Networking in AWS

Presenter Name, Email

Overview

AWS networking services including:

VPC – Extend your network into a virtual private cloud

EIP – Elastic IP

Direct Connect – Physical cross connect into AWS

ELB – Managed load balancer service

Route53 – Managed DNS service

aws

Amazon VPC

Amazon Virtual Private Cloud (VPC)

Your own logically isolated section of AWS

Bring your own network:

- IP Addresses
- Subnets
- Network Topology
- Routing Tables

Multiple Connectivity Options

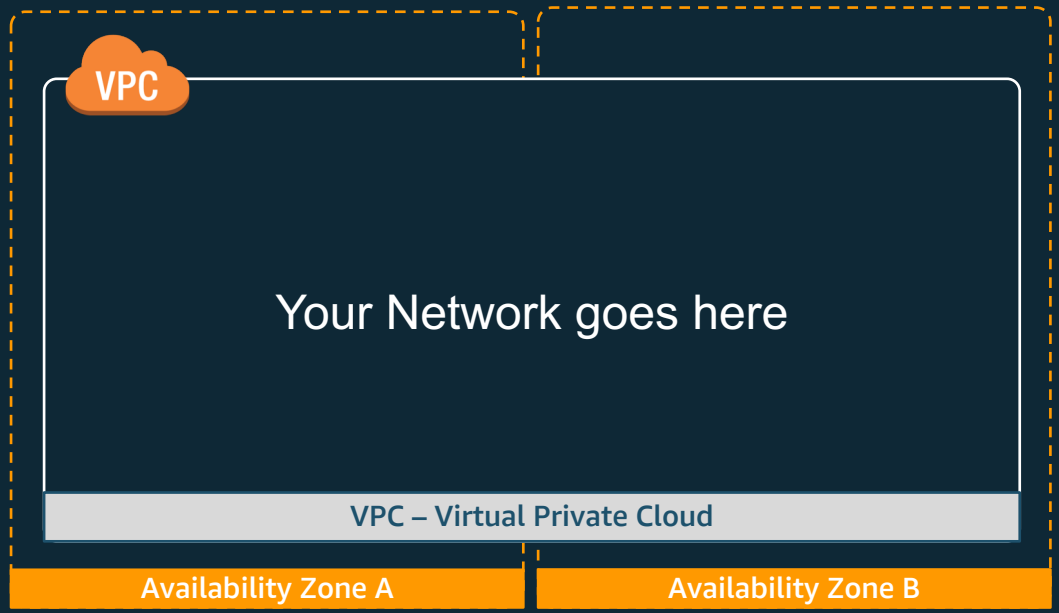
Advanced Security Features

aws

Networking Building Blocks

Amazon Virtual Private Cloud (VPC)

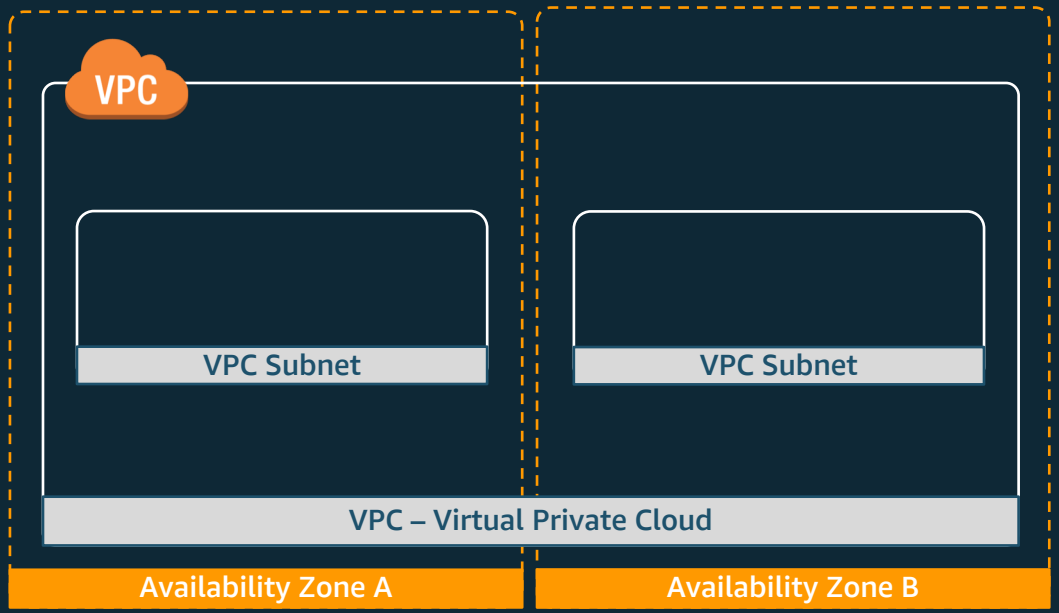
- Bring your own network



Networking Building Blocks

Amazon Virtual Private Cloud (VPC)

- Bring your own network
- Create your own subnets



Plan your VPC IP space before creating it

IP Addressing

- Consider future AWS region expansion
- Consider future connectivity to corporate networks
- Consider subnet design
- VPC can be /16 between and /28
- CIDR cannot be modified once created
    - But you can add new CIDRs to expand the VPC IP addressing
- Overlapping IP spaces = future headache

aws

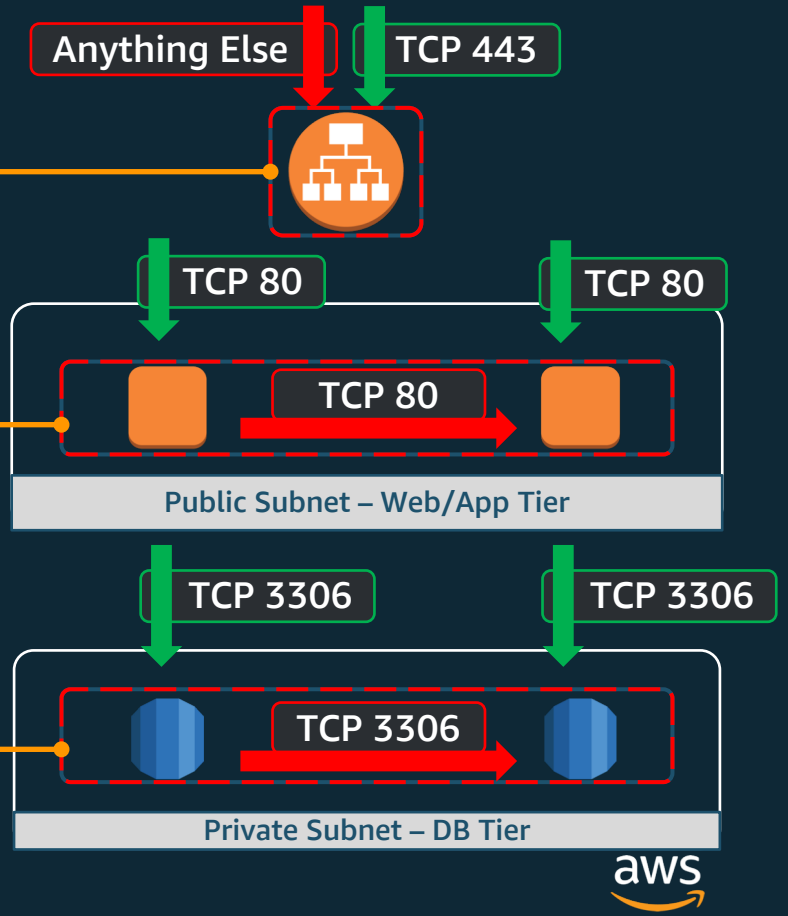
Network Building Blocks

Network Control – Security Groups

Inbound Security Group **SG-WebELB**				
Traffic from	**Protocol**	**L4**	**Port**	**Action**
0.0.0.0/0	HTTPS	TCP	443	Allow
*	*	*	*	Deny

Inbound Security Group **SG-WebTier**				
Traffic from	**Protocol**	**L4**	**Port**	**Action**
SG-WebELB	HTTP	TCP	80	Allow
*	*	*	*	Deny

Inbound Security Group **SG-DatabaseTier**				
Traffic from	**Protocol**	**L4**	**Port**	**Action**
SG-WebTier	MySQL	TCP	3306	Allow
*	*	*	*	Deny



Network Building Blocks

Network Control – Security Groups

Inbound / Outbound

Instance level inspection

- Microsegmentation
- Mandatory, all instances have an associated Security Group

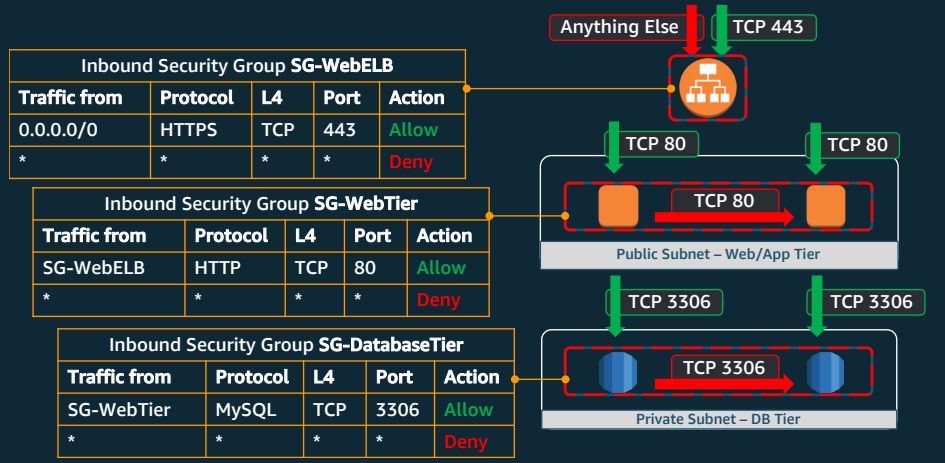
Stateful

Can be cross referenced

- Works across VPC Peering

Only supports allow rules

- Implicit deny all at the end

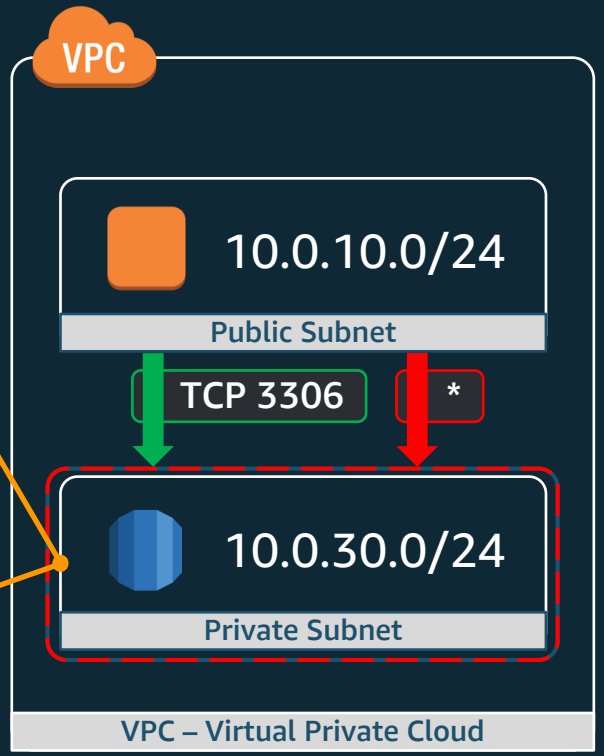


Network Building Blocks

Network Control – Network Access List

Inbound Network ACL				
Source	Protocol	L4	Port	Action
10.0.10.0/0	TCP	MySQL	3306	Allow
*	*	*	*	Deny

Outbound Network ACL				
Destination	Protocol	L4	Port	Action
10.0.10.0/0	TCP	*	*	Allow
*	*	*	*	Deny



aws

Network Building Blocks

Network Control – Network Access List

Optional level of security

- By default, allow all traffic

Subnet level inspection

Stateless

IP and TCP/UDP port based

Supports allow and deny rules

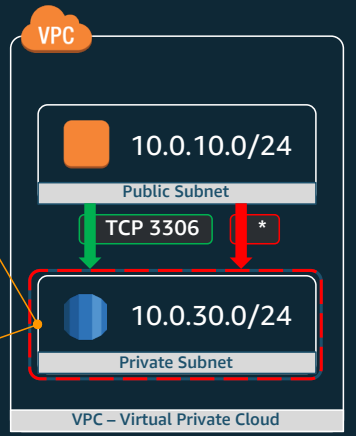
- Deny all at the end

Inbound Network ACL

Source	Protocol	L4	Port	Action
10.0.10.0/0	TCP	MySQL	3306	Allow
*	*	*	*	Deny

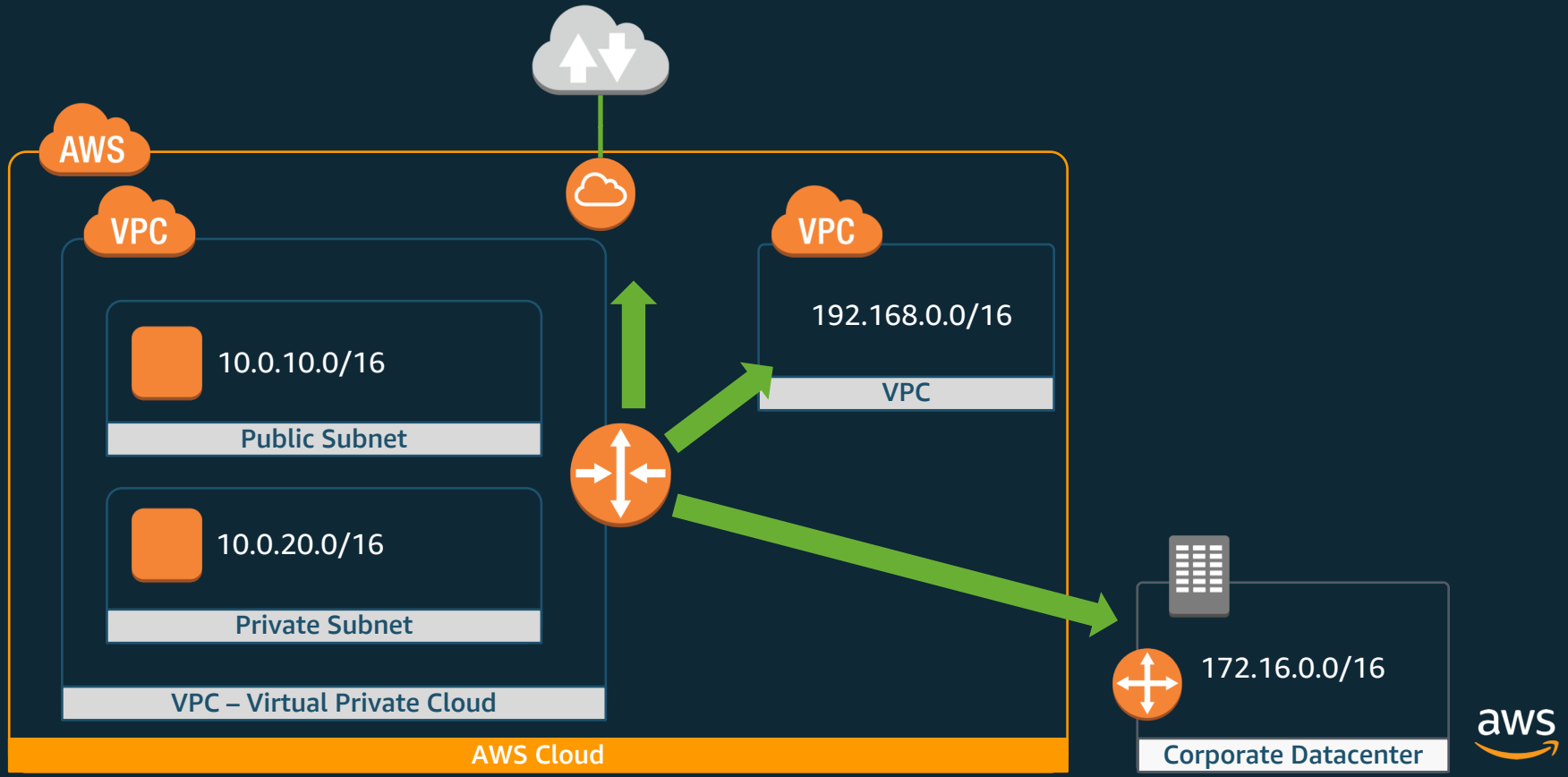
Outbound Network ACL

Destination	Protocol	L4	Port	Action
10.0.10.0/0	TCP	*	*	Allow
*	*	*	*	Deny



Network Building Blocks

Network Control – Route Rules



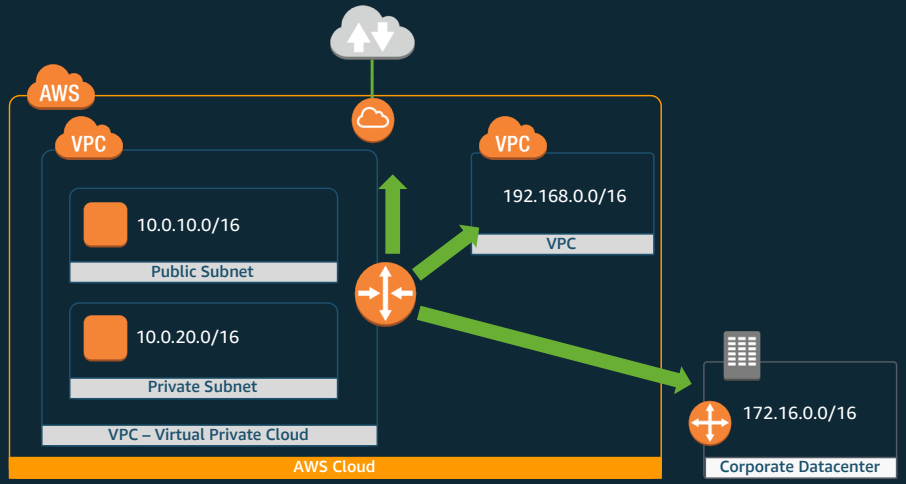
Network Building Blocks

Network Control – Route Rules

Each subnet can have a unique Route Table

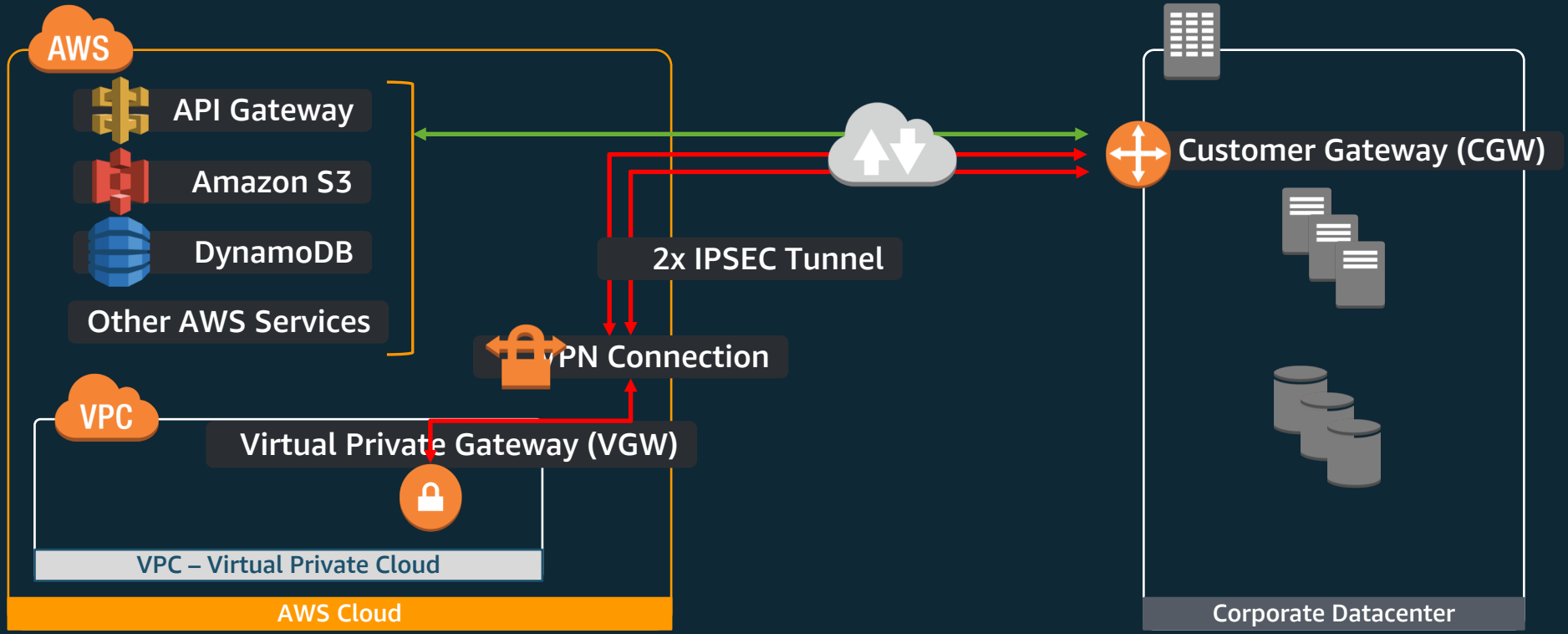
Direct traffic out of the VPC

- IGW
- VGW
- VPC Endpoints
- Direct Connect
- VPC Peering



Network Building Blocks

VPN – Virtual Private Network (1.25 Gbps max)



How to connect my Datacenter to AWS?

VGW – Virtual Private Gateway

One VGW per VPC

Redundant VPN Tunnels

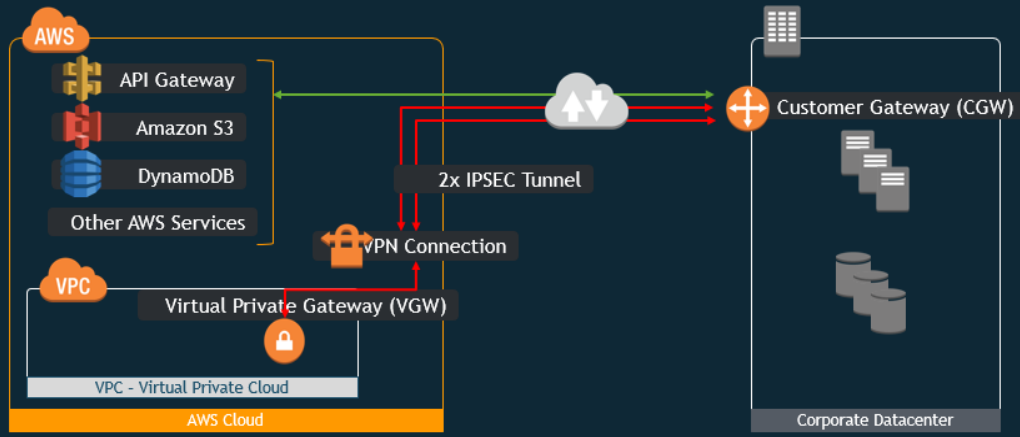
- Terminating in different AZ

IPSec

- AES 256-bit encryption
- SHA-2 hashing

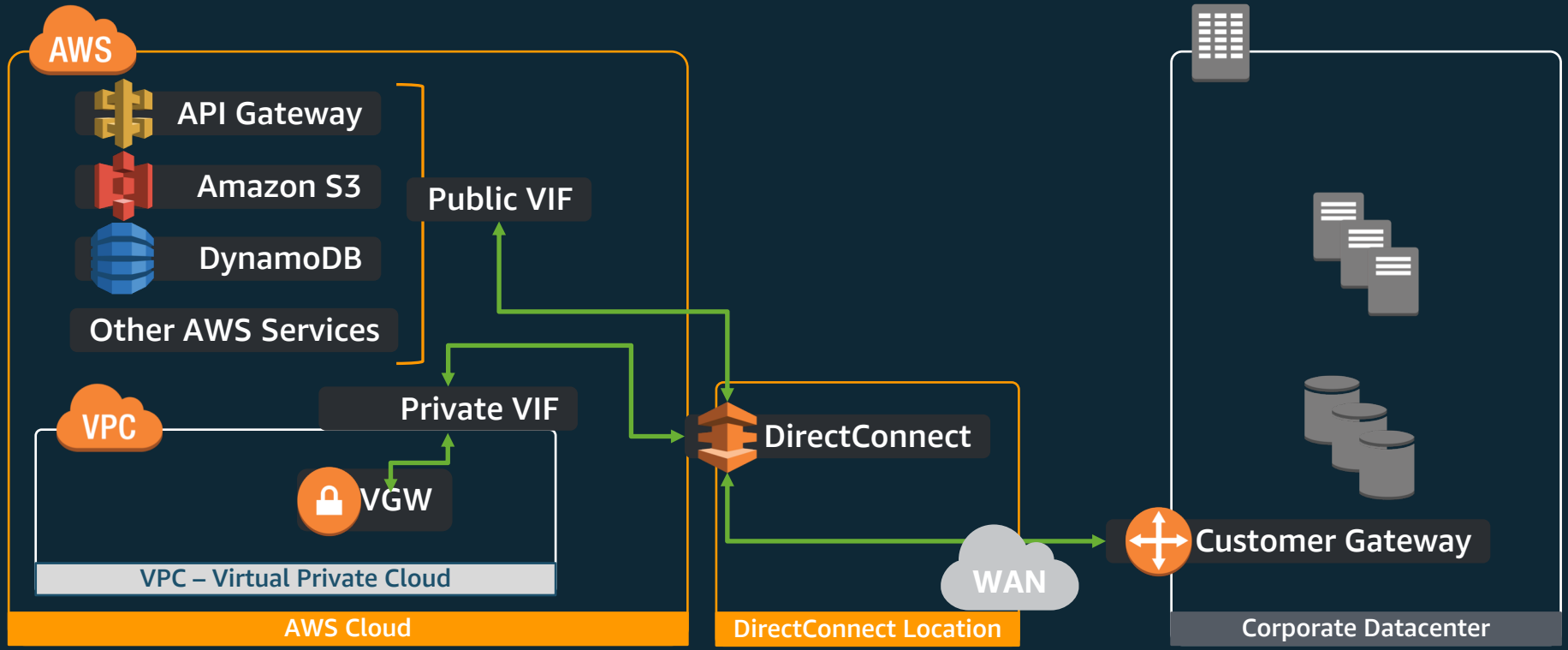
Scalable

BGP or Static Routing



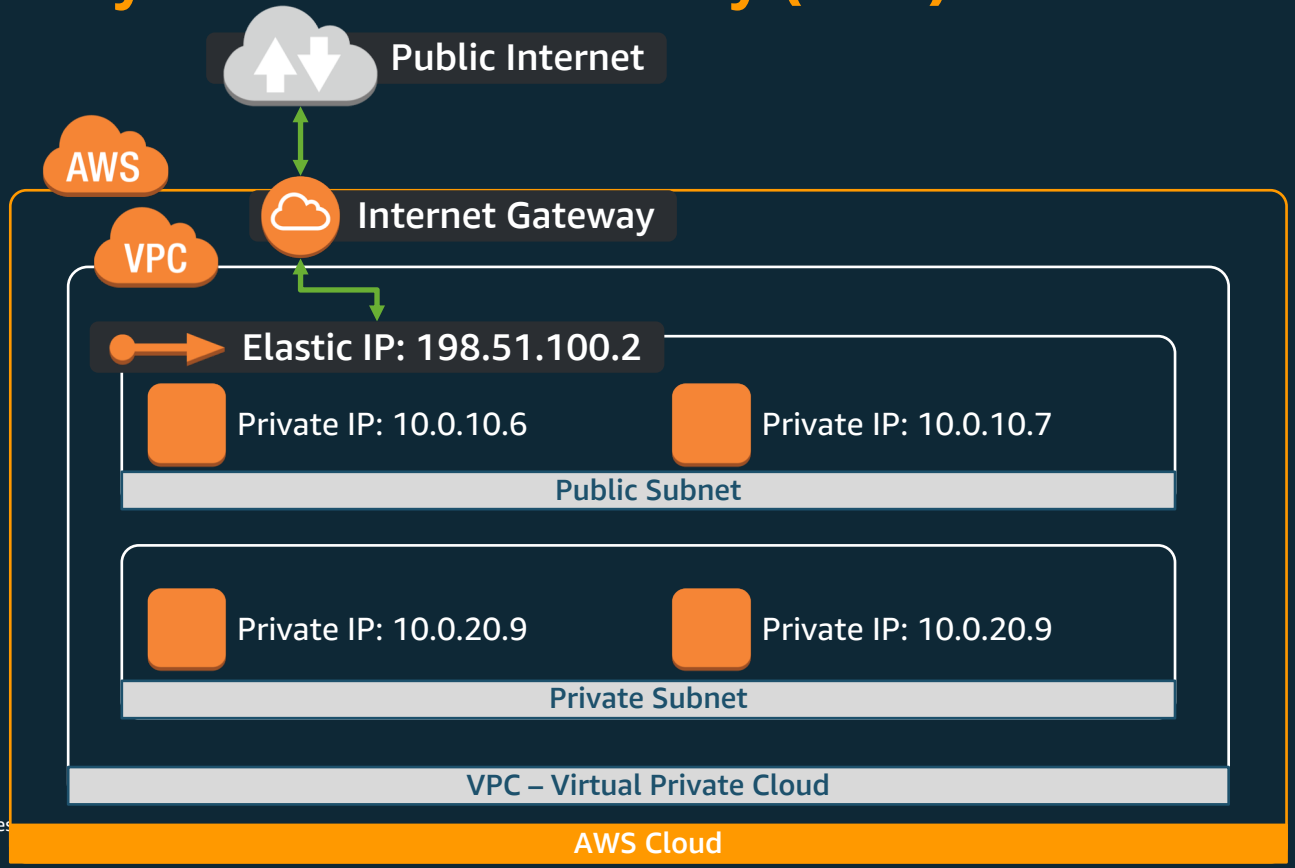
Network Building Blocks

AWS Direct Connect (10 Gbps max)



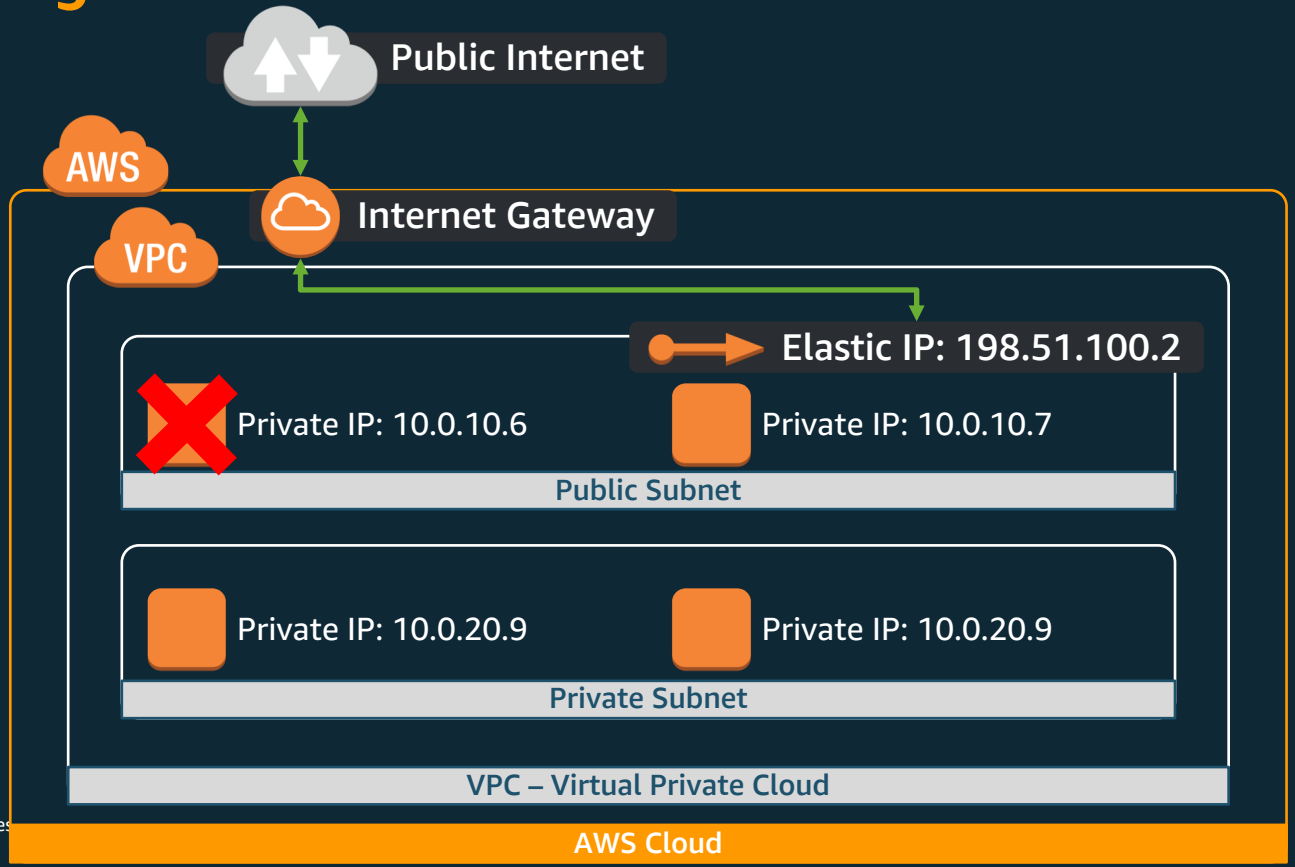
Network Building Blocks

VPC Gateways – Internet Gateway (IGW)



Network Building Blocks

Connecting to Instances – Elastic IP Address



Network Building Blocks

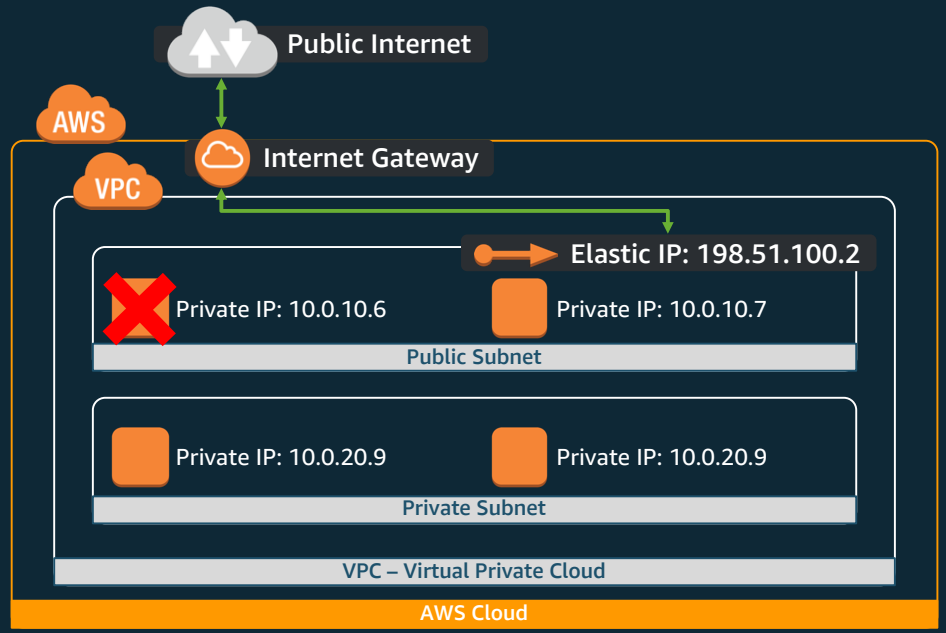
Internet Gateway + Elastic IPs

IGW - Internet Gateway

- One per VPC
- Horizontally scaling
- Redundant
- Highly available

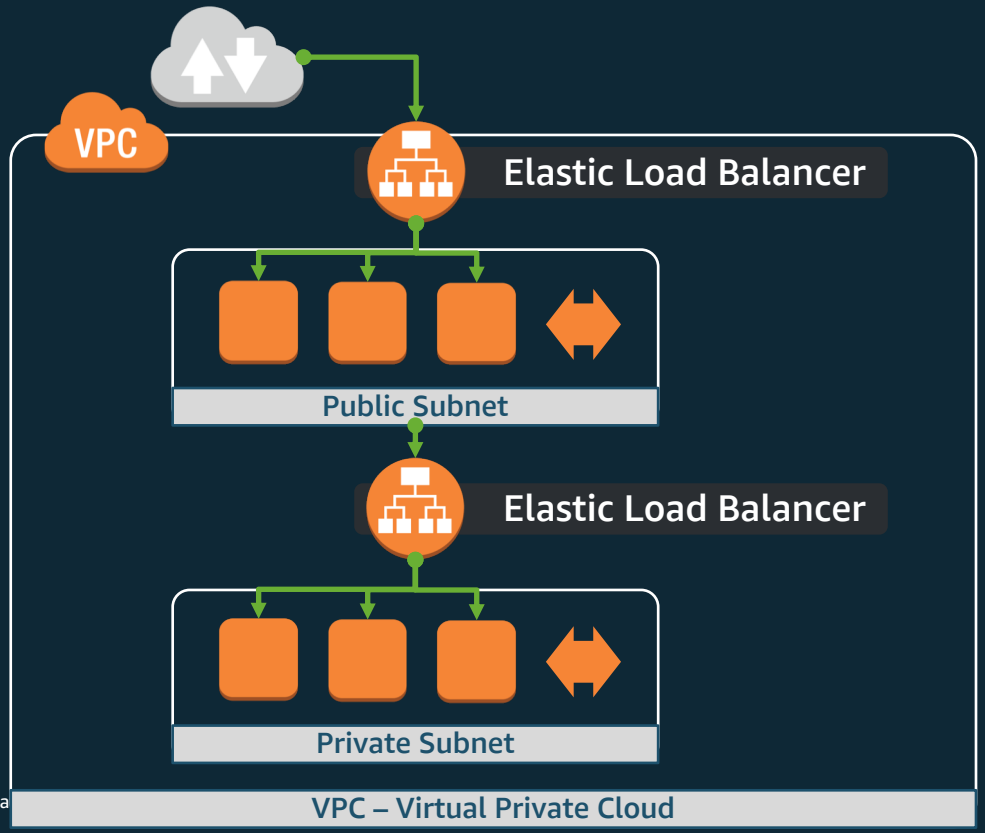
EIP - Elastic IPs

- Public IP address
- Can be reassociated



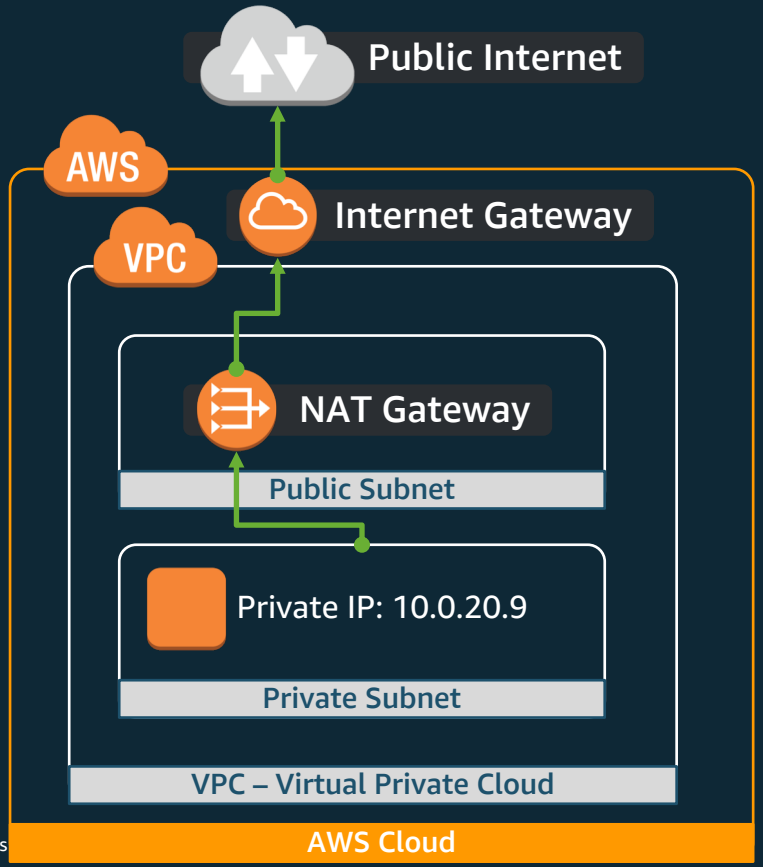
Network Building Blocks

Connecting to Instances – Load Balancer



Network Building Blocks

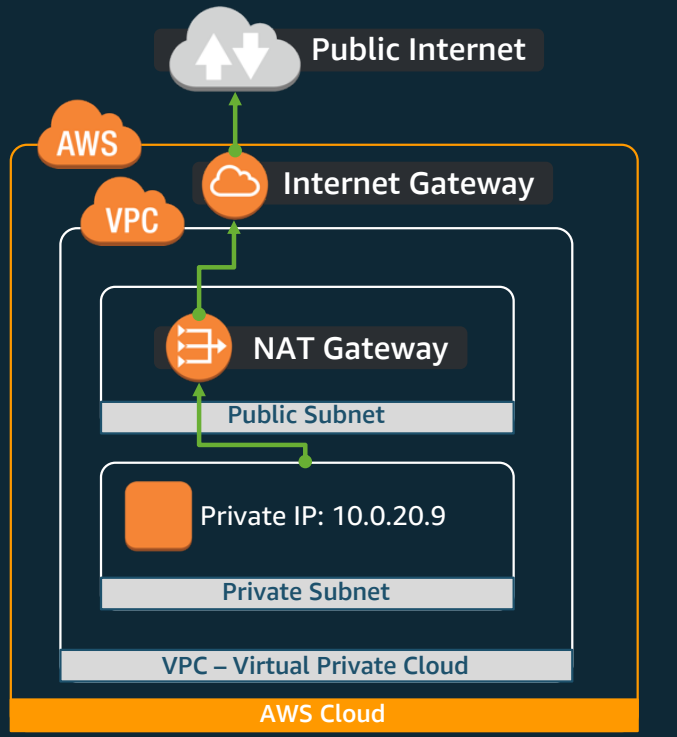
NAT Gateway



Network Building Blocks

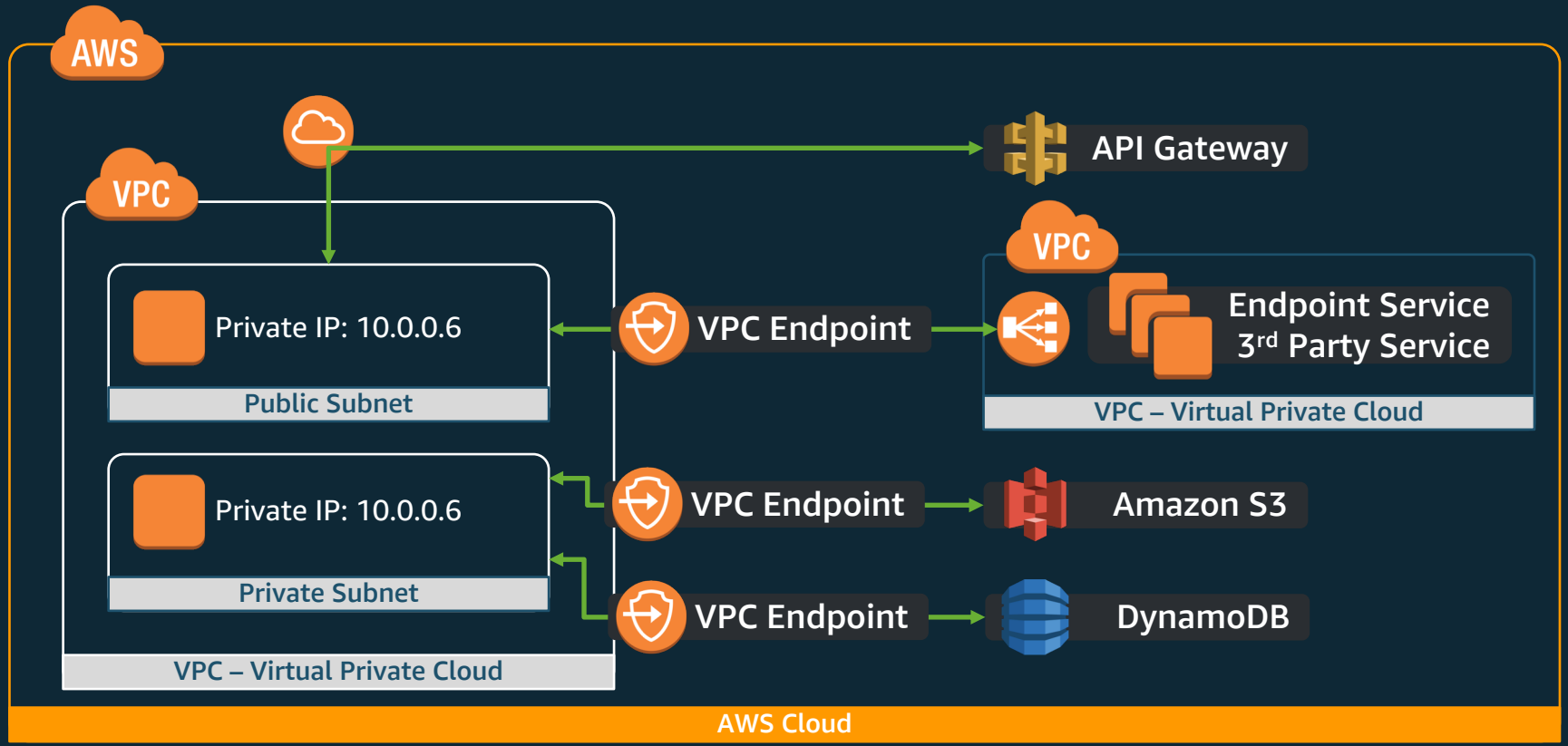
NAT Gateway

- Connect to the internet
- No incoming connection
- High available
- Up to 10Gbps bandwidth
- Fully managed by AWS
- Supports TCP, UDP, and ICMP protocols
- Network ACLs apply to NAT gateway's traffic



How to connect to public AWS Services?

VPC Endpoints



How to connect to public AWS Services?

VPC Endpoints

Scalable and high available

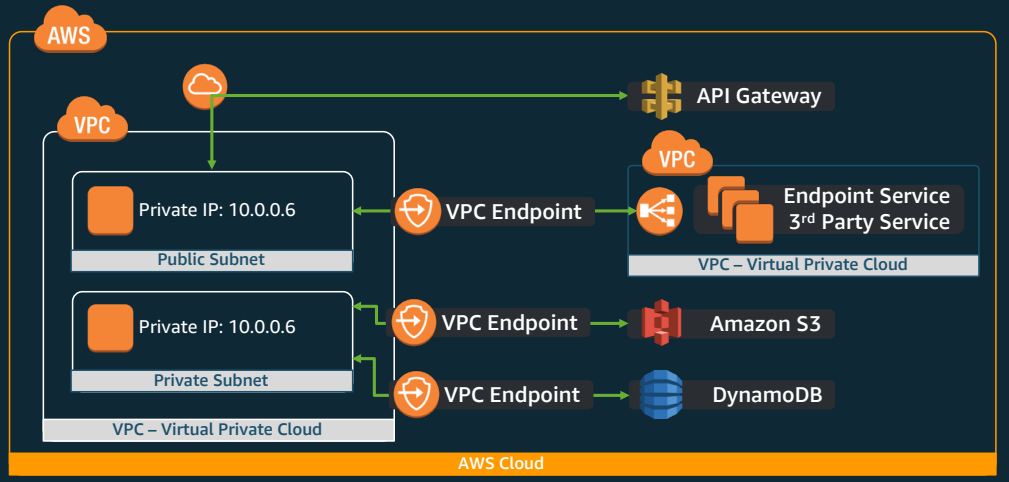
Don’t require public IPs

Robust access control

Private connection to supported AWS services

Connection to VPC Endpoint Services

- Other VPCs
- SaaS Providers



How to connect to public AWS Services?

VPC Endpoints

There are two types of VPC endpoints:

Gateway: A gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service.

Supported Services: Amazon S3 and DynamoDB

Interface: An elastic network interface with a private IP address that serves as an entry point for traffic destined to a supported service.

Supported Services: EC2 and ELB API, AWS Systems Manager, Kinesis Data Streams, AWS KMS, AWS Service Catalog, etc, Endpoint Services hosted by other accounts and AWS Marketplace Partner services

aws

How to connect to public AWS Services?

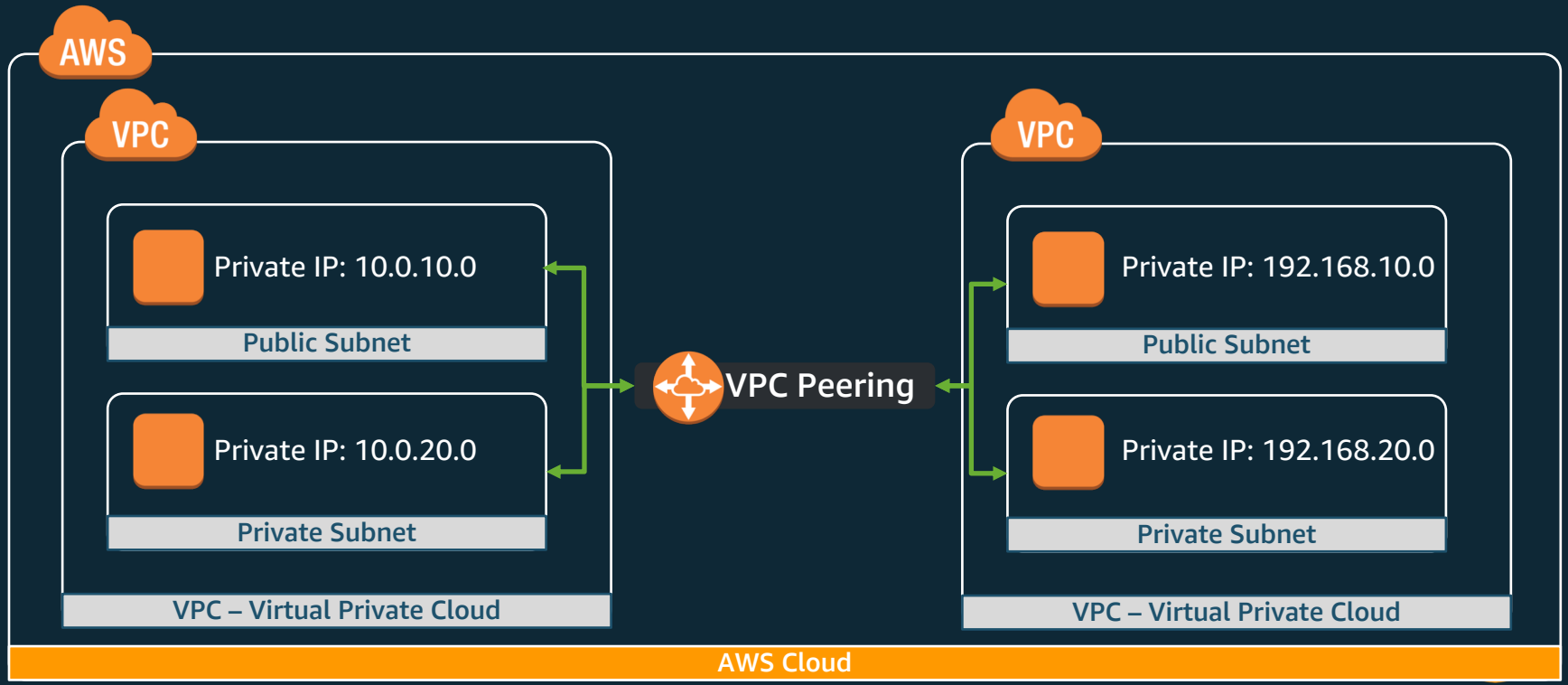
VPC Endpoints – Interface VPC Endpoints

- Enables customers to connect to services powered by AWS PrivateLink
- IP connectivity is private—no public IP addresses
- Endpoints have regional and zonal names
- Private DNS Support for default AWS Service DNS name – no configuration changes required
- Works with Amazon VPC security groups
- Works with IAM policies

aws

How to connect to another VPC?

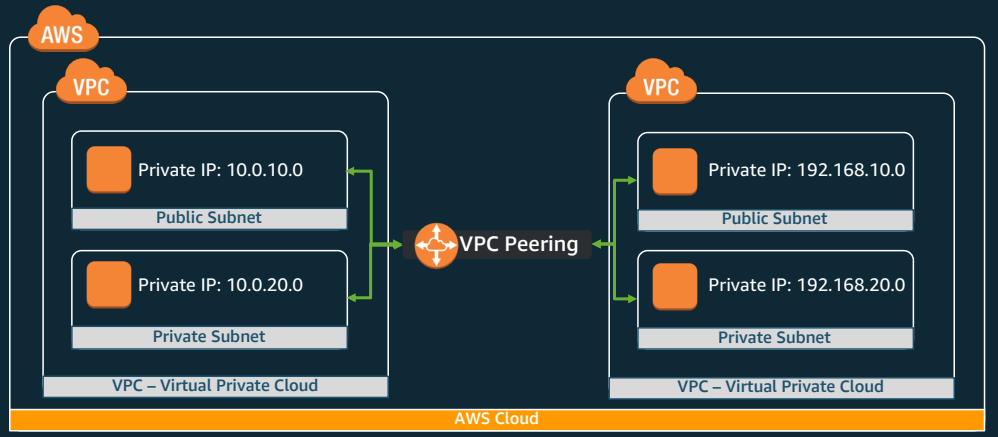
VPC Peering



How to connect to another VPC?

VPC Peering

- Scalable and high available
- Inter-account peering
- Inter-region peering
- Remote Security groups can be referenced
- Routing policy with Route Tables
- No transitive routing



How to isolate my resources inside AWS?

Default VPC

Default VPC

- Simplicity and Convenience
- Automatically assigned network and subnets

Security of VPC

- Customer may create additional subnets and change routing rules
- Additional network controls (Security Groups, NACLs, routing)
- Hardware VPN options between corporate networks
- Instances in default subnets have Security Group–controlled public and private IPs

aws

Recap

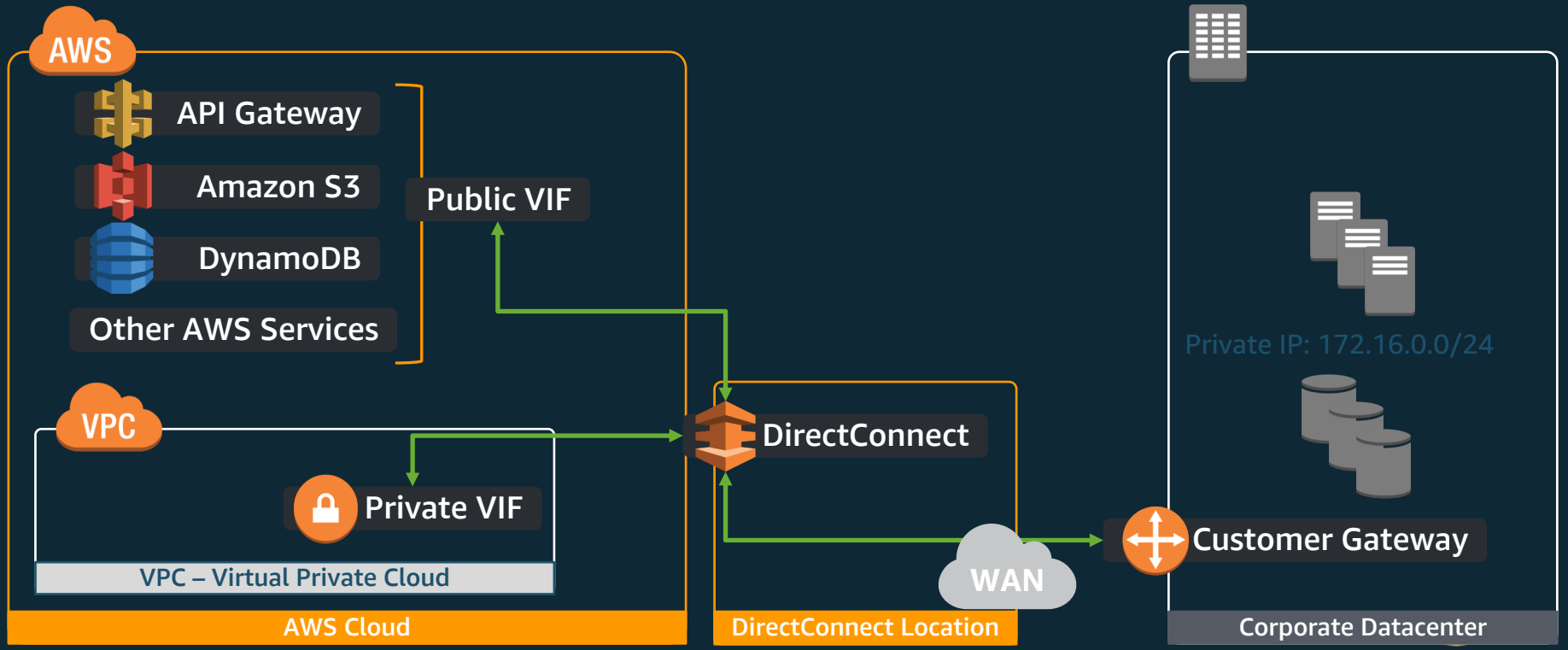
1. Create VPC
2. Create Subnets – Across Multiple AZ's
3. Configure Route Tables
4. Create Gateways – IGW and VGW (VPN and DX)
5. Configure Security – Security Groups and NACLs
6. Create VPC Endpoints
7. Create NAT Gateway
8. Configure VPC Peering
9. **Create Instances**

aws

Direct Connect

How to connect to my Datacenter to AWS?

Dedicated Connection - AWS Direct Connect



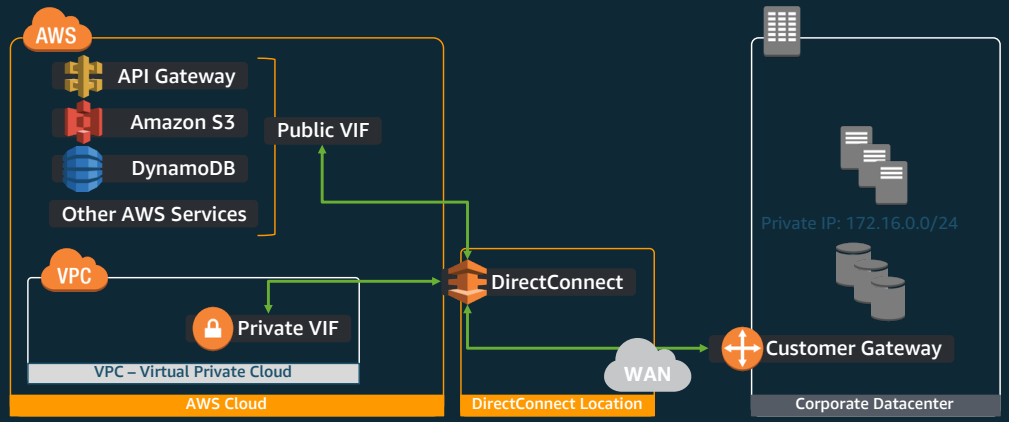
How to connect to my Datacenter to AWS?
Direct Connect, aka DX (1/2)

1 Gbps or 10 Gbps fiber cross connect

- 50M - 500M available through APN Partners
- Single VIF per connection through APN Partners

Consistent Network Performance

Lower latency compared to a VPN connection



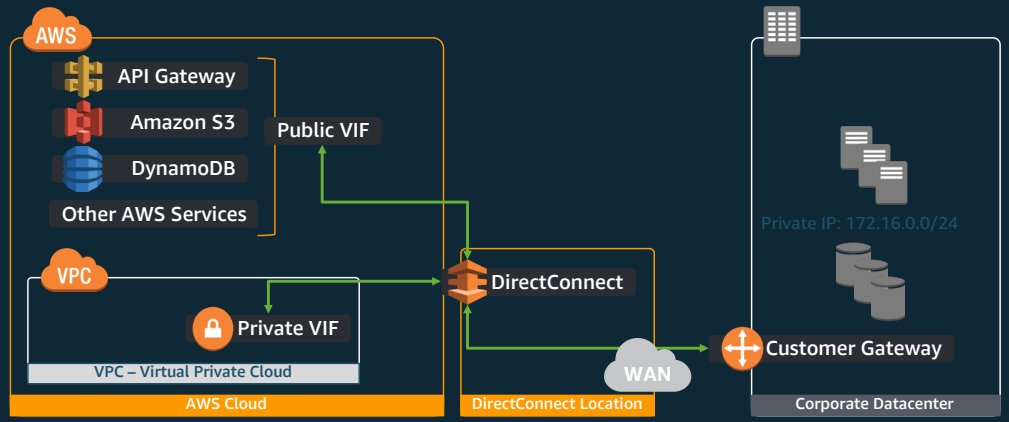
How to connect to my Datacenter to AWS?
Direct Connect, aka DX (1/2)

Reduced Bandwidth Charges

Public and Private VIF options

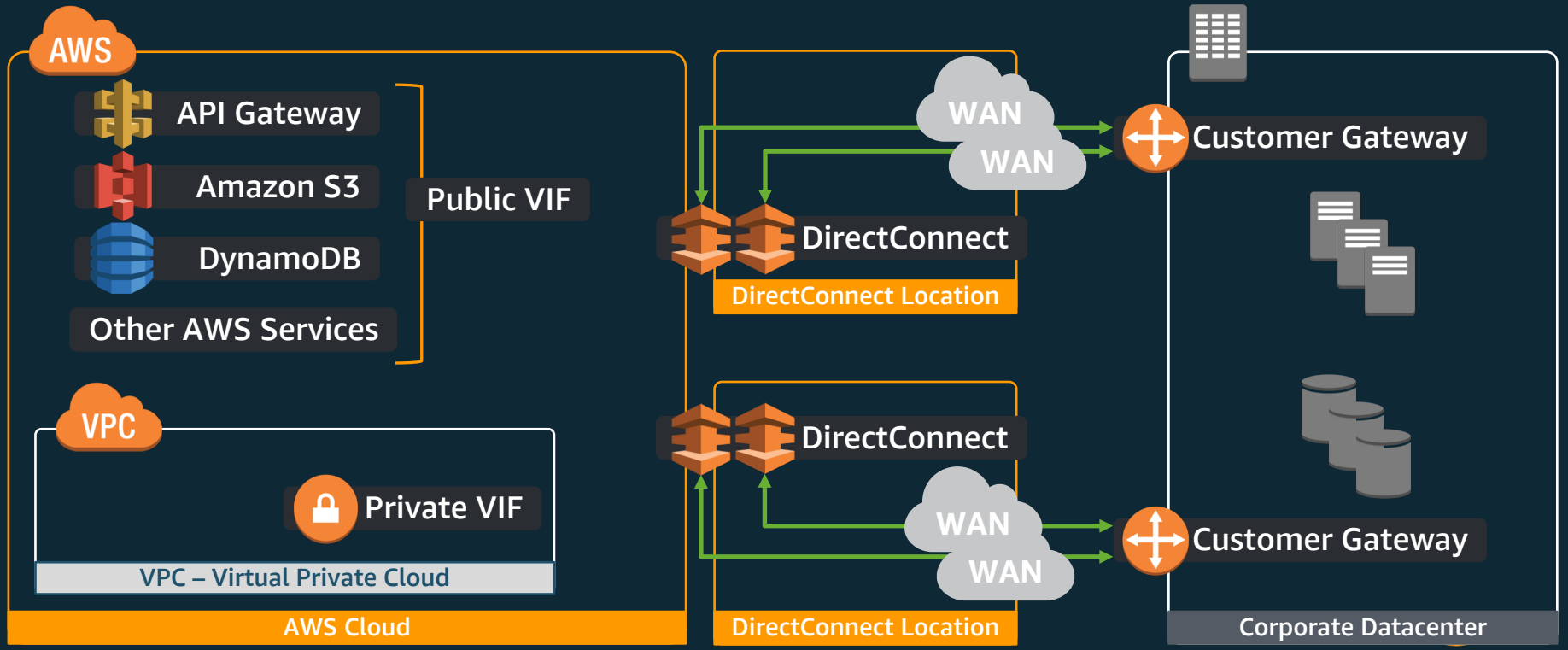
- Multiple Private VIFs on the 1G or 10G links

BGP Supported



How to connect to my Datacenter to AWS?

Dedicated connection + Redundancy



How to connect to my Datacenter to AWS?
Direct Connect redundancy

Redundant DX locations

Redundant DX Connections

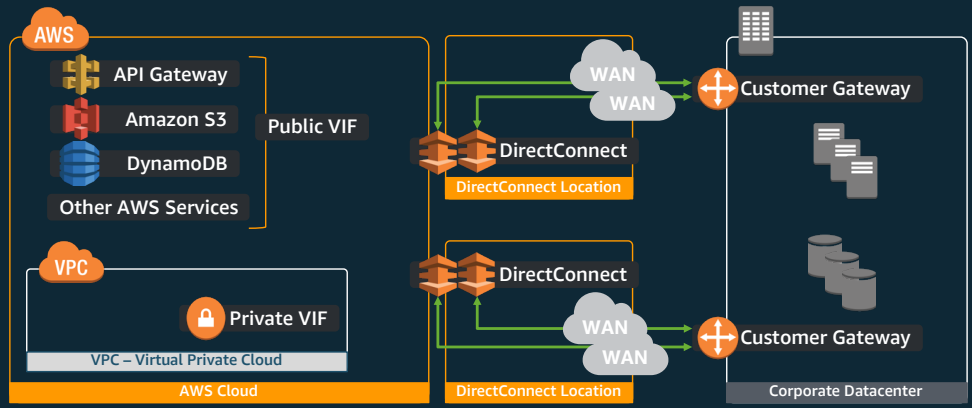
- LAG/LACP Supported

Redundant AWS DX routers

- Every DX location

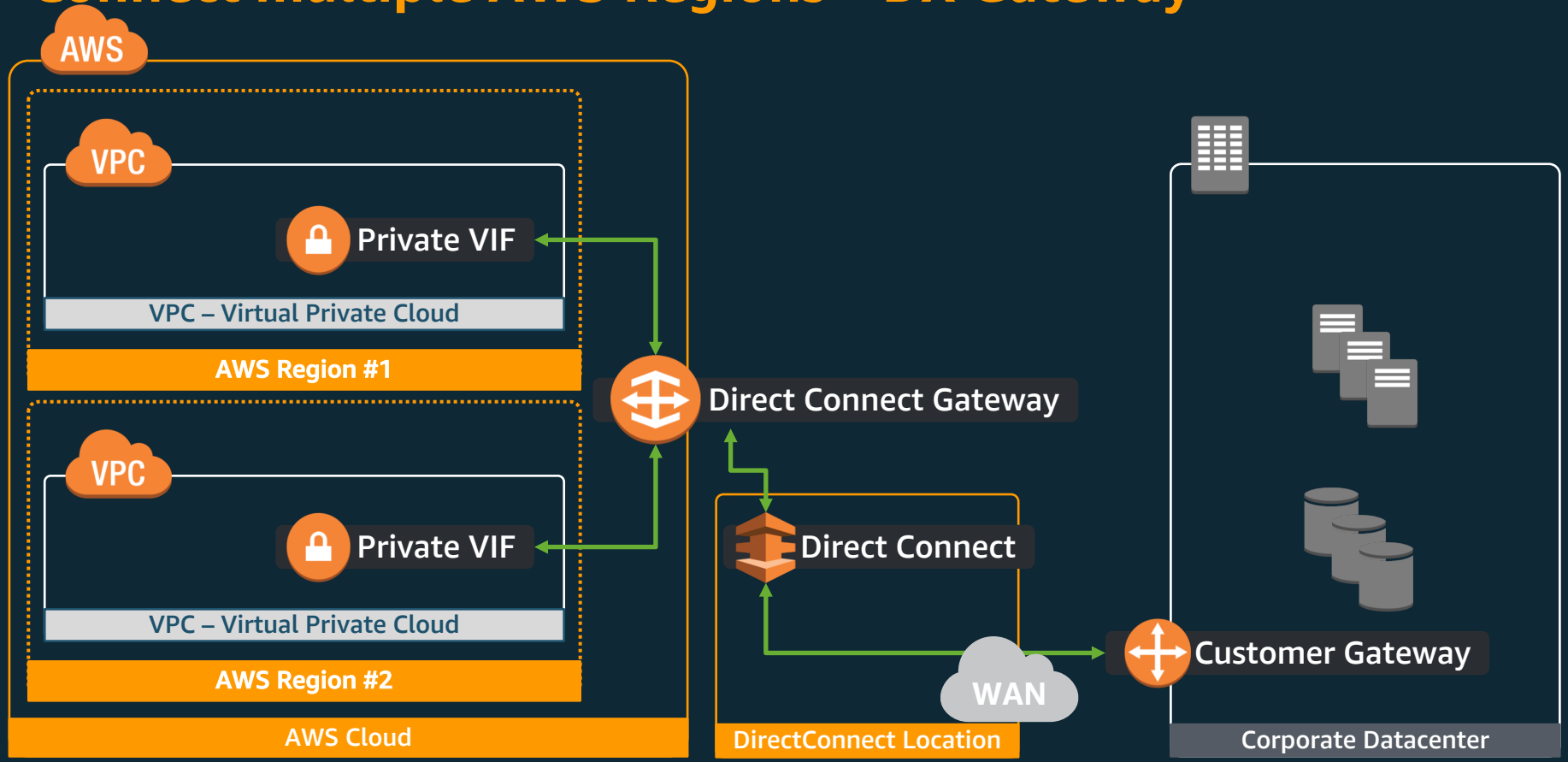
Routing policies

- AS Path Prepend
- Scope BGP Communities
- Local Preference BGP Communities



How to connect to my Datacenter to AWS?

Connect multiple AWS Regions – DX Gateway



AWS Direct Connect
Cross-Connect Details

- Decide on an AWS DX location and port size
- Use AWS Management Console to create connection request(s)
  - Sends Letter of Authorization – Connecting Facility Assignment (LOA-CFA) via email
- Establish WAN connectivity to DX location*
  - APN Partner or a network carrier of your choice
- Provide LOA-CFA to an APN Partner or your service provider to establish the connection at the DX location
- Use AWS Management Console to configure one or more virtual interfaces

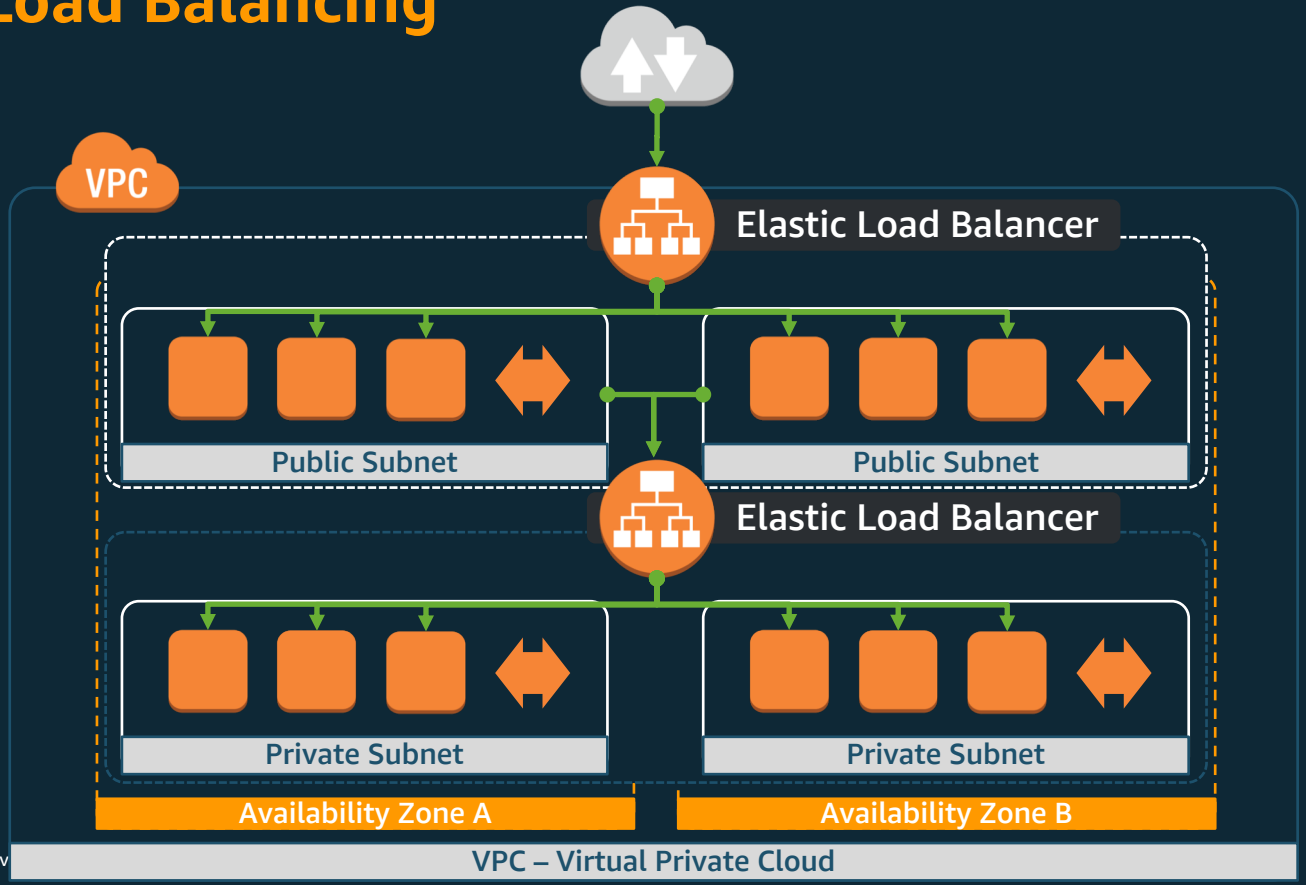
* Can be done in parallel with remaining steps once the AWS DX location has been selected

aws

ELB

How to distribute traffic across Instances?

Elastic Load Balancing



aws

How to distribute traffic across Instances?

Elastic Load Balancer (ELB) – Classic Load Balancer

Layer 4 & Layer 7 Load Balancing

Region level service

- Cross AZ

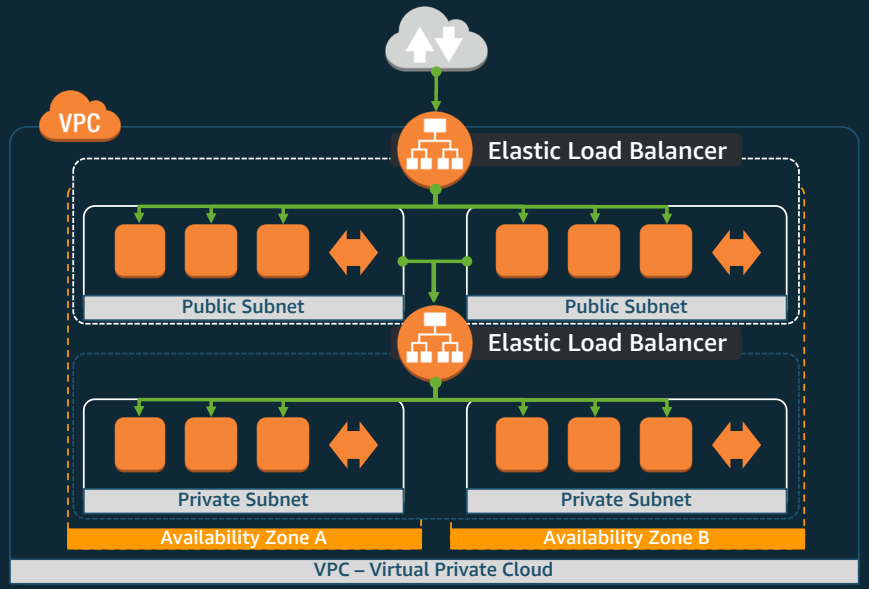
Built-in Health Check

Auto Scaling Integration

SSL Supported

- Client SSL Termination
- Backend ELB-to-Server mutual SSL

Sticky Sessions

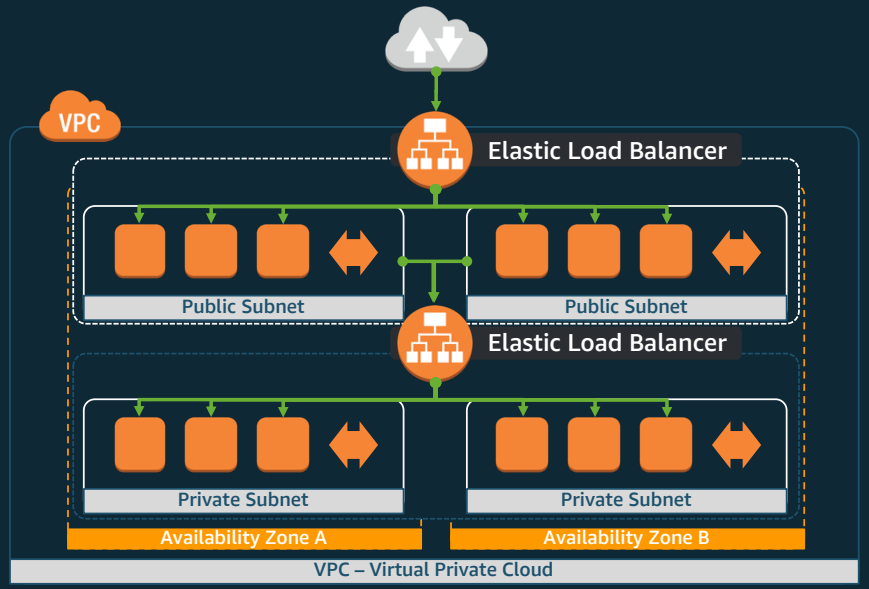


aws

How to distribute traffic across Instances?

ELB - Application Load Balancer

- Layer 7 Load Balancing
- Content-Based Routing (host and path based)
- Containerized Application Support (ECS, EKS)
- HTTP/2 Support
- WebSockets Support
- Deletion Protection
- Request Tracing
- Web Application Firewall (WAF) integration

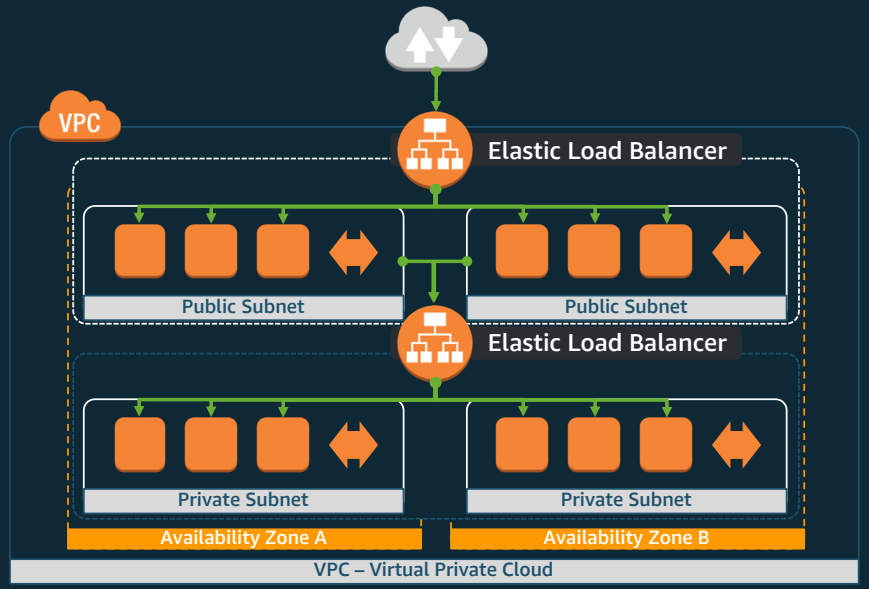


aws

How to distribute traffic across Instances?

ELB - Network Load Balancer

- Layer 4 Load Balancing
- Connection-based Load Balancing
- High Throughput
- Low Latency
- Preserve source IP address
- Static IP and Elastic IP
- Long-lived TCP Connections
  - Ideal for WebSockets
- IP addresses as Targets



aws

Elastic Load Balancing

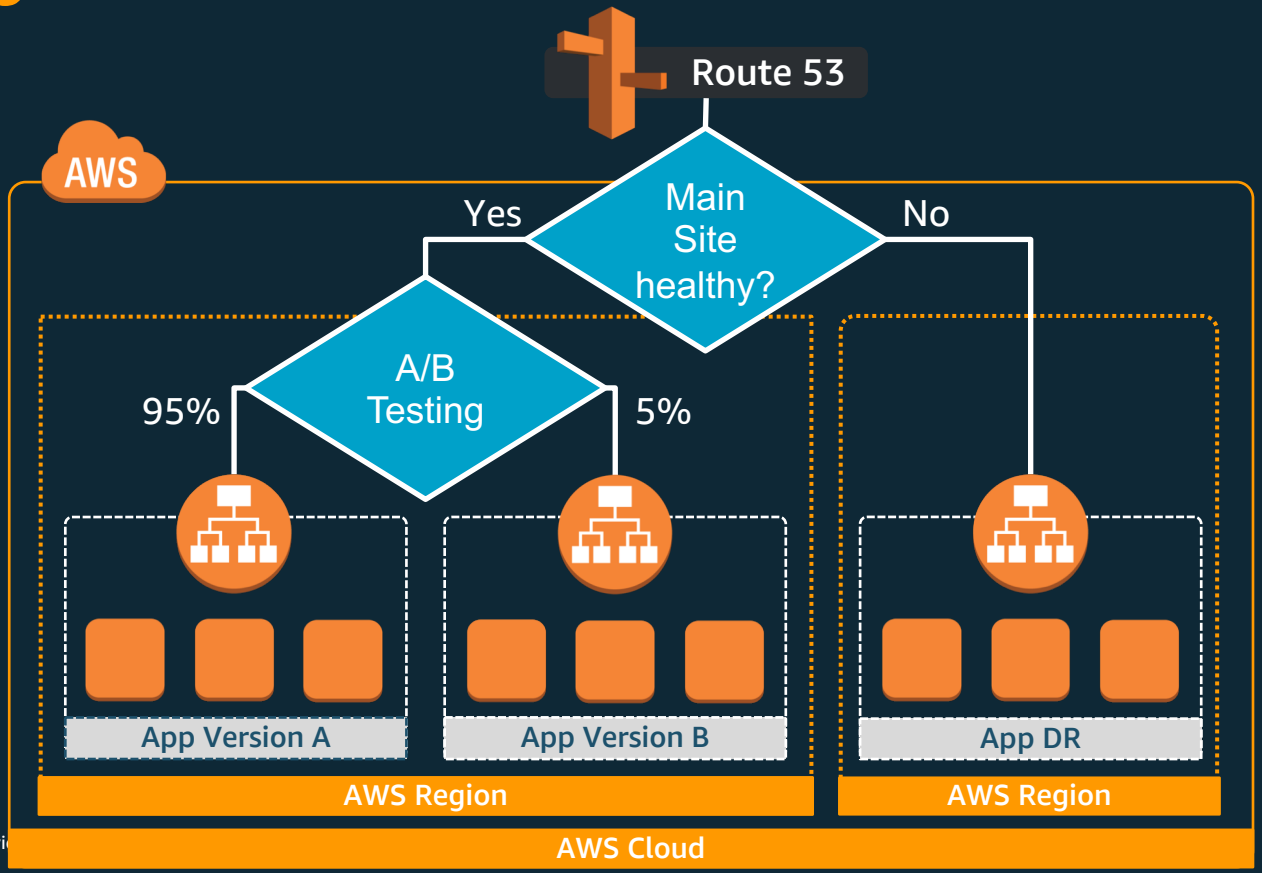
Features Comparison

Feature	Application Load Balancer	Network Load Balancer
Protocols	HTTP, HTTPS	TCP
Platforms	VPC	VPC
Health checks	Yes	Yes
CloudWatch metrics	Yes	Yes
Logging	Yes	Yes
Path-Based Routing	Yes	
Host-Based Routing	Yes	
Native HTTP/2	Yes	
Configurable idle connection timeout	Yes	
SSL offloading	Yes	
Server Name Indication (SNI)	Yes	
Sticky sessions	Yes	
Back-end server encryption	Yes	
Static IP		Yes
Elastic IP address		Yes
Preserve Source IP address		Yes

Route53

How to direct traffic to my domain?

Route 53



aws

How to direct traffic to my domain?

Route 53

AWS DNS service

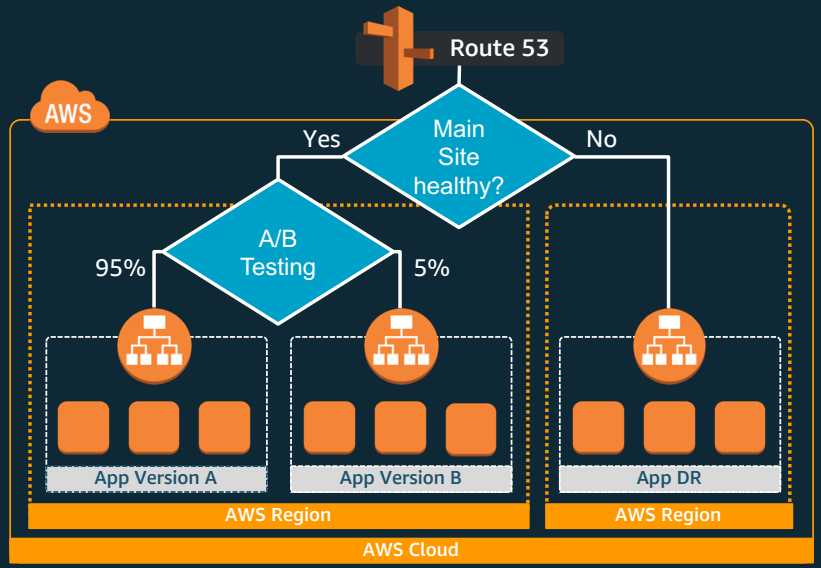
100% availability SLA

Domain Registration

Domain name resolution

- Health Checks
- DNS Failover
- Latency Based Routing
- Geo Based Routing
- Weighted Round Robin

Private DNS for VPC



Route53

- Zone Apex integration
  - ELB, S3, CloudFront
- Private DNS within VPC
  - Internal DNS names not exposed to Internet
  - Supports split-horizon DNS

aws

Route53 Pricing Dimensions

- Pay only for managing domains through the service
  - the number of domains
  - the number of queries that the service answers for each of your domains
- No minimum fees
- No minimum usage commitments
- No overage charges

aws

Route53

Getting Started

- Register DNS name with Route 53 or transfer from external registrar
- Create a Route53 hosted zone
  - AWS Management Console or API
- Update your domain registrar (if transferred)
  - Provide Route53 name servers associated with your hosted zone
- Create DNS resource records for your domain

aws

Any Questions?