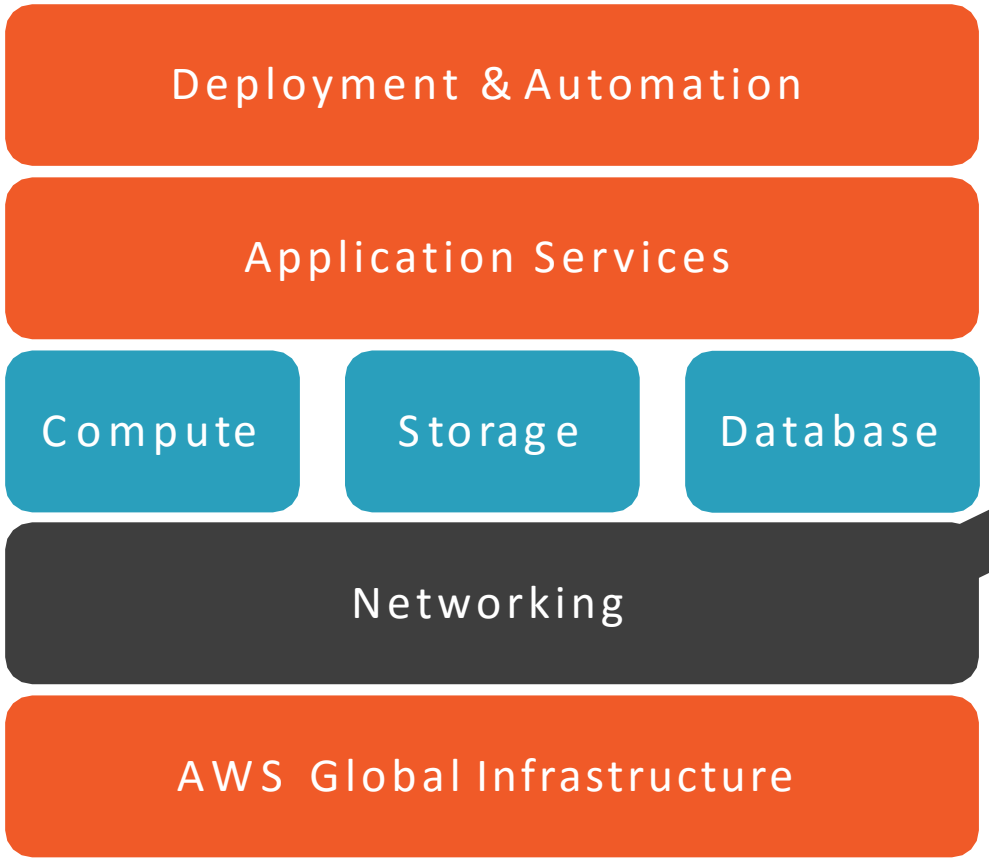
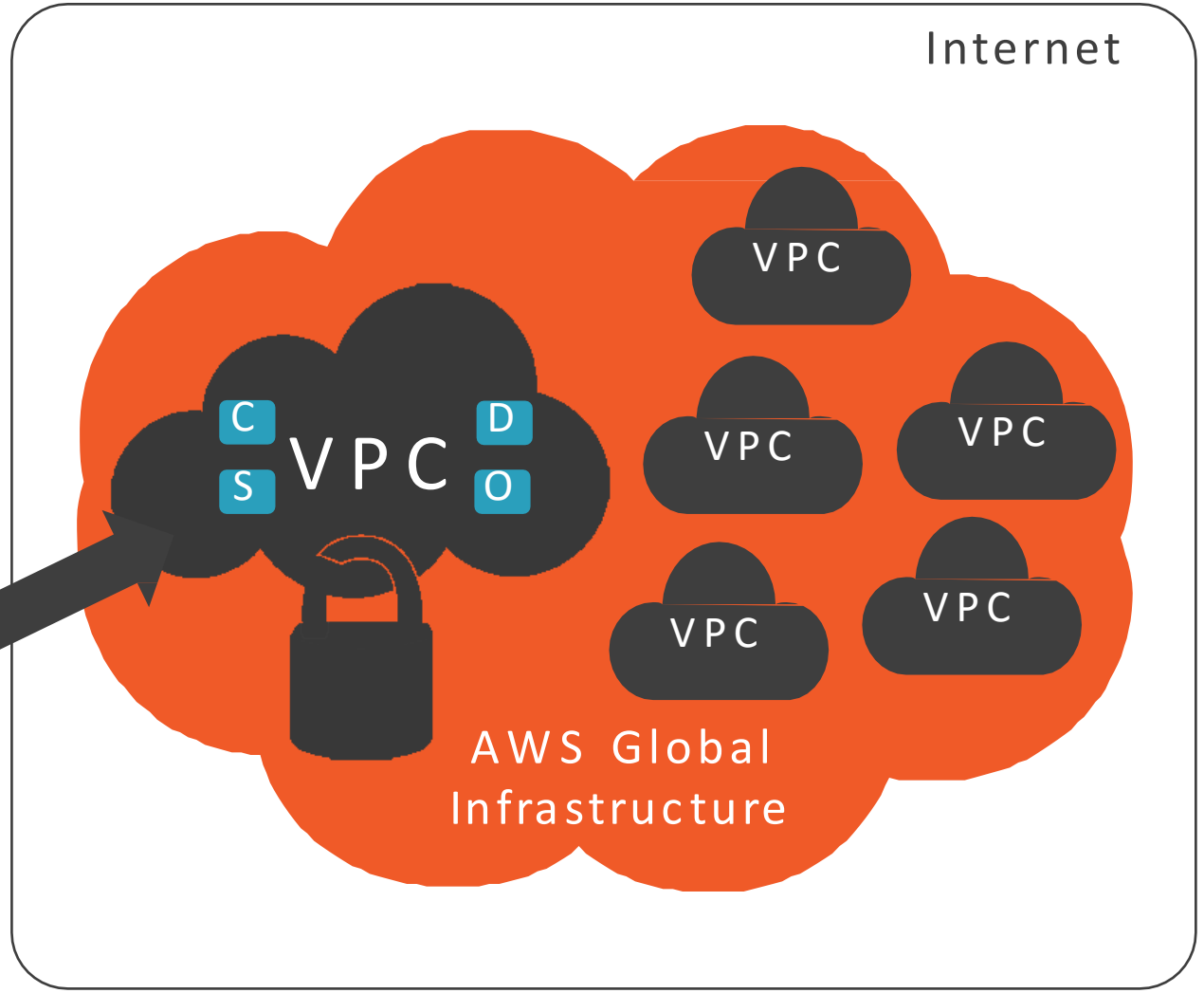
Understanding and Configuring Amazon Virtual Private Cloud (VPC)

Virtual Private Cloud Overview

- Logically isolated network in the AWS cloud
- Control of network architecture
- Enhanced security
- Internetwork with other organizations
- Elastic IP Address
- Enable hybrid cloud (site-to-site VPN)
- Single tenant dedicated server hardware
- VPC cost = $0 / VPN cost is $0.05/hr

AWS Reference Model





VPC Elements

Subnets

Route Tables

Internet Gateways

Elastic IPs

Endpoints

NAT Gateways

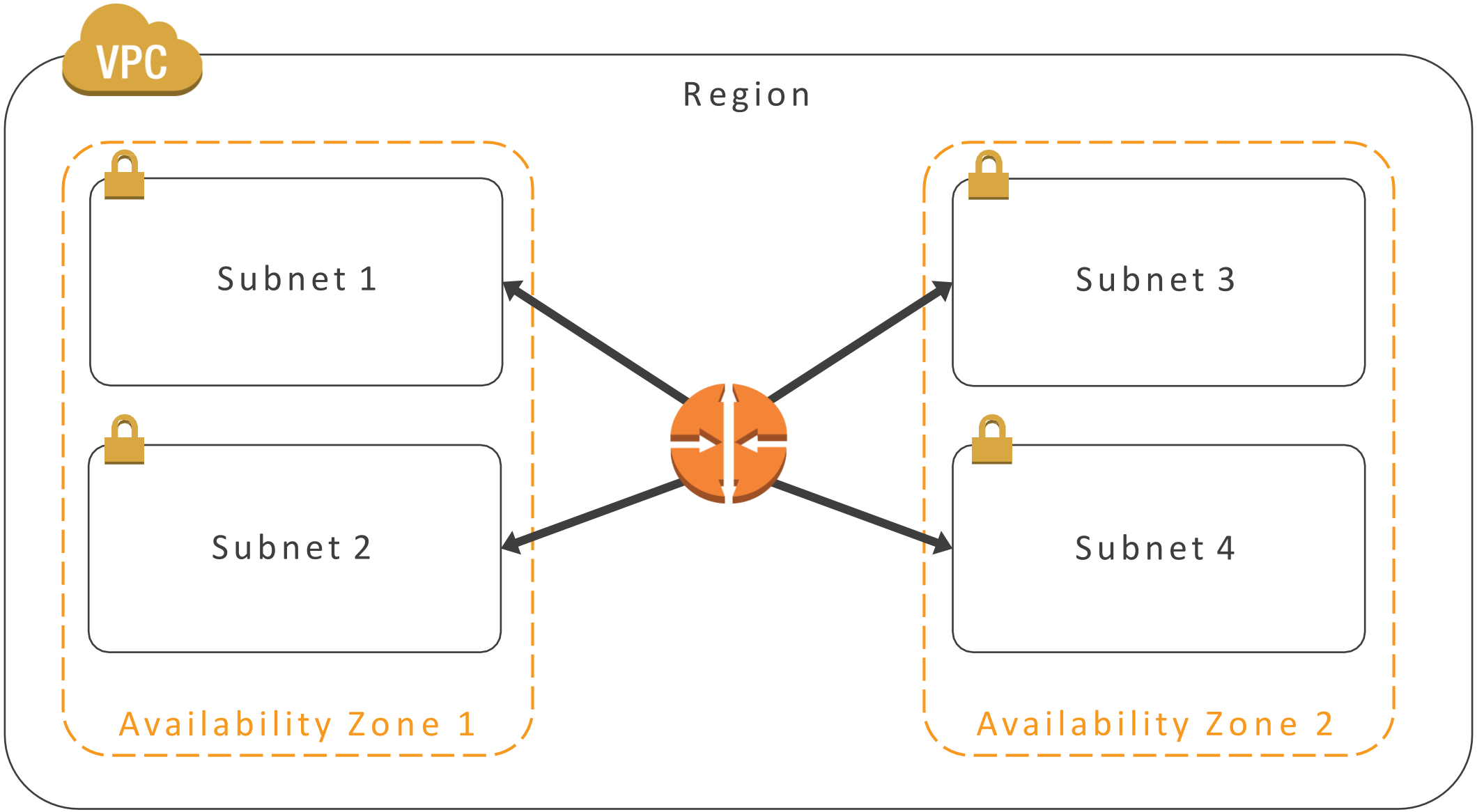
VPC Elements

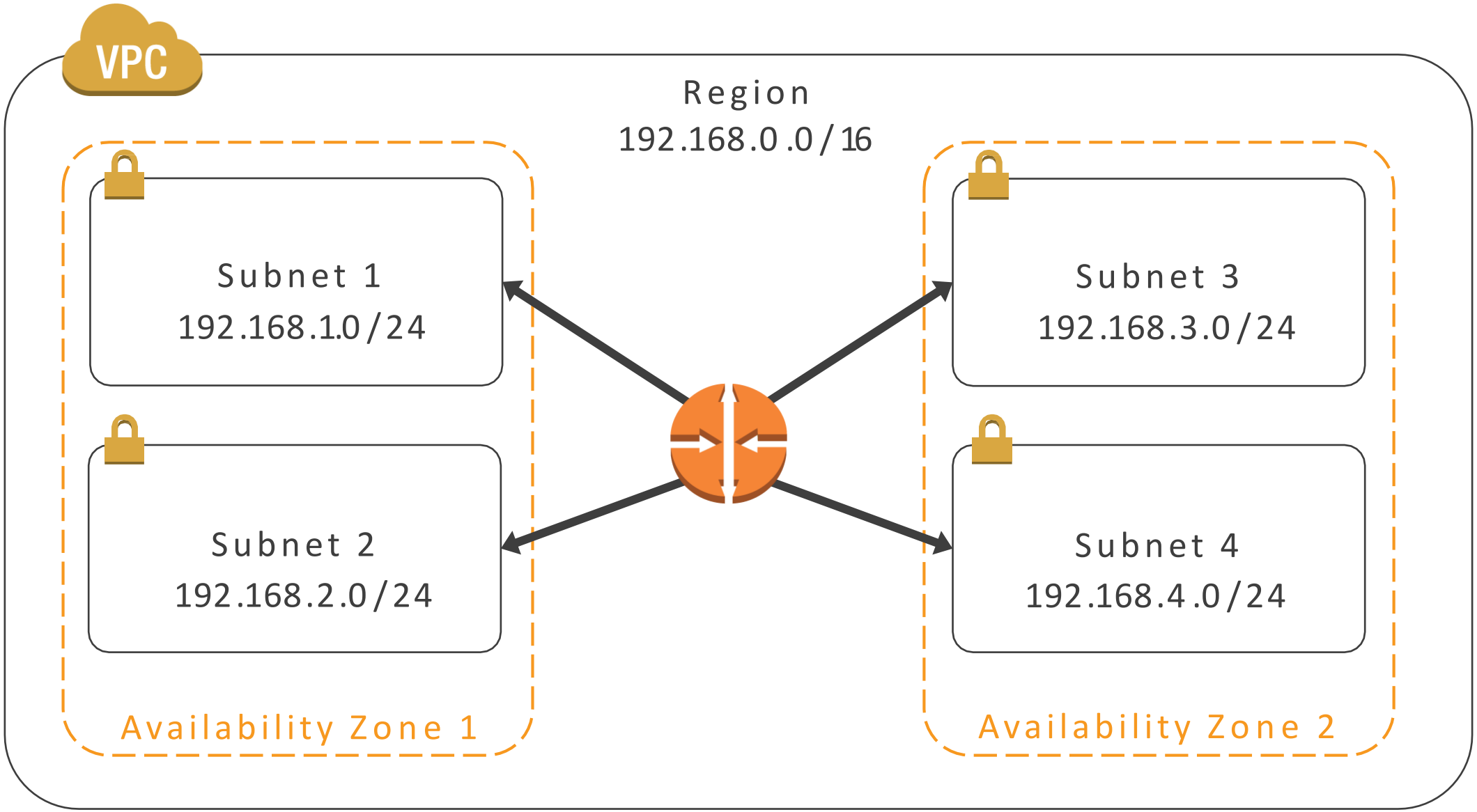
Peering Connections

Network ACLs

Security Groups

VPN


VPC
Region
Subnet 1
Subnet 2
Subnet 3
Subnet 4
Availability Zone 1
Availability Zone 2


VPC
Region
192.168.0.0/16
Subnet 1
192.168.1.0/24
Subnet 2
192.168.2.0/24
Subnet 3
192.168.3.0/24
Subnet 4
192.168.4.0/24
Availability Zone 1
Availability Zone 2

VPC Characteristics

AWS reserves 5 IP addresses per subnet (first 4 and last 1)

Private, public or VPN subnets

Subnets do not span AZs

Single Region, multi-AZ

CIDR 16 – 28

Select IP prefix

VPC Security

Security Groups

Resource level traffic firewall

- Instance, ELB, etc…

Ingress and egress

Stateful

- Return traffic allowed

Access Control Lists

Source and protocol filtering

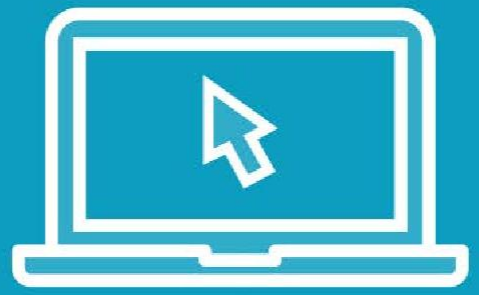
Subnet level traffic firewall

- Separate inbound and outbound rule set

Stateless

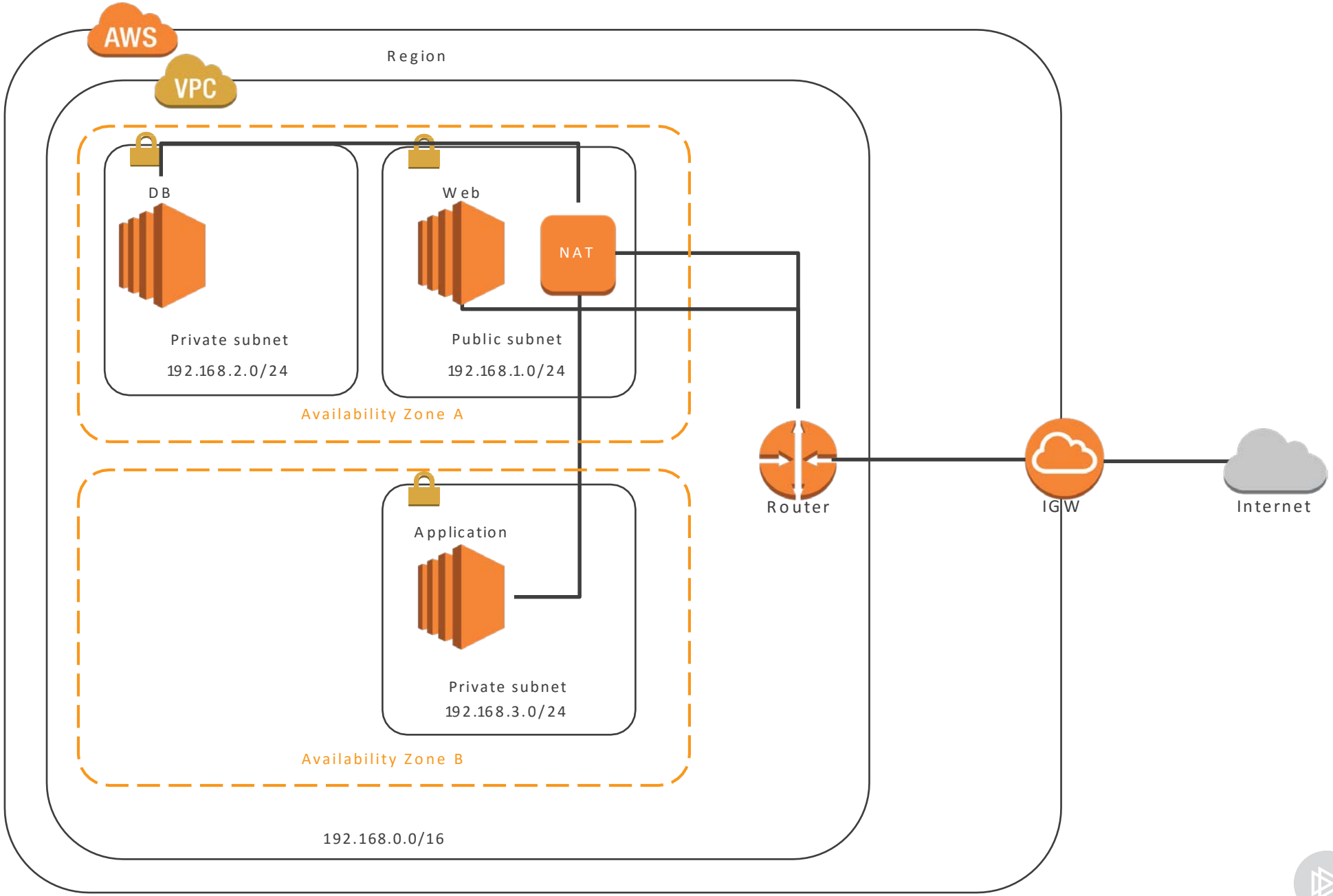
- Traffic strictly filtered

Demo



Configure Wired Brain Coffee (WBC) VPC

Wired Brain Coffee
VPC



Summary

VPC overview

VPC elements

VPC security