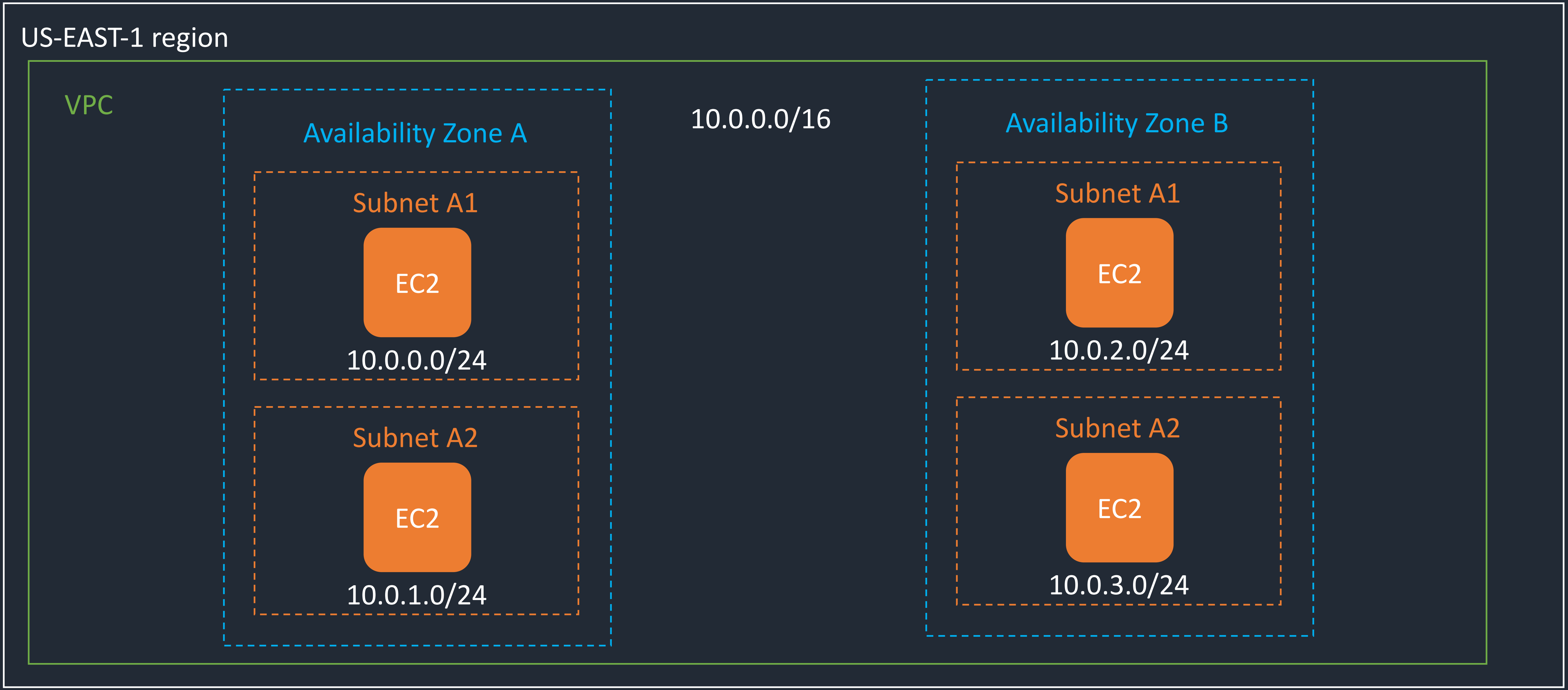
AWS Networking

Thomas Le Moullec. AWS Solutions Architect
September 29th 2020

Agenda

- VPC
- Connecting resources to Internet
- Load Balancing
- VPC Security
- External Connectivity (Hybrid Cloud, OnPremises)
- DNS

Amazon Virtual Private Cloud - VPC



VPC configuration

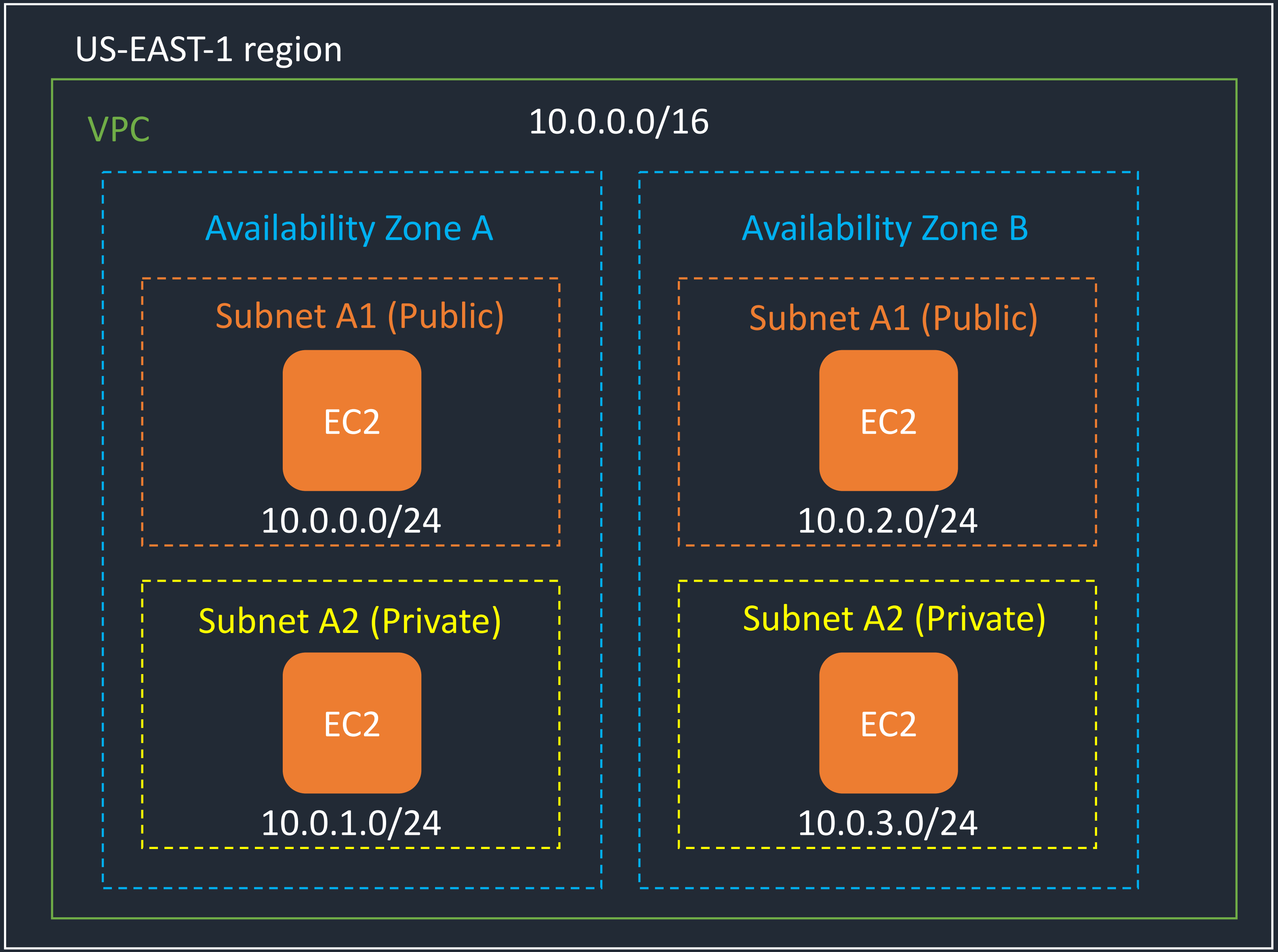
Plan IP Design Before creation: Avoid overlapping, multiple VPCs / regions / subnets, external connectivity

VPC IP addressing: between /16 and /28, supports subnetting, CIDR cannot be modified but CIDR addition possible

External Connectivity: Can bring your own IP range, Support IPv4 and IPv6

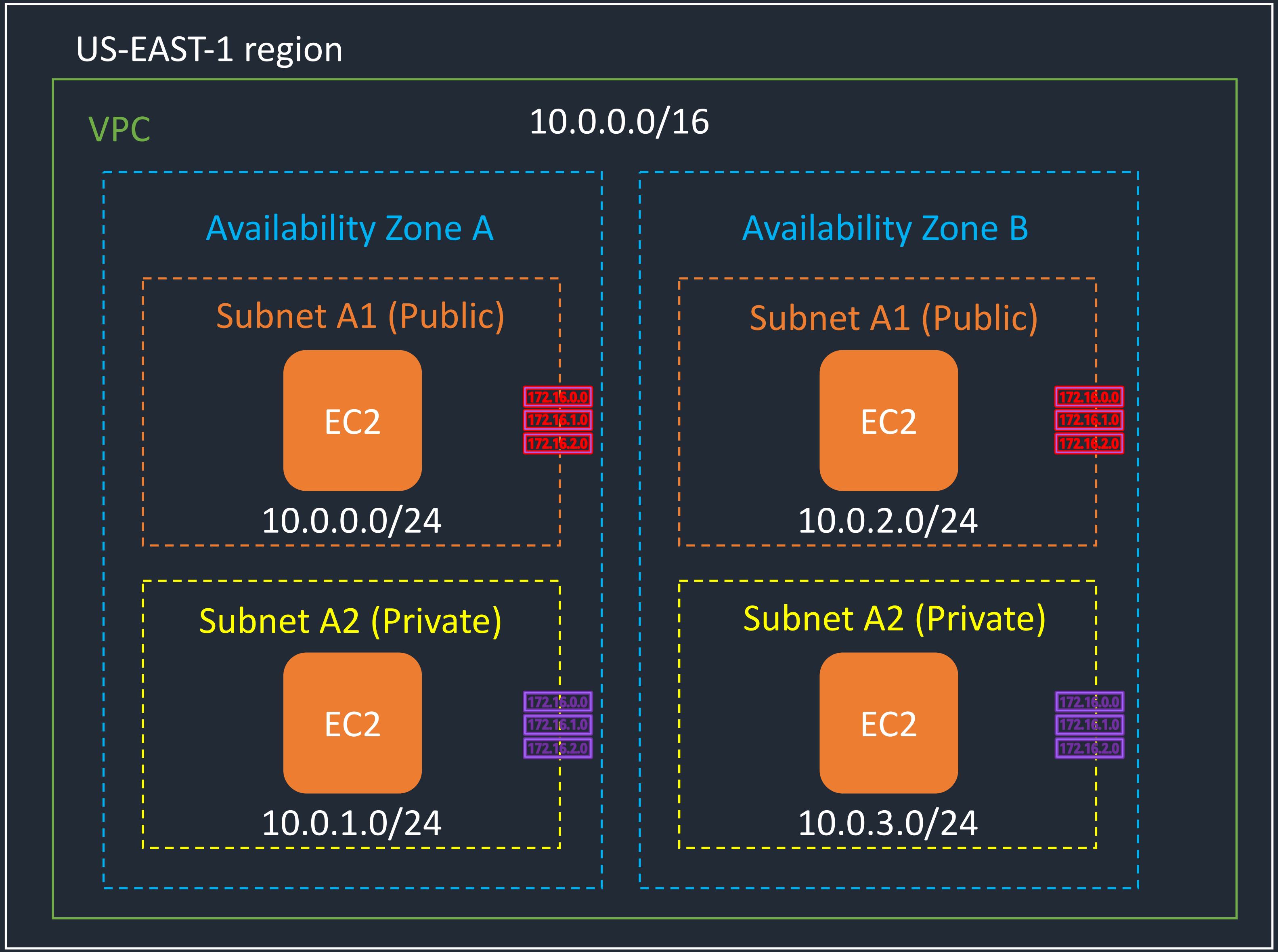
VPC - Subnets

- VPC spans all AZ in a region
- After creating VPC, add one or more subnets in each AZ
- Subnets cannot span AZ
- Subnet are allocated as subset of primary VPC CIDR range
- Default & Implicit route between subnets within VPC
- Subnets can be private or public



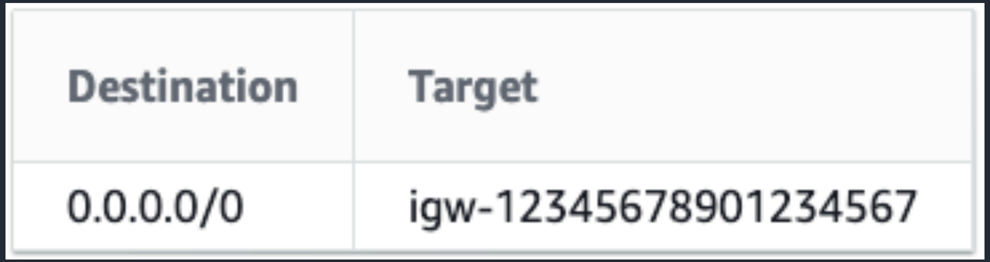
VPC – Routing

- Subnet has 1 Routing Table
- 1 Routing Table can be attached to multiple subnets
- Contains a set of rules, called routes defining where network traffic from subnet or gateway is directed
- Each route in a table specifies a destination (IPs) and a target (AWS)
- Targets:
  - Internet / Nat Gateway
  - VPC Endpoints
  - VPC peering

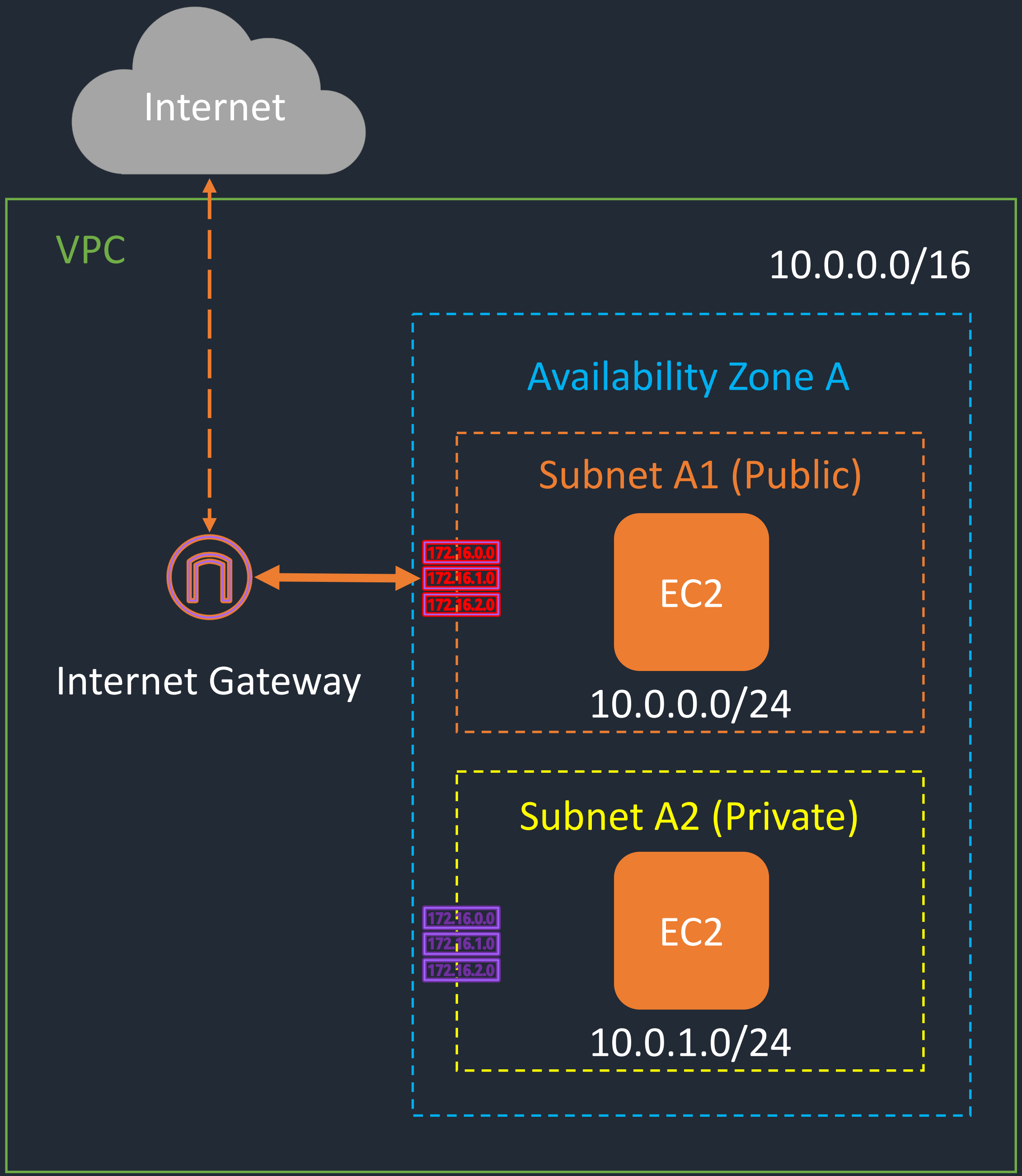


Internet Gateway

- Connect Subnets to internet
- Subnets are “Public Subnets” if there is a route to an Internet Gateway
- Managed Feature (HA, Scale, Reliability)
- Needs to add a route in the Route Table of Public Subnets

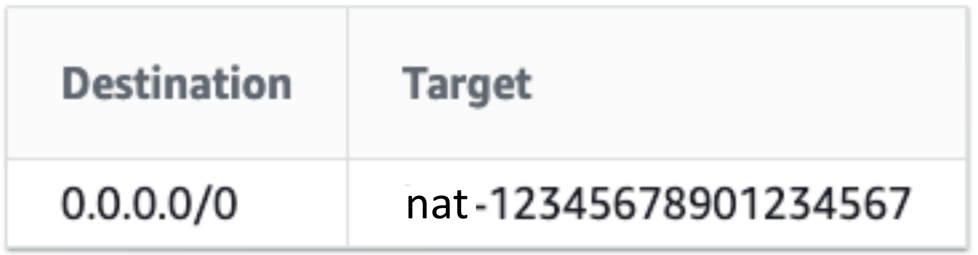


Destination	Target
0.0.0.0/0	igw-12345678901234567

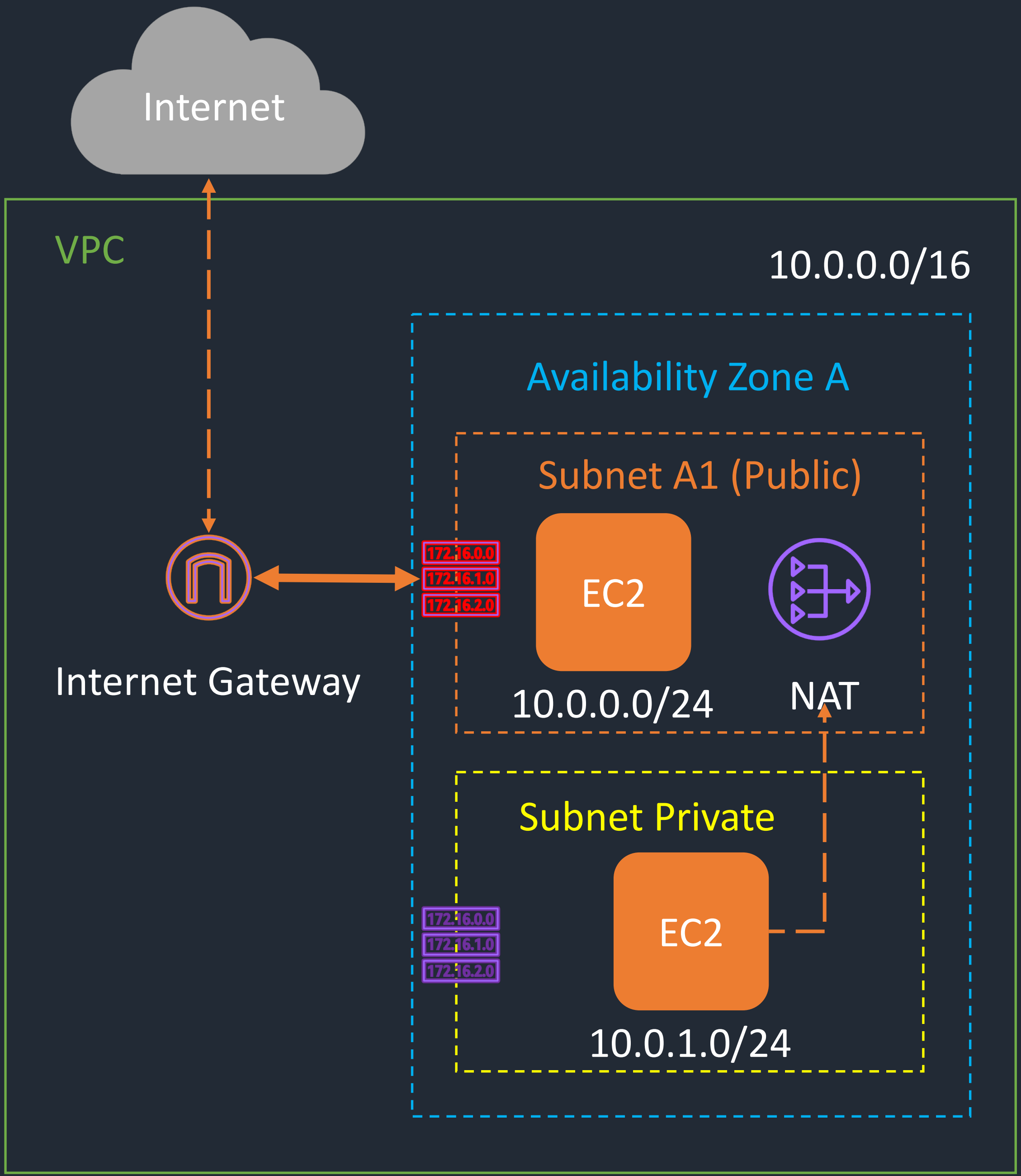


NAT Gateway

- Outbound connection to internet
- Managed Feature useful for Package updates
- Needs to add a route in the Route Table of Private Subnets



Destination	Target
0.0.0.0/0	nat-12345678901234567



Load Balancing

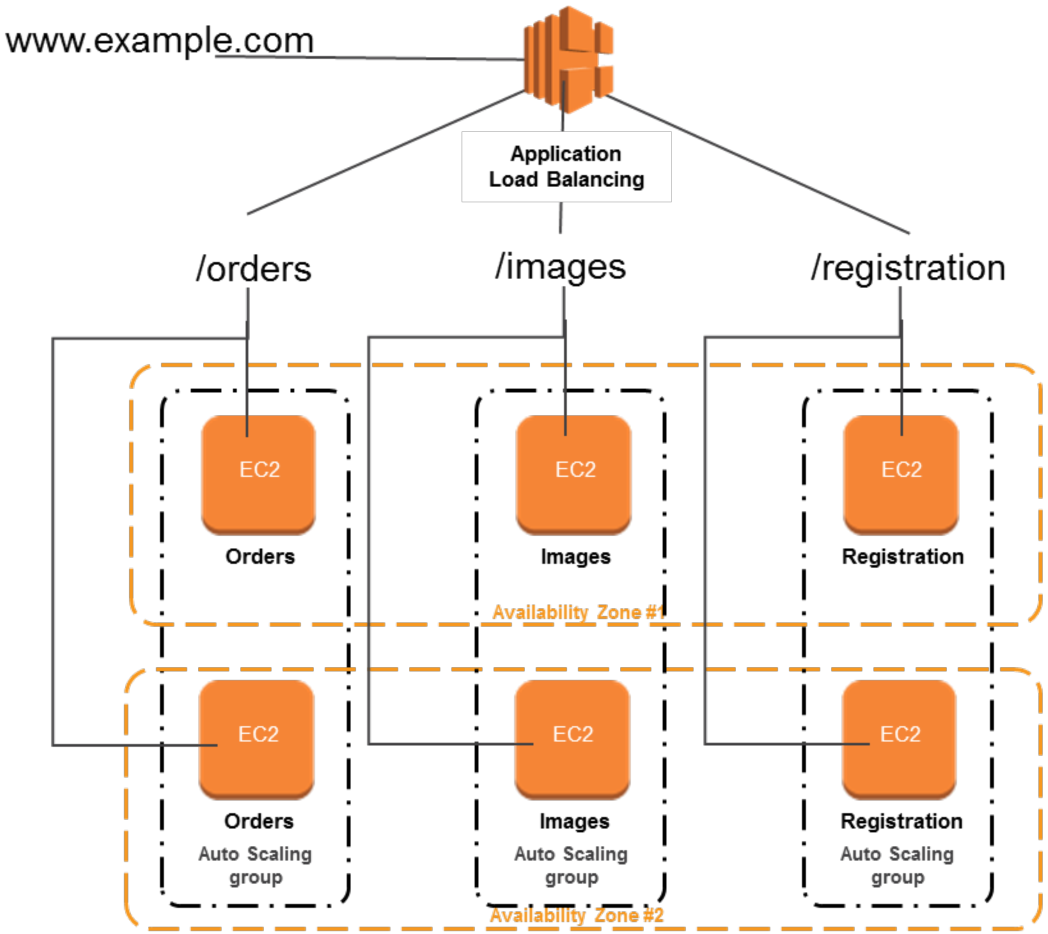
- Distribute Traffic to multiple targets

- Managed Feature (HA, Scale), spans multi AZ

- Autoscaling group as target: For Scale and Failover

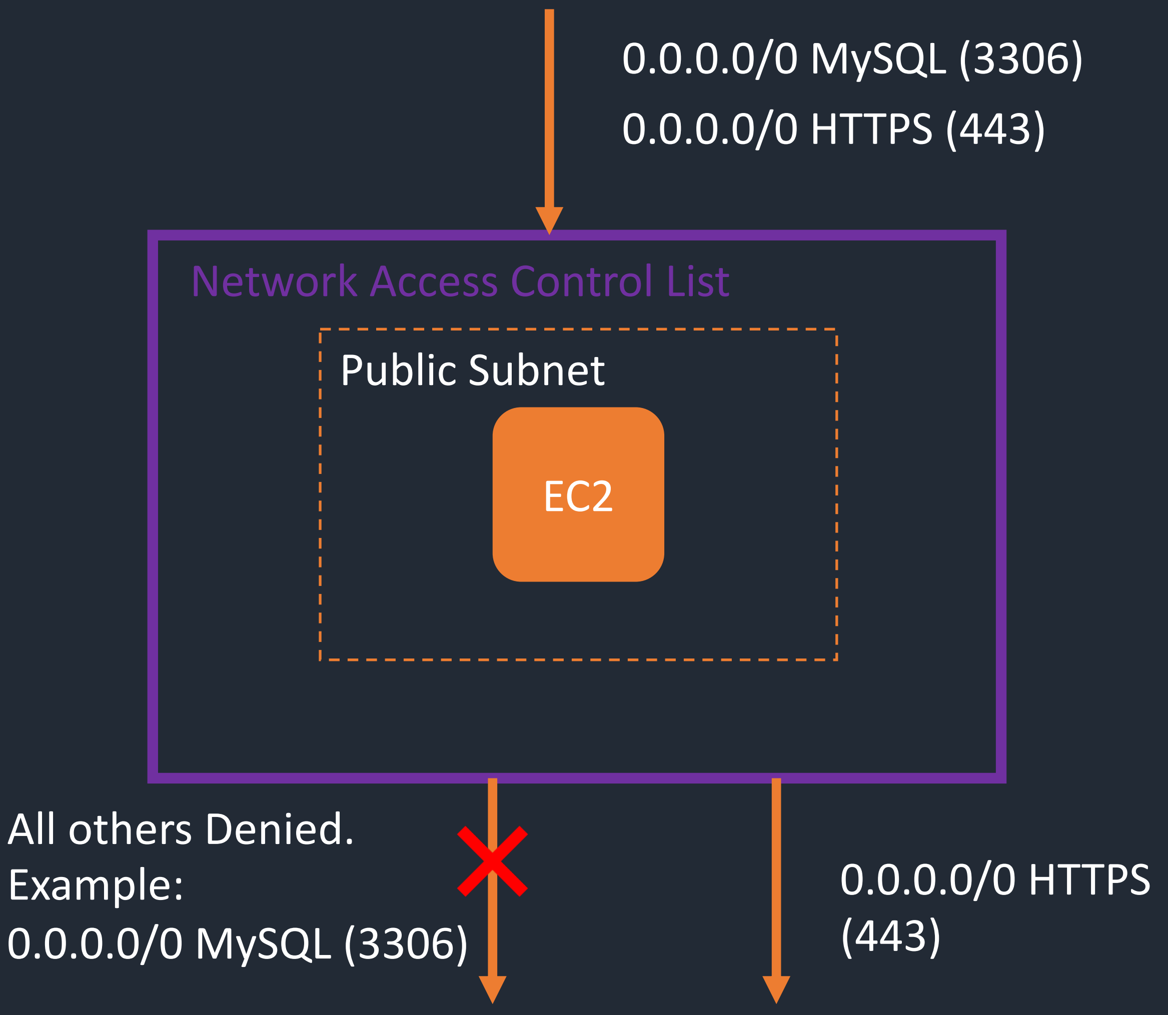
- Application (Layer 7) or Network (Layer 4) Load Balancer types

- <u>Alternative</u>: Elastic IPs (remapping of IP) for redundancy



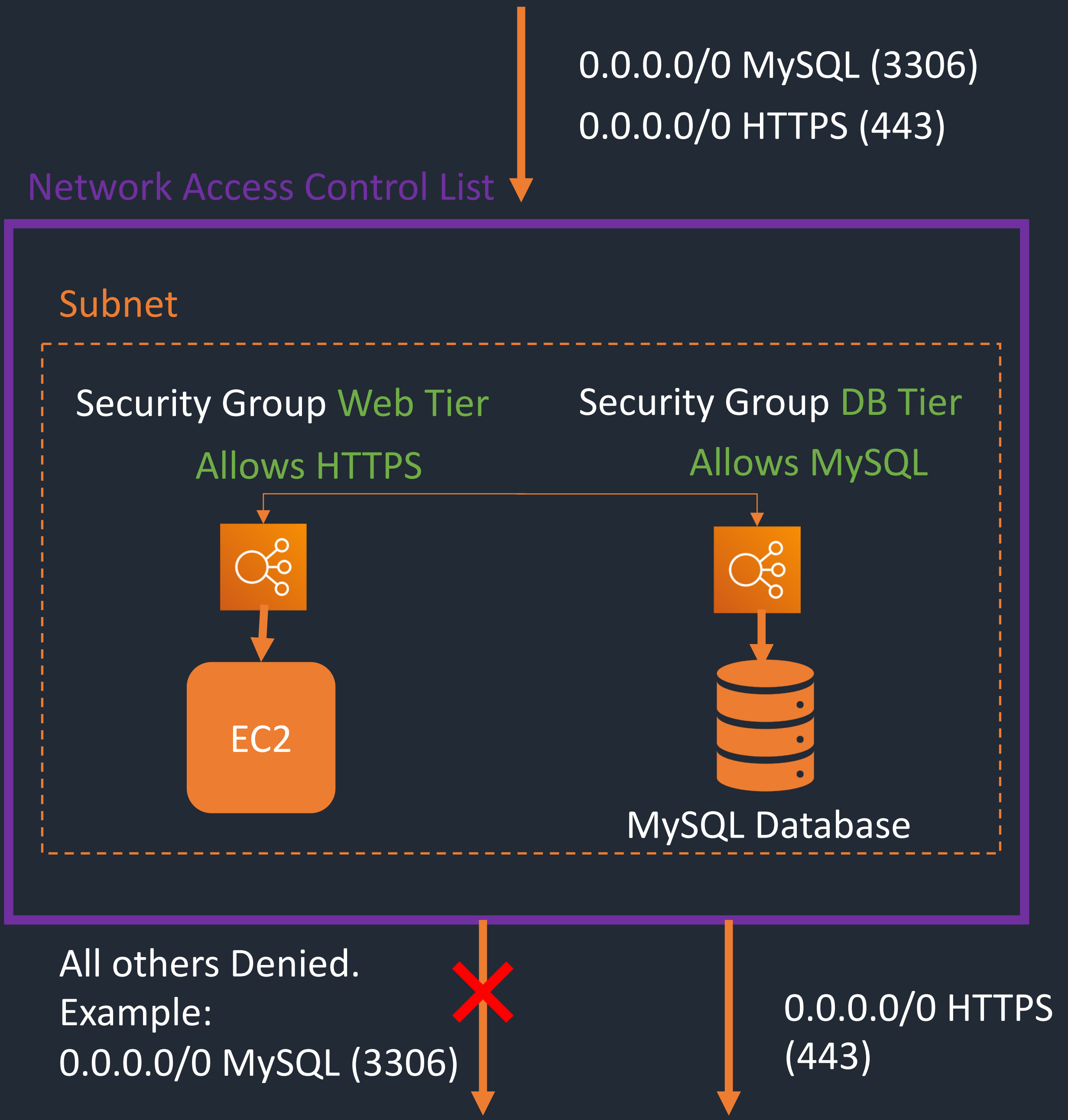
VPC Security – NACL

- Network Access Control List
- Optional layer of Security for Subnet level
- Be default allow all traffic but can configure Inbound and Outbound
- Stateless, Allow and Deny rules



VPC – Security Groups

- Virtual Firewall at the instance level
- Stateful: No Inbound / Outbound configuration
- Mandatory Security
- Only allow rules (No Deny)



VPC – Connectivity

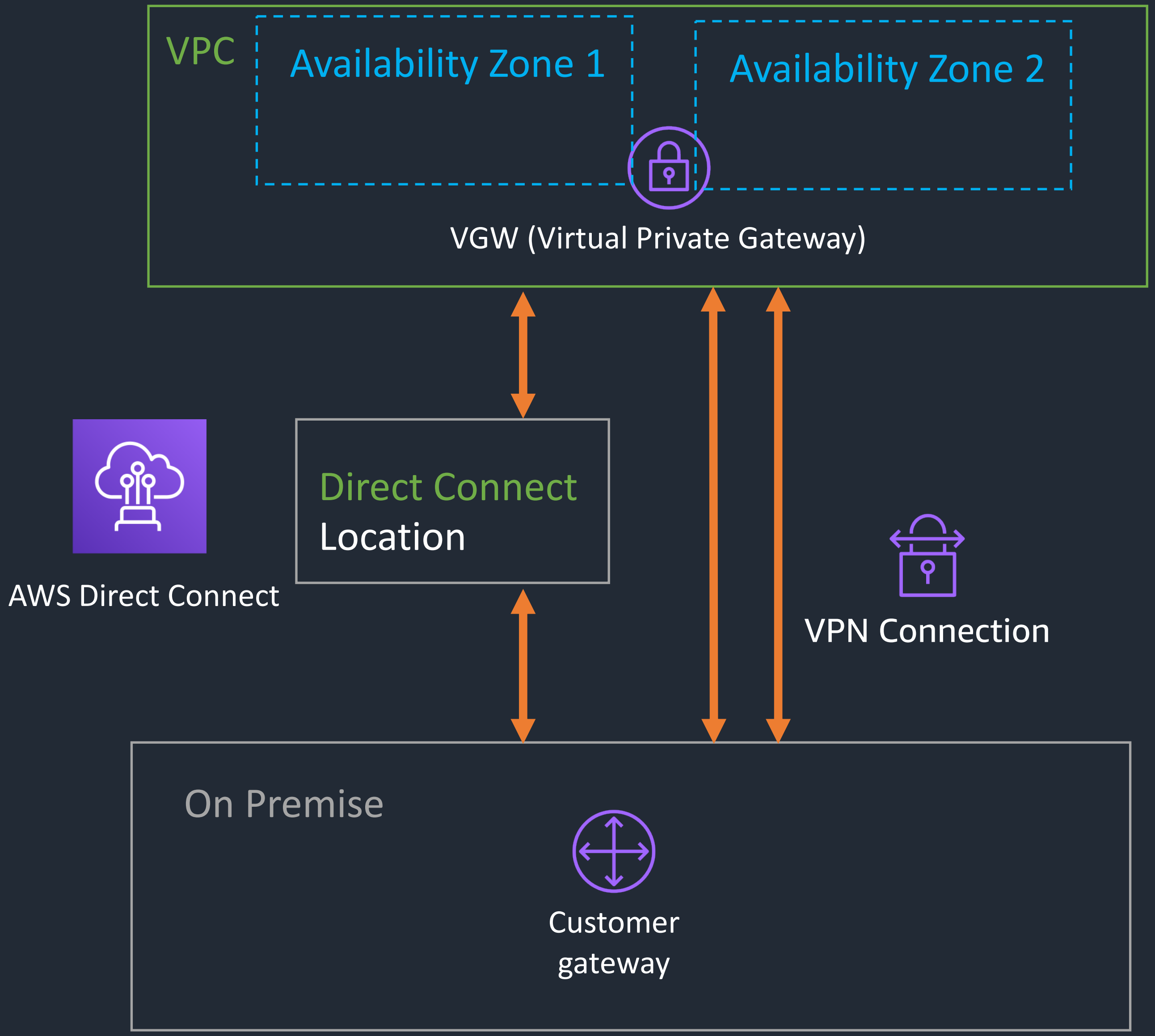
VPC
Endpoint

VPC Peering

AWS Transit
Gateway

VPC – External Connectivity

- VPN: Redundant IPSec connections (AES 256-bit encryption)
- VPN: Managed tunnels terminating in multiple az
- DX: Dedicated Connection (1 or 10 Gbps)
- DX: Consistent with dedicated bandwidth and Low latency
- DX: 97 Direct Connection Locations worldwide
- Dynamic BGP possible



DNS - Route53

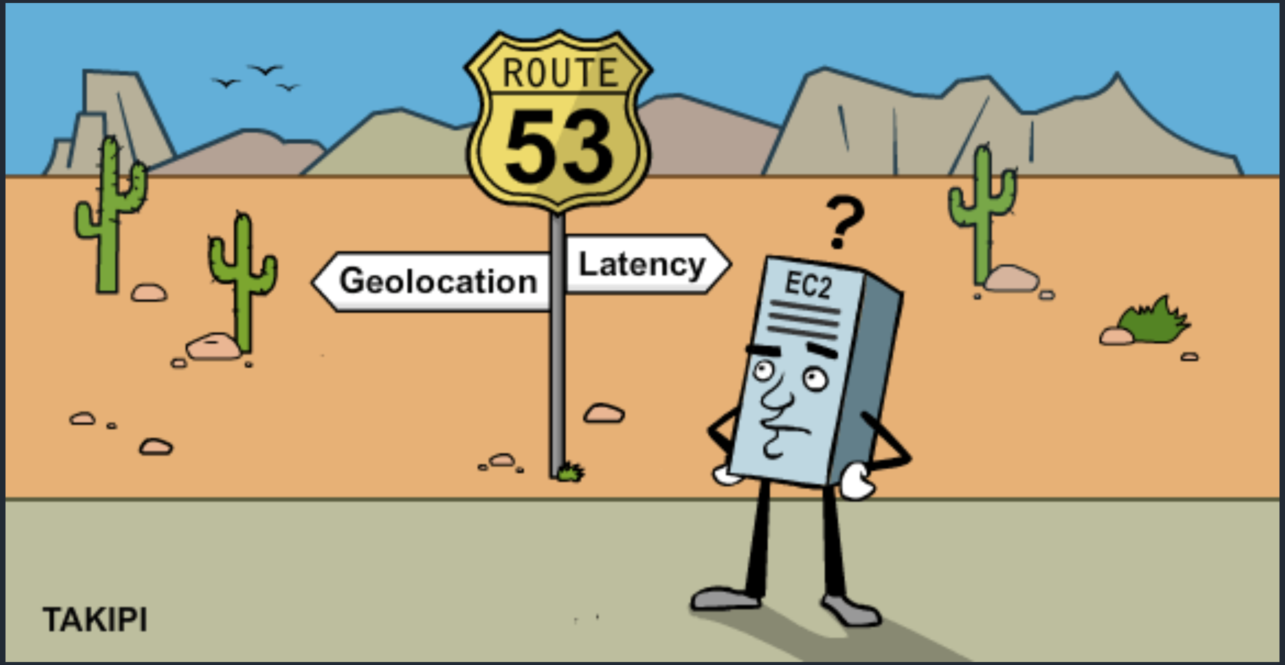
- Worldwide DNS service

- Domain Registration

- Domain Name resolution

- Send traffic to AWS IPs/ressources

- Routing Policies:
  - Health Checks
  - Failover
  - Latency
  - Geolocation
  - Weighted Round Robin



Thank you !

Find me on Linkedin:
Thomas LE MOULLEC