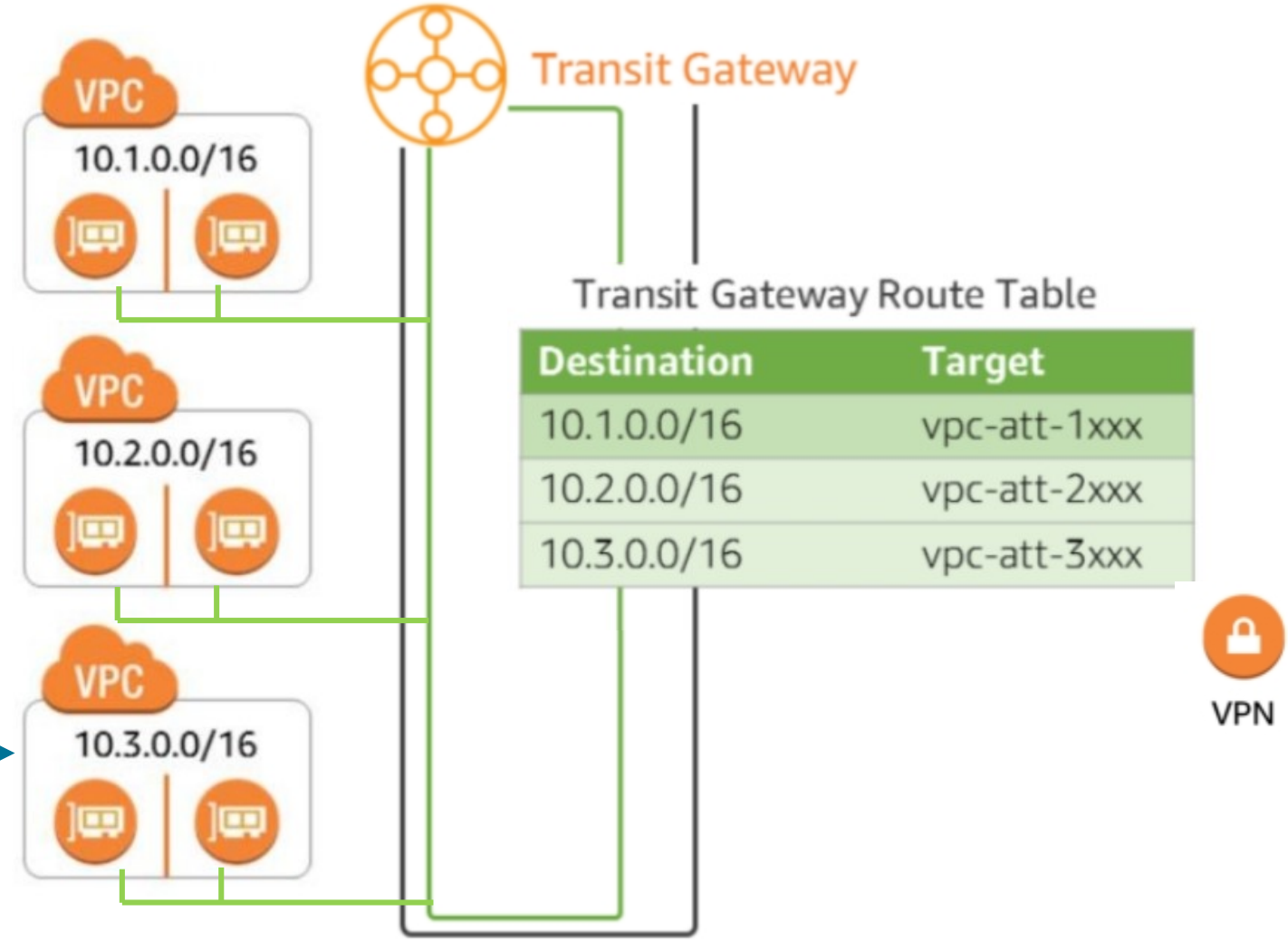


Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Transit Gateway in Action - Connected

Scenario: We now want isolated connectivity and VPN access

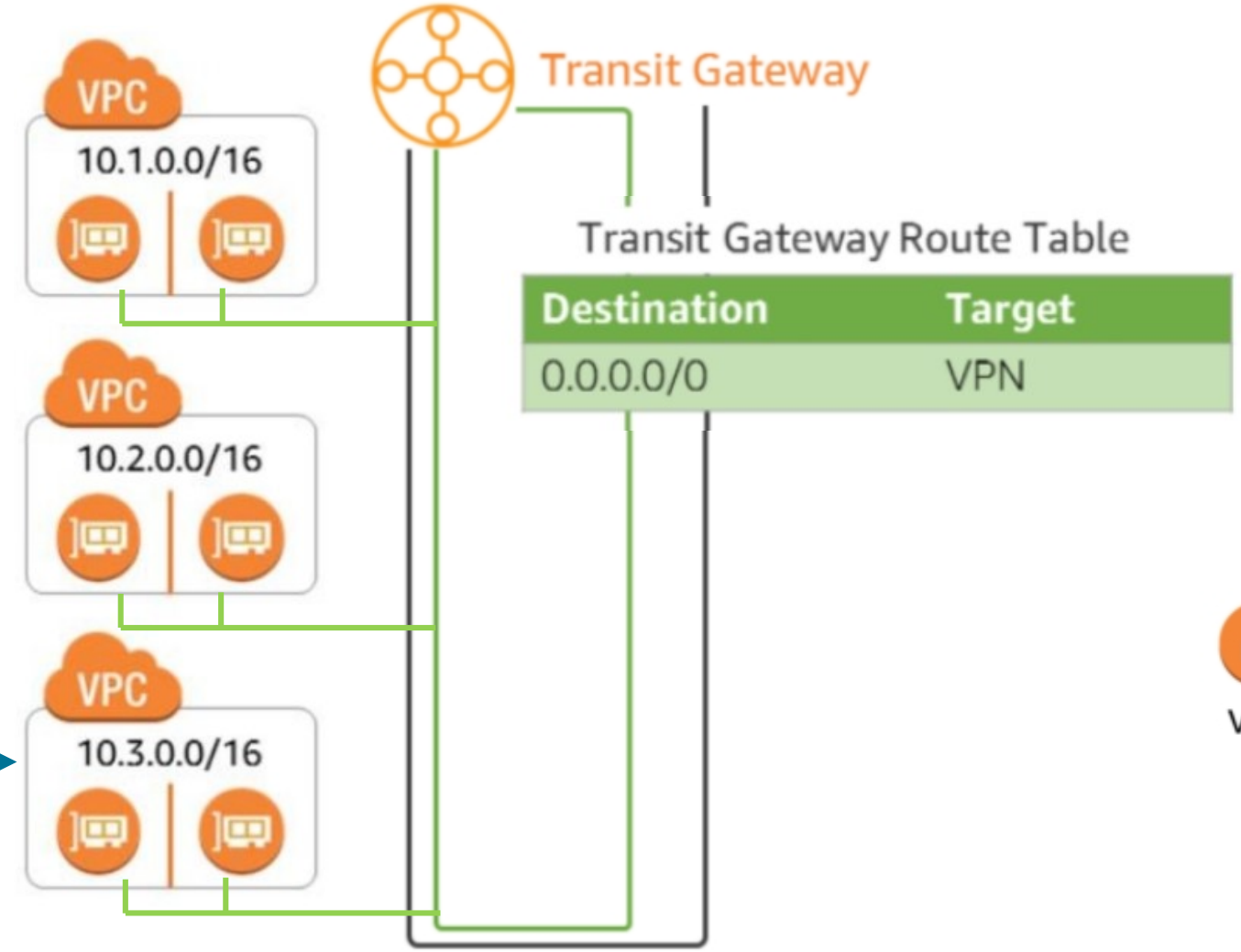


Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Transit Gateway in Action - Connected

Scenario: We now want isolated connectivity and VPN access

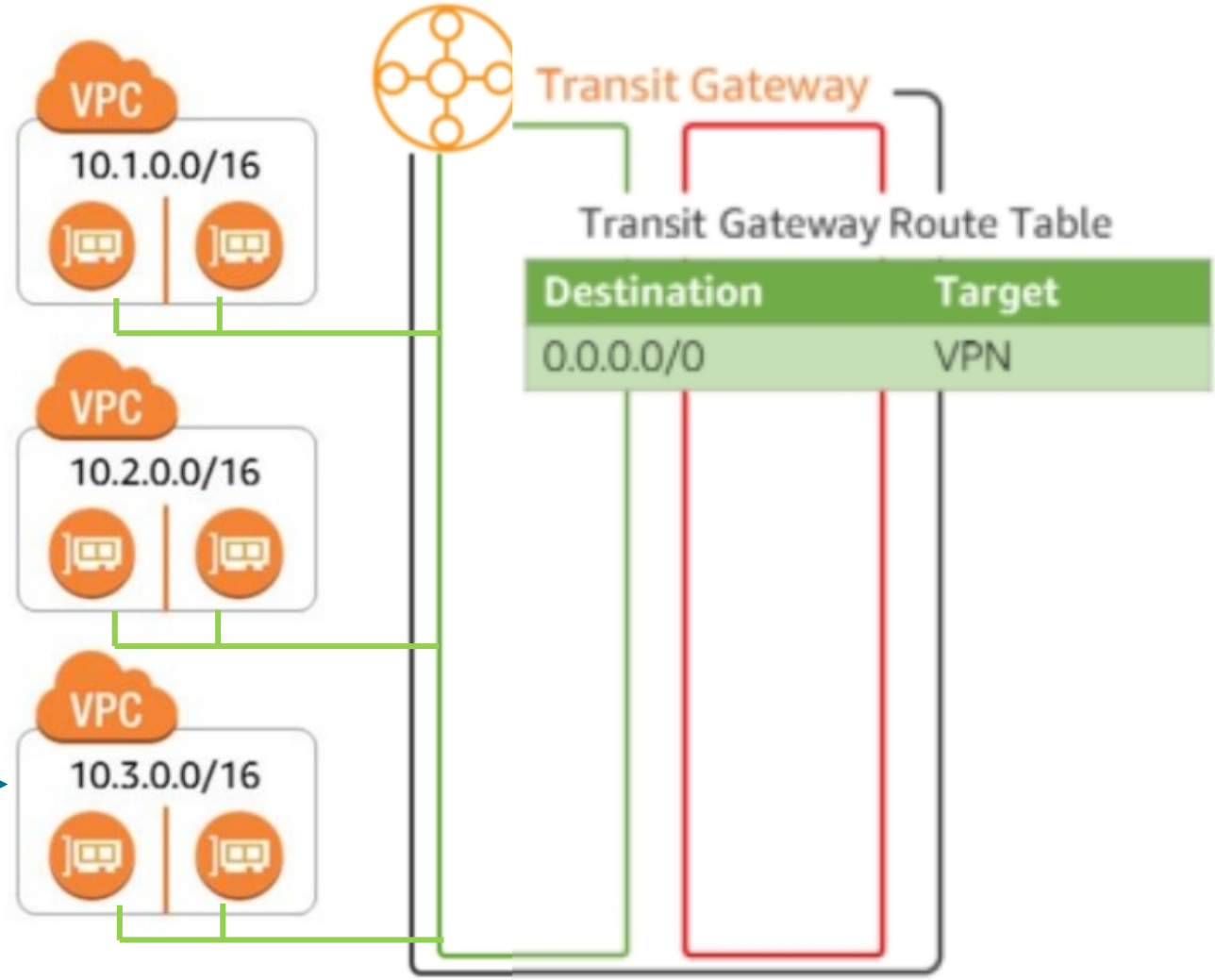


Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Transit Gateway in Action - Connected

Scenario: We now want isolated connectivity and VPN access

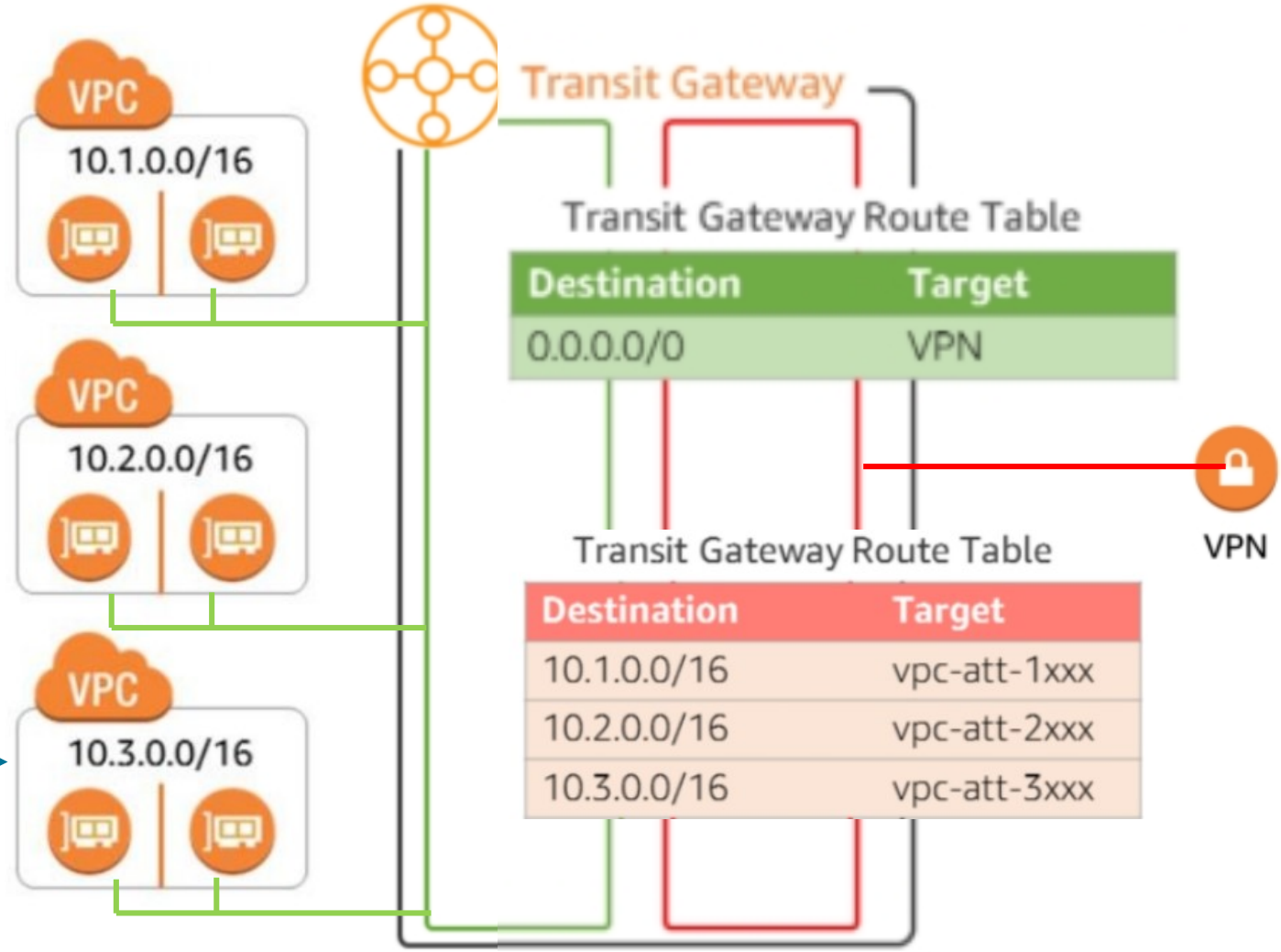


Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Transit Gateway in Action - Connected

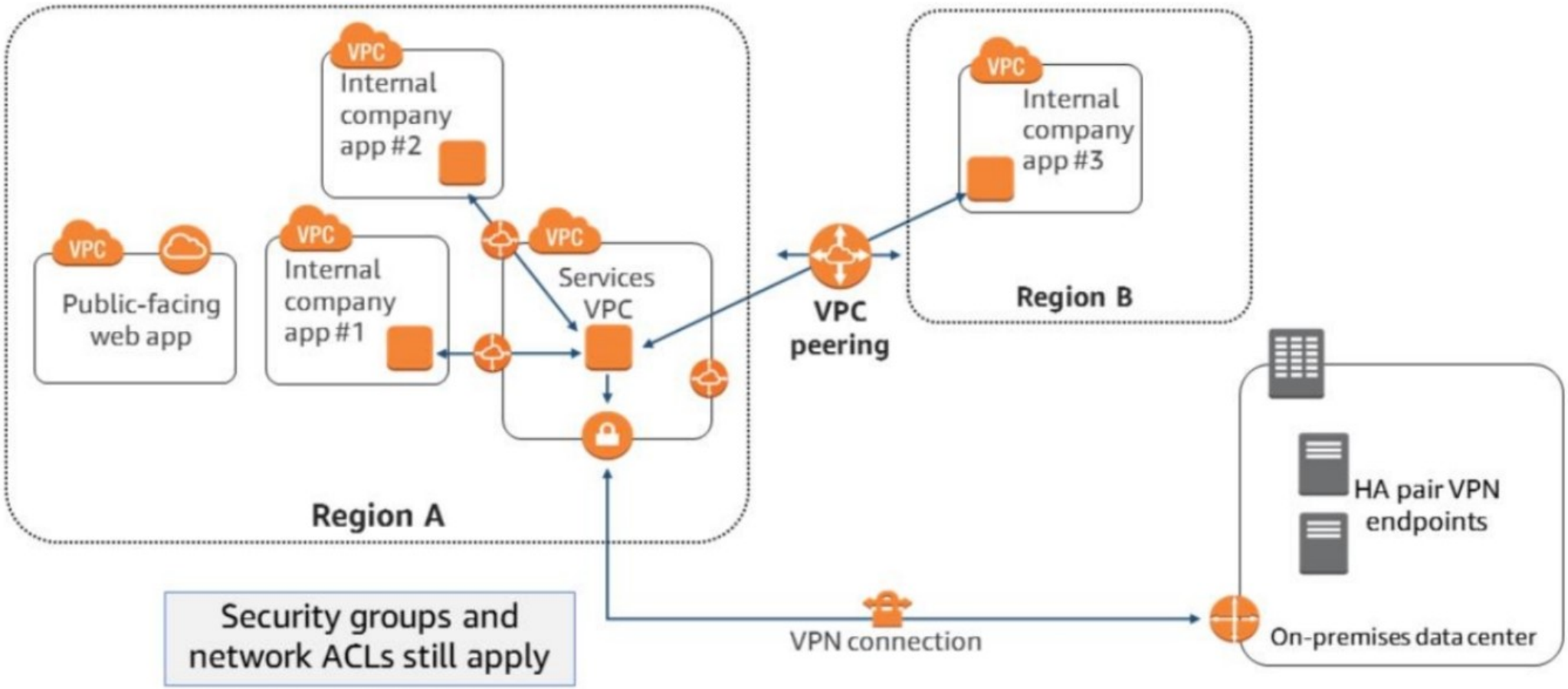
Scenario: We now want isolated connectivity and VPN access



Per VPC Route Table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Example: VPC Peering for Shared Services



VPC Endpoints

Privately connect your EC2 instances to services outside your VPC without leaving AWS.

Don't need to use an internet gateway, VPN, network address translation (NAT) devices, or firewall proxies.

- Does not require traversal over the internet
- Must be in the same region
- They are horizontally scaled, redundant and highly available

Two Types of Endpoints

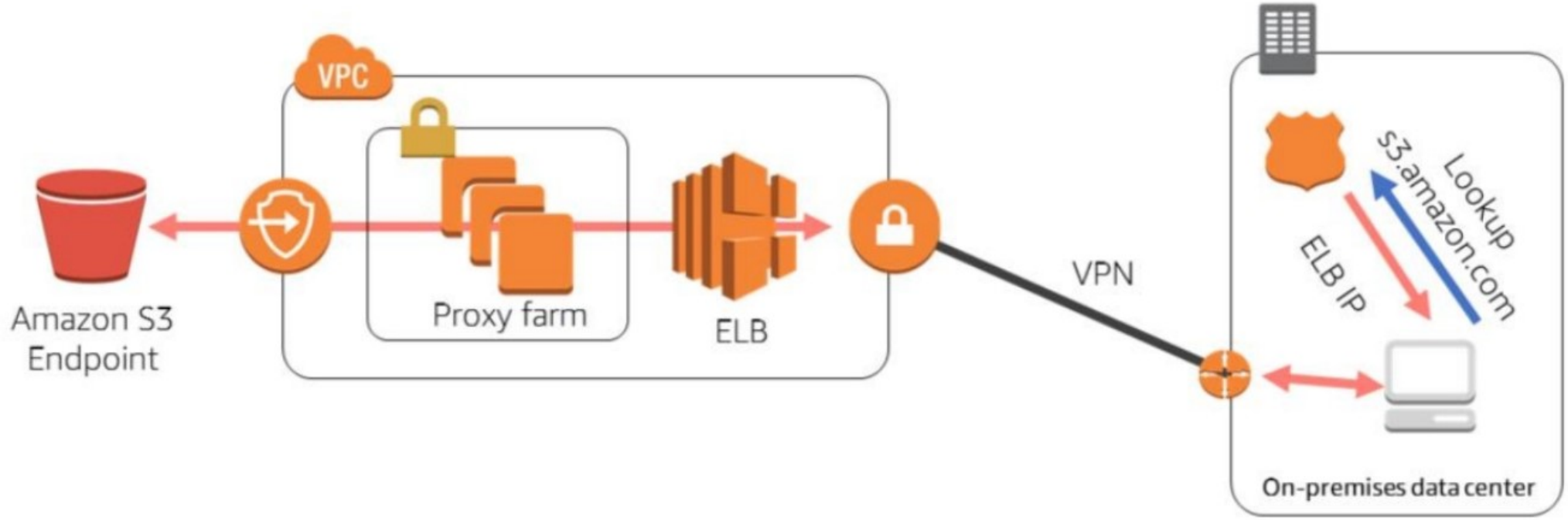
Interface Endpoint

- Amazon CloudWatch Logs
- AWS CodeBuild
- Amazon EC2 API
- Elastic Load Balancing API
- AWS Key Management Service (AWS KMS)
- Amazon Kinesis Data Streams
- AWS Service Catalog
- Amazon Simple Notification Service (Amazon SNS)
- AWS Systems Manager
- Endpoint services hosted by other AWS accounts

Gateway Endpoint

- Amazon Simple Storage Service (Amazon S3)
- Amazon DynamoDB

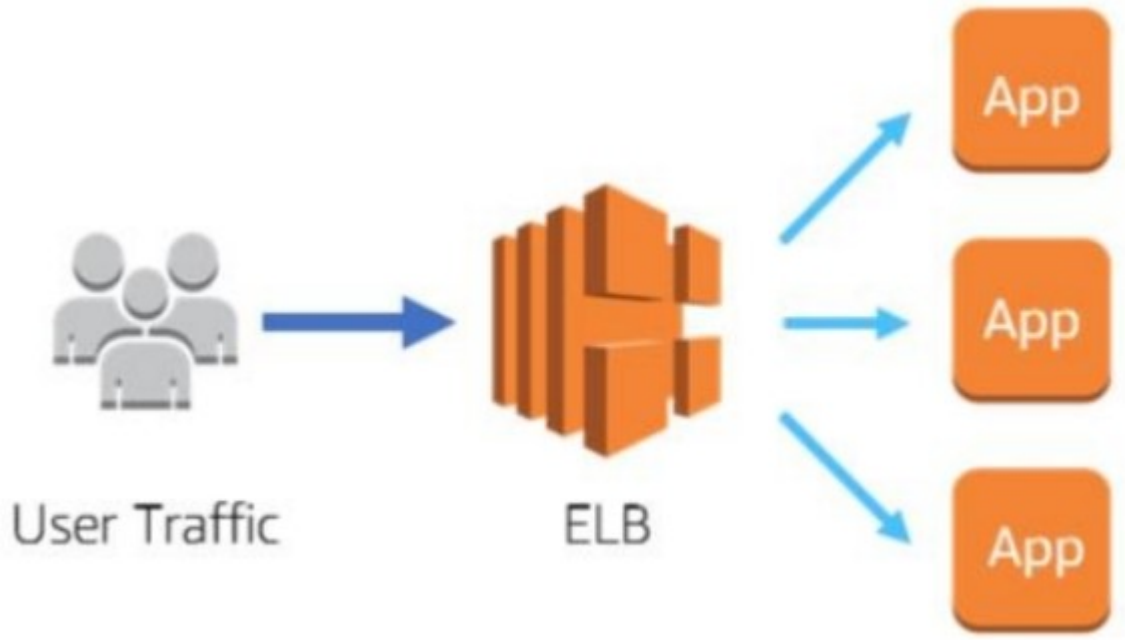
Accessing VPC Endpoints from outside the VPC



Load Balancing on AWS

Elastic Load Balancing (ELB)

A **managed load balancing service** that distributes incoming application traffic across multiple Amazon EC2 instances, containers and IP addresses.



ELB: Features

- Uses **HTTP, HTTPs, TCP and SSL** (Secure TCP) protocols.
- Can be **external or internal** facing
- Each load balancer is given a **DNS name**
- Recognizes and responds to **unhealthy instances**

ELB: Options

Application Load Balancer

- Flexible application management
- Advanced load balancing of HTTP and HTTPS traffic
- Operates at the request level

(Layer 7)

ELB: Options

Application Load Balancer

- Flexible application management
- Advanced load balancing of HTTP and HTTPS traffic
- Operates at the request level (Layer 7)

Network Load Balancer

- Extreme performance and static IP for your application
- Load balancing of TCP traffic
- Operates at the connection level (Layer 4)

ELB: Options

Application Load Balancer

- Flexible application management
- Advanced load balancing of HTTP and HTTPS traffic
- Operates at the request level (Layer 7)

Network Load Balancer

- Extreme performance and static IP for your application
- Load balancing of TCP traffic
- Operates at the connection level (Layer 4)

Classic Load Balancer

PREVIOUS GENERATION
for HTTP, HTTPS, and TCP

- Existing application that was built within the EC2 Classic network
- Operates at both the request level and connection level

Why You Should Use ELB

High availability

Health checks

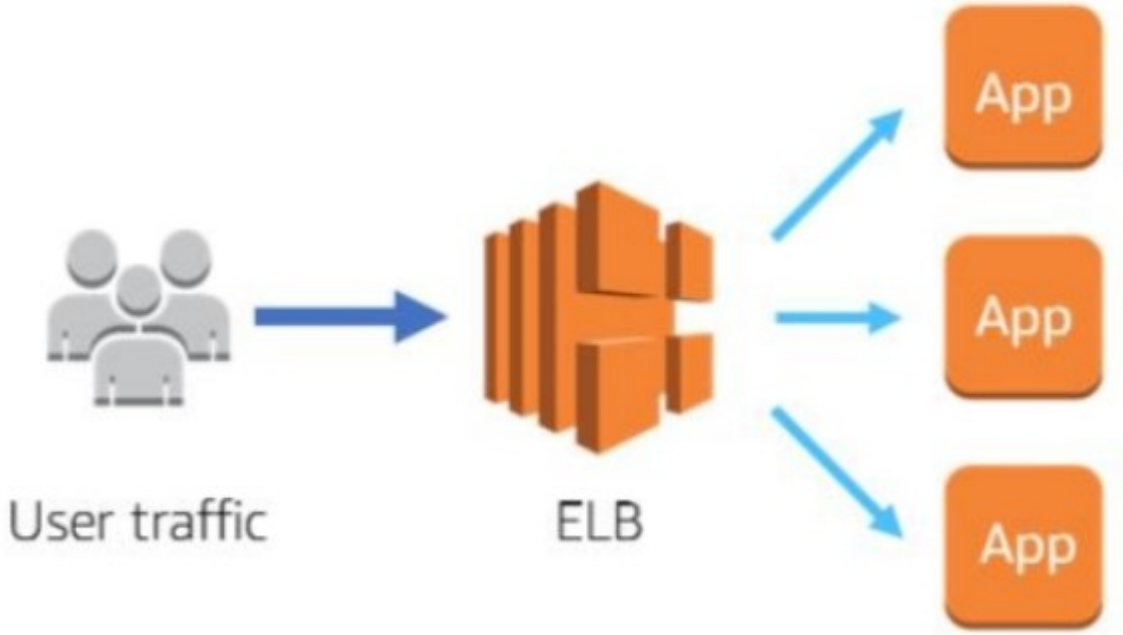
Security features

TLS termination

Connection Draining

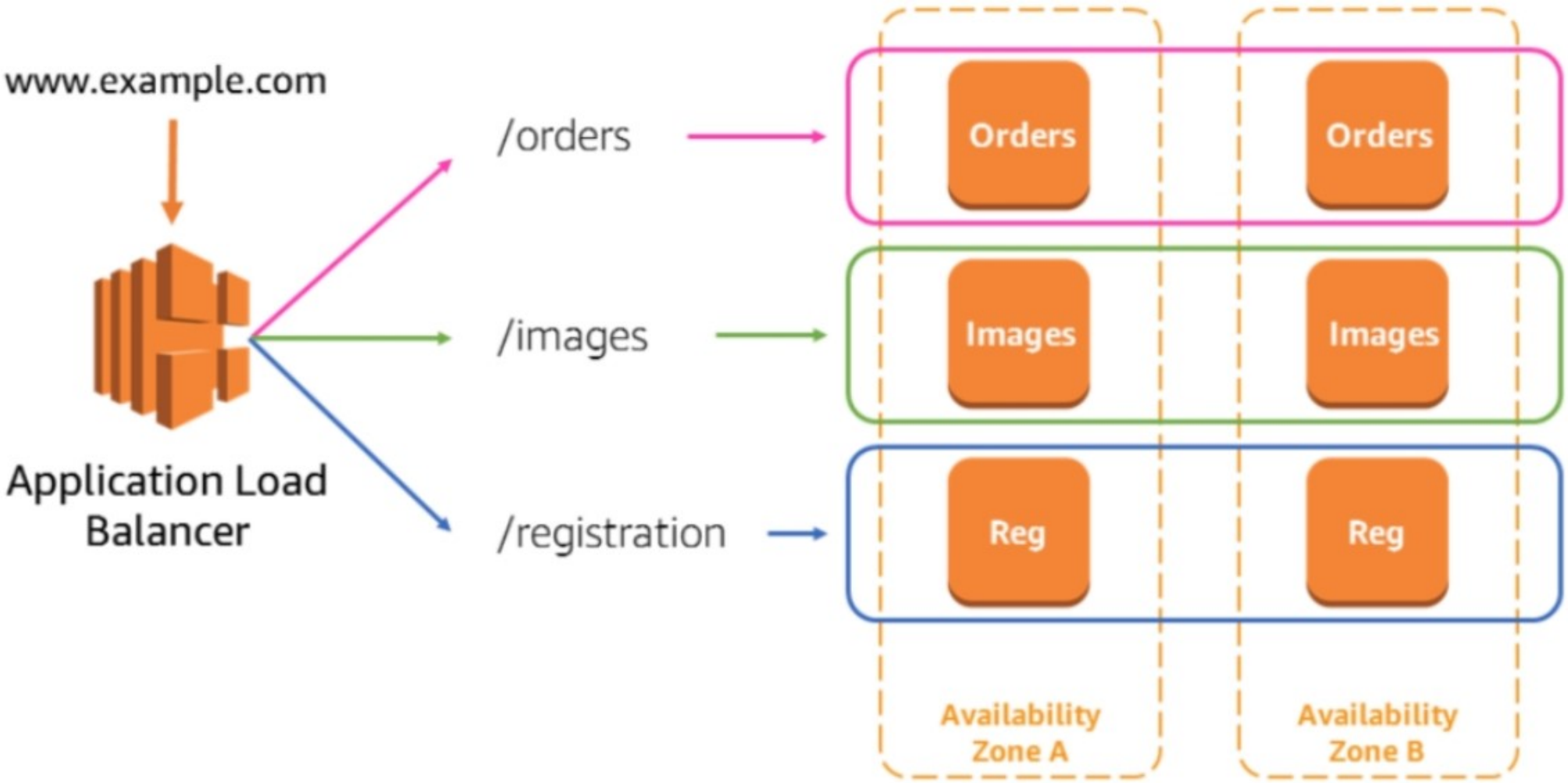
If you need to **remove an instance** from your production fleet, but **don't want to affect your users:**

Affected backend instances will complete requests in progress before deregistration



Enable connection draining

Cloud Design Pattern: Application Load Balancer



High Availability

What is High Availability?

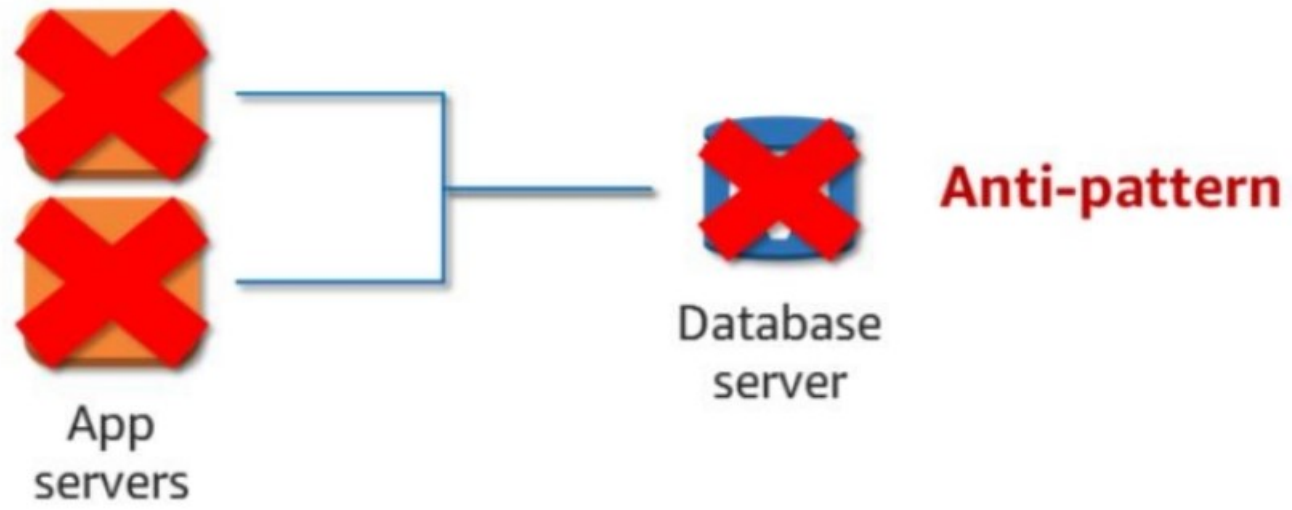
Your application can **recover from a failure or roll over to a secondary source** with an **acceptable** amount of degraded performance time.

Percent of Uptime	Max Downtime per Year	Equivalent Downtime per Day
90%	36.5 days	2.4 hrs
99%	3.65 days	14 min
99.9%	8.76 hrs	86 sec
99.99%	52.6 min	8.6 sec
99.999%	5.25 min	.86 sec

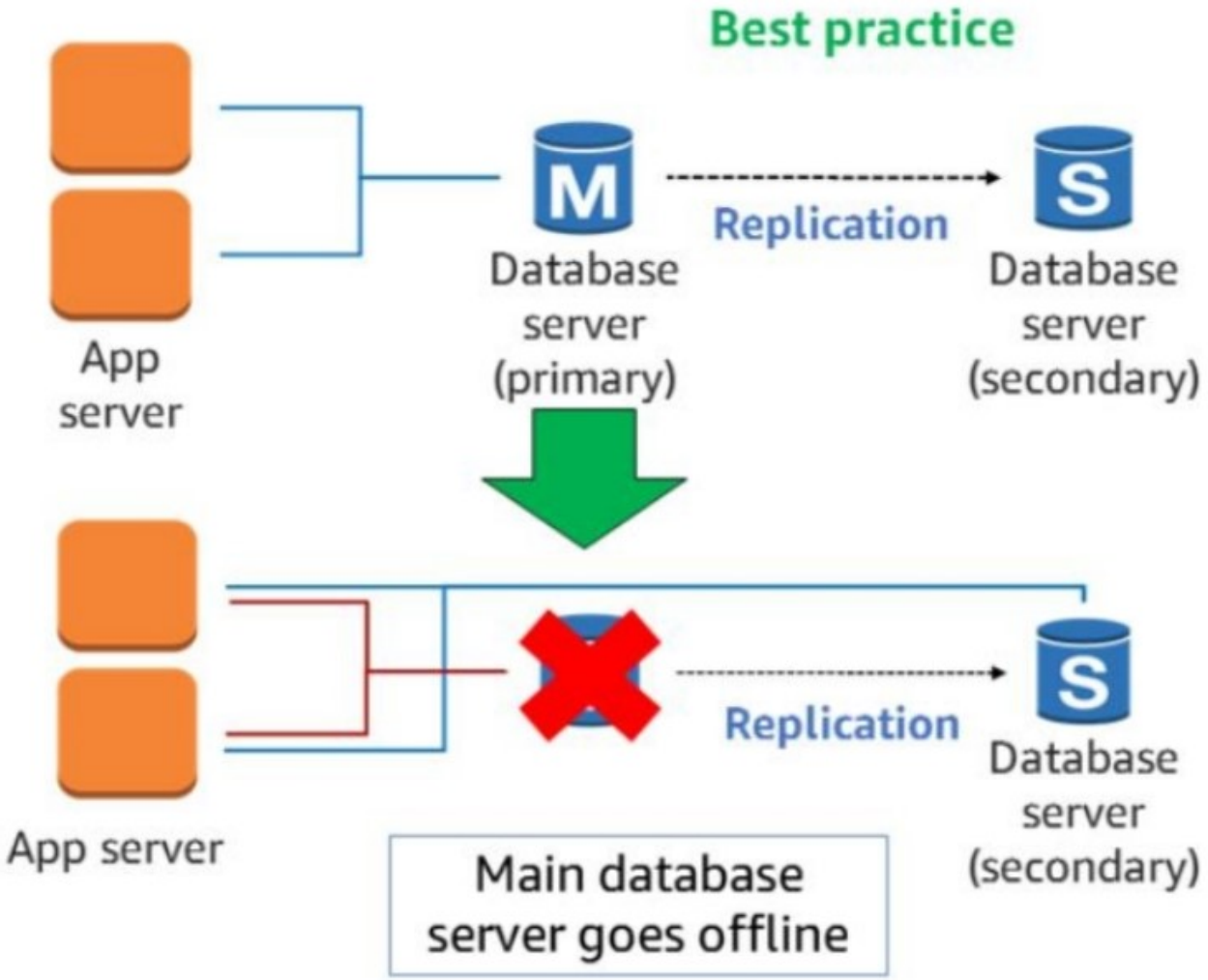
High Availability Example

Assume everything fails, and design backward

Implement redundancy where possible in order to prevent single failures from bringing done an entire system.



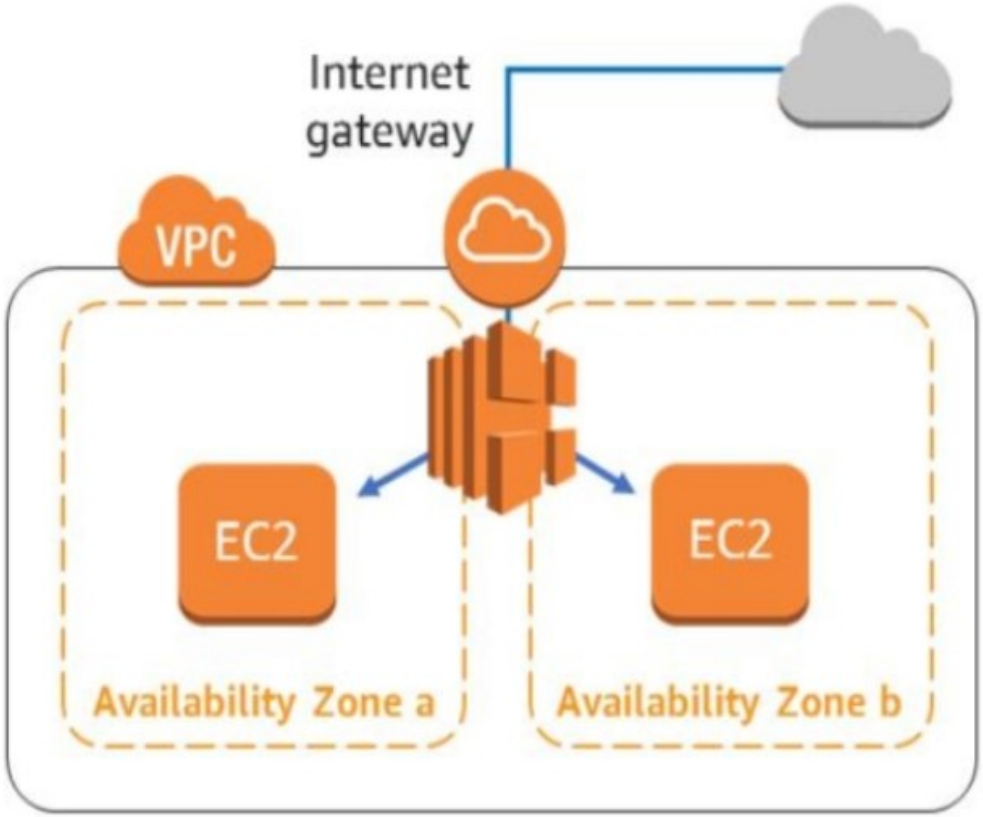
High Availability Example



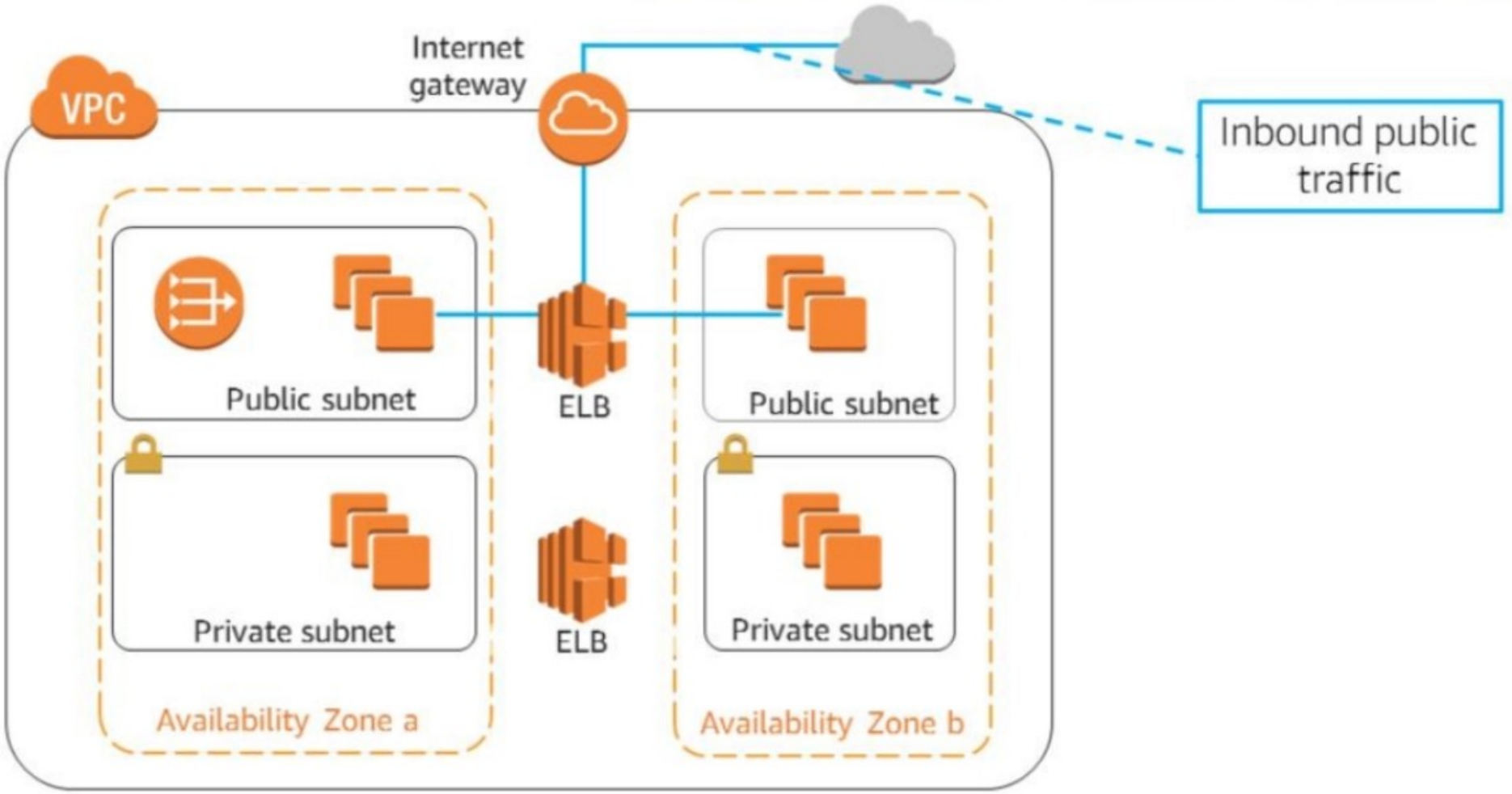
How many Availability Zones Should I Use?

Start with two Availability Zones per AWS Region.

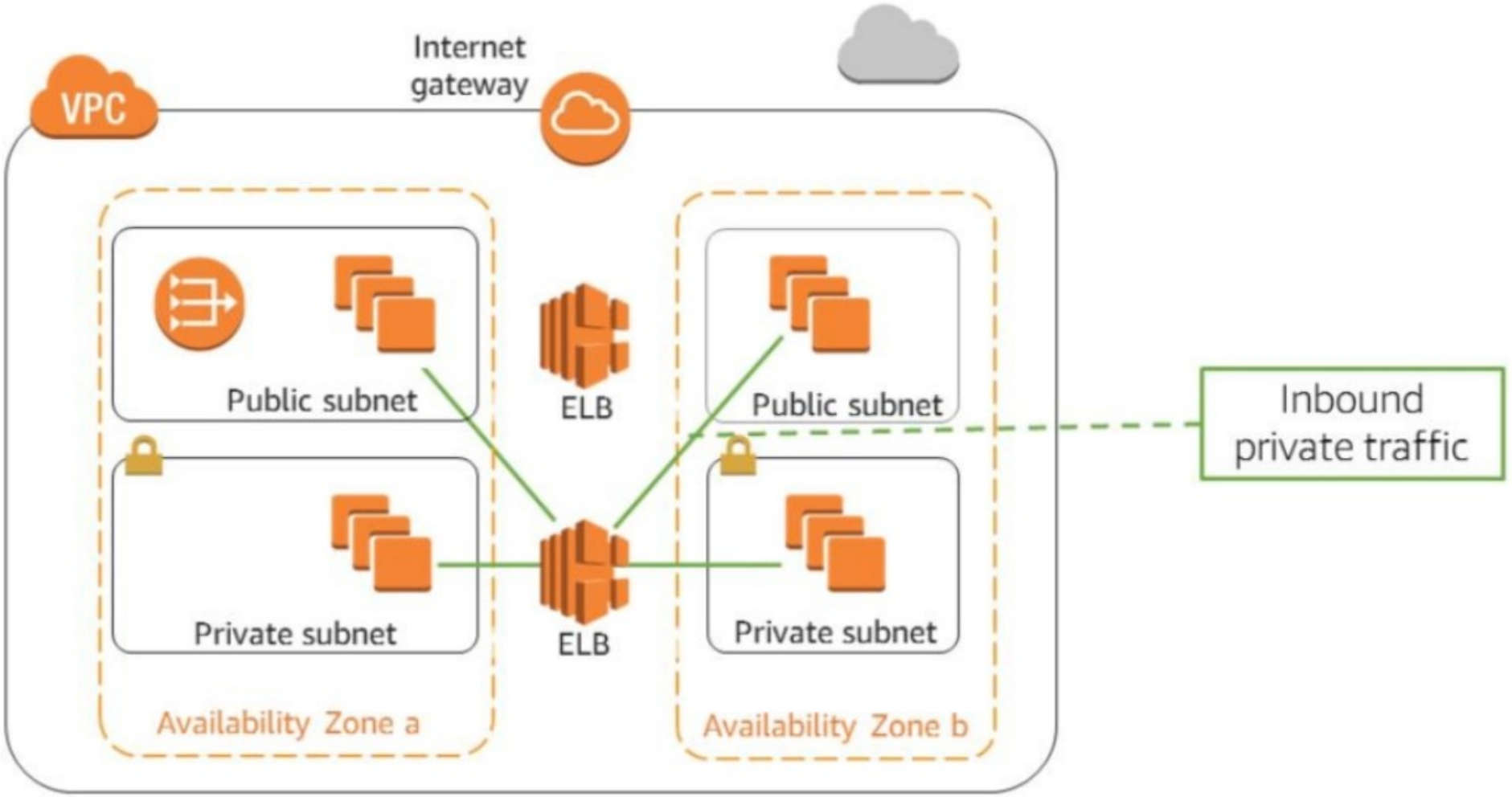
If resources in one Availability Zone are unreachable, your application shouldn't fail.



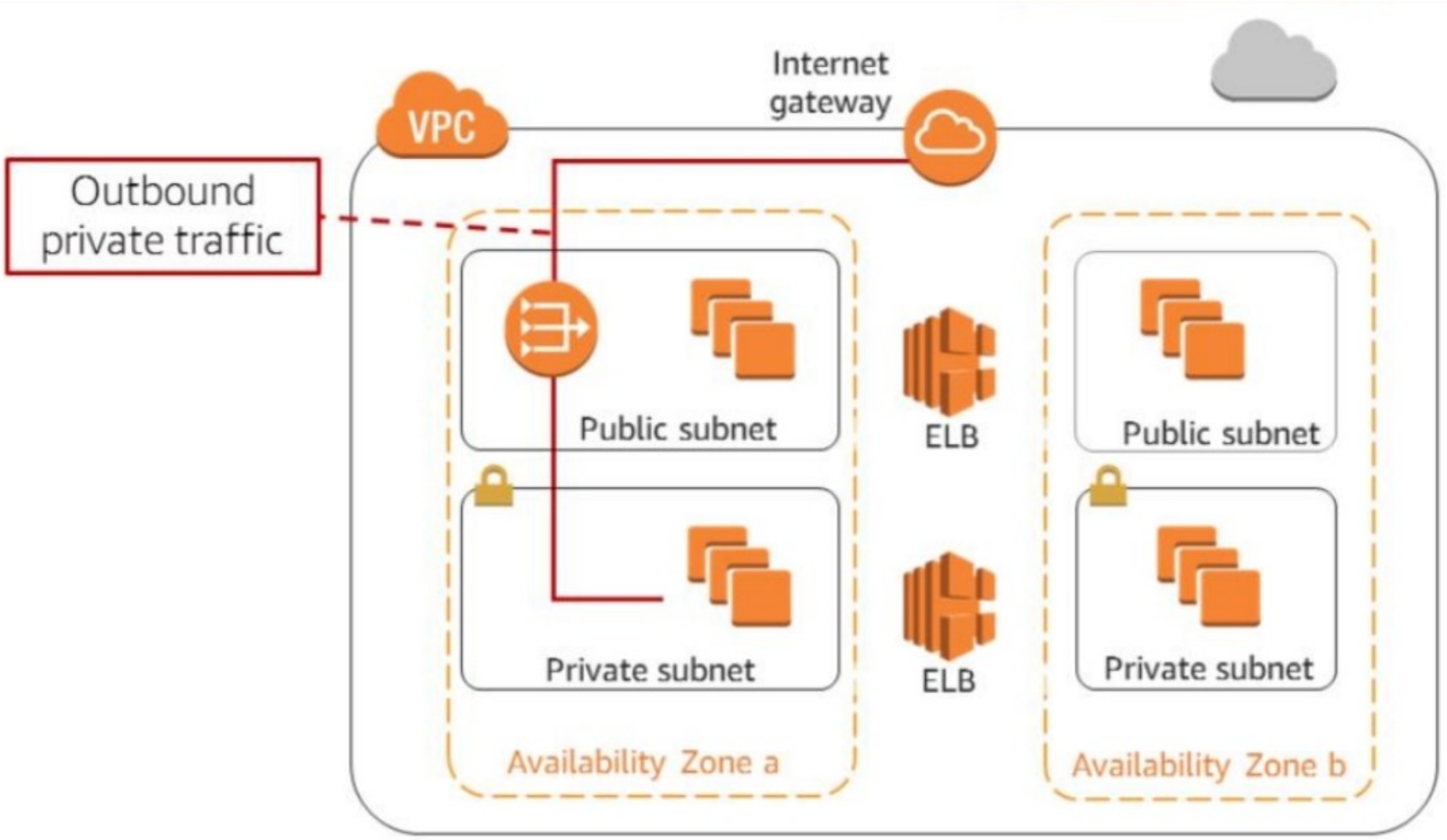
Example Architecture Diagram



Example Architecture Diagram



Example Architecture Diagram



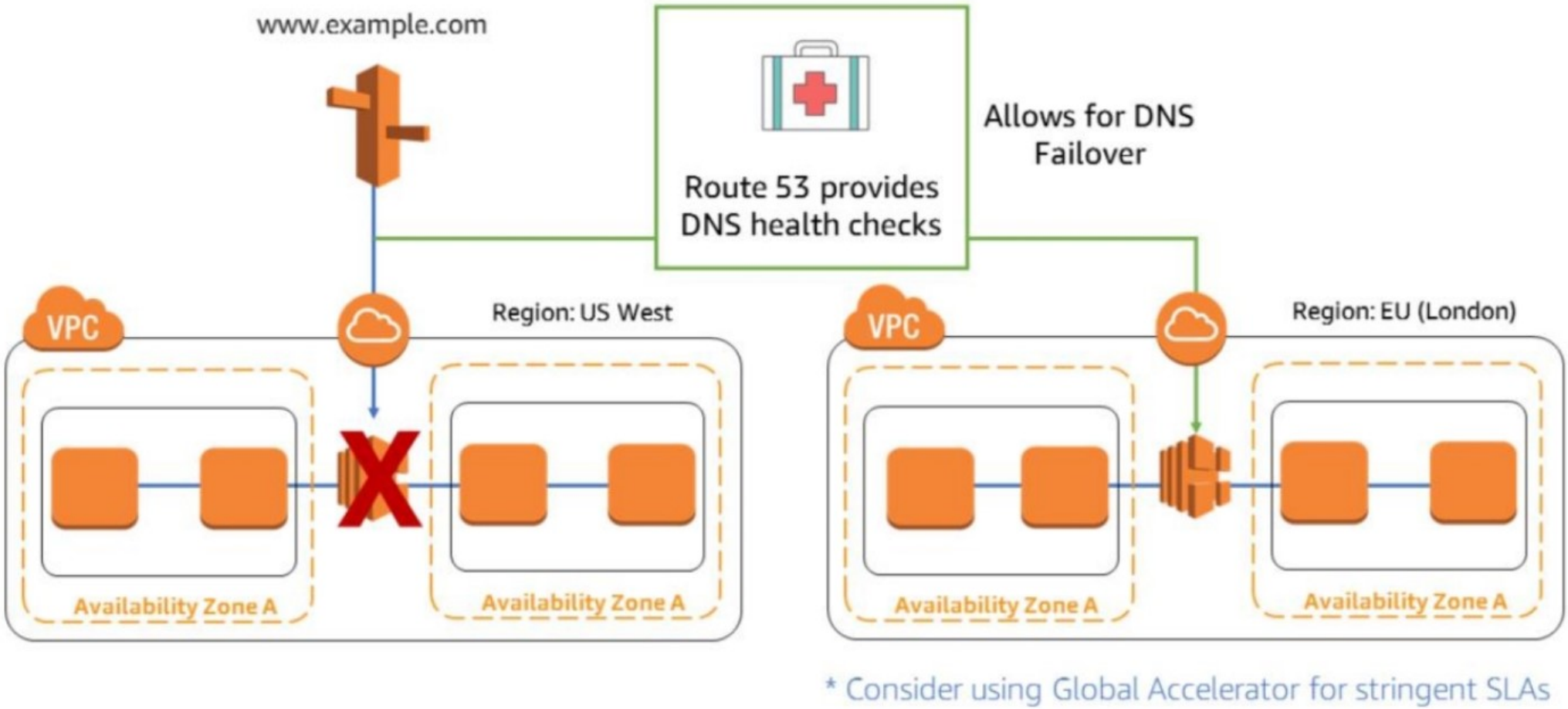
Multi-Region High Availability and DNS

Amazon Route 53

Route 53 is highly available and scalable cloud Domain Name System (DNS) service.

- DNS translates domain names into IP addresses
- Able to purchase and manage domain names and automatically configure DNS settings
- Provides tools for flexible, high-performance, highly available architectures on AWS
- Multiple routing options

How Does Route 53 Help with High Availability?



Route 53 Routing Options

- Simple routing (round robin)
- Weighted round robin
- Latency-based routing (LBR)
- Health checks and DNS failover
- Geolocation routing
- Geoproximity routing with traffic biasing
- Multi-value answers

Capgemini

CONSULTING.TECHNOLOGY.OUTSOURCING

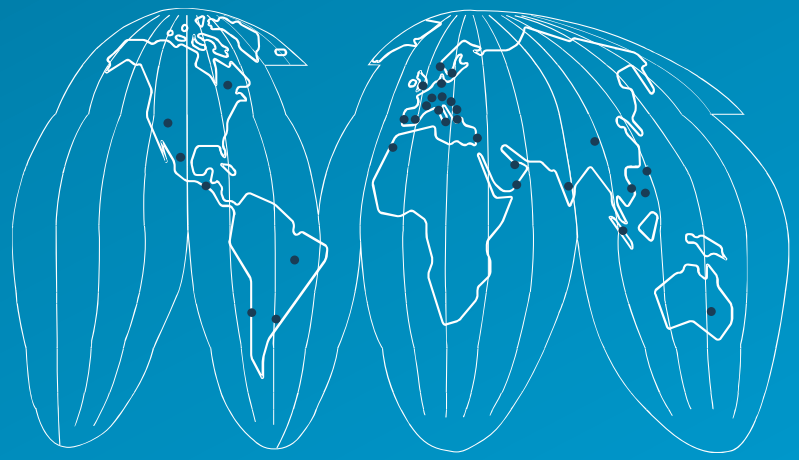
People matter, results count.

About Capgemini

With more than 145,000 people in 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2014 global revenues of EUR 10.5 billion.

Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Rightshore® is a trademark belonging to Capgemini



www.capgemini.com