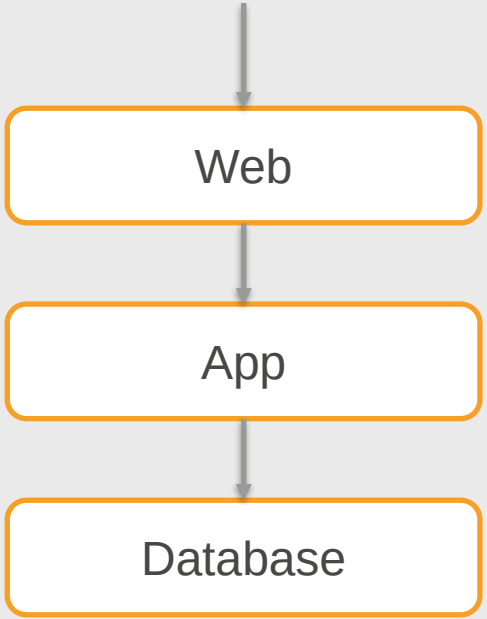
Virtual Private Cloud

Virtual Private Cloud

Your own private cloud on AWS

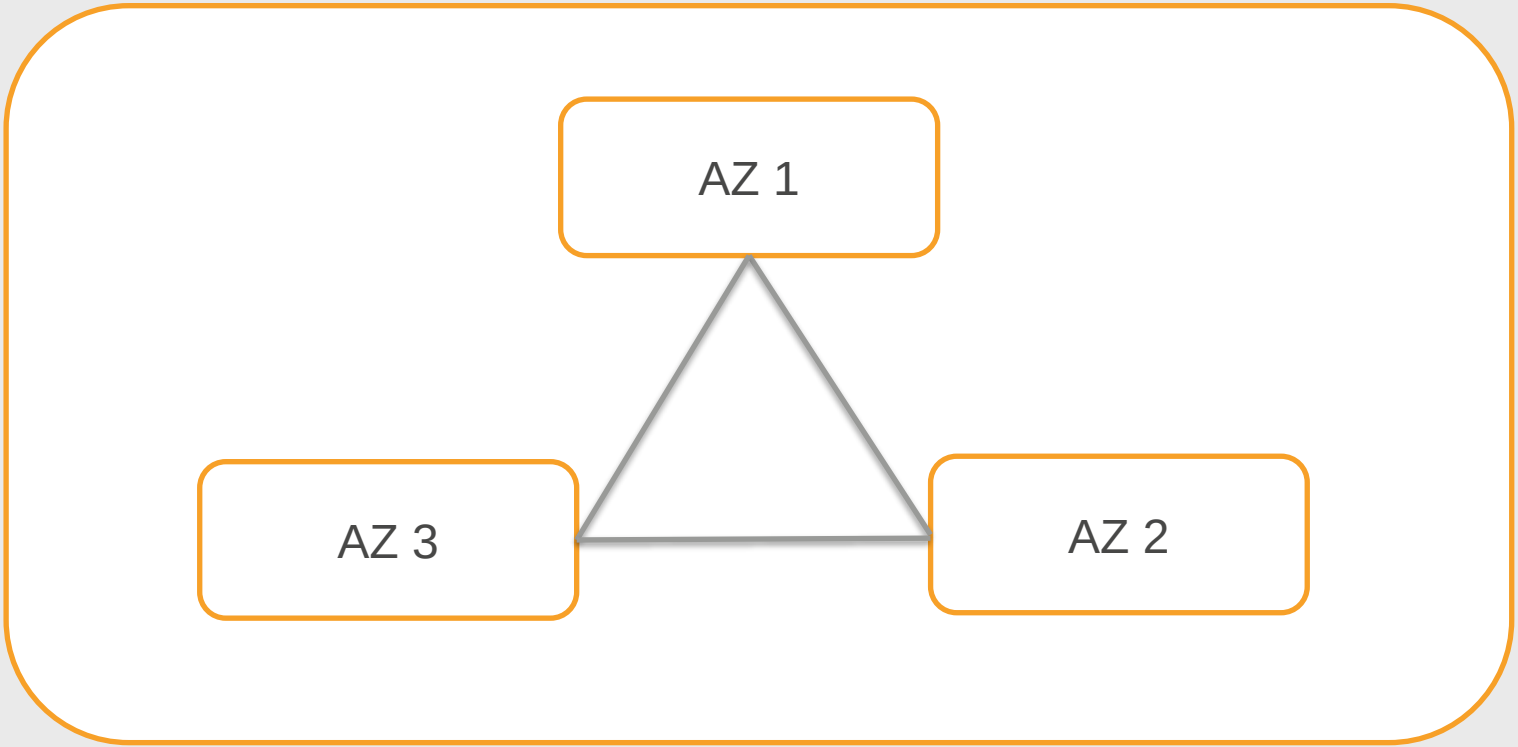
Full control of your cloud

Online Order Processing Application



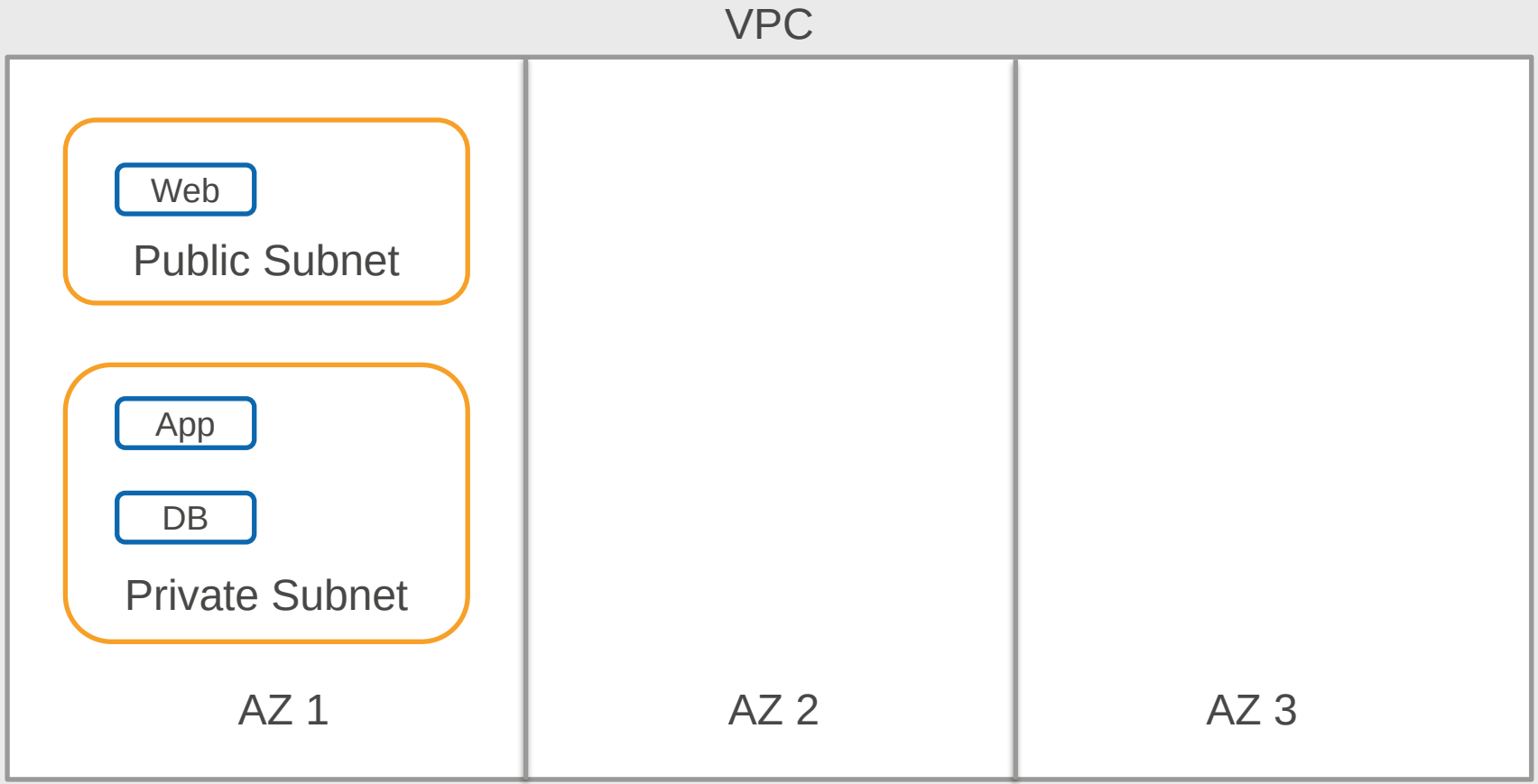
- Resilient
- Scaling
- Security
- Cost

Region

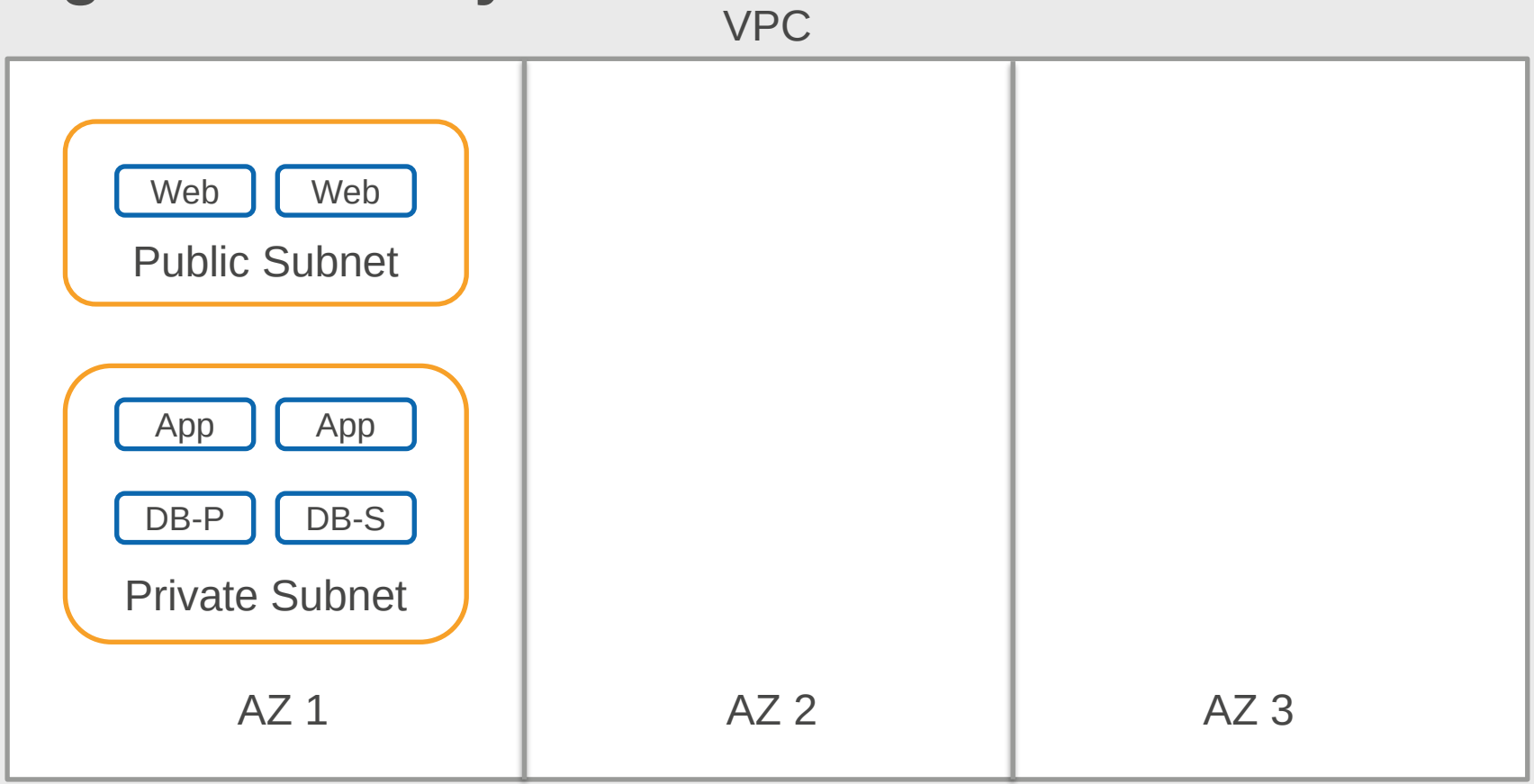


Application should be spread across two or more availability zones

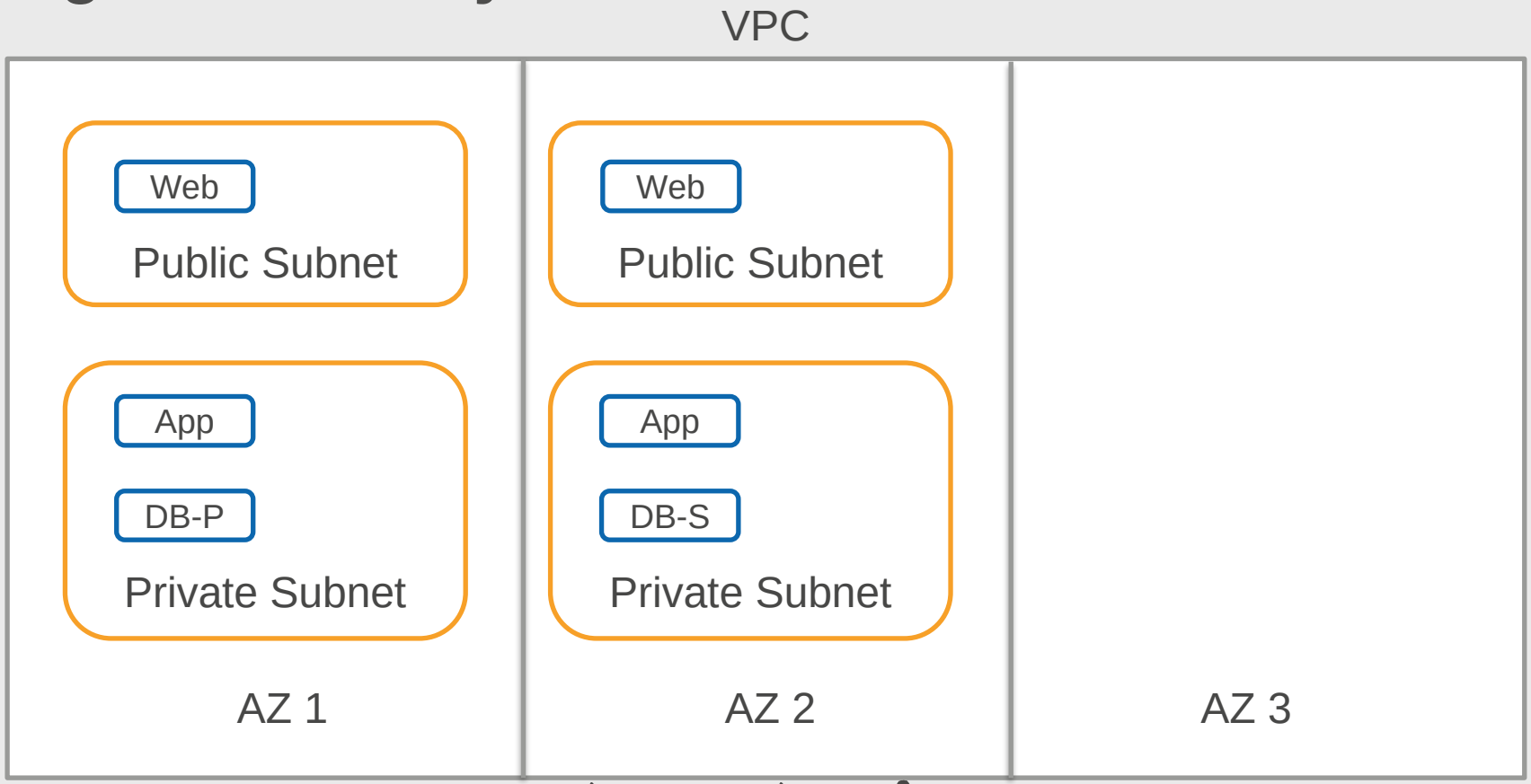
Network



High Availability

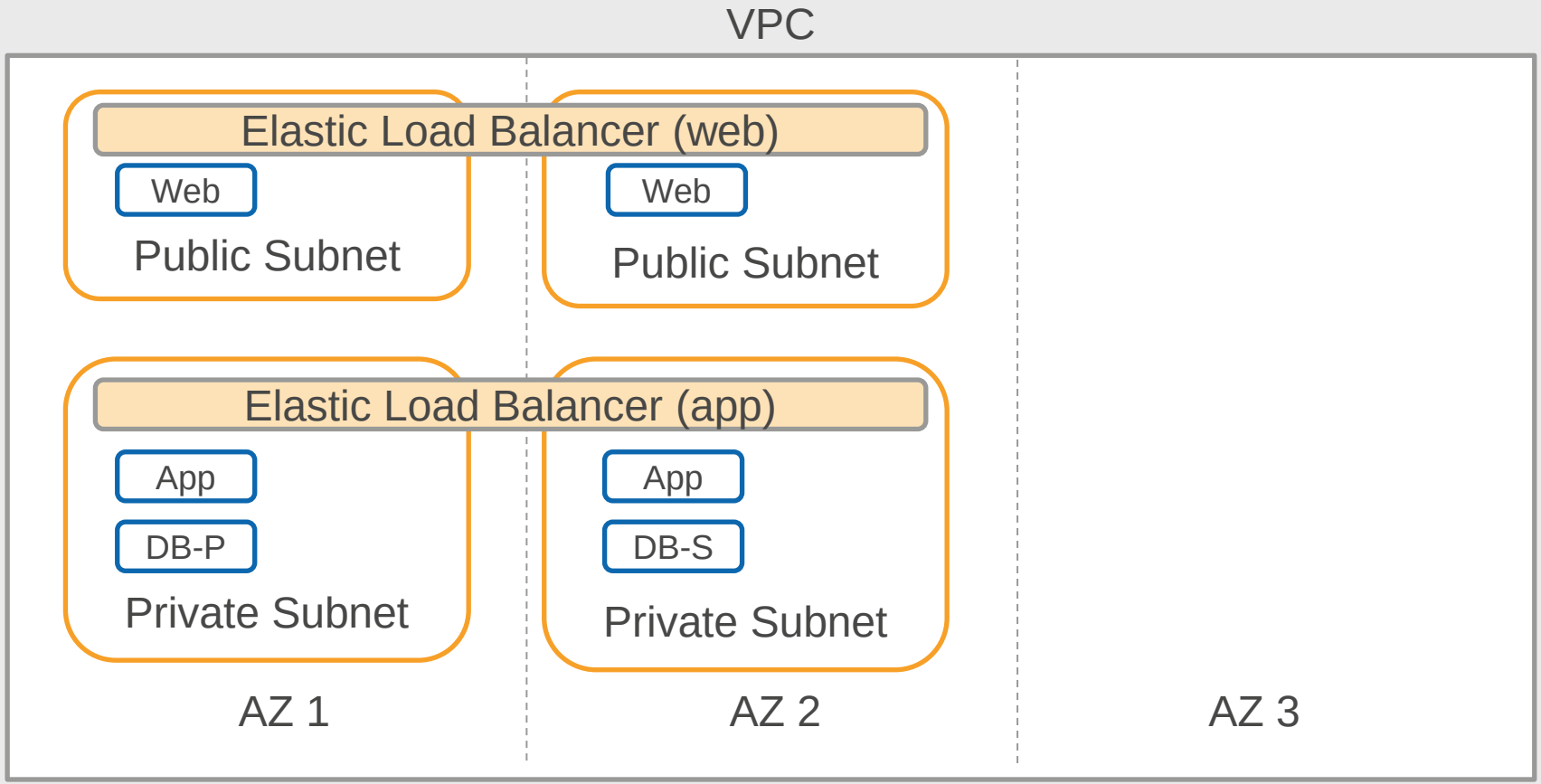


High Availability – Multi-AZ

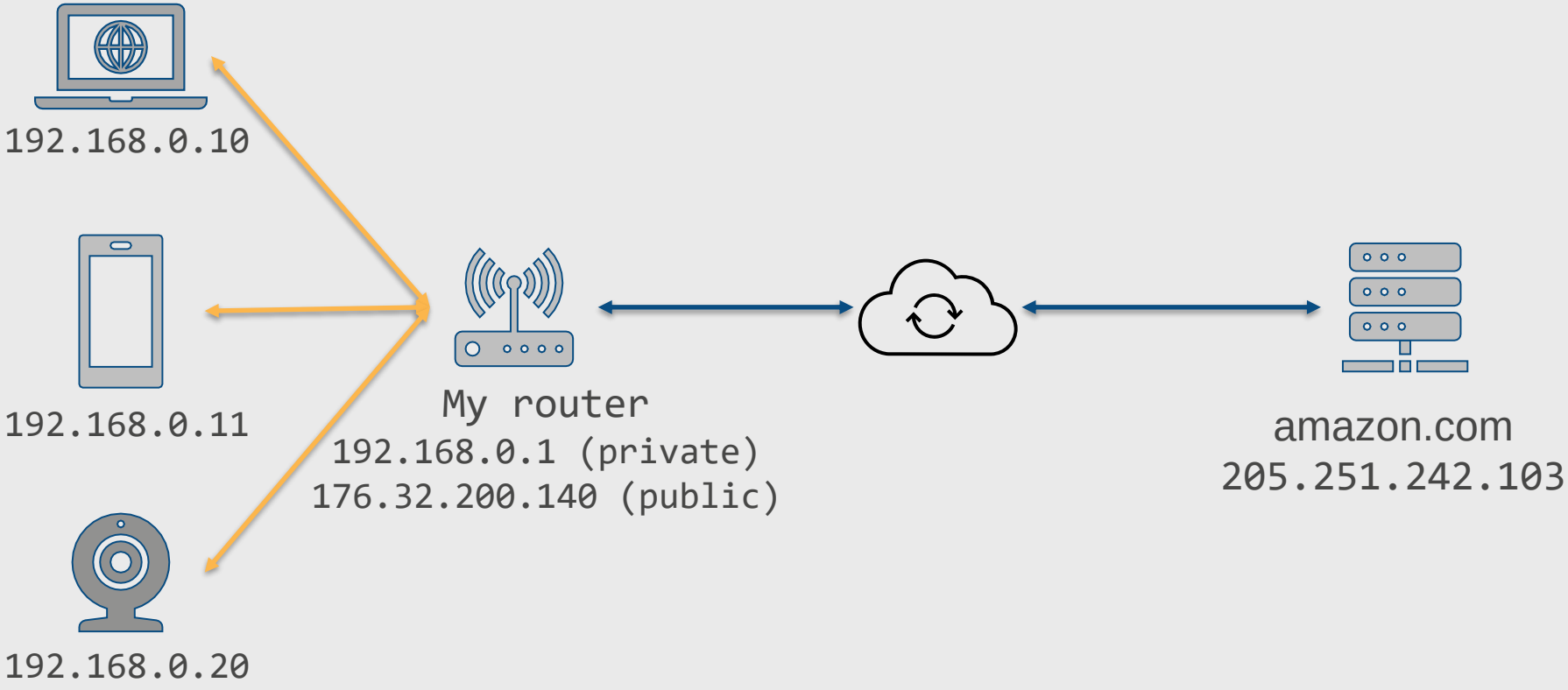


No single point of entry

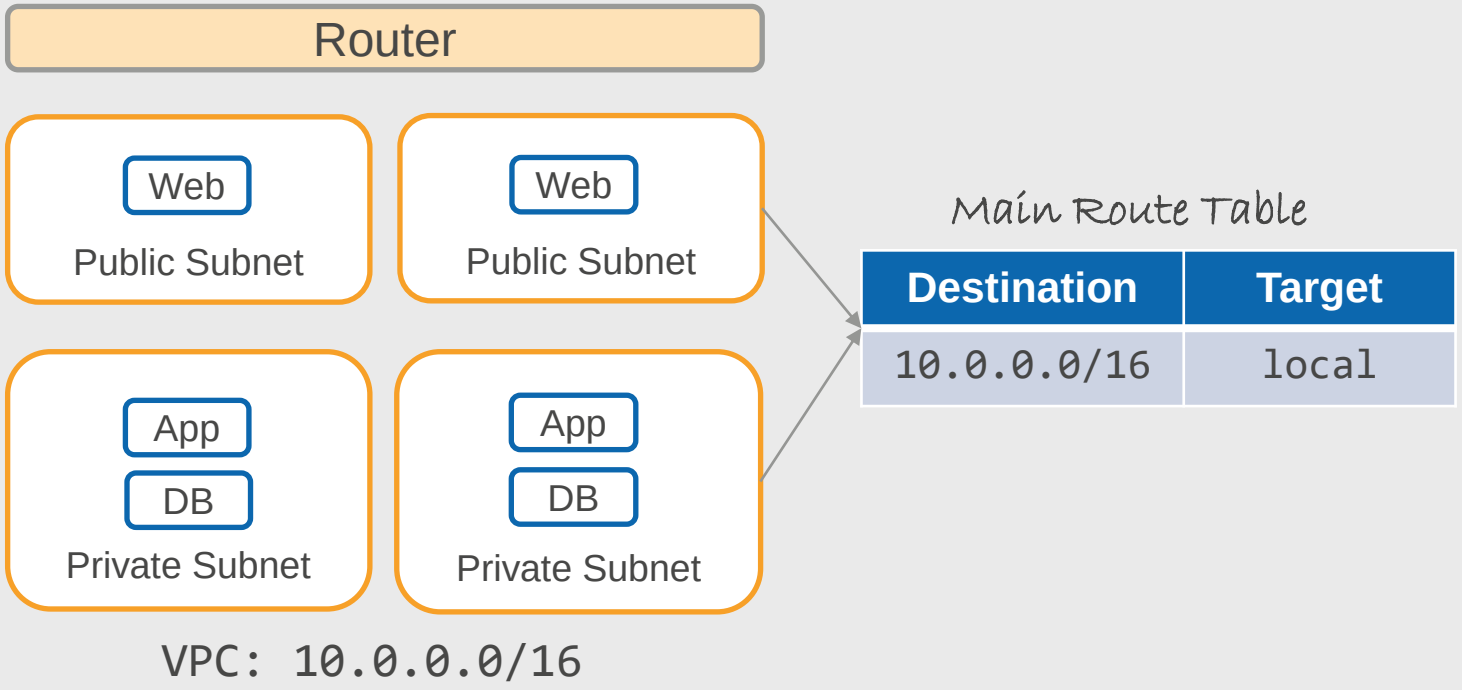
With ELB



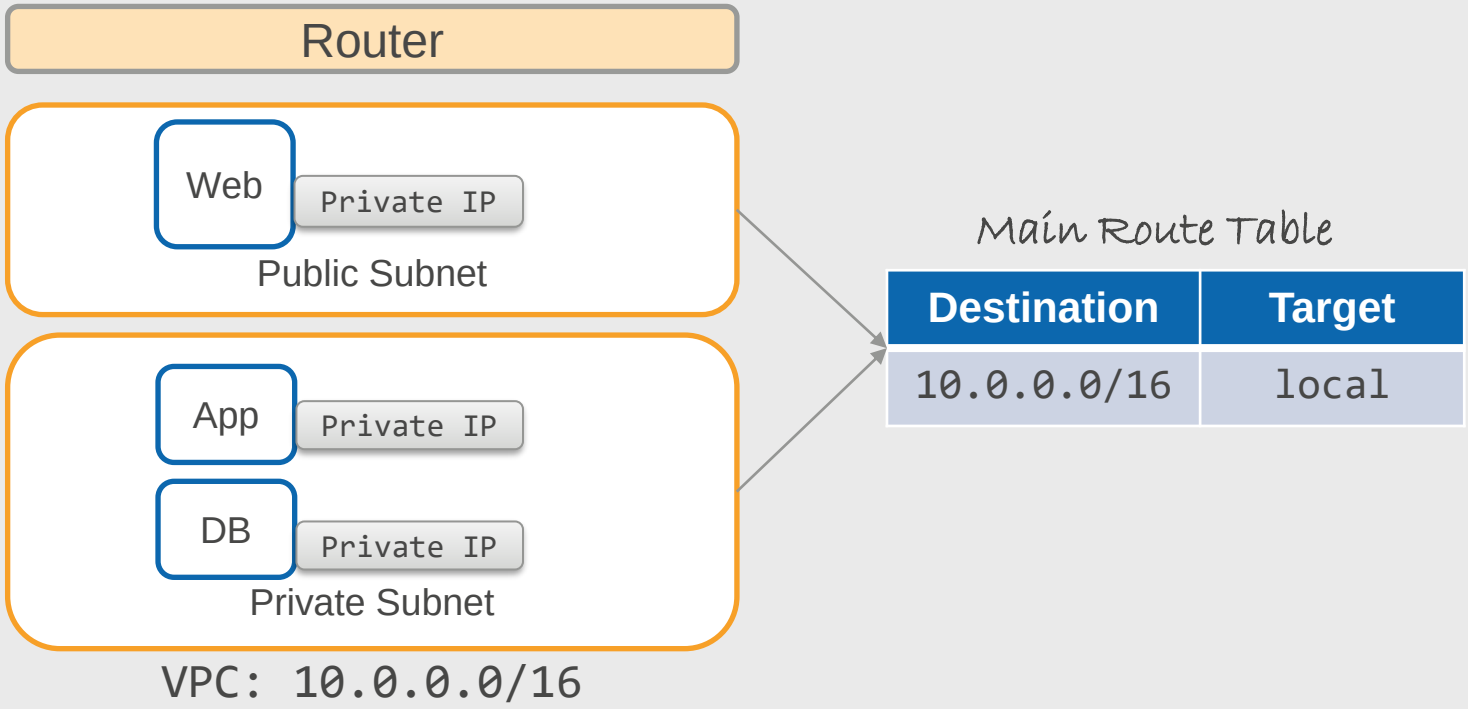
Home Network



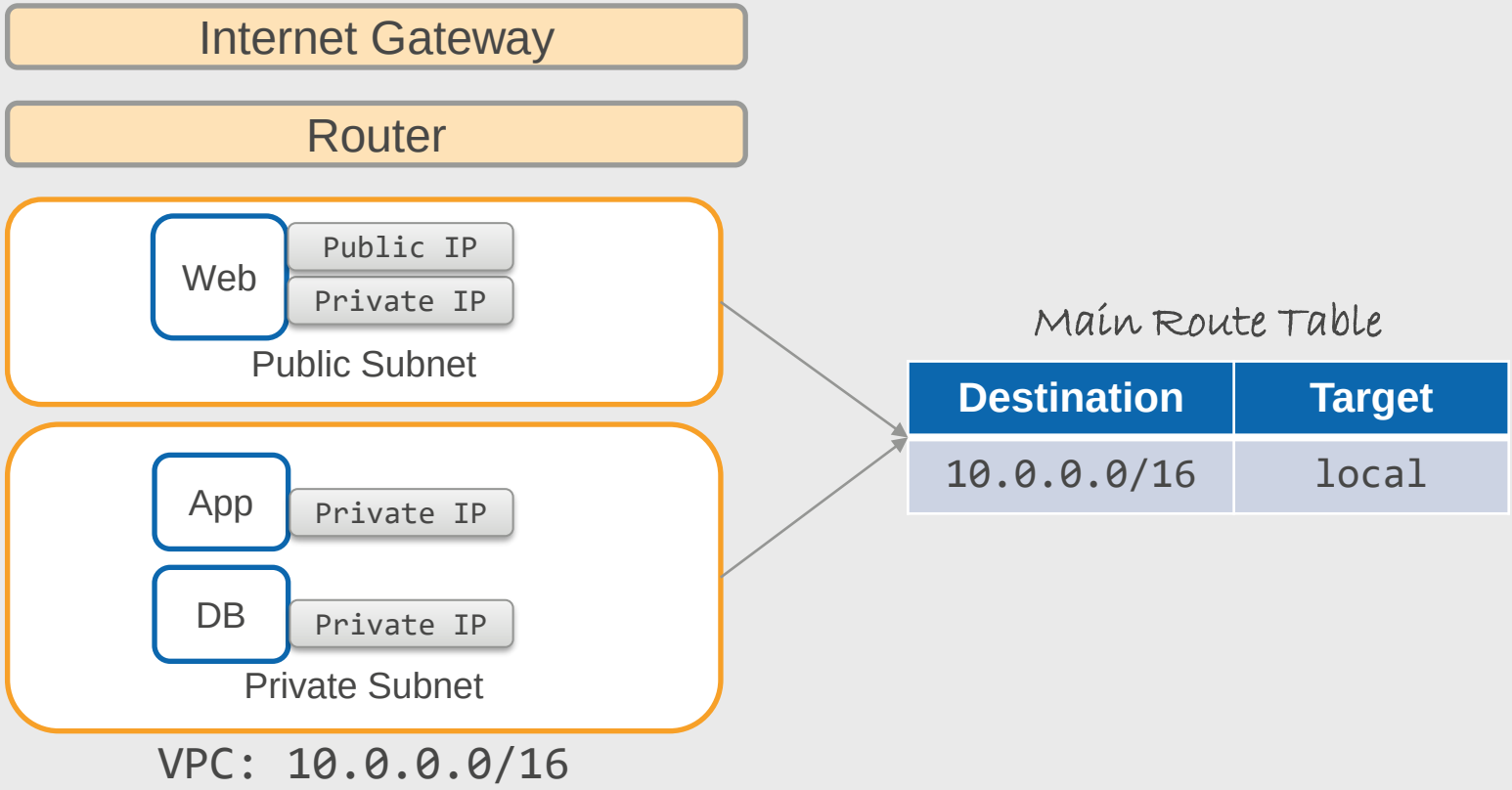
VPC Router



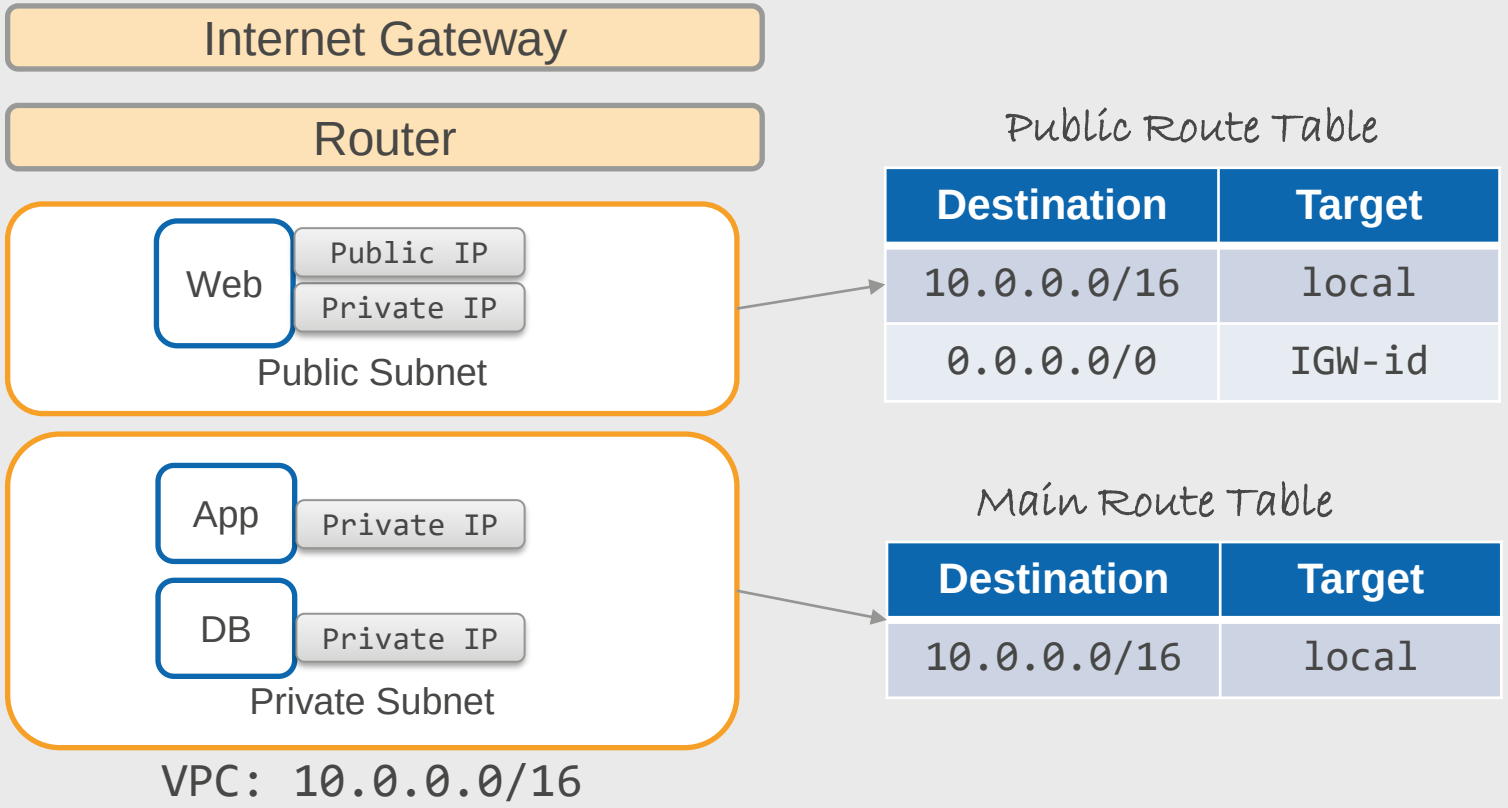
VPC IP



VPC Internet Gateway



VPC Internet Gateway Route

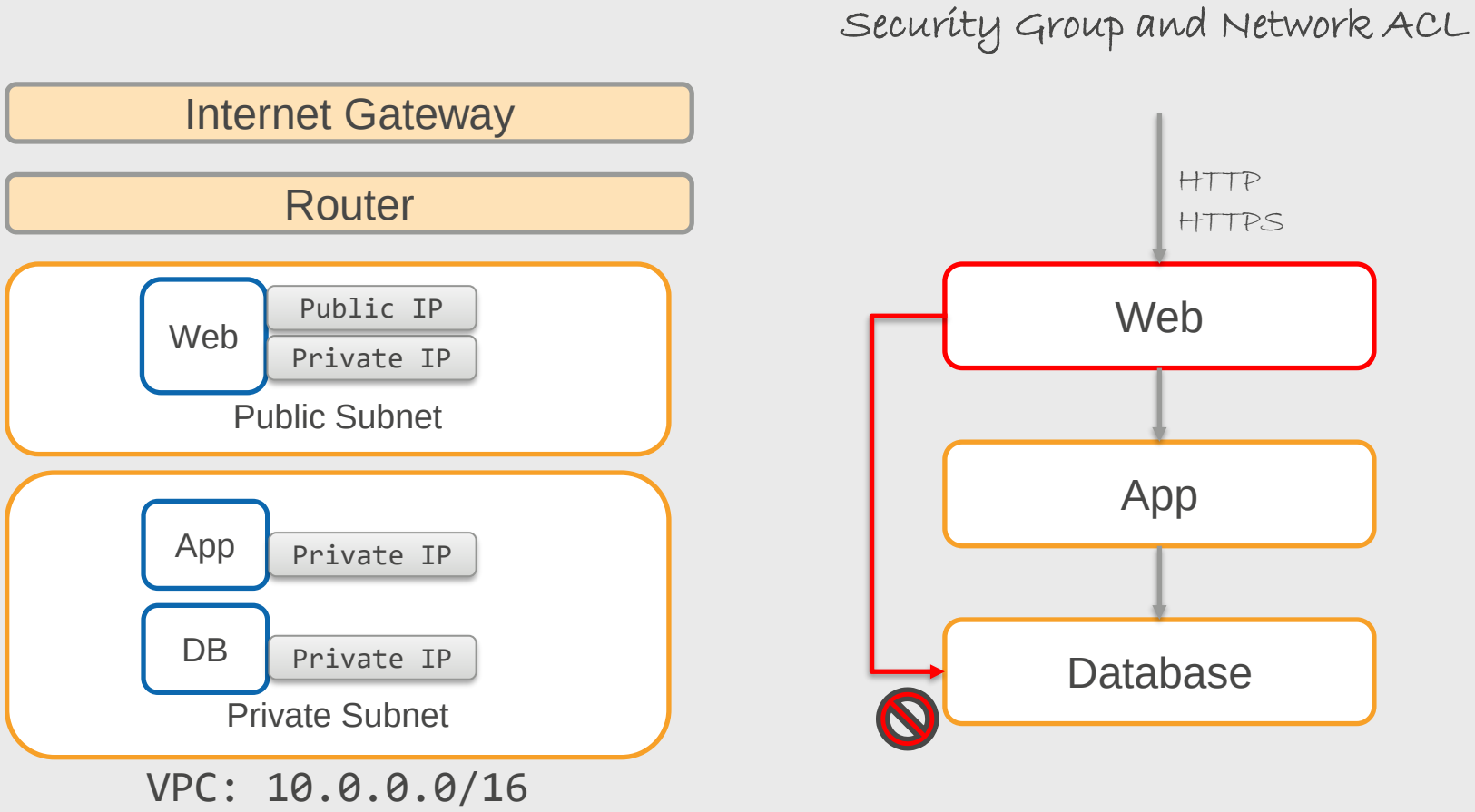


Firewall

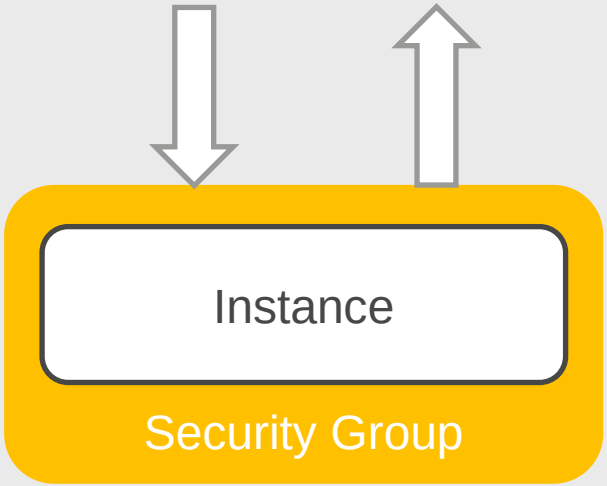
Security Group

Network Access Control List (NACL)

Firewall



Security Group – Instance Firewall



Specify what traffic is ALLOWED

Default Security Group

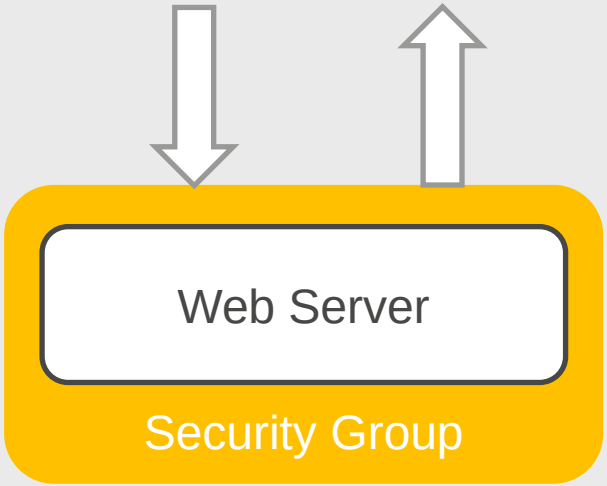
Inbound Rules

Source	Protocol	Port Range	Type
Default SG-ID	ALL	ALL	All Traffic

Outbound Rules

Destination	Protocol	Port Range	Type
0.0.0.0/0	ALL	ALL	All Traffic

Web Server Security Group



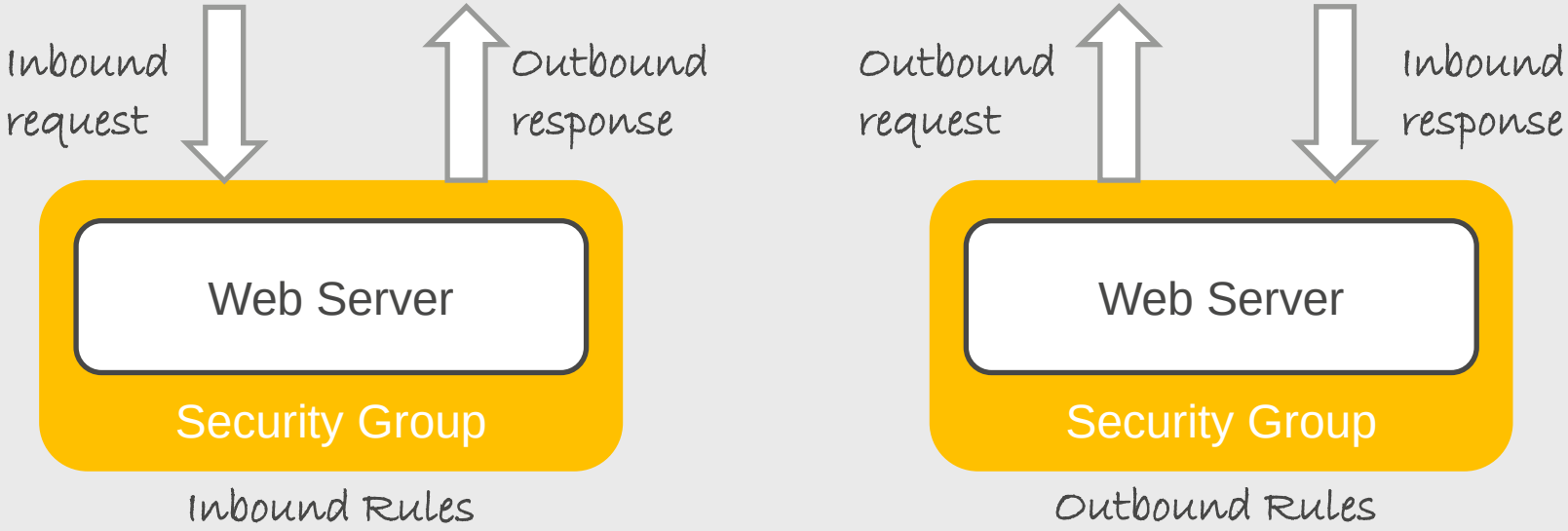
Inbound Rules

Source	Protocol	Port Range	Type
0.0.0.0/0	TCP	80	HTTP
0.0.0.0/0	TCP	443	HTTPS

Outbound Rules

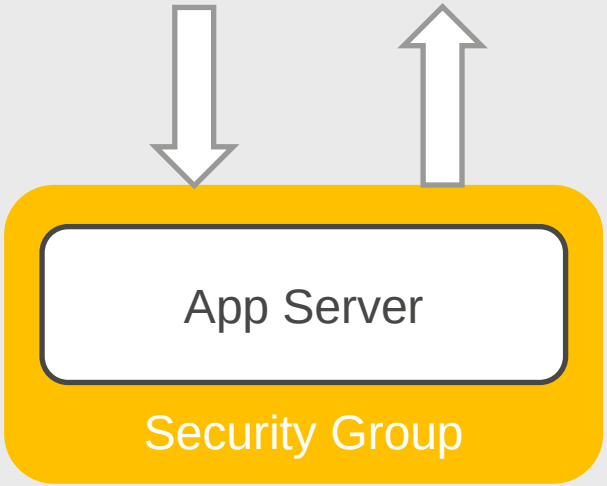
Destination	Protocol	Port Range	Type
0.0.0.0/0	ALL	ALL	All Traffic

Security Group is Stateful



If a request is allowed, the response for the request is automatically allowed

App Server Security Group



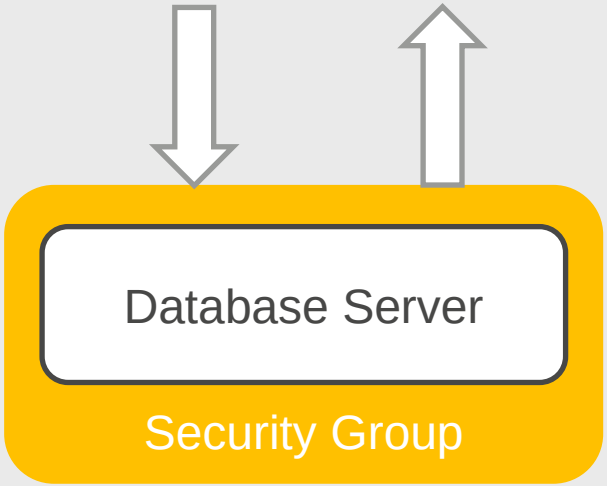
Inbound Rules

Source	Protocol	Port Range	Type
WebServerSG-ID	TCP	80	HTTP
WebServerSG-ID	TCP	443	HTTPS

Outbound Rules

Destination	Protocol	Port Range	Type
0.0.0.0/0	ALL	ALL	All Traffic

Database Server Security Group



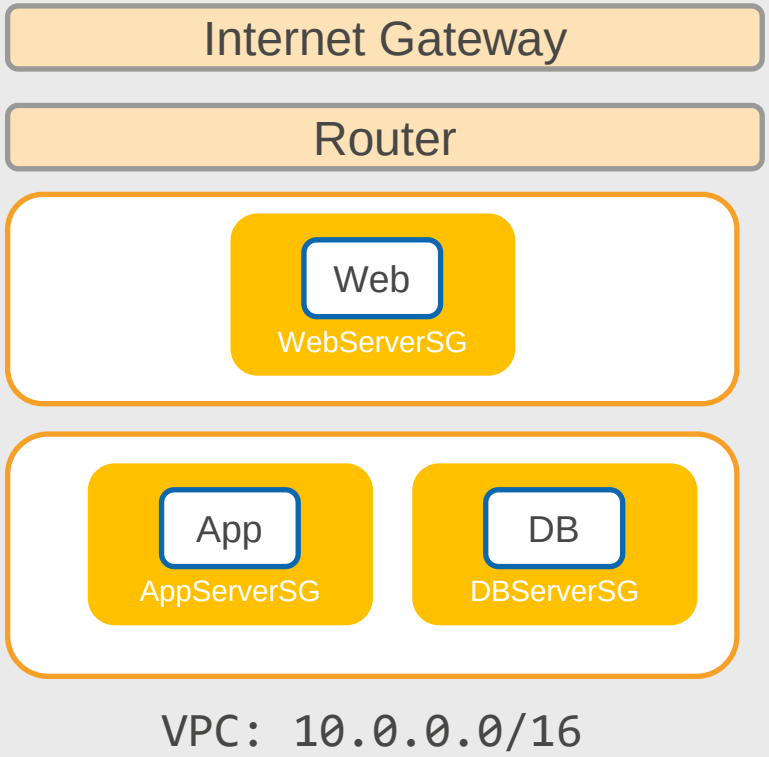
Inbound Rules

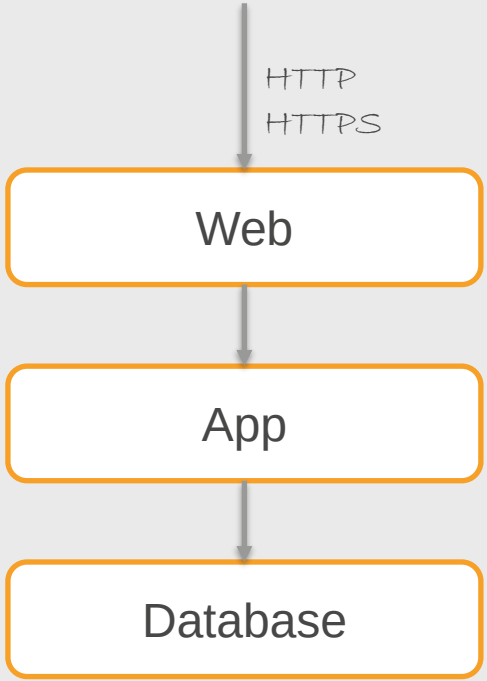
Source	Protocol	Port Range	Type
AppServerSG-ID	TCP	3306	MySQL Aurora

Outbound Rules

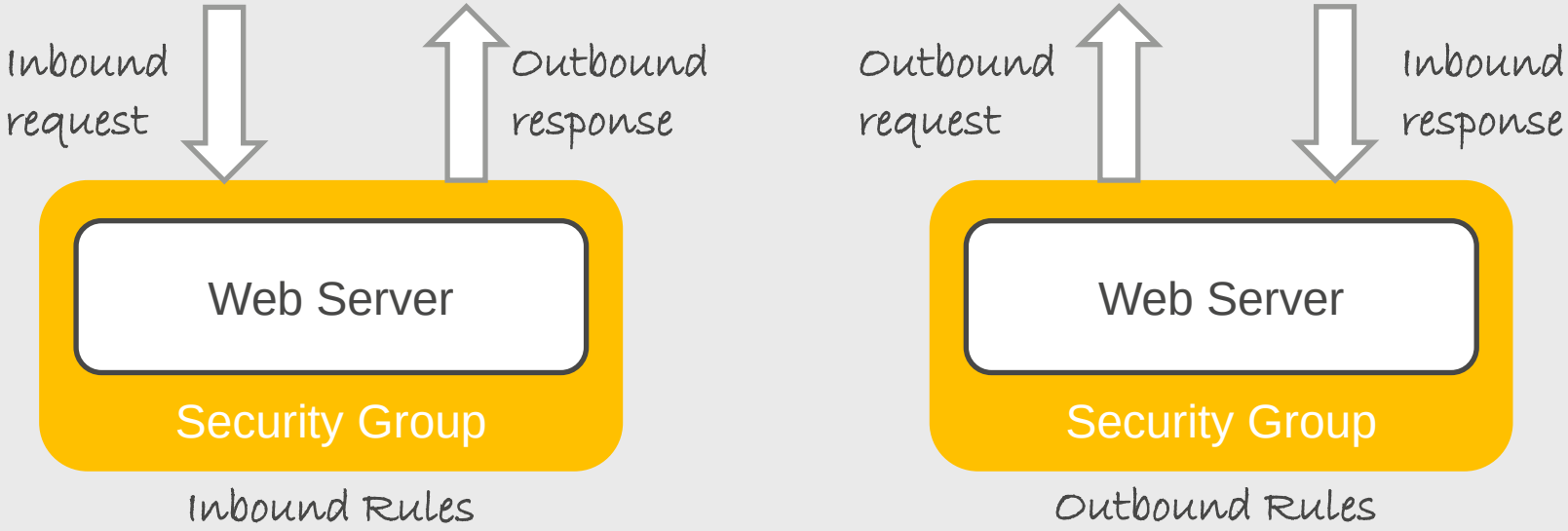
Destination	Protocol	Port Range	Type
0.0.0.0/0	ALL	ALL	All Traffic

Security Group



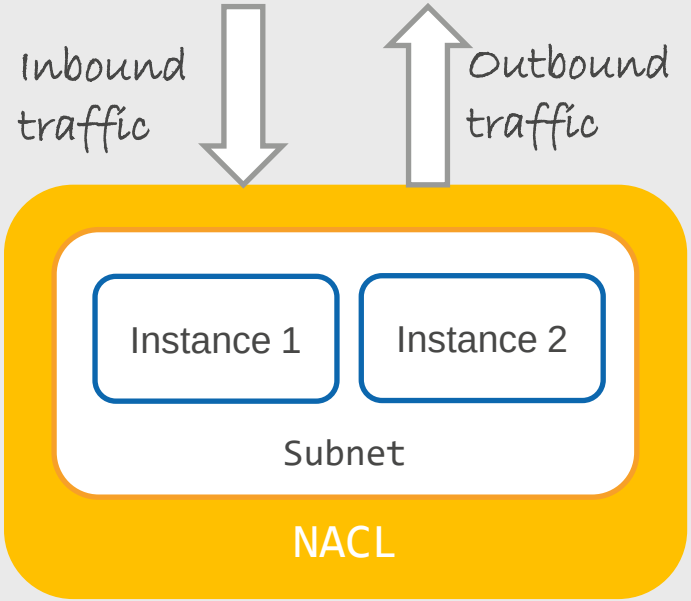


Security Group is Stateful



If a request is allowed, the response for the request is automatically allowed

Network Access Control List (NACL) – Subnet Firewall



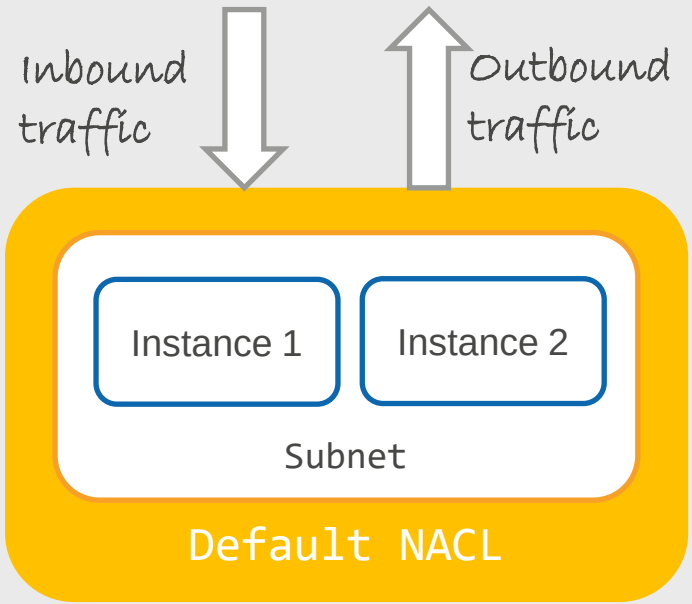
Specify what traffic is ALLOWED or DENIED in a subnet

All instances in the subnet are automatically protected

Stateless firewall – you need to allow both inbound and outbound traffic

Rules are evaluated in numeric order – lowest numbered rule that matches traffic decides the outcome

Default Network ACL



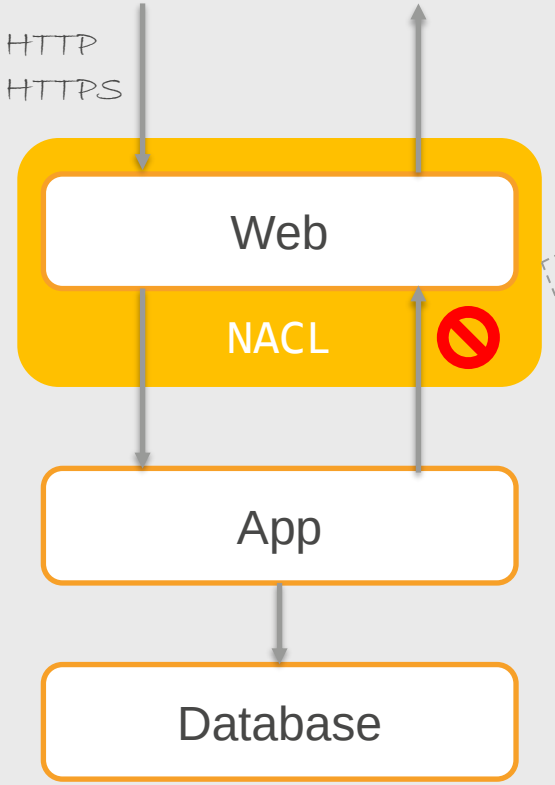
Inbound Rules

Rule #	Protocol	Port Range	Type	Source	Allow/ Deny
100	ALL	ALL	All Traffic	0.0.0.0/0	ALLOW
*	ALL	ALL	All Traffic	0.0.0.0/0	DENY

Outbound Rules

Rule #	Protocol	Port Range	Type	Destination	Allow/ Deny
100	ALL	ALL	All Traffic	0.0.0.0/0	ALLOW
*	ALL	ALL	All Traffic	0.0.0.0/0	DENY

Network ACL is tricky - Stateless



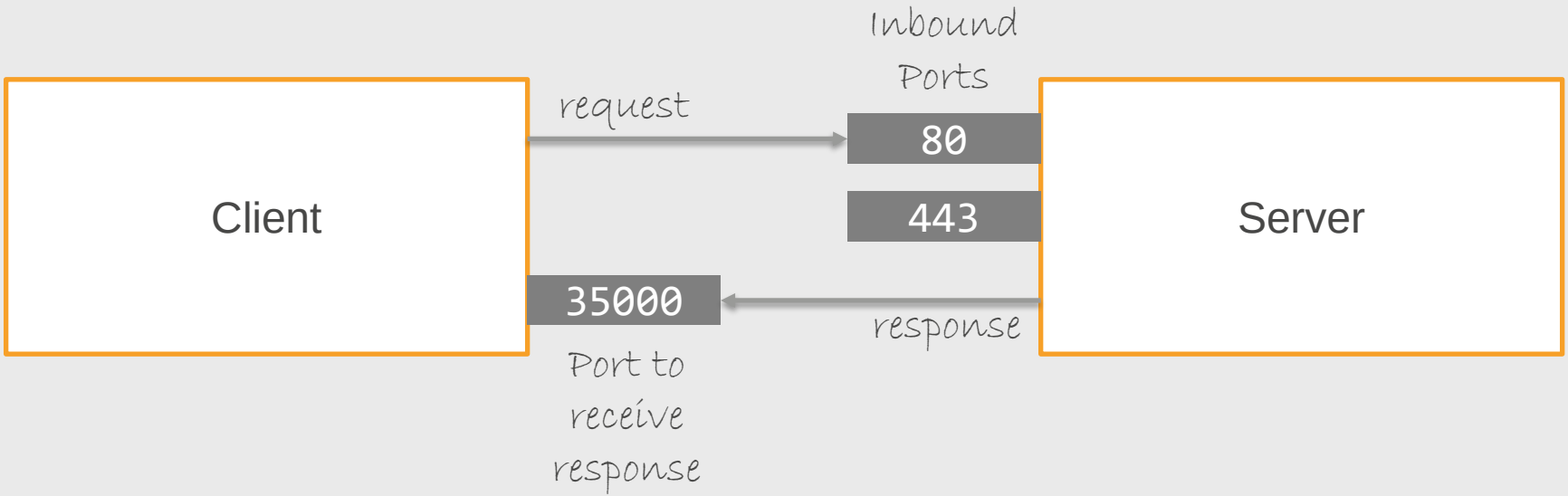
Public Subnet - Inbound Rules

Rule #	Protocol	Port Range	Type	Source	Allow/ Deny
100	TCP	80	HTTP	0.0.0.0/0	ALLOW
110	TCP	443	HTTPs	0.0.0.0/0	ALLOW
*	ALL	ALL	All Traffic	0.0.0.0/0	DENY

Public Subnet - Outbound Rules

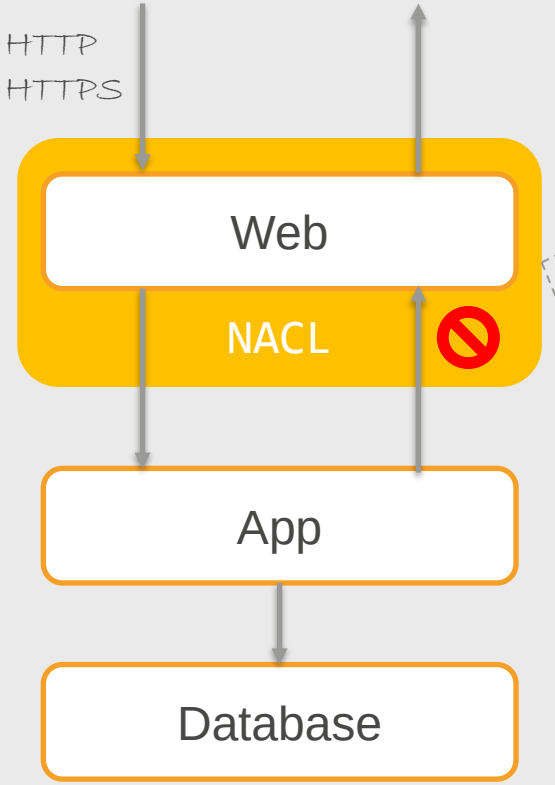
Rule #	Protocol	Port Range	Type	Destination	Allow/ Deny
100	ALL	ALL	All Traffic	0.0.0.0/0	ALLOW
*	ALL	ALL	All Traffic	0.0.0.0/0	DENY

Ephemeral Ports



Linux OS ephemeral port range is `32768-61000`

Network ACL is tricky - Stateless



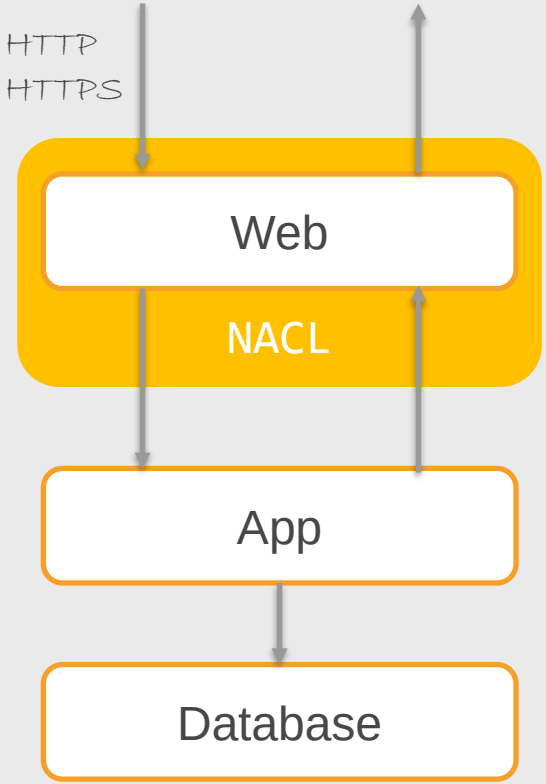
Public Subnet - Inbound Rules

Rule #	Protocol	Port Range	Type	Source	Allow/ Deny
100	TCP	80	HTTP	0.0.0.0/0	ALLOW
110	TCP	443	HTTPs	0.0.0.0/0	ALLOW
*	ALL	ALL	All Traffic	0.0.0.0/0	DENY

Public Subnet - Outbound Rules

Rule #	Protocol	Port Range	Type	Destination	Allow/ Deny
100	ALL	ALL	All Traffic	0.0.0.0/0	ALLOW
*	ALL	ALL	All Traffic	0.0.0.0/0	DENY

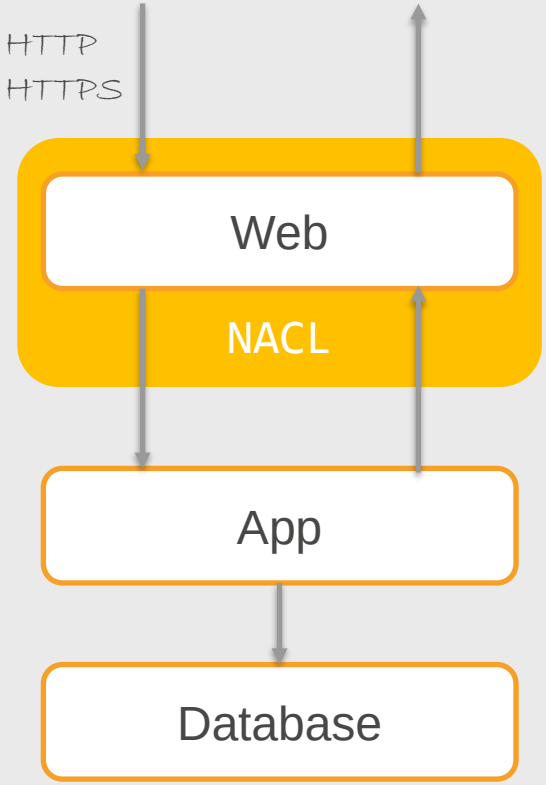
Network ACL – Fix Allow Local Traffic



Public Subnet - Inbound Rules

Rule #	Protocol	Port Range	Type	Source	Allow/ Deny
90	ALL	ALL	All Traffic	10.0.0.0/16	ALLOW
100	TCP	80	HTTP	0.0.0.0/0	ALLOW
110	TCP	443	HTTPS	0.0.0.0/0	ALLOW
*	ALL	ALL	All Traffic	0.0.0.0/0	DENY

Network ACL - Deny

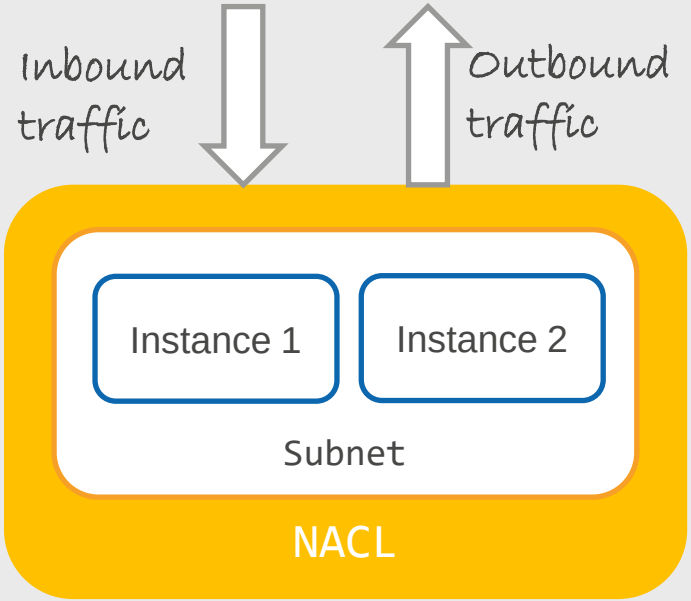


DENY suspicious requests

Public Subnet - Inbound Rules

Rule #	Protocol	Port Range	Type	Source	Allow/ Deny
50	ALL	ALL	All Traffic	123.123.0.0/16	DENY
90	ALL	ALL	All Traffic	10.0.0.0/16	ALLOW
100	TCP	80	HTTP	0.0.0.0/0	ALLOW
110	TCP	443	HTTPS	0.0.0.0/0	ALLOW
*	ALL	ALL	All Traffic	0.0.0.0/0	DENY

Network Access Control List (NACL) – Subnet Firewall



Specify what traffic is ALLOWED or DENIED in a subnet

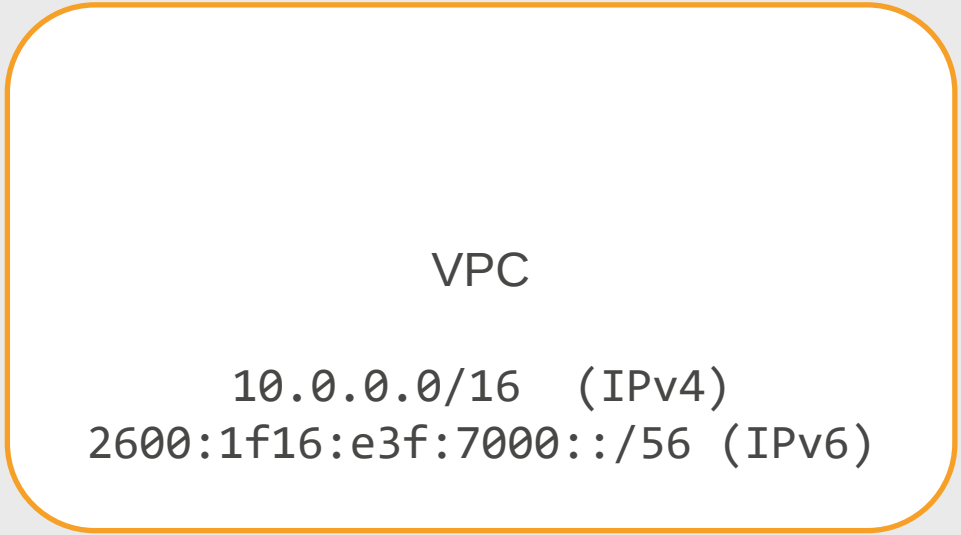
All instances in the subnet are automatically protected

Stateless firewall – you need to allow both inbound and outbound traffic

Rules are evaluated in numeric order – lowest numbered rule that matches traffic decides the outcome

Private, Public and Elastic IP

VPC CIDR



IPV4 and IPV6 Traffic are routed separately

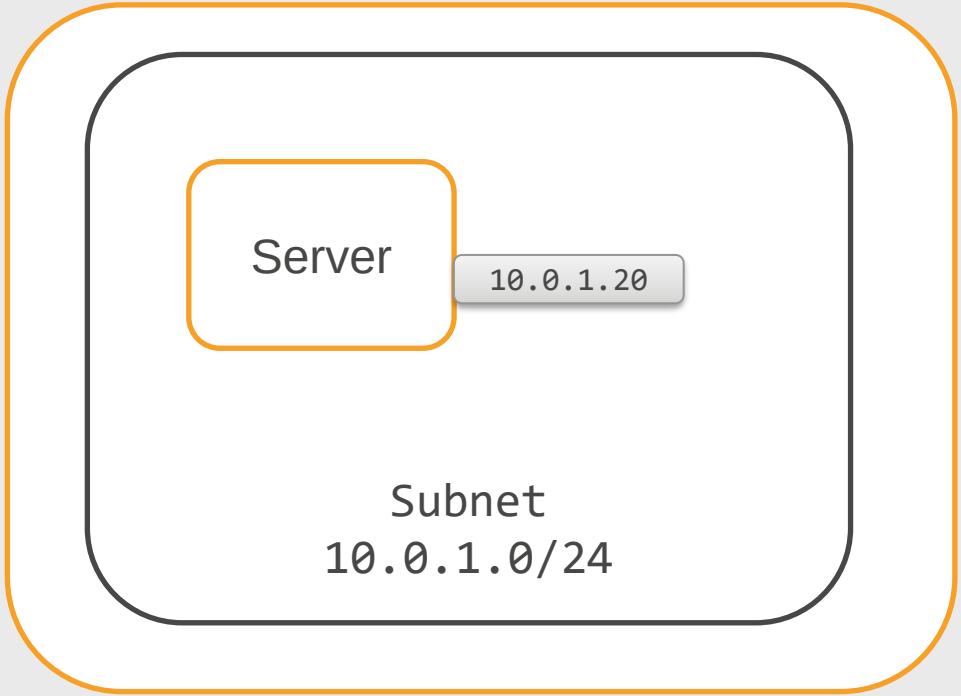
Configure

- Route table
- Security Group
- Network ACL

Private IPV4 CIDR

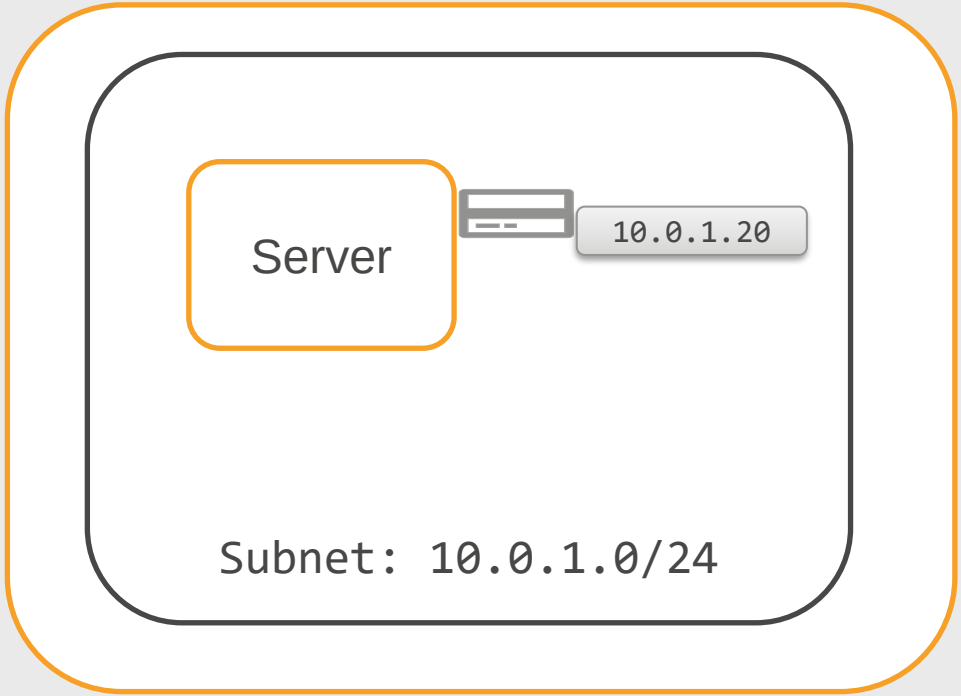
10.0.0.0 - 10.255.255.255 (10.0.0.0/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16.0.0/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168.0.0/16 prefix)

Private IP



Private IP automatically assigned from subnet CIDR block

Elastic Network Interface (ENI)

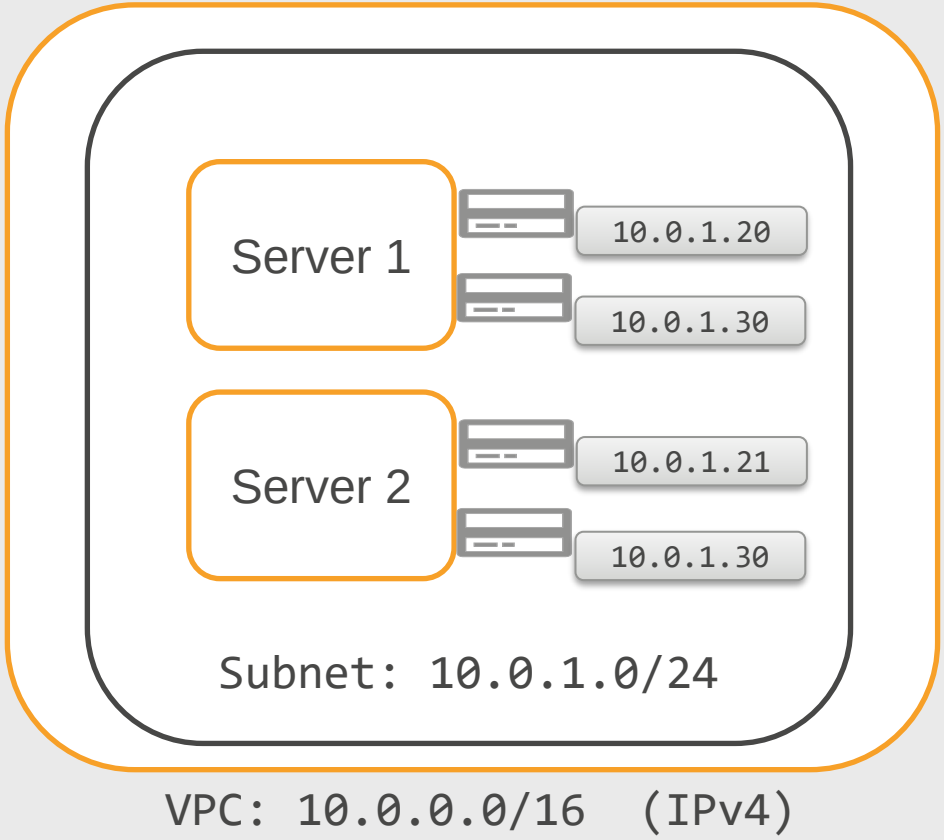


IP address is assigned to the primary network interface `eth0`

Private DNS Hostname

Primary network interface and private IP address stays with the instance until instance is terminated

Multiple Elastic Network Interfaces (ENI)

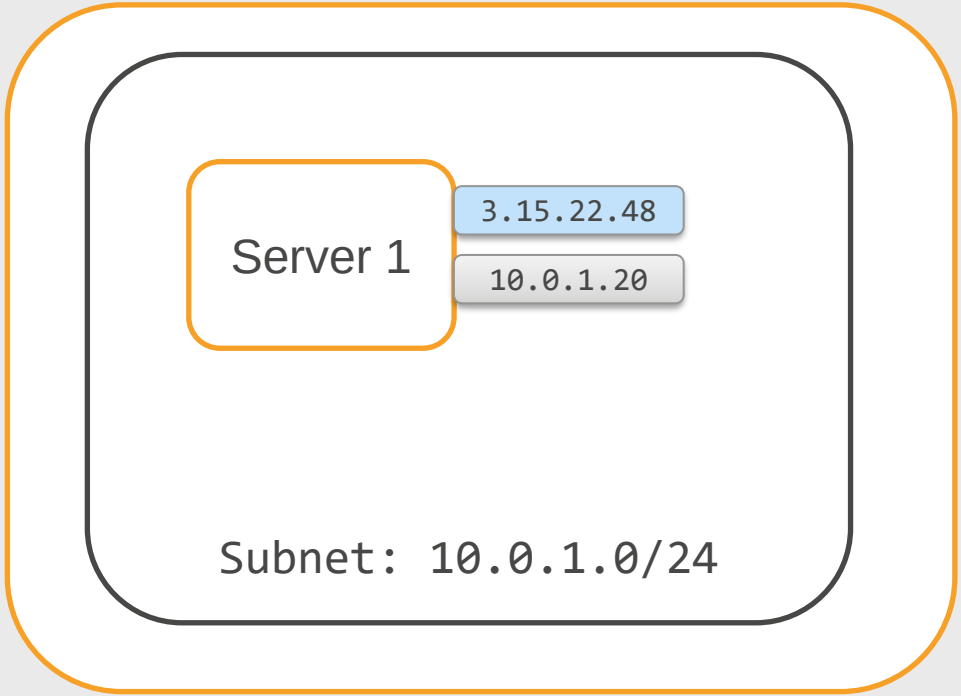


Multiple network interfaces can be attached to an instance

Secondary ENI can be detached and attached to another instance

Network traffic to that IP address is redirected to the new instance

Public IP



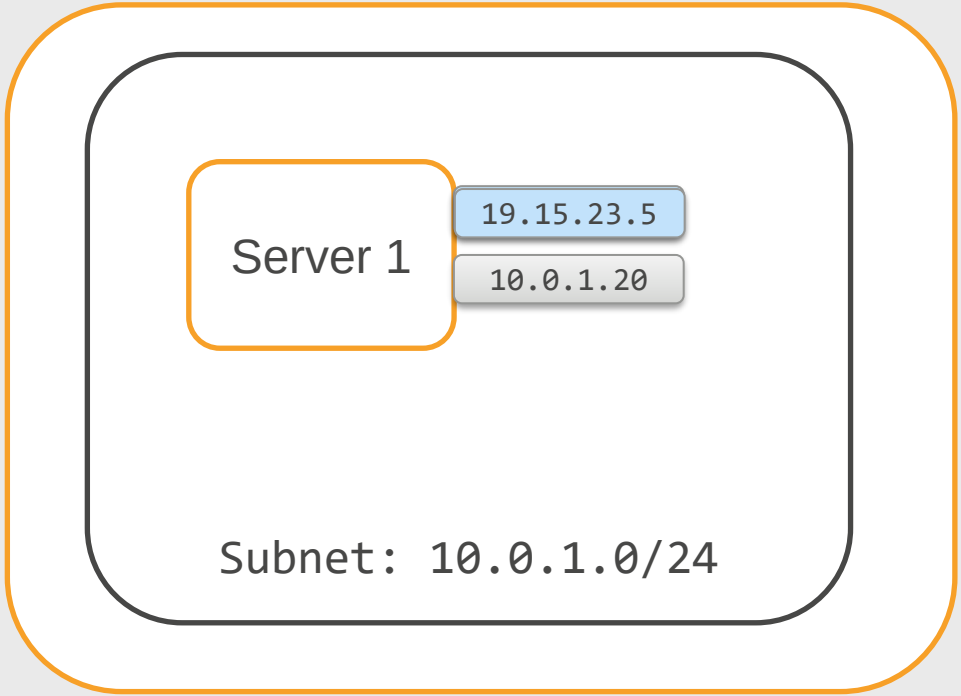
Public IP required to send or receive request from the internet

Public IP Assignment:

- Specify at the time of launching the instance
- Subnet setting to auto-assign public IP

Assigned from Amazon's Public IP pool

Public IP – Instance Start/Stop/Terminate



Stop or Terminate instance

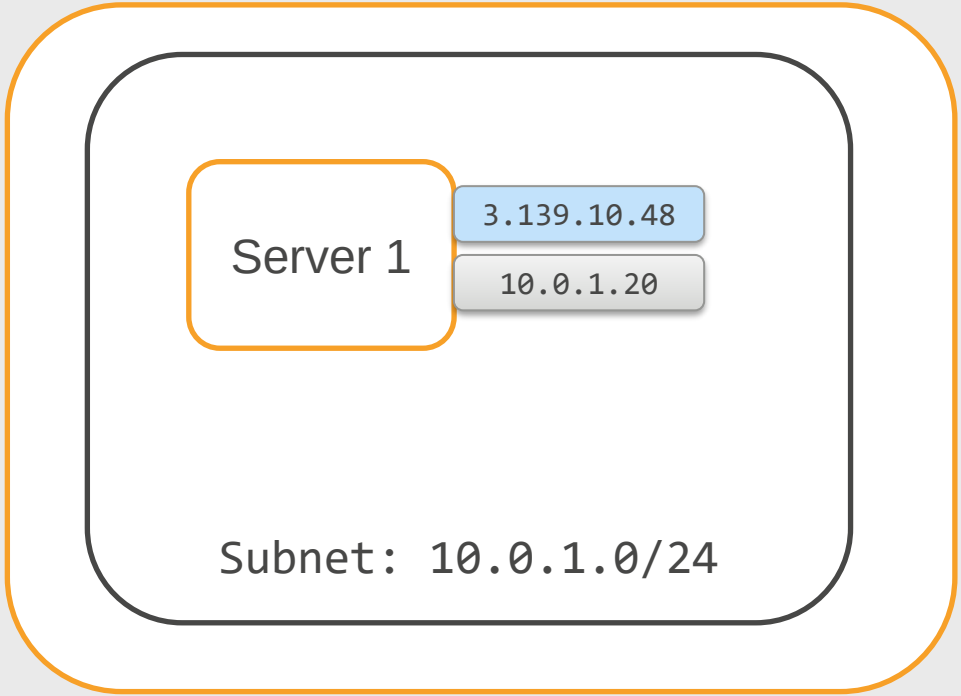
- Public IP is released back to pool

Restart a stopped instance

- New Public IP is assigned

Public IP will change if you stop and restart an instance

Elastic IP



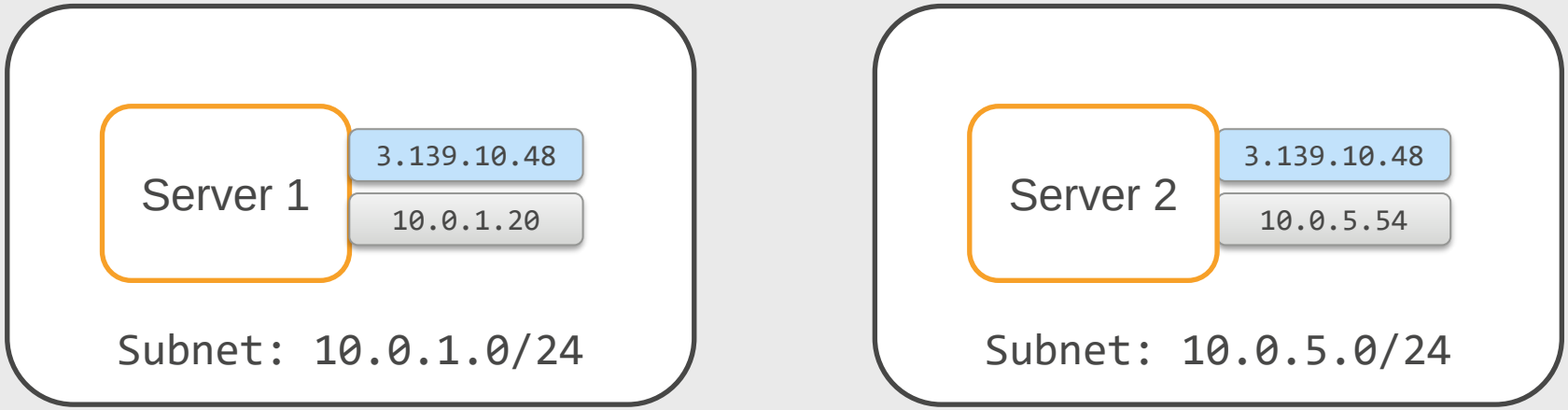
Elastic IP is static-public IP address

Assign to any instance

Stays attached to stopped instance

Limit of 5 Elastic IP per account per region

Elastic IP – Move to a different instance



Detach and attach to a different instance in the same region in your account

Redirect traffic to the new instance

Elastic IP remains allocated to your account until you release it

Private, Public, Elastic

1. Private – Each instance is assigned a Private IP. Stays for the life of the instance

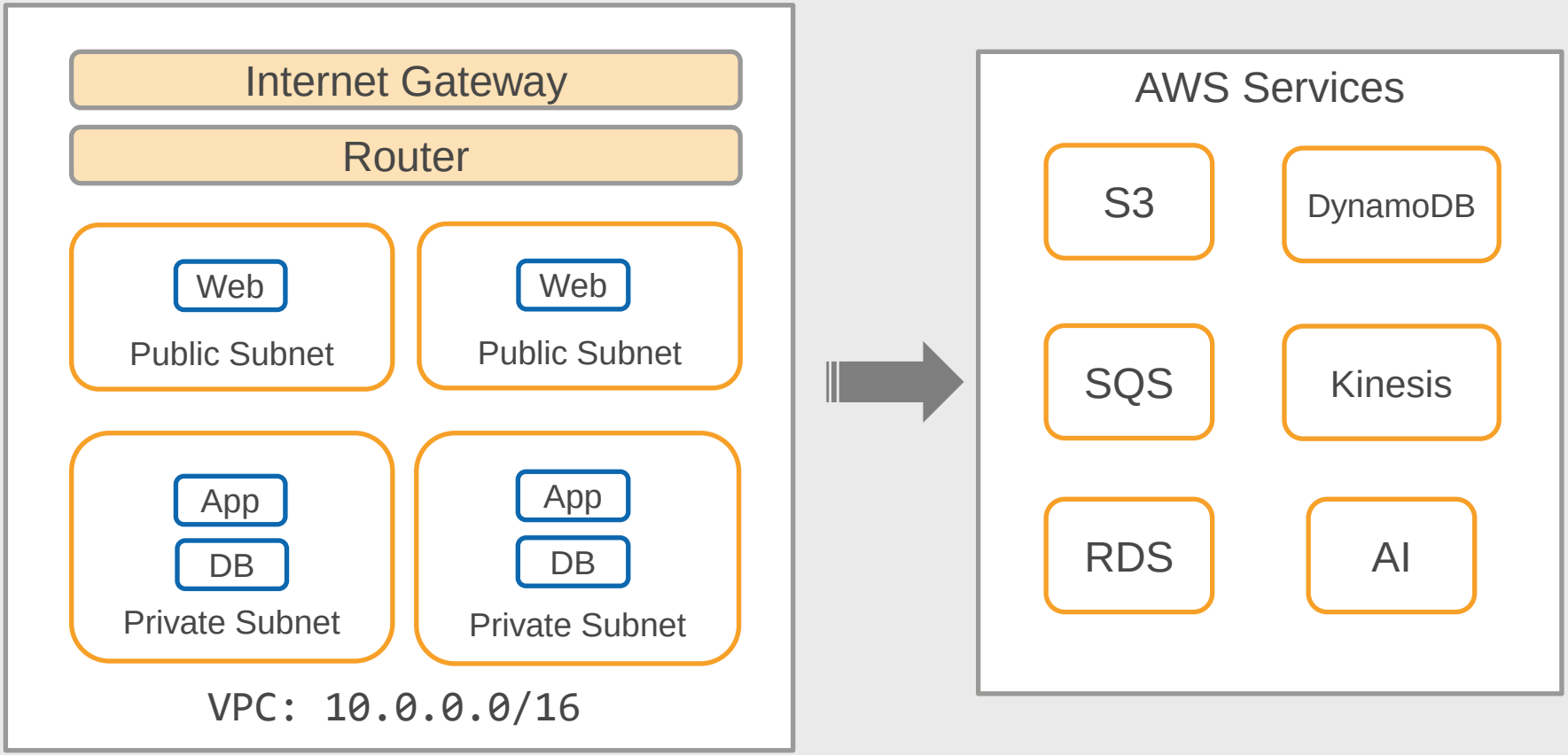
2. Public – Optional. Enabled when launching the instance. Required to send or receive traffic from the internet

3. Elastic – Optional. Persistent/Static IP address assigned to your account/region. Required to send or receive traffic from the internet. You can reassign to any instance in the region

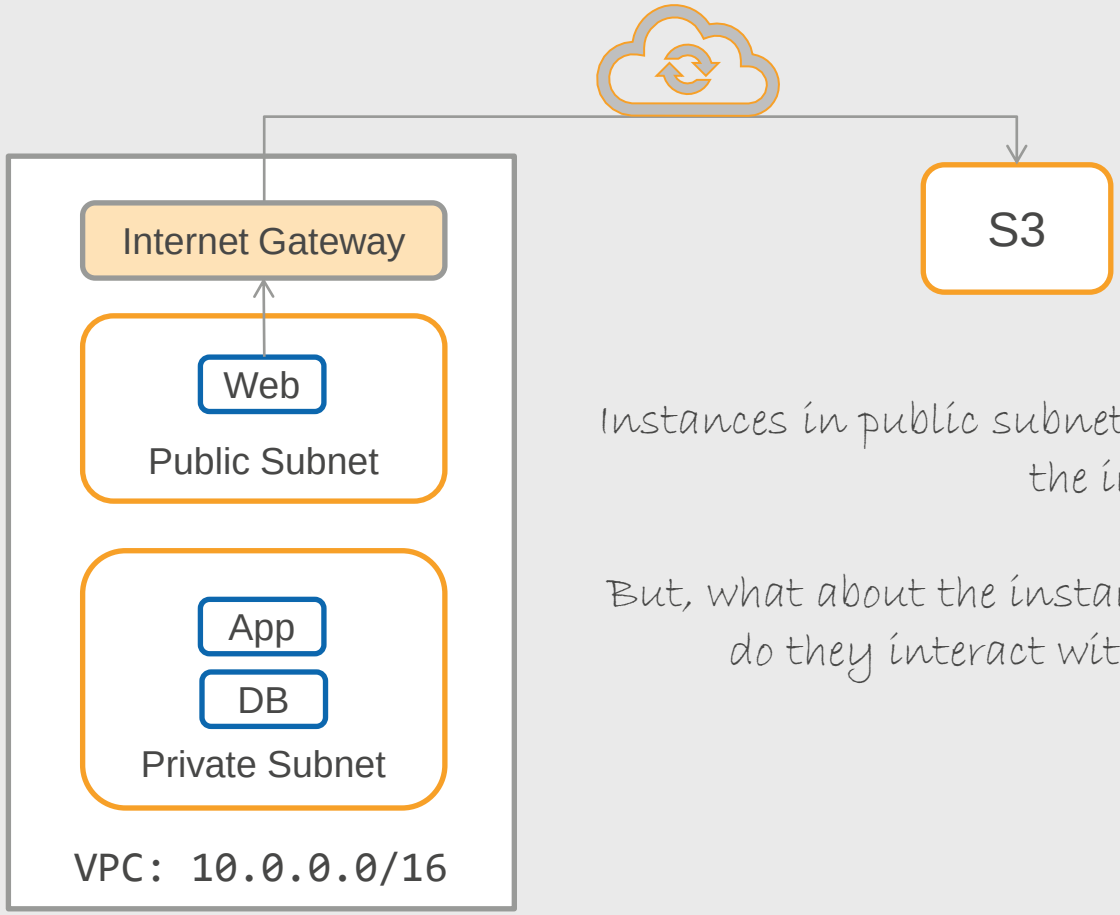
Integrating with other AWS Services

Internet
Gateway Endpoint
Interface Endpoint

How to integrate with other AWS services?



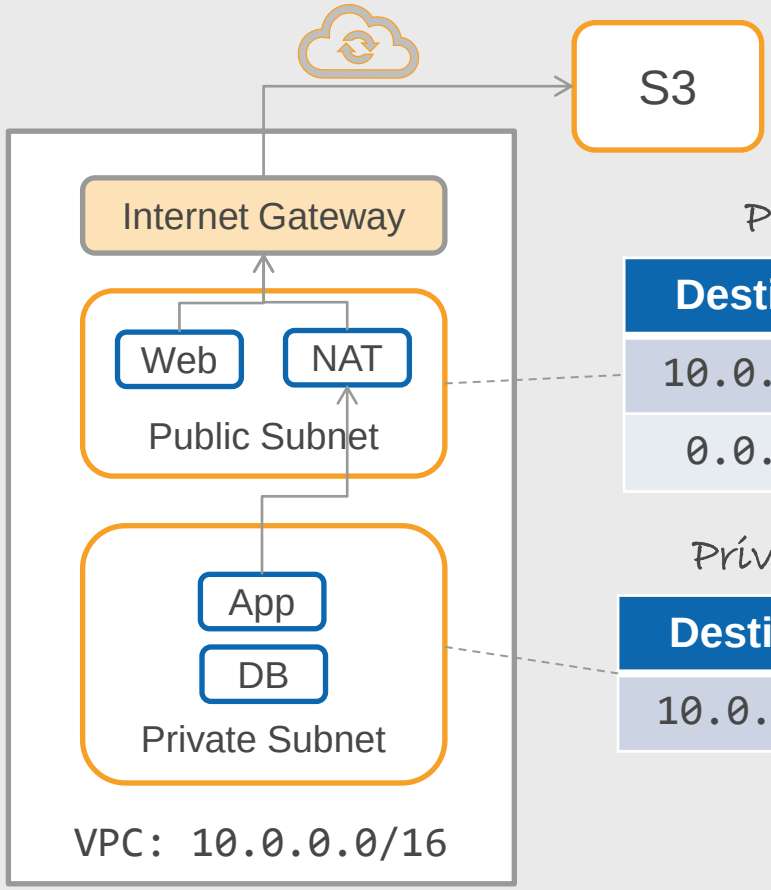
Option 1: Public instances use the internet



Instances in public subnet can make outbound calls to the internet

But, what about the instances in private subnet? How do they interact with other AWS services?

Option 1: Private instances use the internet with NAT



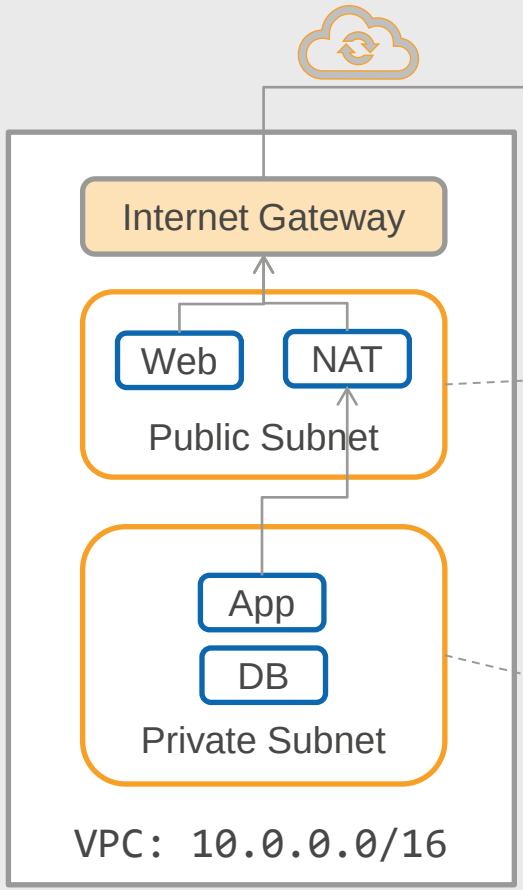
Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW-id

Private Route Table

Destination	Target
10.0.0.0/16	local

Option 1: Private instances use the internet with NAT



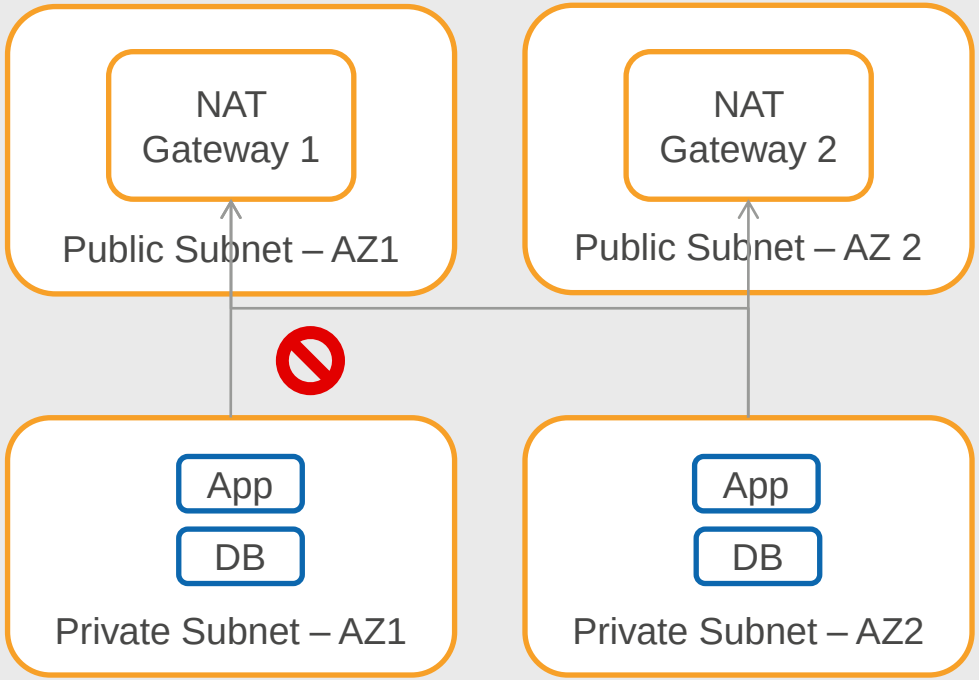
Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW-id

Private Route Table (include path to NAT)

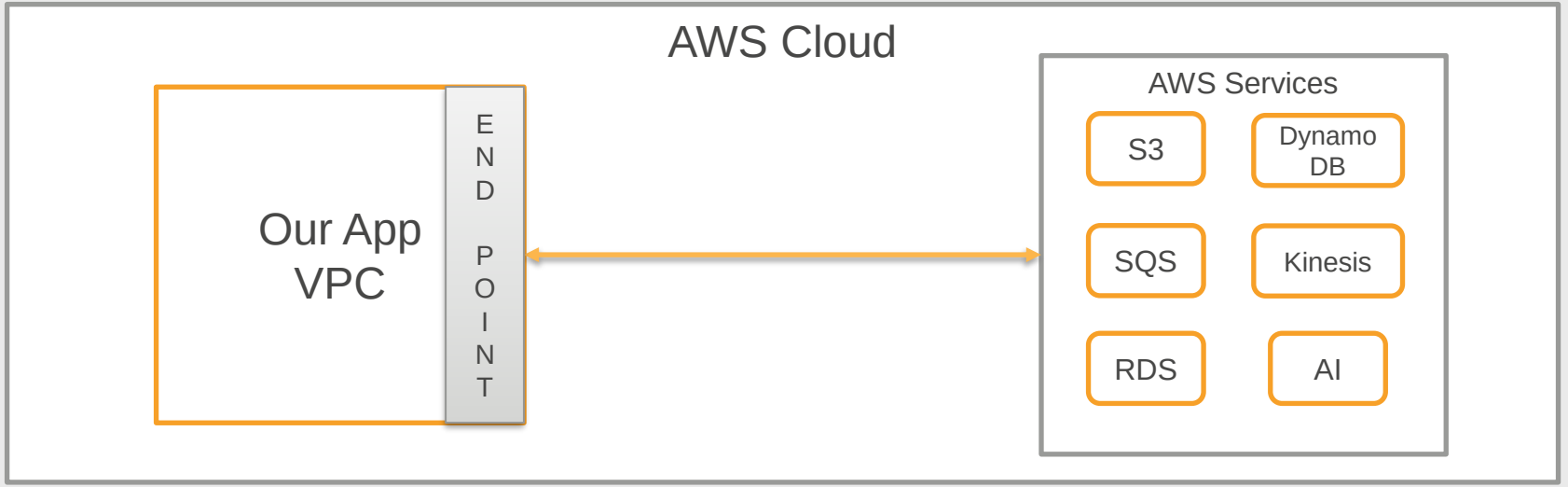
Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT-GW-id

NAT



- NAT Gateway is a managed service
- Automatically scales
- Elastic IP required
- Deployed in Public Subnet in specific AZ
- High Availability – Deploy one per AZ
- Blocks unsolicited inbound requests
- NAT Instance – single server NAT. You handle HA, Scalability

Why not talk directly to AWS services?



With endpoints, you can privately talk to AWS services (without using the internet)

Endpoint Types

Gateway Endpoint - S3, DynamoDB

Interface Endpoint – All newer services use interface endpoint

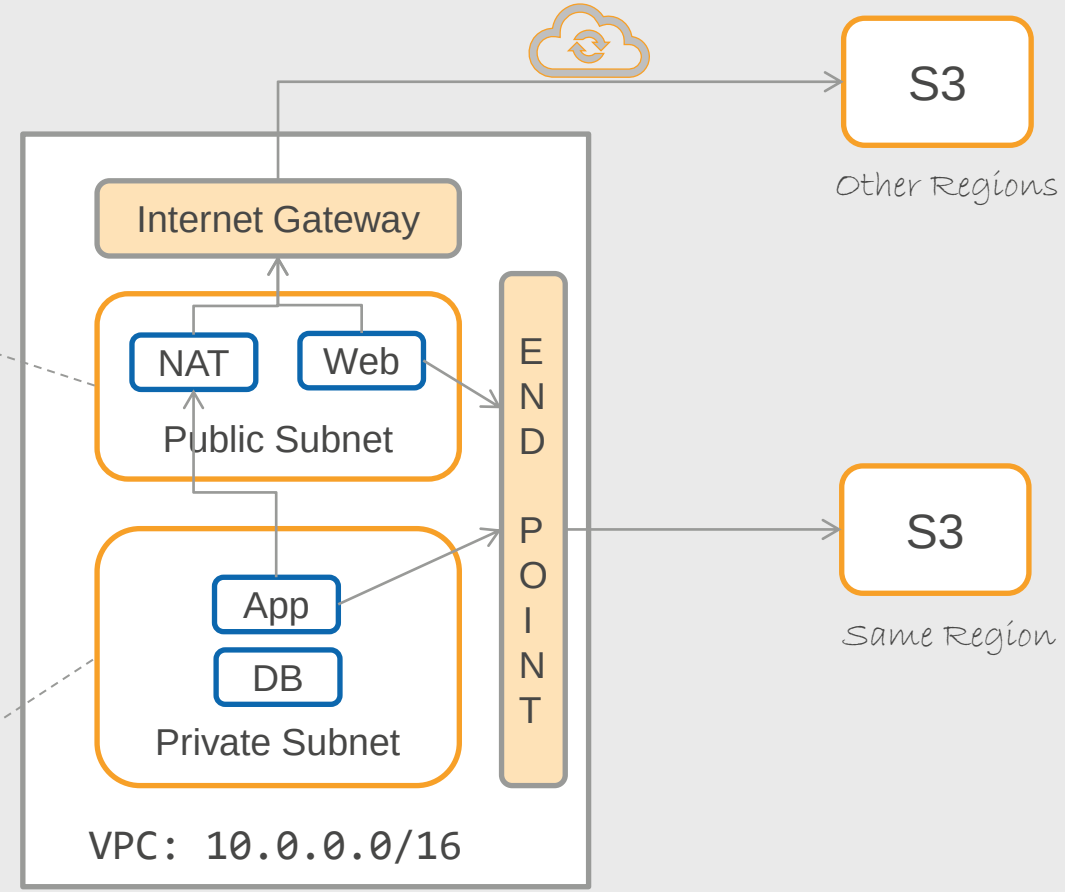
Gateway Endpoint

Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW-id
Pl-id	VPCE-id

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT-GW-id
Pl-id	VPCE-id



Gateway Endpoint

1. With endpoint, you can access S3 and DynamoDB using Private IP address

2. Endpoint is regional - Used for S3 and DynamoDB in the same region

3. For other regions, use internet gateway +NAT

Endpoint Types

Gateway Endpoint - S3, DynamoDB

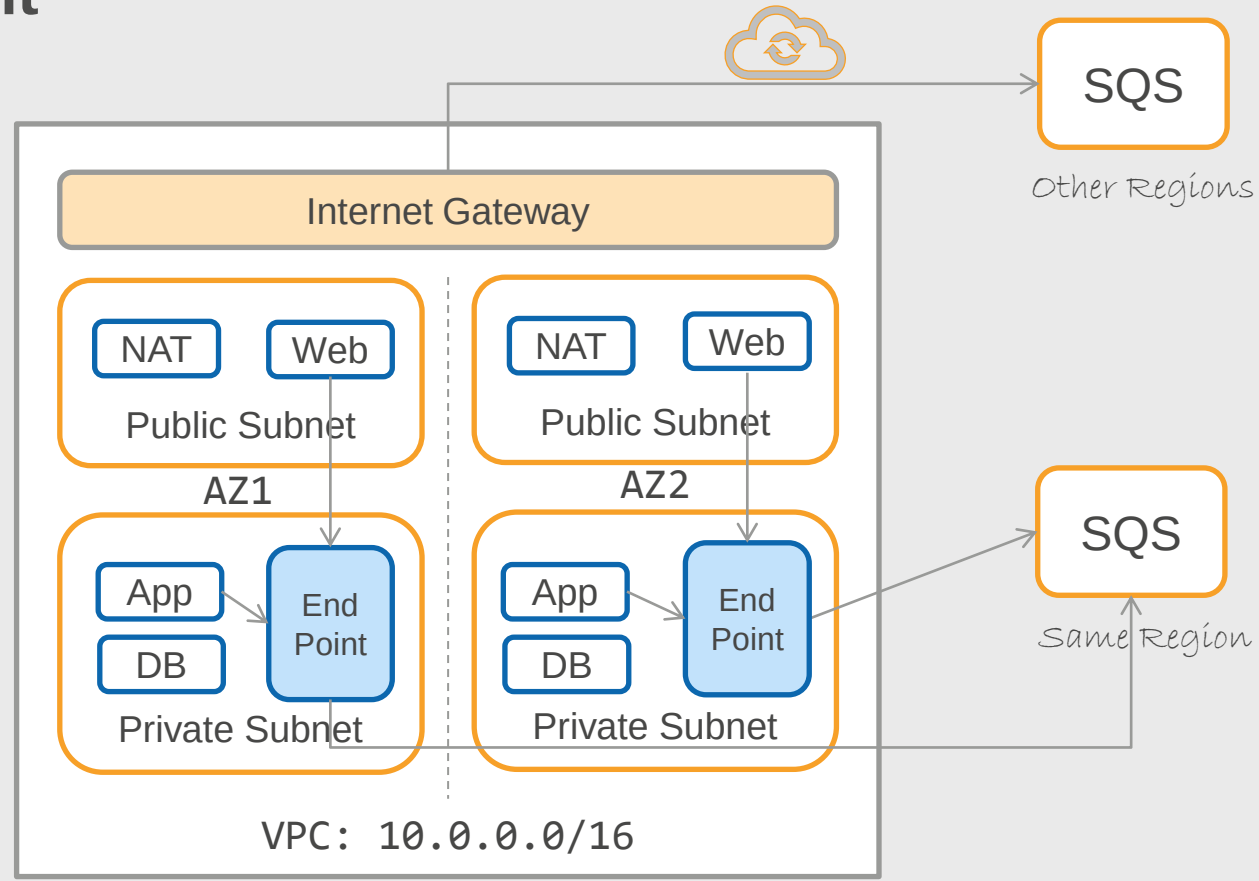
Interface Endpoint – All newer services use interface endpoint

Interface Endpoint

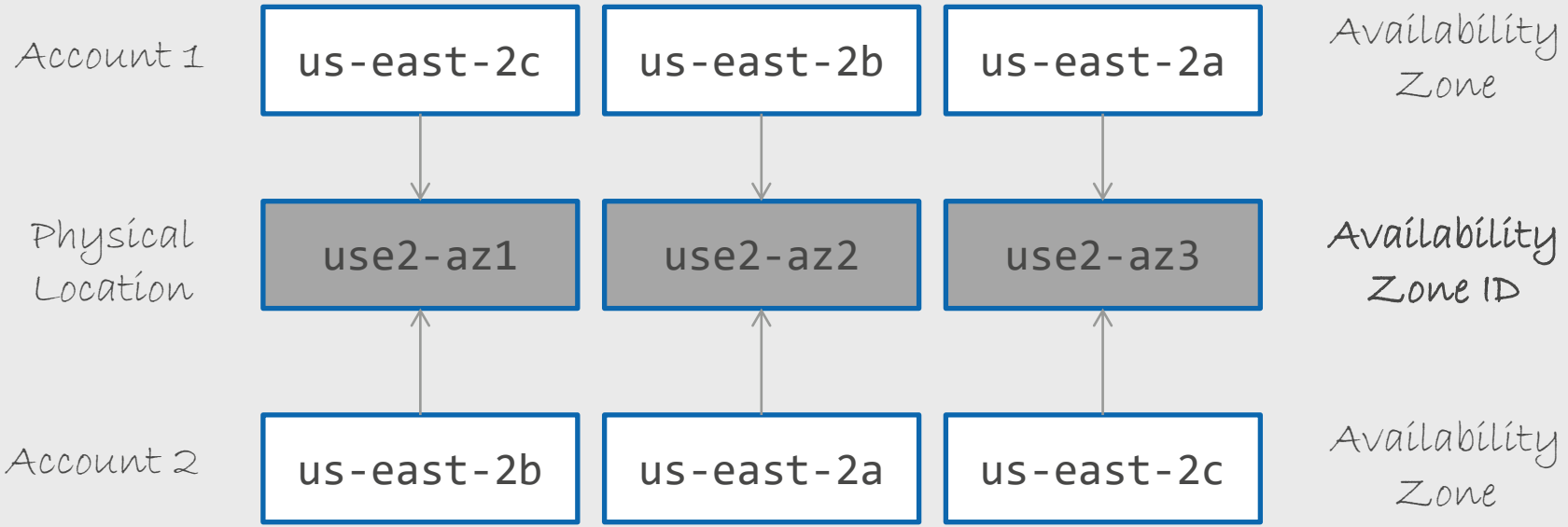
No need to update route table to use endpoint – Private IP

Queue Name:
sqs.us-east-1.amazonaws.com

With Private DNS HostName option, Service DNS name is automatically mapped to Endpoint IP address



Availability Zone ID



Interface endpoint and service could end-up in different AZs. To prevent this scenario, check the Availability Zone ID

Interface Endpoint Summary

1. Interface endpoints are also known as PrivateLink
2. Privately interact with many AWS services (same-region)
3. Interface endpoint creates a network interface with private IP (easy to remember)
4. Flexibility to expose your service to other customers

Summary – Integrating with AWS services

Internet

- Useful for both cross-region, same-region access
- Public instances – Internet Gateway
- Private instances – NAT + Internet Gateway

Gateway Endpoint

- Private connectivity to S3, DynamoDB in the same region
- For other regions, use the internet

Interface Endpoint

- Private connectivity to many AWS services in the same region
- For HA, create an interface endpoint in each AZ
- For other regions, use the internet

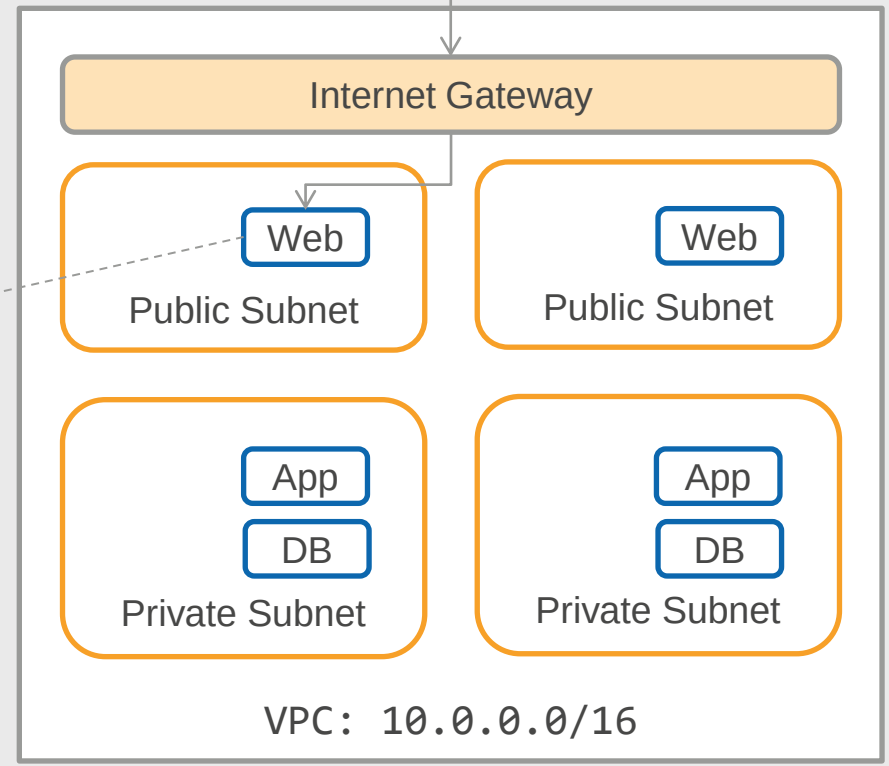
Log in to instance

Directly login (Public Instances)
Bastion Host
Systems Manager – Session Manager

How to log in to public instance?

Public Instance Security Group
Inbound Rules

Source	Protocol	Port Range	Type
0.0.0.0/0	TCP	22	SSH
99.29.0.0/16	TCP	22	SSH
99.29.0.0/16	TCP	3389	RDP

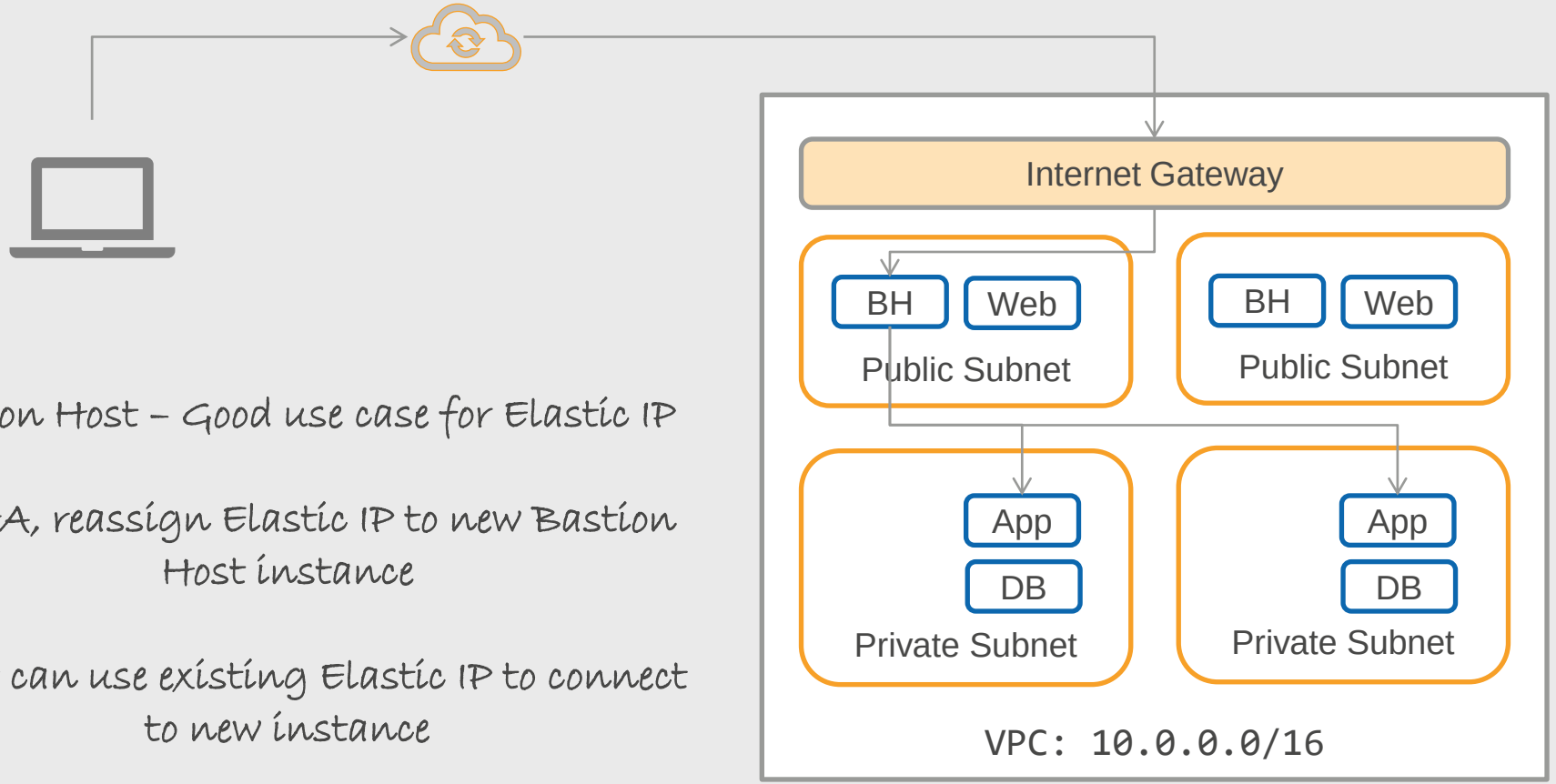


How to Log in to Private instance?

Bastion Host

Systems Manager – Session Manager

How to log in to private instance with Bastion Host



Bastion Host – Good use case for Elastic IP

For HA, reassign Elastic IP to new Bastion Host instance

Client can use existing Elastic IP to connect to new instance

Security Group

Bastion Host Security Group - Inbound Rules

Source	Protocol	Port Range	Type
99.29.0.0/16	TCP	22	SSH
99.29.0.0/16	TCP	3389	RDP

Web-App-DB Security Group - Inbound Rules

Source	Protocol	Port Range	Type
BastionHost-SG-id	TCP	22	SSH
BastionHost-SG-id	TCP	3389	RDP

Bastion Host Drawback

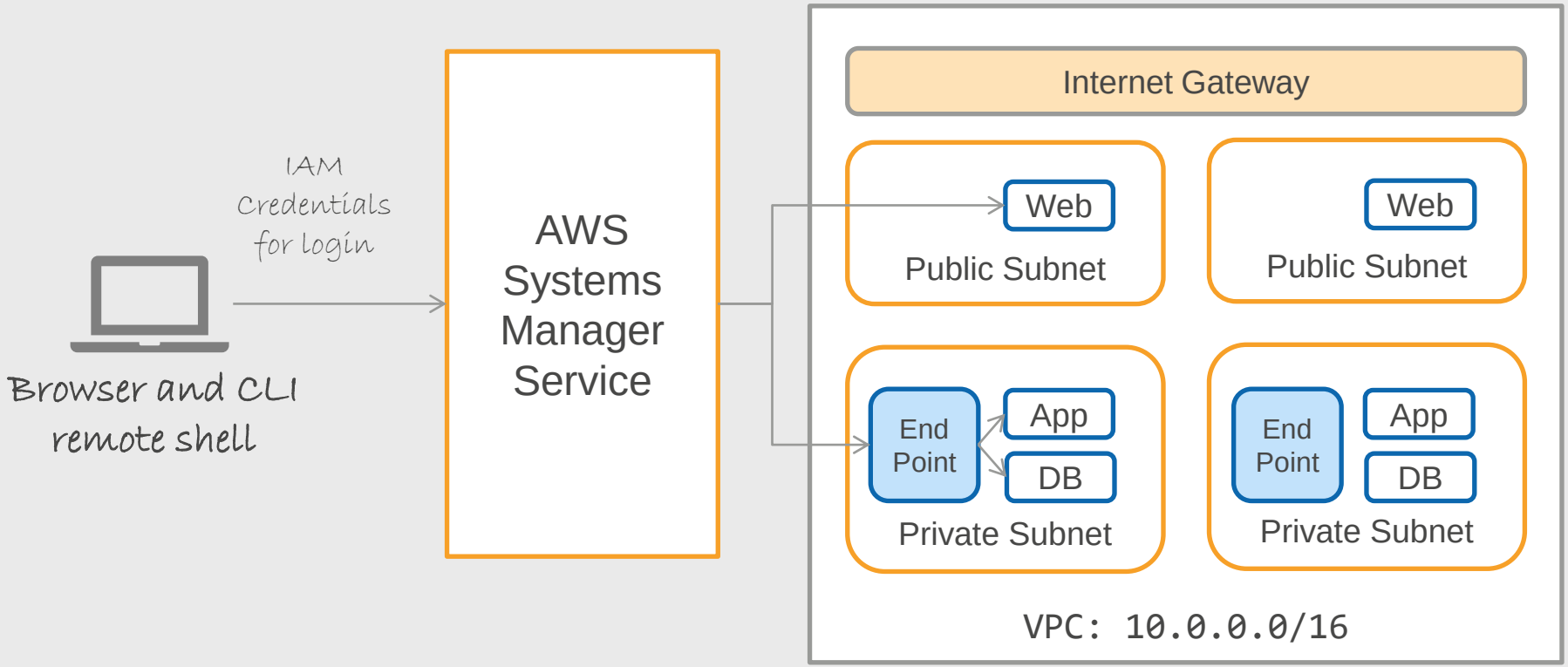
EXTRA SERVERS TO MANAGE

MANAGE SERVER LOGIN CERTIFICATES AND CREDENTIALS

Systems Manager

1. Automated patching of servers
2. Automation of routine administrative tasks
3. Session Manager – interactive remote shell for Linux and Windows, macOS
4. Agent required – AWS preinstalls in many instances

Session Manager - Login



Systems Manager – Session Manager

Simpler and Safer when compared to Bastion Host

Grant login access for IAM credentials

Close SSH and RDP ports in Security Group

Login - Summary

Public instances – directly connect to the instance

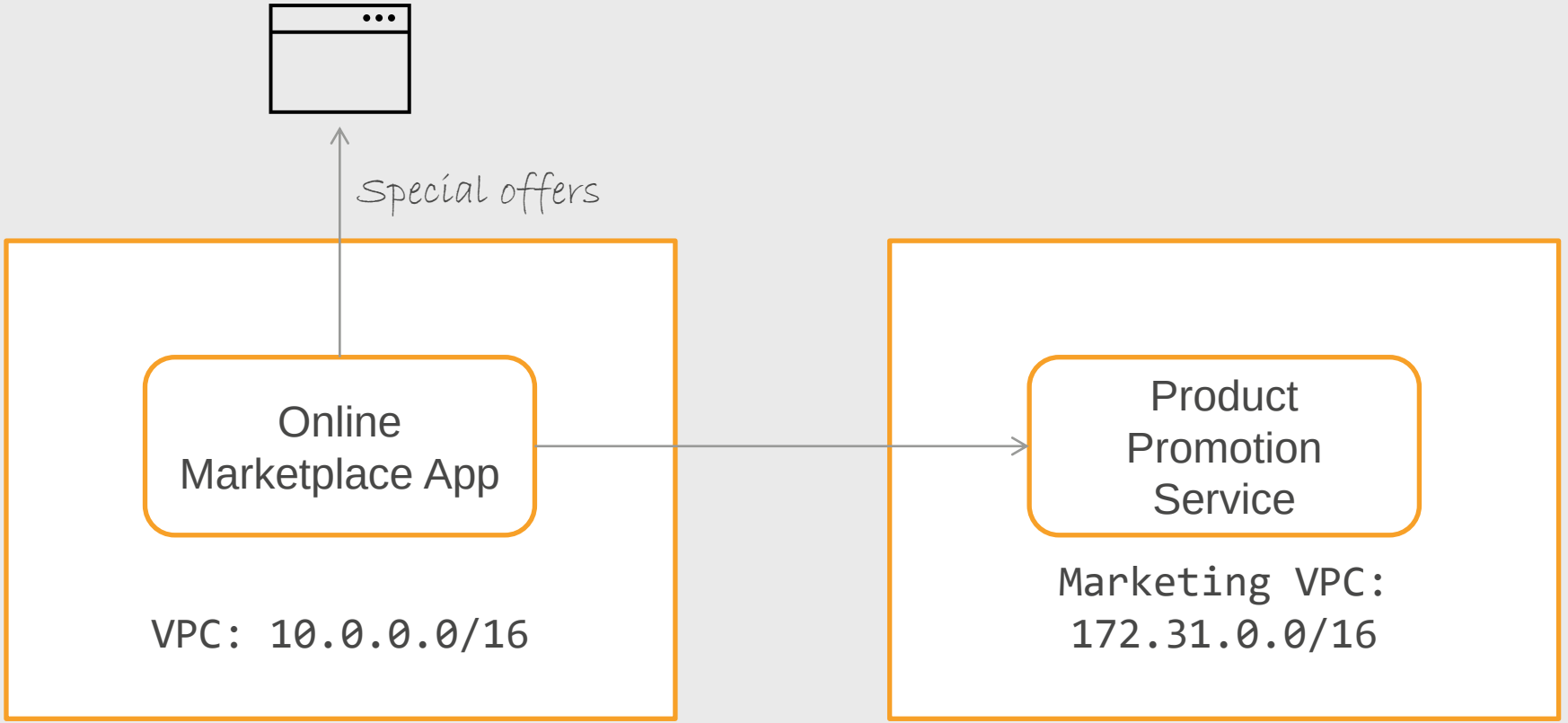
Bastion Host – requires additional servers

Session Manager (Systems Manager Service) – more secure

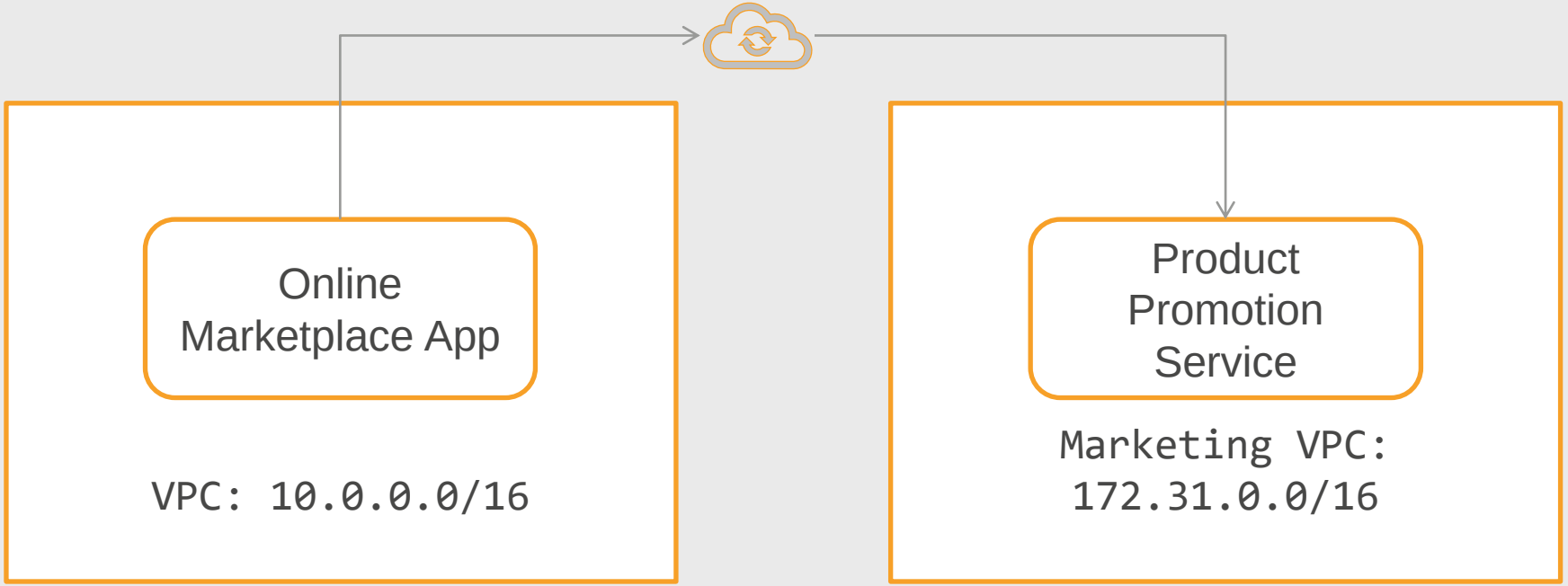
Integrating with other applications

Internet
Peering connection
Transit Gateway

Application integration

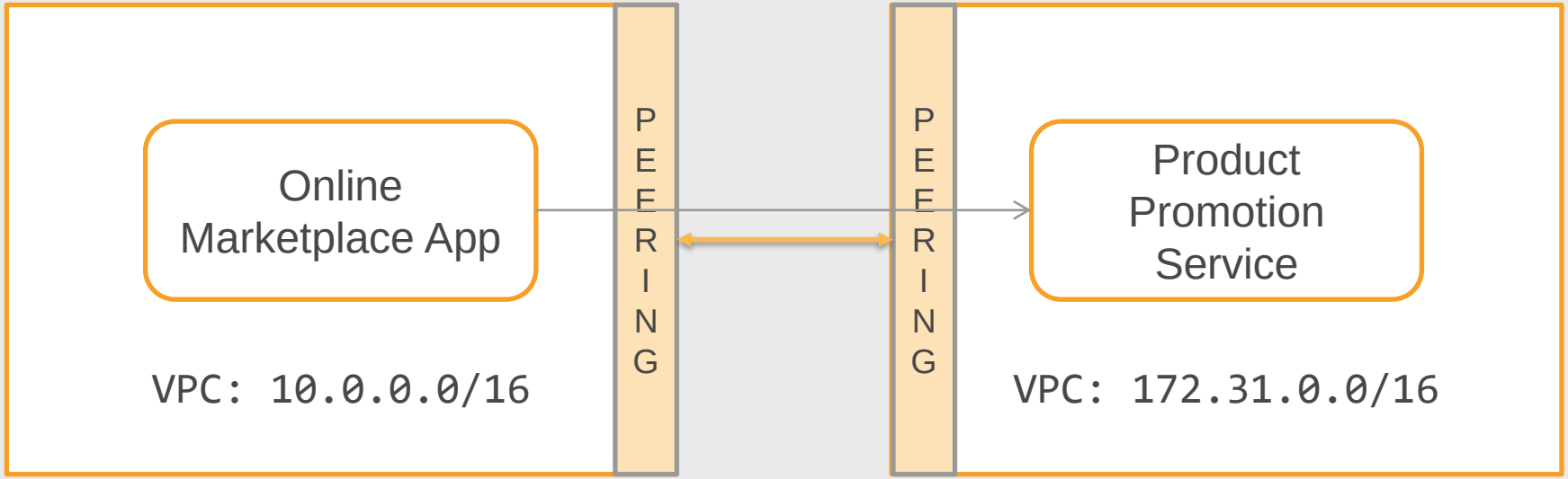


Application integration over internet



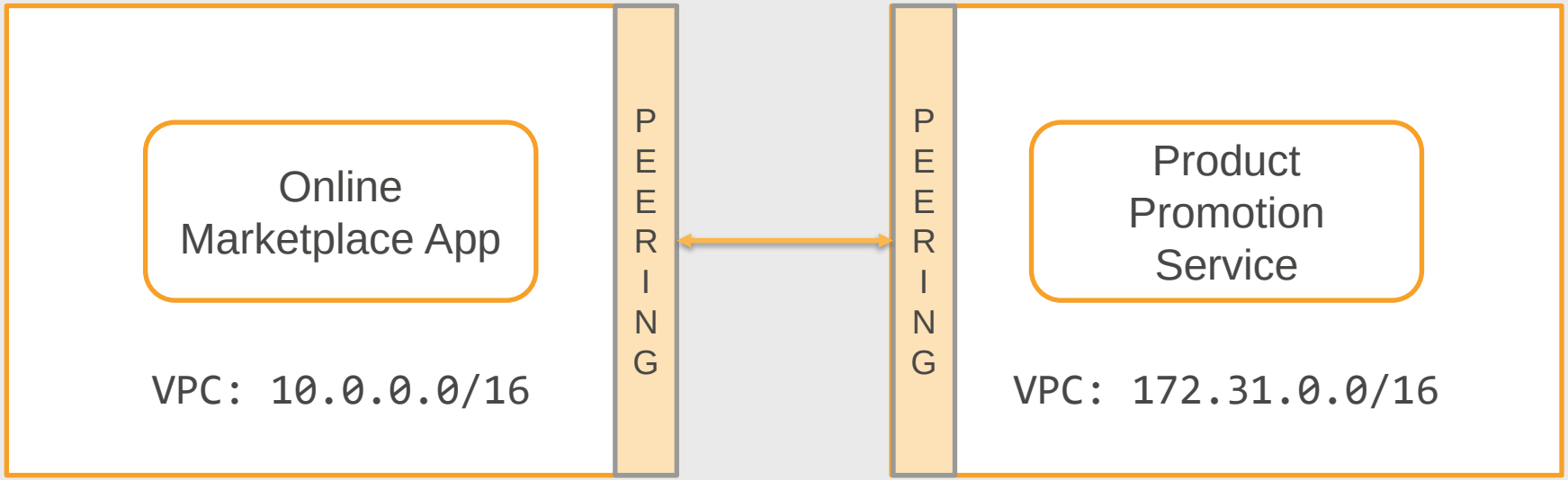
But why can't these two applications talk directly using AWS network?

VPC Peering Connection



- Connect VPCs into single logical network with Peering Connection
- Communicate using Private IP
- AWS managed – no single point of failure
- CIDR block must not overlap

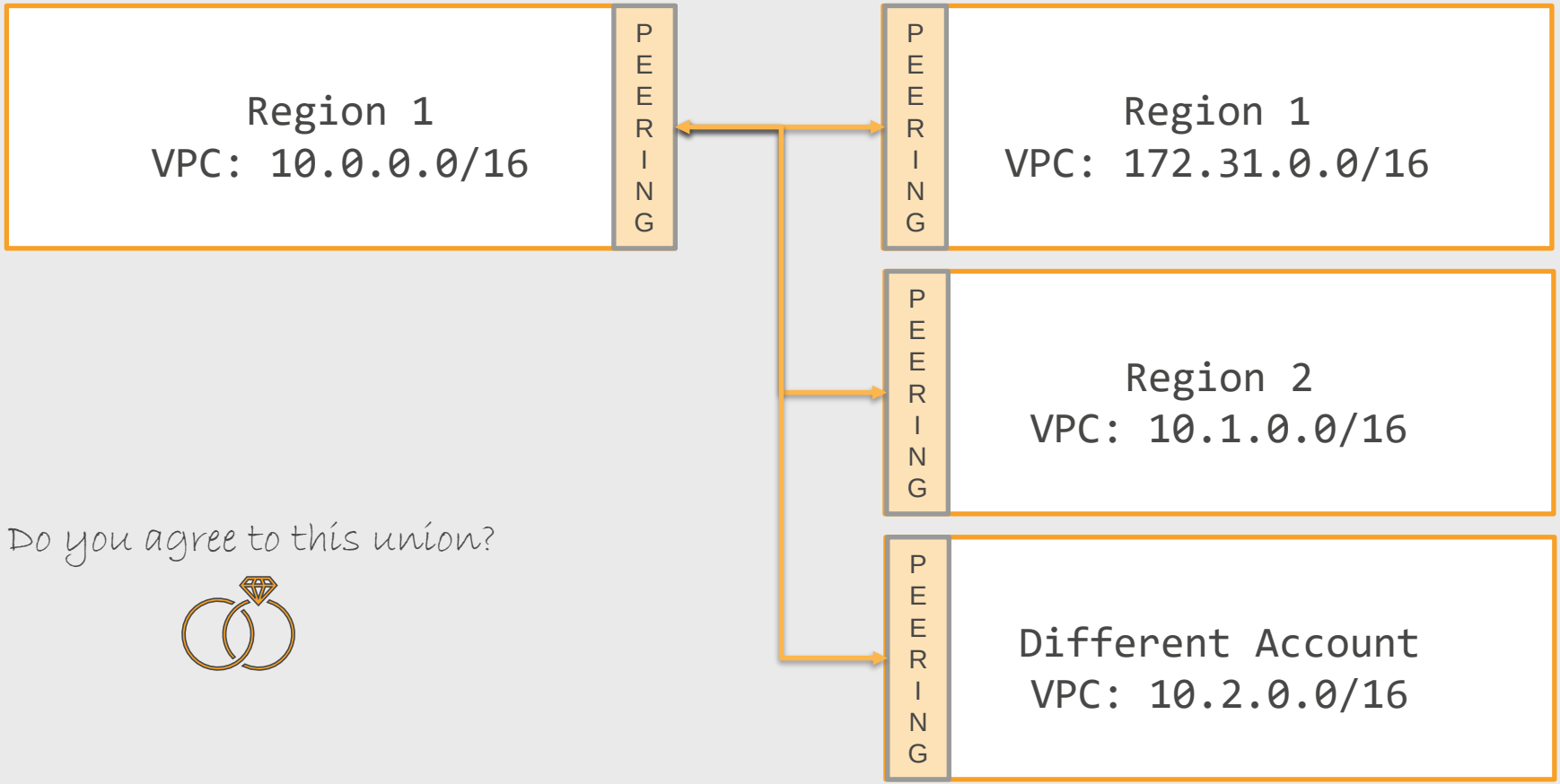
VPC Peering Connection – Route Table



Destination	Target
10.0.0.0/16	local
172.31.0.0/16	PCX-id

Destination	Target
172.31.0.0/16	local
10.0.0.0/16	PCX-id

VPC Peering Options

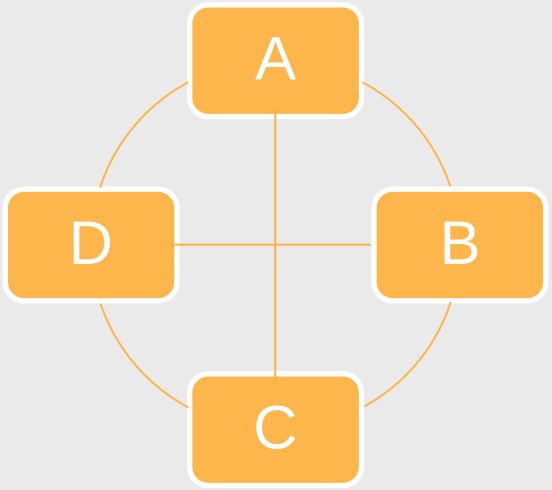


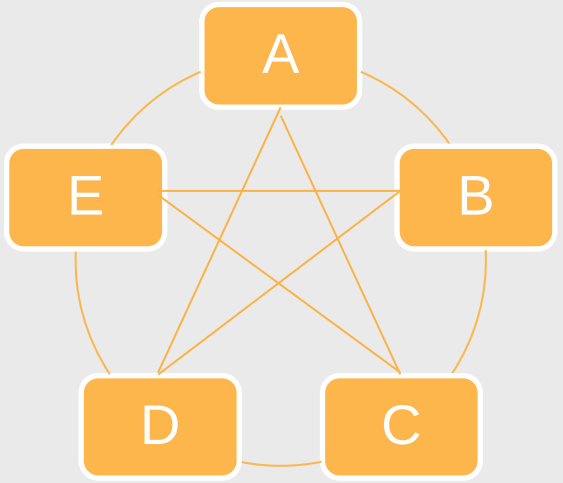
Do you agree to this union?

VPC Peering

- Bi-directional
- Not-Transitive

VPC Peering Issues





Fully connected mesh configuration requires several VPC Peering connections

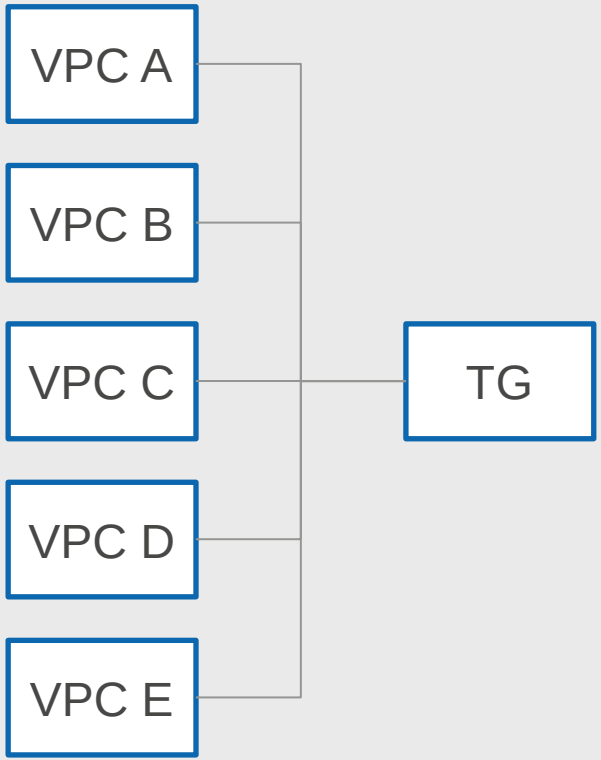
Transit Gateway

Cloud router - Central networking hub

Connect VPCs to Transit Gateway once

Route table to control which VPCs can talk to each other

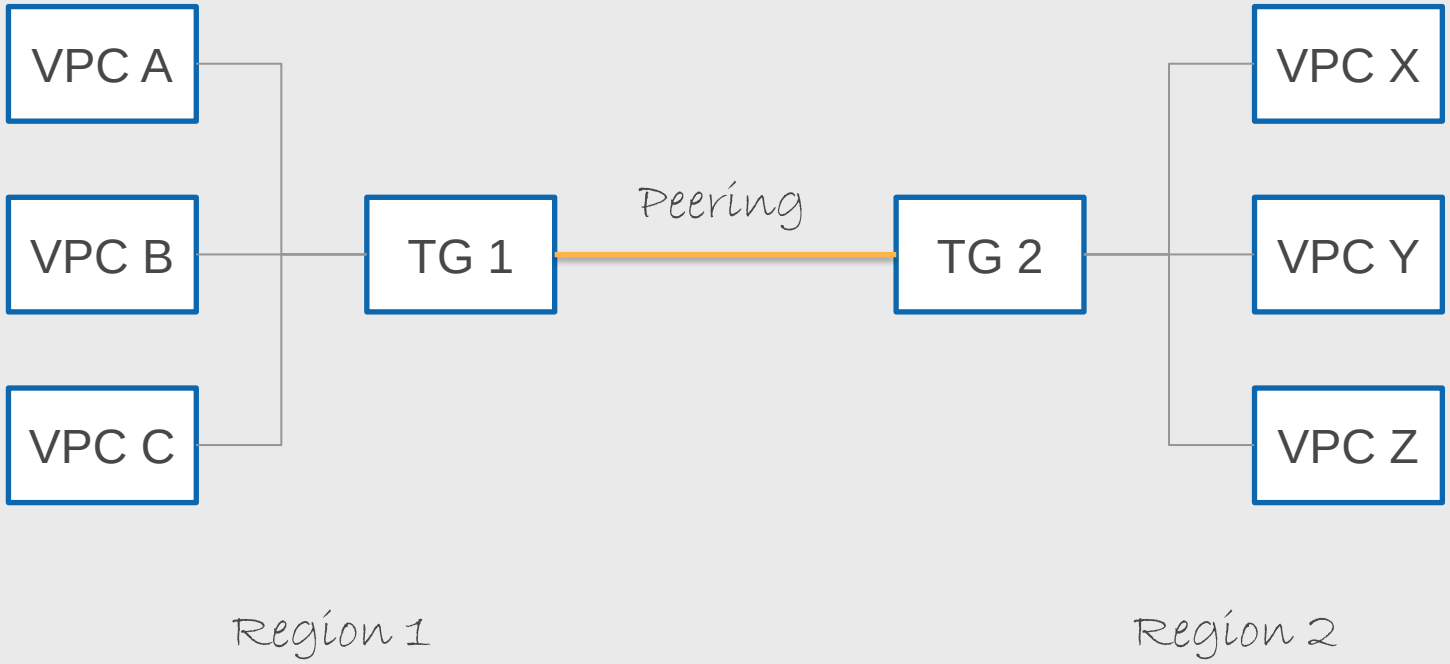
Transit Gateway



One connection from VPC to TG

TG Route table to control flow of traffic

Transit Gateway Peering – Cross Region



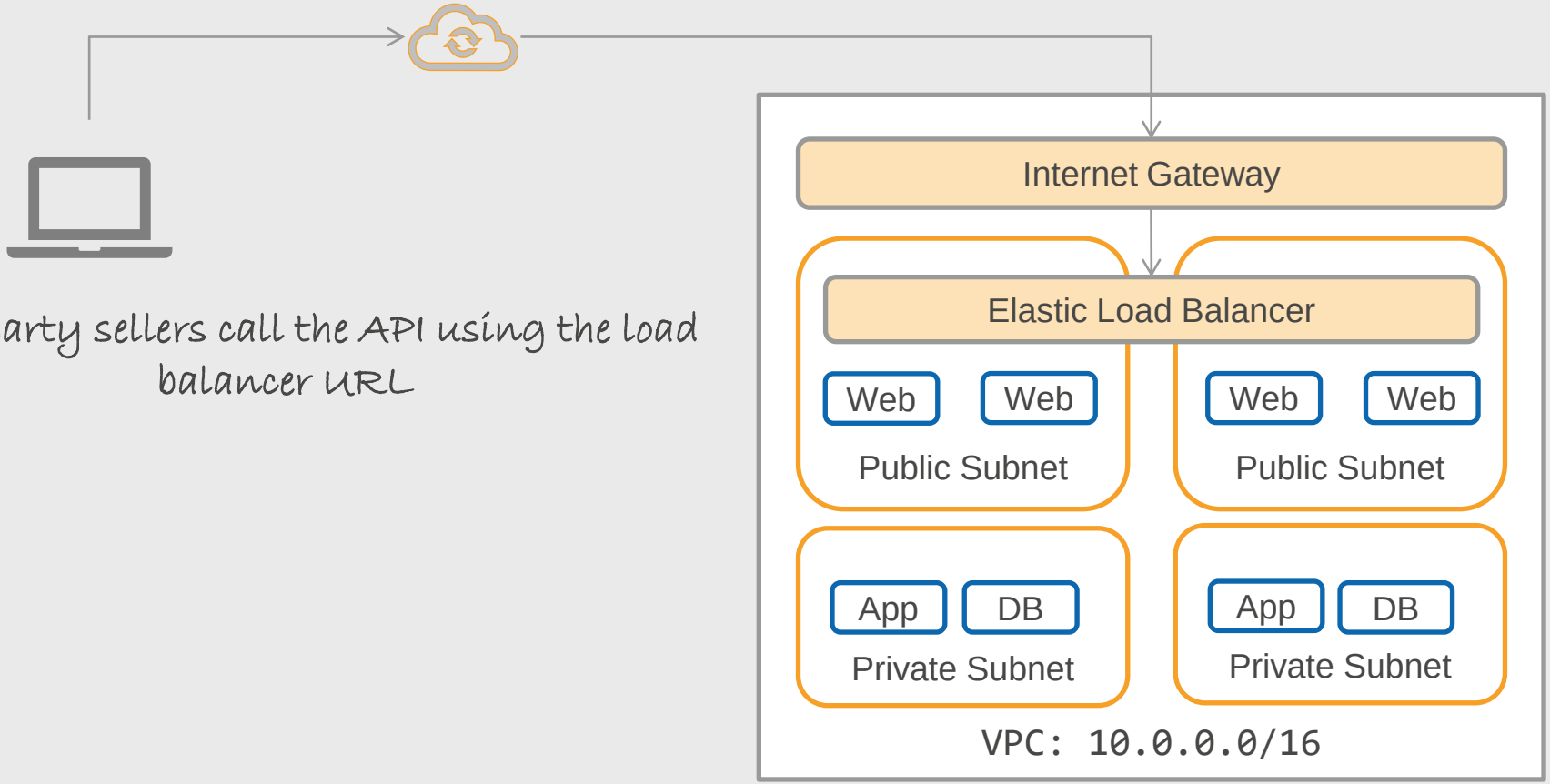
Enabling third-parties to call our App

Internet

Endpoint

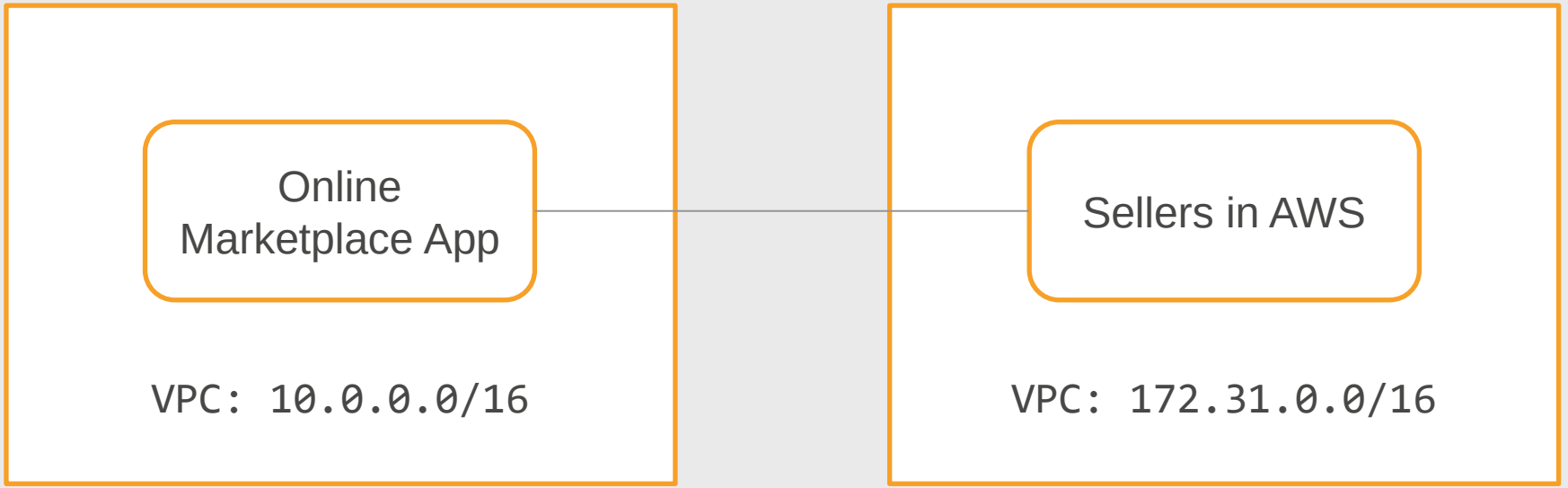
Application integration

Access using the Internet



Application integration inside AWS

Third party sellers are in AWS cloud



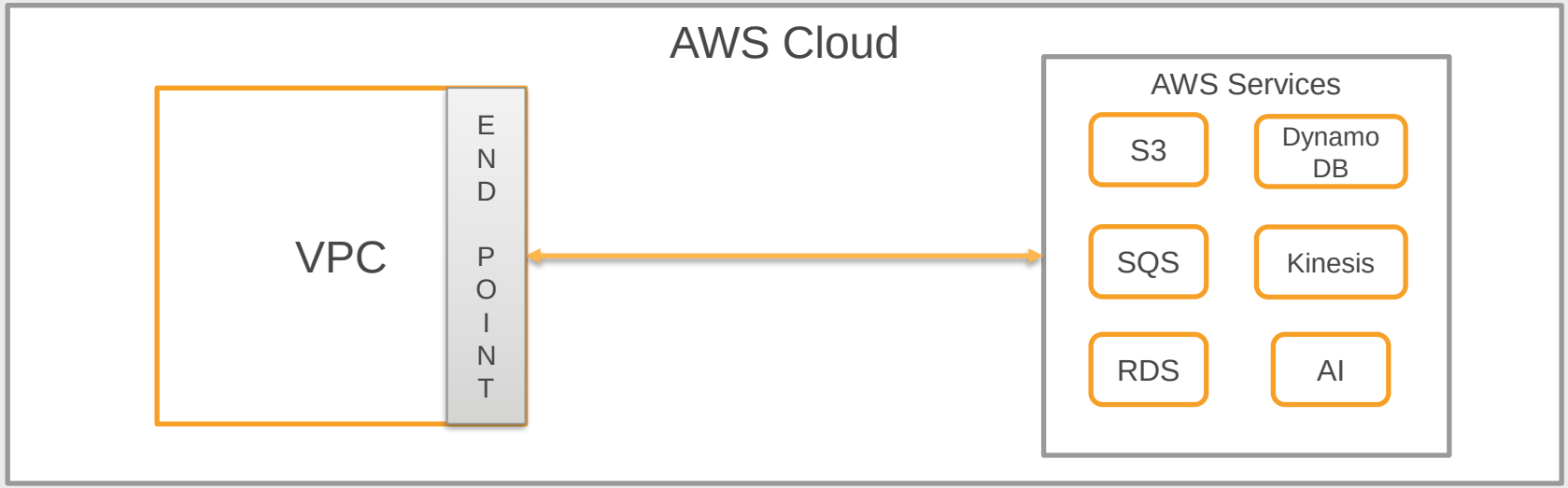
Why not Peering Connection or TG?

VPCs are not part of the same enterprise

Connecting third-party VPCs with your VPC is a security risk

Privately share only the App

Endpoints (recap)



With endpoints, you can privately talk to AWS services (without using the internet)

Endpoint Types (recap)

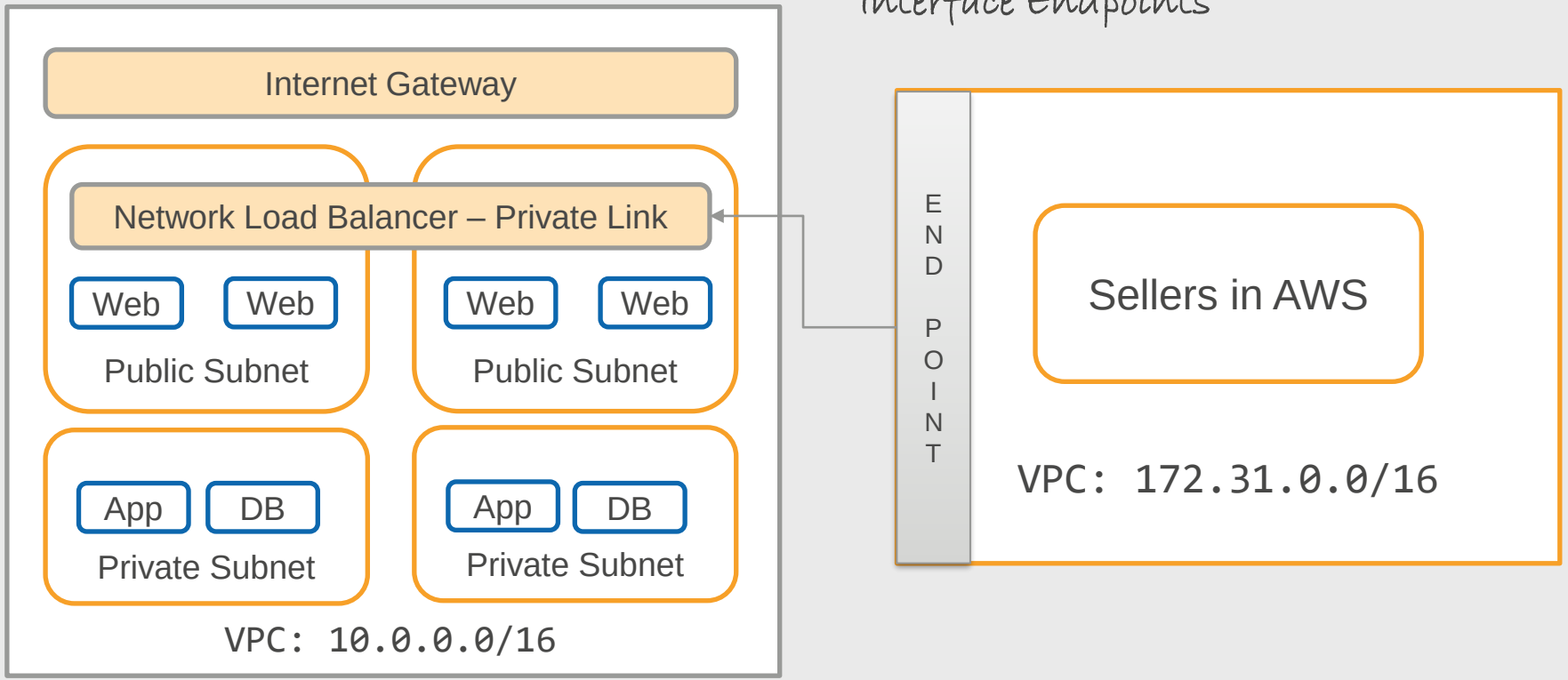
Gateway Endpoint - S3, DynamoDB

Interface Endpoint – All newer services use interface endpoint

Privately share your application using Interface Endpoints

Access using the Endpoint (PrivateLink)

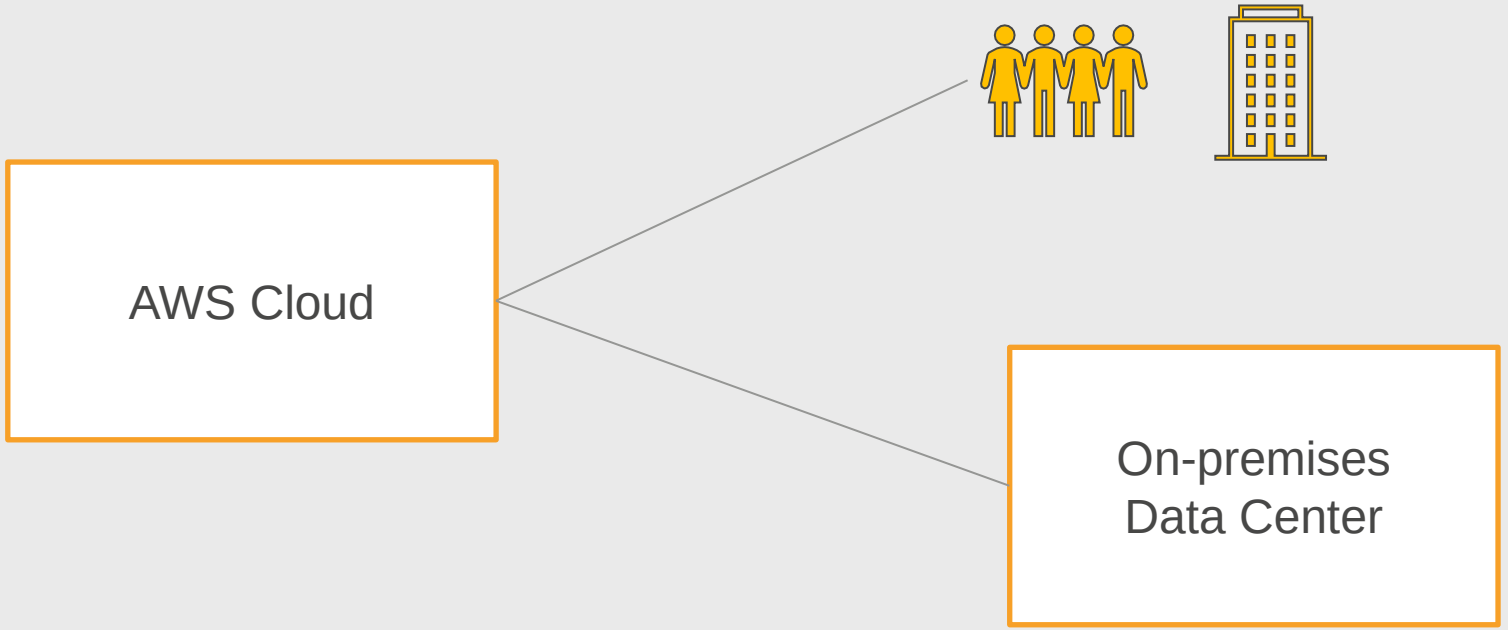
Privately share your application using Interface Endpoints



Hybrid Infrastructure

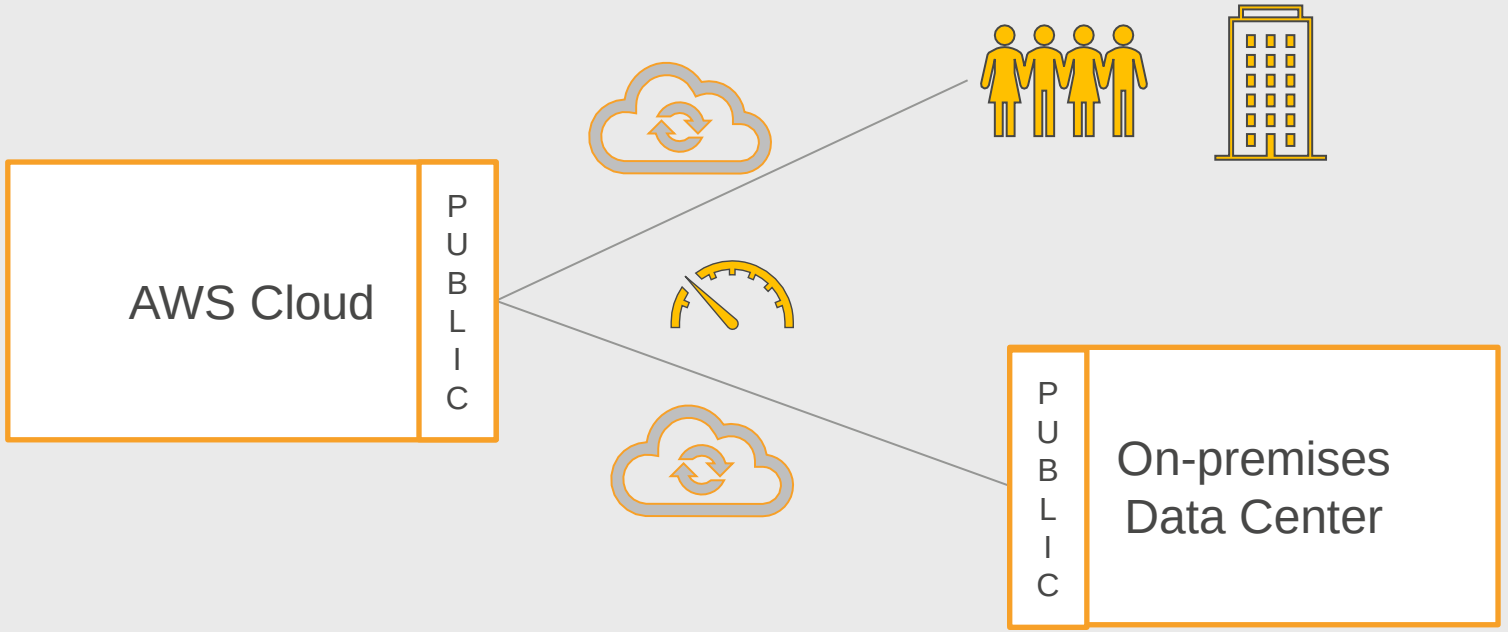
On-premises to AWS Cloud connectivity

Hybrid Infrastructure



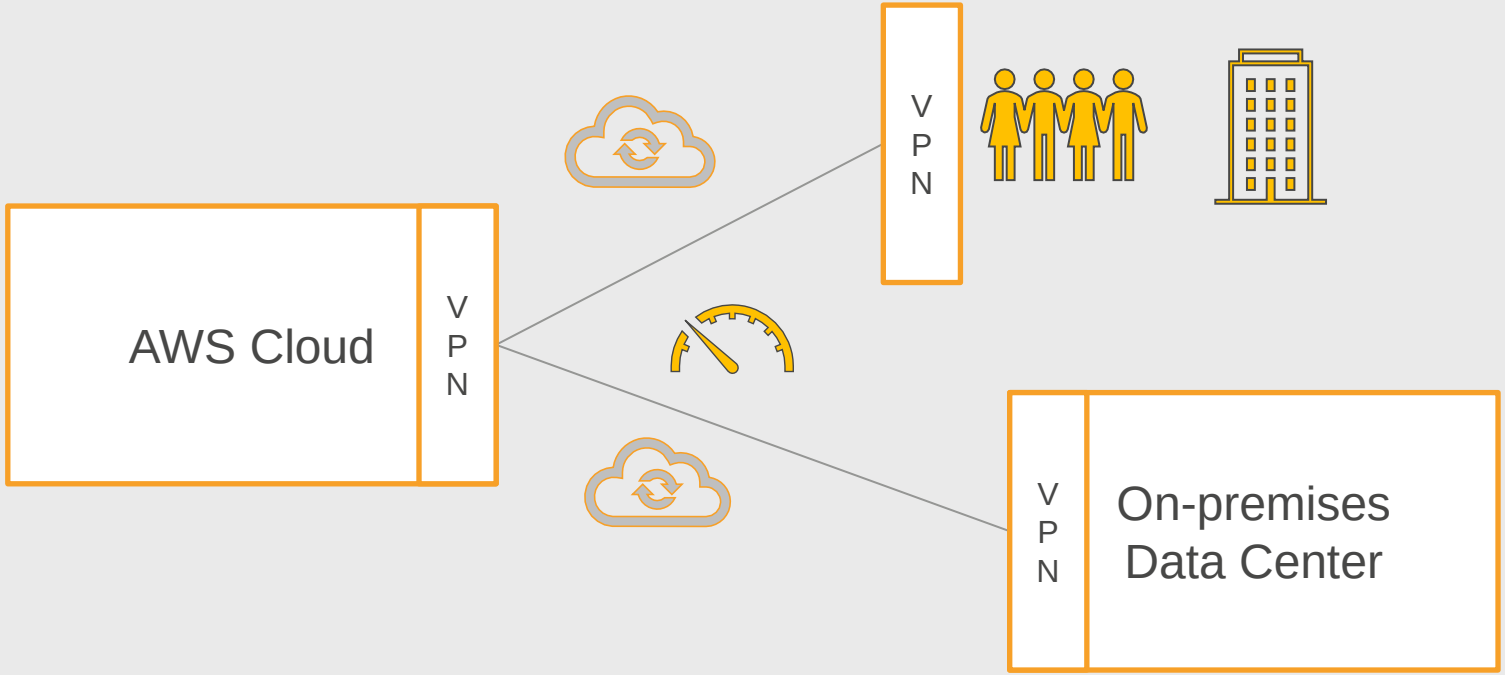
How to provide secure access to the cloud?

Internet



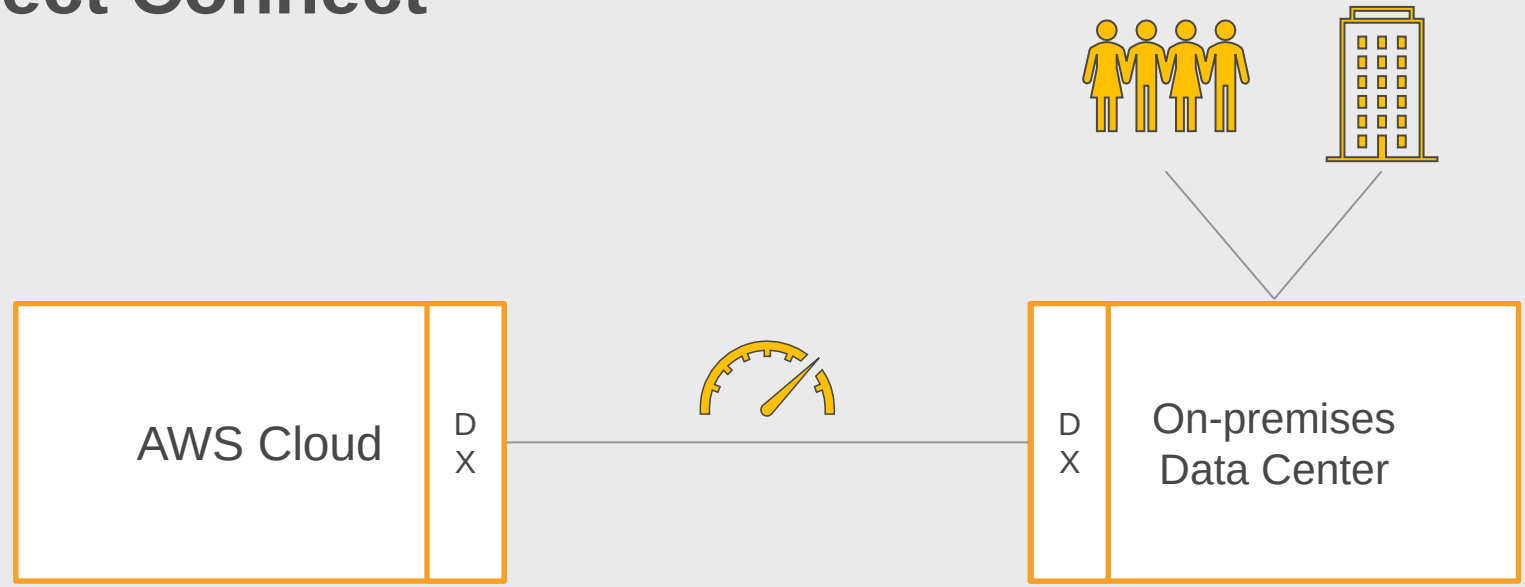
Both on-premises and cloud needs Public IP
Internet performance may not be consistent

VPN over Internet



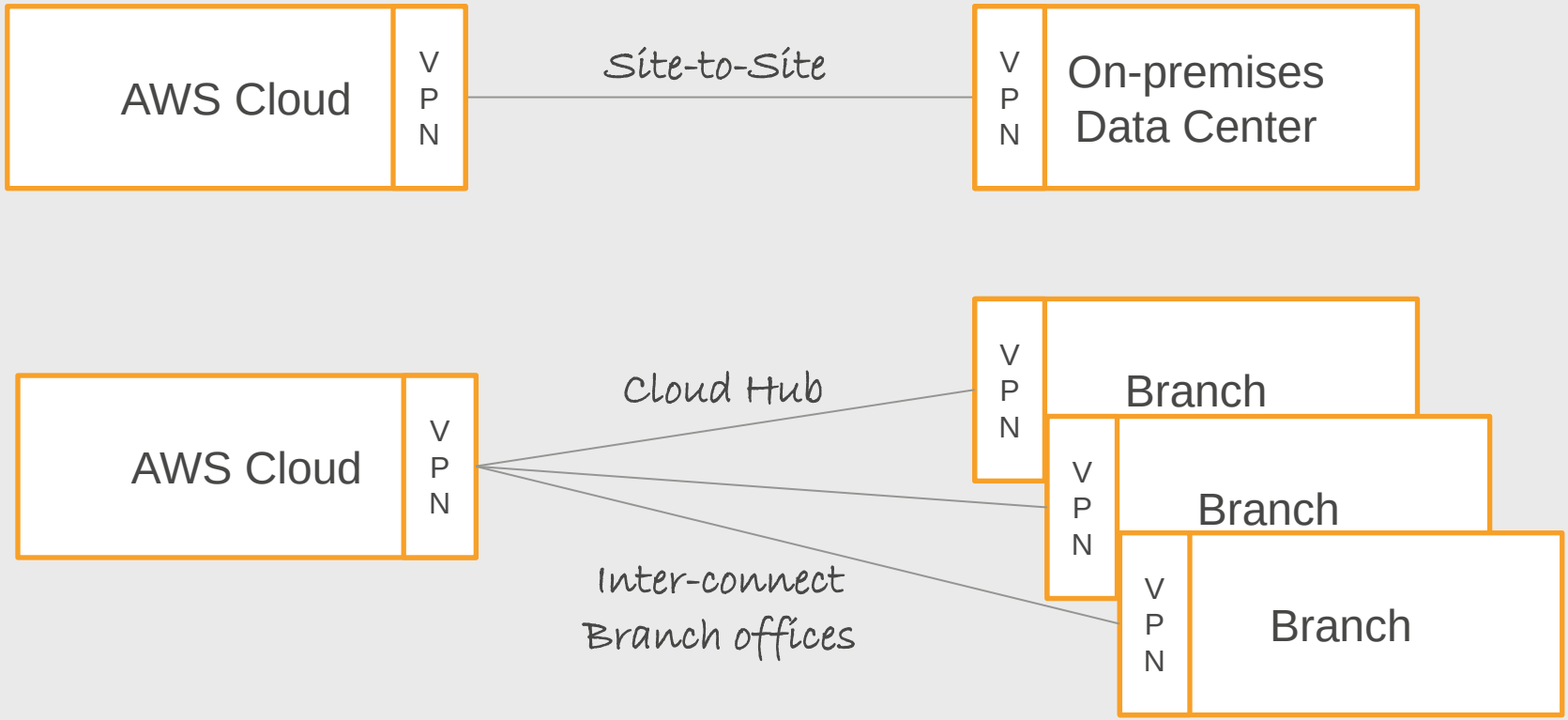
VPN provides IPSec encrypted connection
Cloud is an extension of your datacenter – access using private IP
Internet performance may not be consistent

Direct Connect

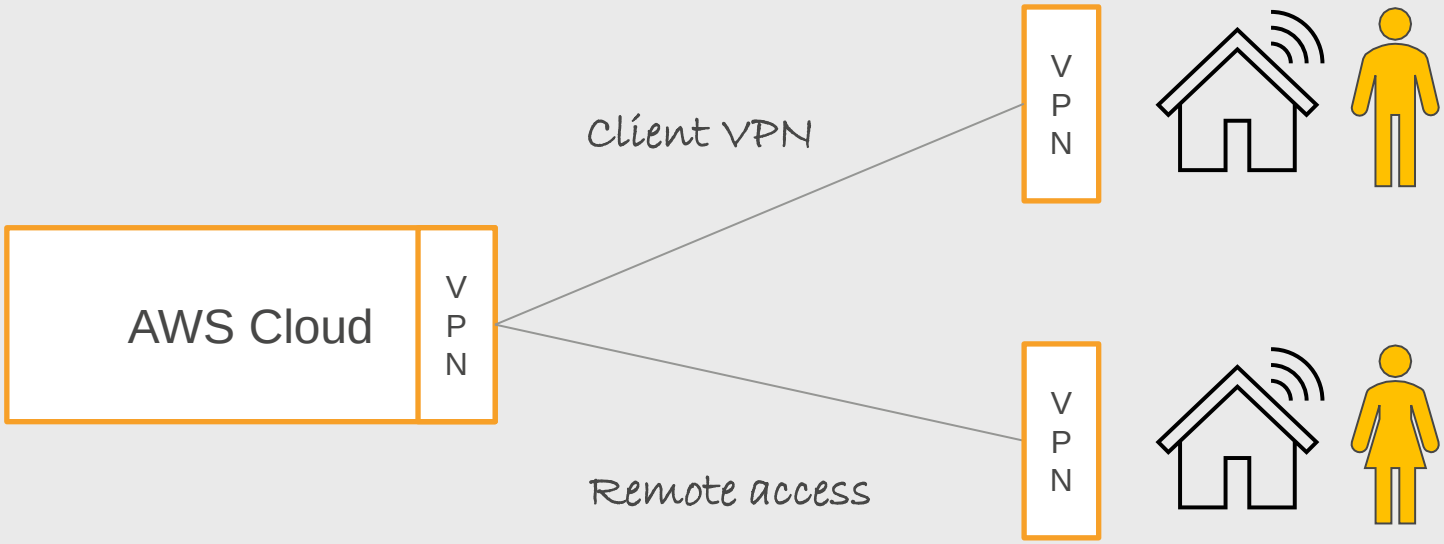


Bypass internet with a dedicated link between on-premises and AWS
Cloud is an extension of your datacenter – access using private IP
Consistent network performance and throughput
Complex setup

VPN Connectivity Options

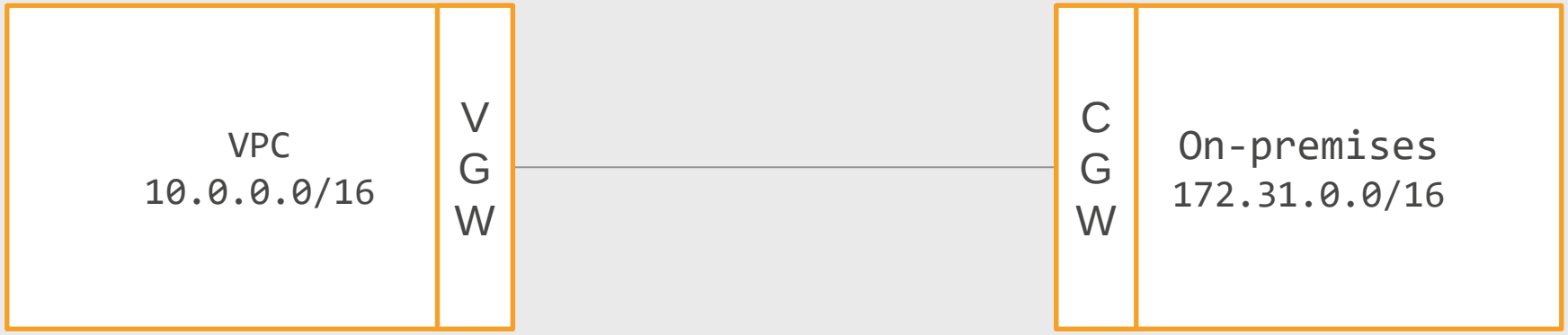


VPN Connectivity



Access for employees working remotely

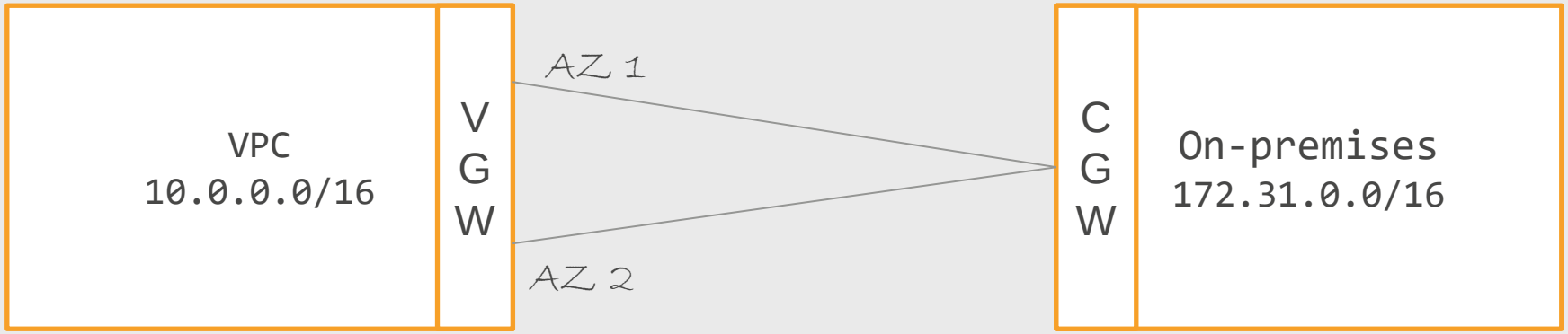
VPN Site-to-Site



Attach Virtual Private Gateway (VGW) to your VPC

Customer Gateway – your existing VPN hardware or software

VPN Site-to-Site (HA-AWS)

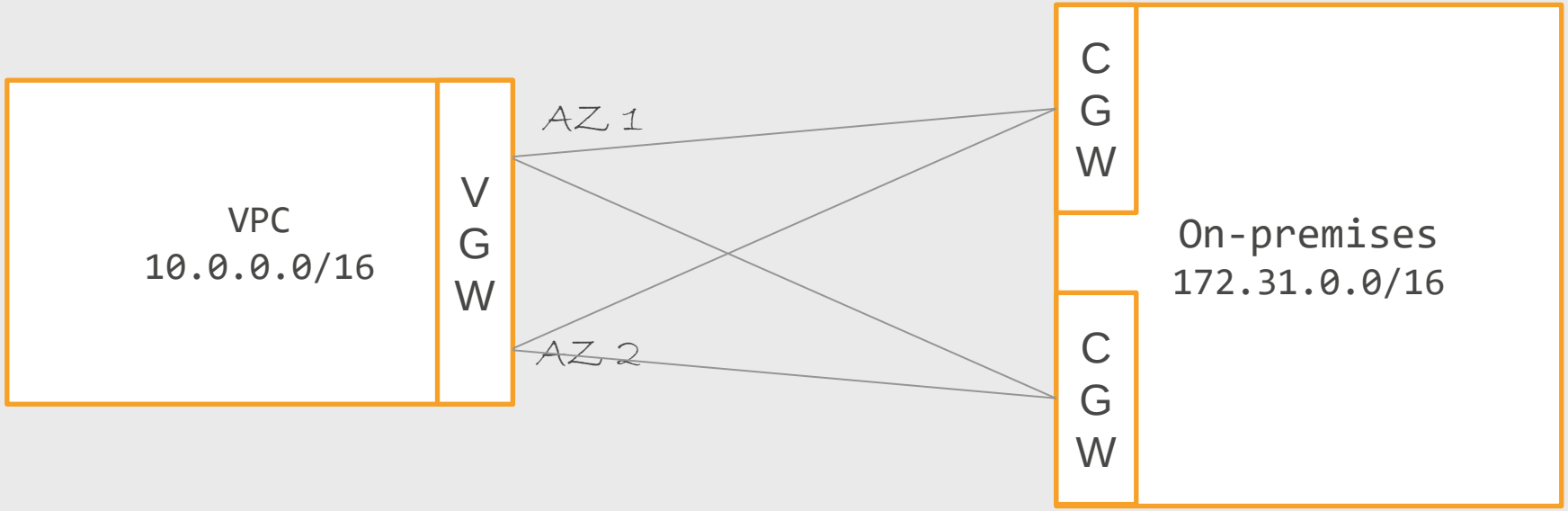


AWS side, a VPN Connection consists of two tunnels each ending in different AZs

Handles AZ failure

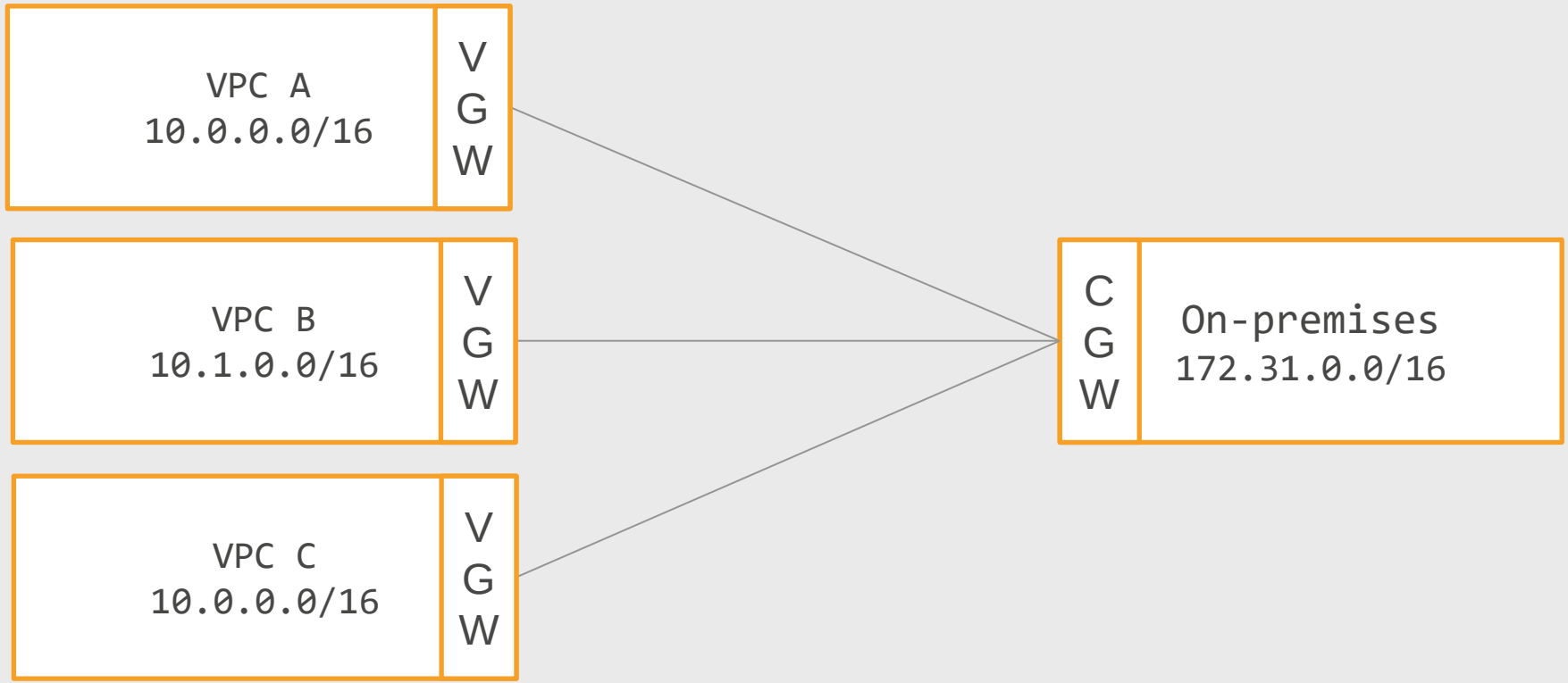
Customer Gateway is a single device and single point of failure

VPN Site-to-Site (HA-AWS-OnPrem)



Two Customer Gateway devices preferably in different data centers
Two VPN connection from the same VGW but to different CGWs
On-premises Connectivity is configured at VPC level

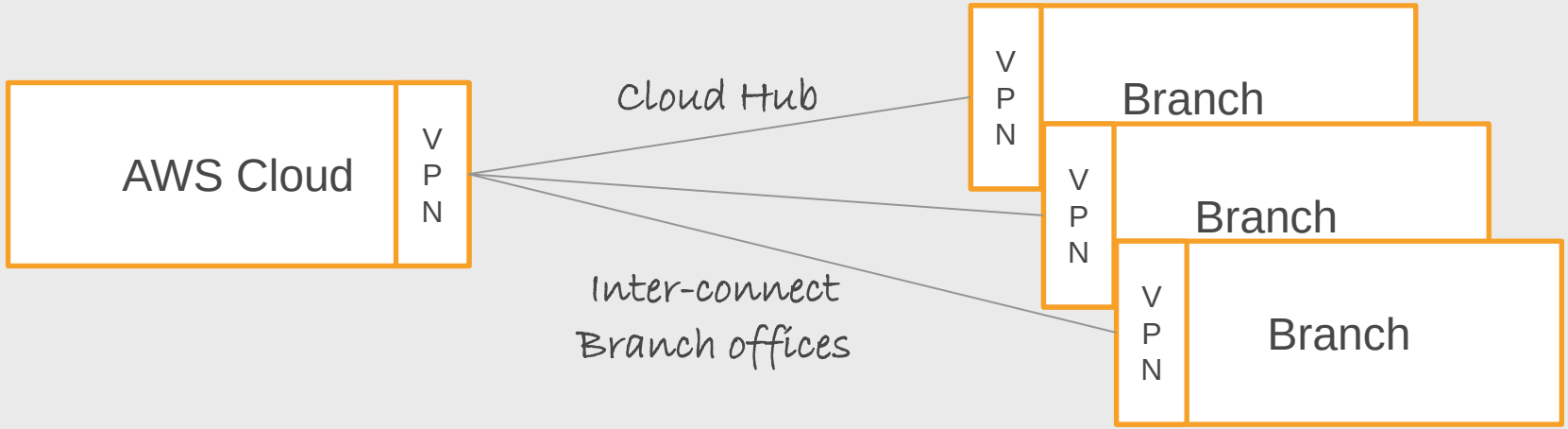
Multiple VPCs – Lots of connections



VPN using Transit Gateway

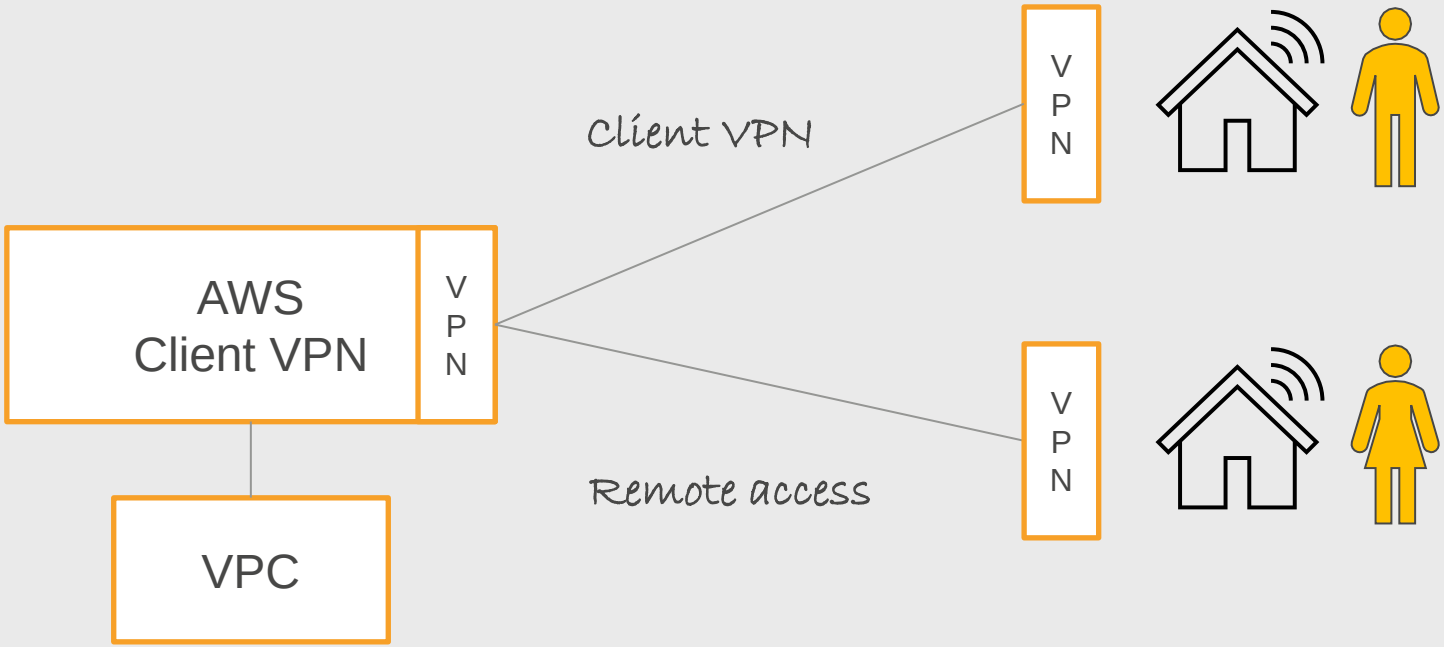
Use Transit Gateway to terminate VPN Connection
Share the same VPN connection with multiple VPCs

Cloud Hub – Multi-Site VPN



For multi-site VPN, we can use Transit Gateway or Virtual Private Gateway

Client VPN



Access for employees working remotely using AWS Client VPN or Third-party VPN Software

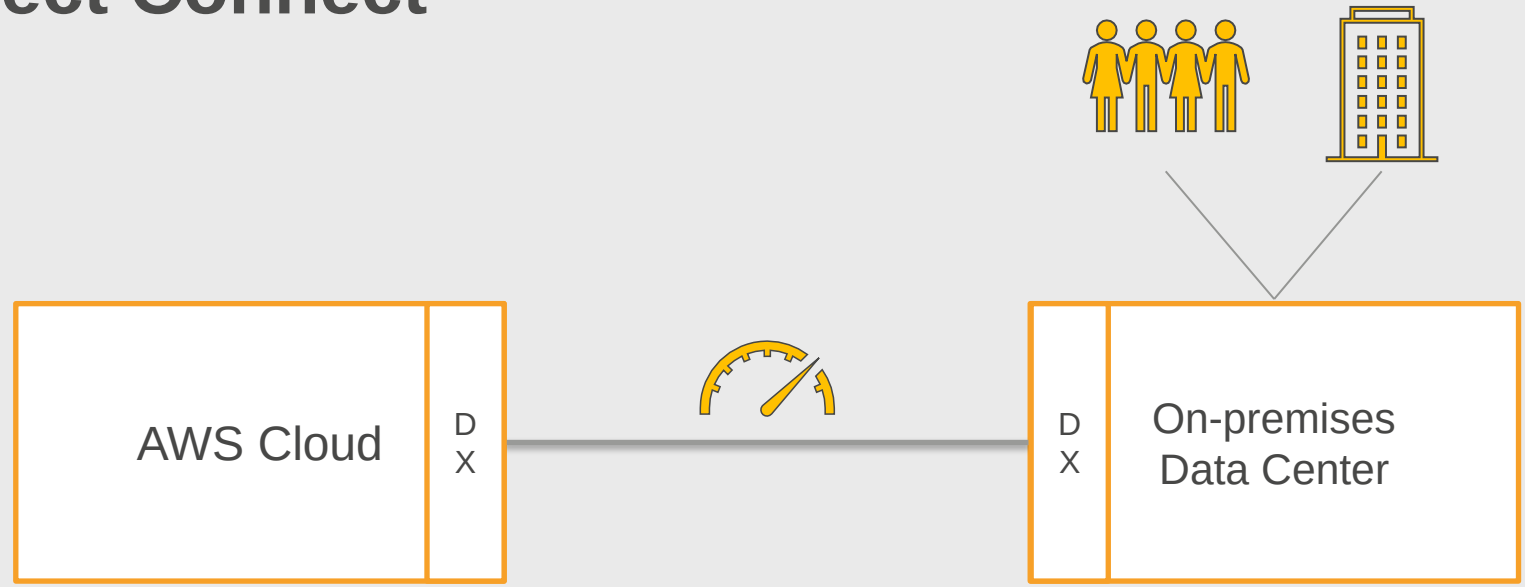
VPN Options

1. Site-to-Site – Connect your data center to AWS

2. Cloud Hub – Interconnect your branch offices

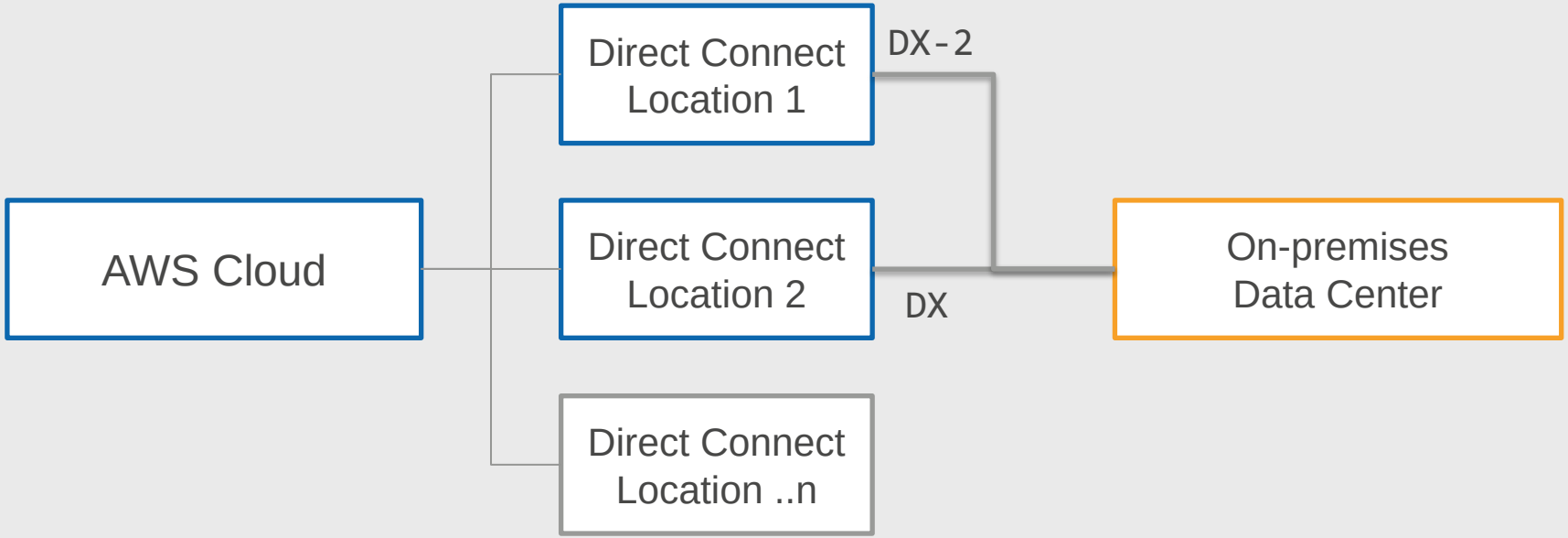
3. Client VPN – Remote access to AWS from any location

Direct Connect



Bypass internet with a dedicated link between on-premises and AWS
Cloud is an extension of your datacenter – access using private IP
Consistent network performance and throughput
Complex setup

Direct Connect Setup



AWS has 100+ Direct Connect locations worldwide. Choose the one closest to your data center.

Access resources in any of the AWS regions

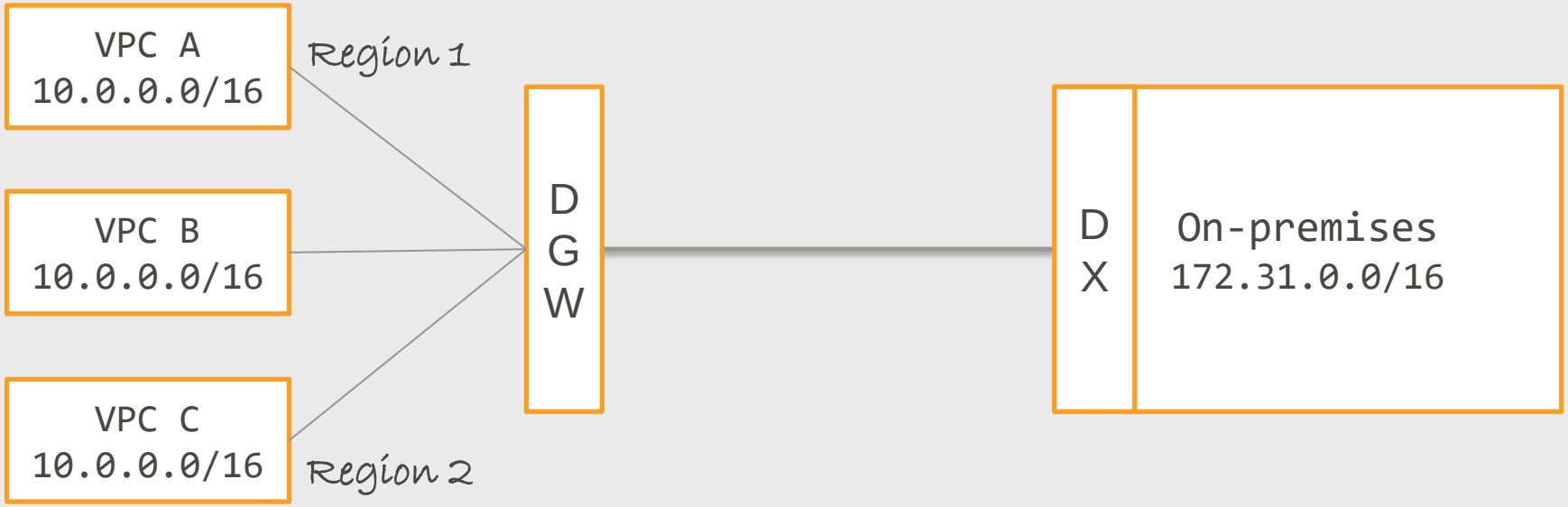
For Critical workloads, use two Direct Connect locations (location or device failure)

Direct Connect with Virtual Private Gateway

Attach Virtual Private Gateway (VGW) to your VPC

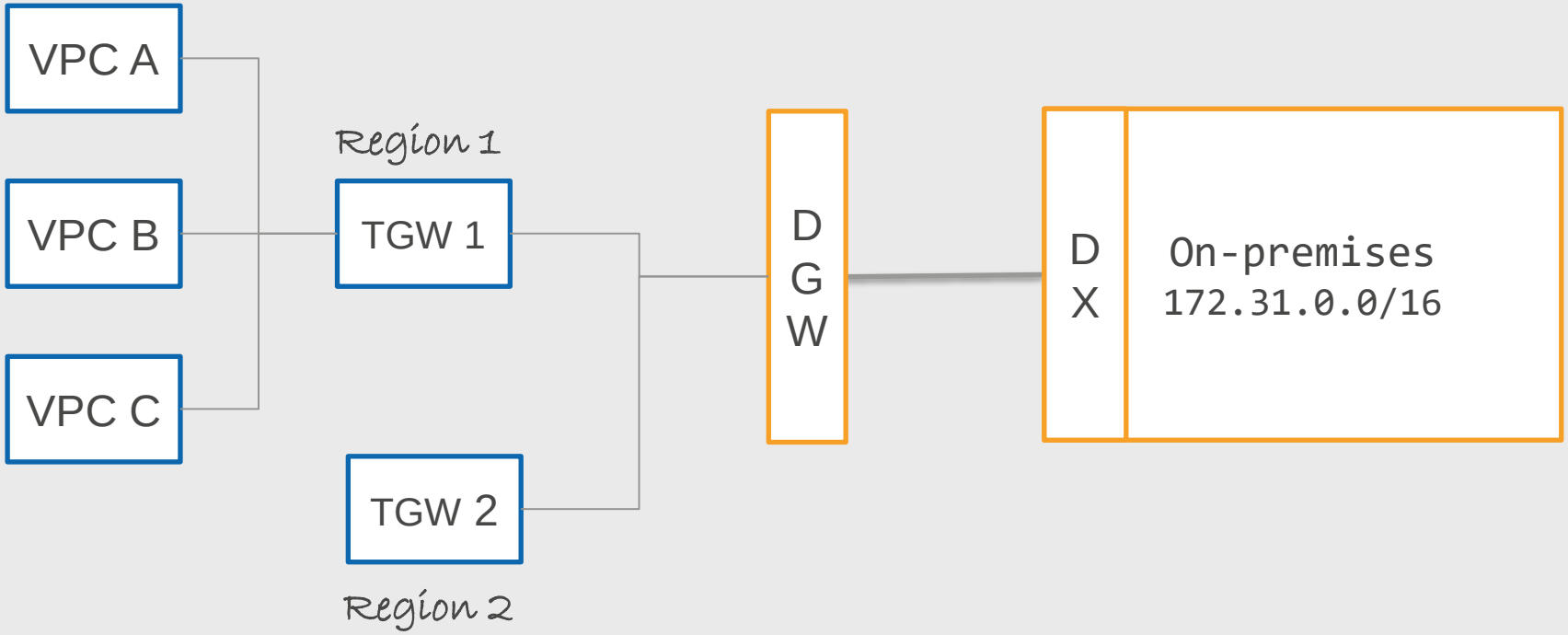
VGW does not support multiple-VPCs, so this option is not particularly useful

Direct Connect with Direct Connect Gateway



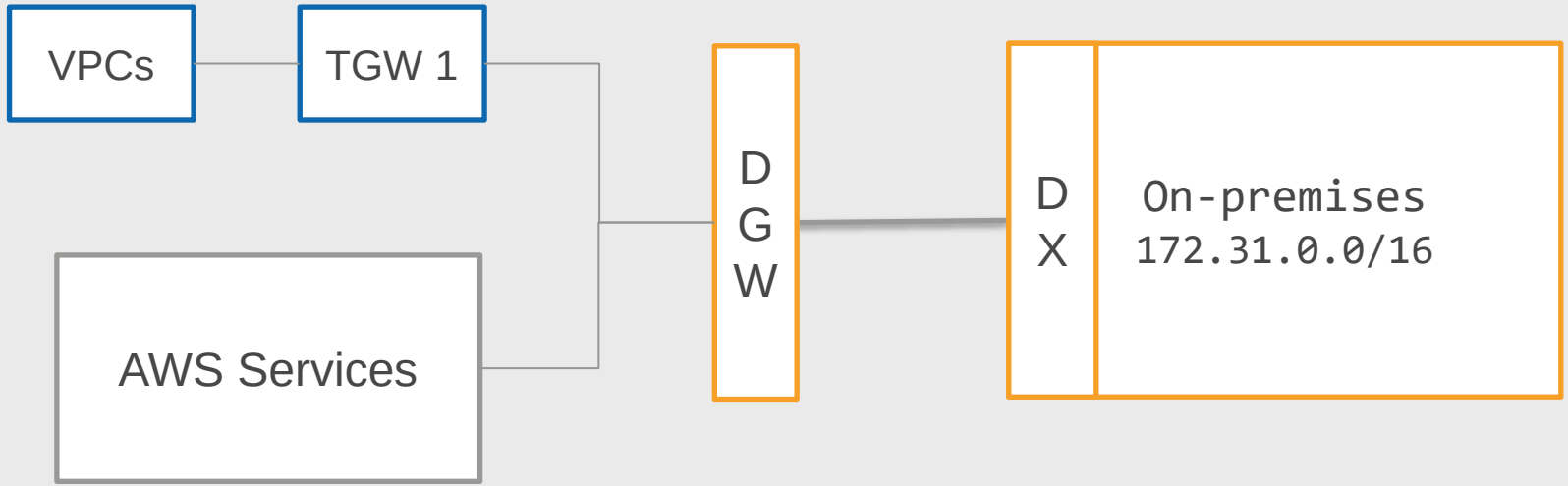
Direct Connect Gateway (DGW) supports multiple VPCs across different regions

Direct Connect sharing with Transit Gateway



Share Direct Connect Link with other VPCs using Transit Gateway

Direct Connect to access other AWS Services



Access AWS services from On-premises using Direct Connect with Public Virtual Interface

Traffic from on-premises is routed through DX and uses AWS Global network to access required service

VPN over Direct Connect

You can also setup a VPN connection inside Direct Connect

Encrypted channel with consistent network performance

VPN as Backup for Direct Connect

If you use only one Direct Connect location, to handle device and location failures, you can setup a backup VPN connection over the internet

Direct Connect Summary

DX - Physical Connection between your data center and AWS

Consistent network performance and throughput

For HA, use multiple DX Locations or use a backup VPN over the internet

VPC Components Summary

Component	Description
VPC	Isolated virtual network in AWS cloud
Subnet	Isolated segment of your VPC
Internet Gateway	VPC side of connection to internet
NAT Gateway	AWS managed Network Address Translation Service to make outbound internet connection from your private subnet (IPv4)
NAT Instance	Customer managed NAT (IPv4)
Egress-only Internet Gateway	IPv6 outbound internet access

VPC Components

Component	Description
Router	Routes traffic inside VPC
Security Group	Instance level stateful firewall. Supports only Allow rules
Network Access Control List	ACLs are subnet level stateless firewall. Supports Allow and Deny rules

VPC Components – Hybrid Architecture

Component	Description
Internet	Suitable for Internet accessible resources
Hardware VPN Connection	Secure connection between your datacenter and VPC (over internet or over direct connect)
Virtual Private Gateway	AWS side of VPN connection
Customer Gateway	Customer side of VPN connection
Direct Connect	Dedicated Private connectivity between customer on-premises network/Offices to AWS
Transit Gateway	Interconnect VPCs, Share Direct Connect and VPN link among VPCs

VPC Components – Connecting VPCs

Component	Description
Peering Connection	Connect two VPCs and access resources with private IP address
Gateway Endpoint	Access AWS resources like S3, DynamoDB without using NAT or Internet Gateway. Limit access to resources from specific VPCs
Interface Endpoint	New Capability powered by AWS Private Link. Setup private connections to AWS Supported Services, Services hosted by AWS Partners, Customers and Marketplace partners

Chandra Lingam

57,000+ Students

aws certified Solutions Architect Associate

aws certified Developer Associate

aws certified SysOps Administrator Associate

aws certified Solutions Architect Professional

aws certified Machine Learning Specialty

For AWS self-paced video courses, visit:

https://www.cloudwavetraining.com/

Cloud Wave LLC