Understanding Virtual Networking on AWS

Elias Khnaser

@ekhnaser | www.eliaskhnaser.com

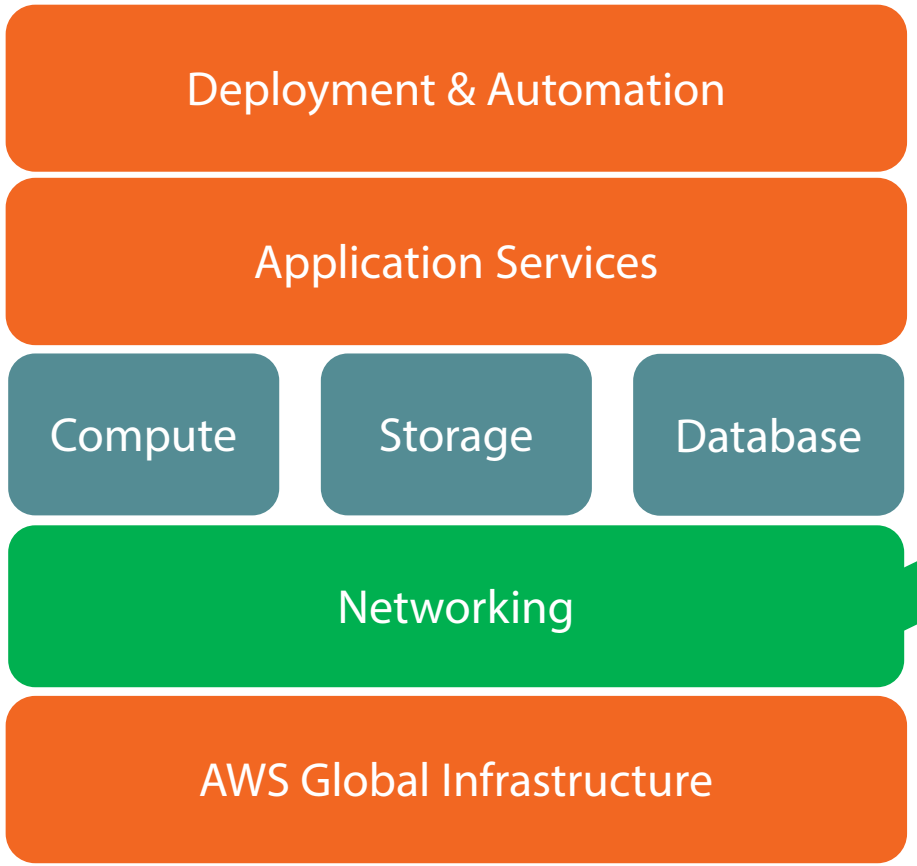
pluralsight

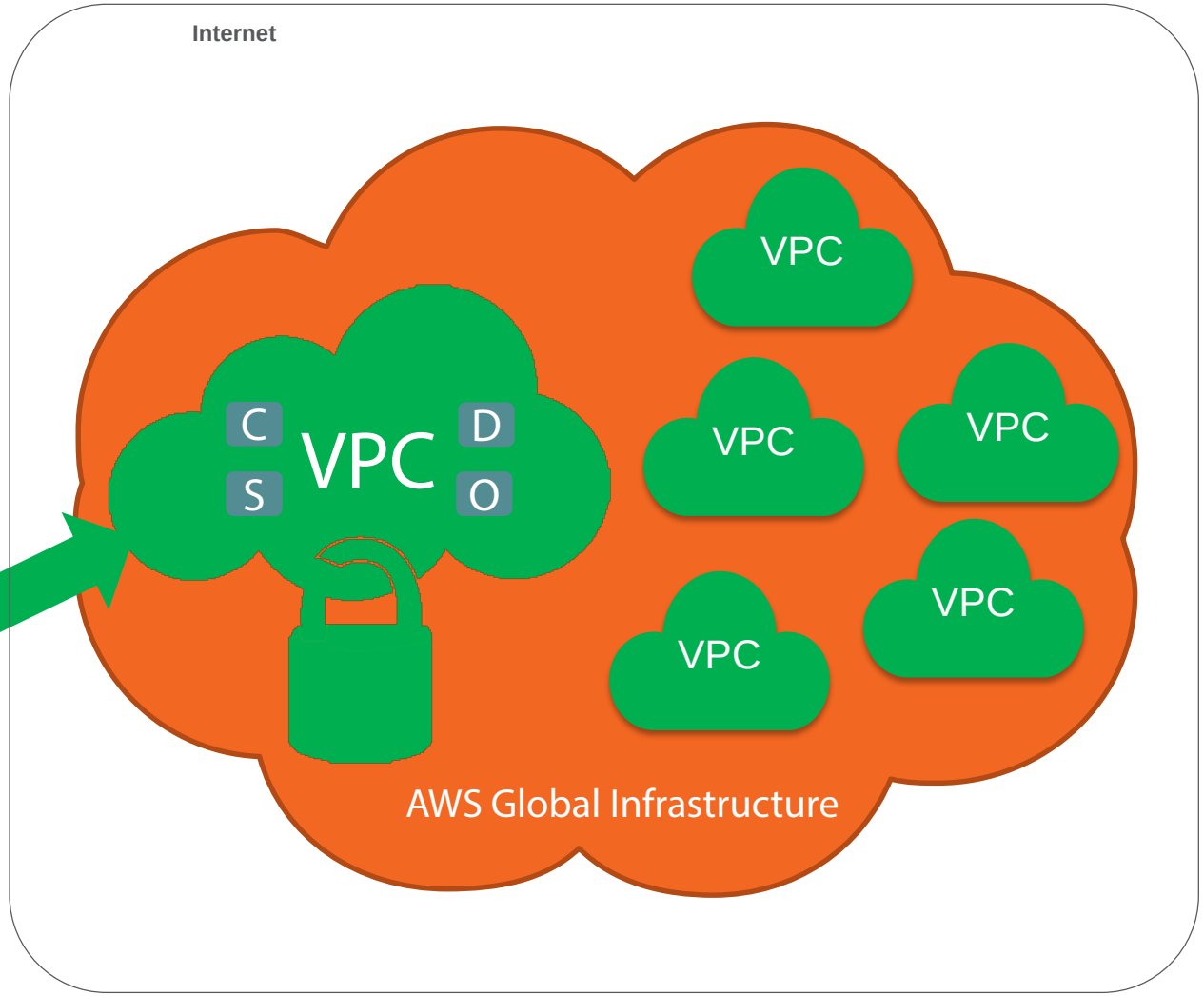
What Is Virtual Private Cloud (VPC)?

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

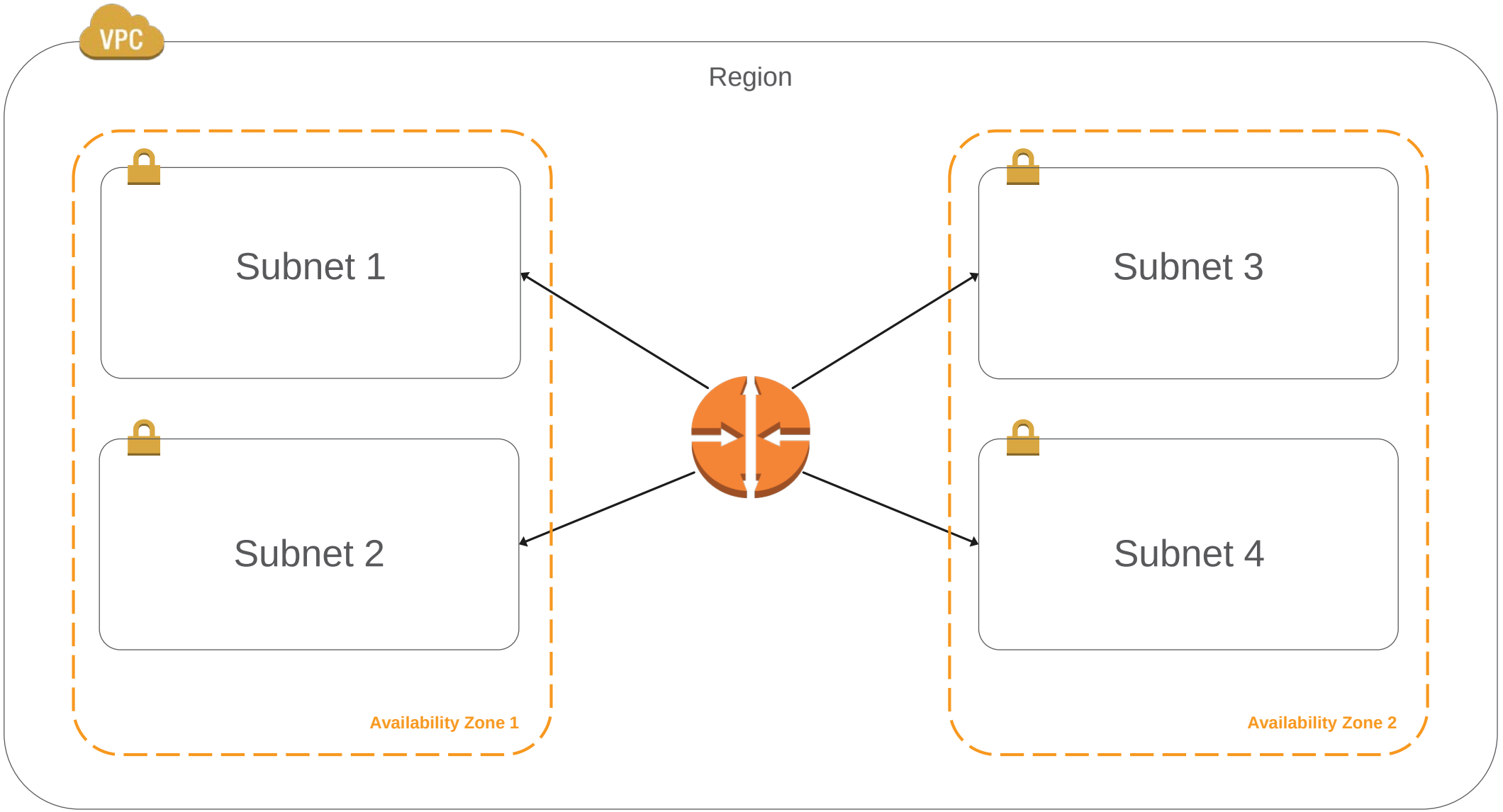
pluralsight

AWS Reference Model

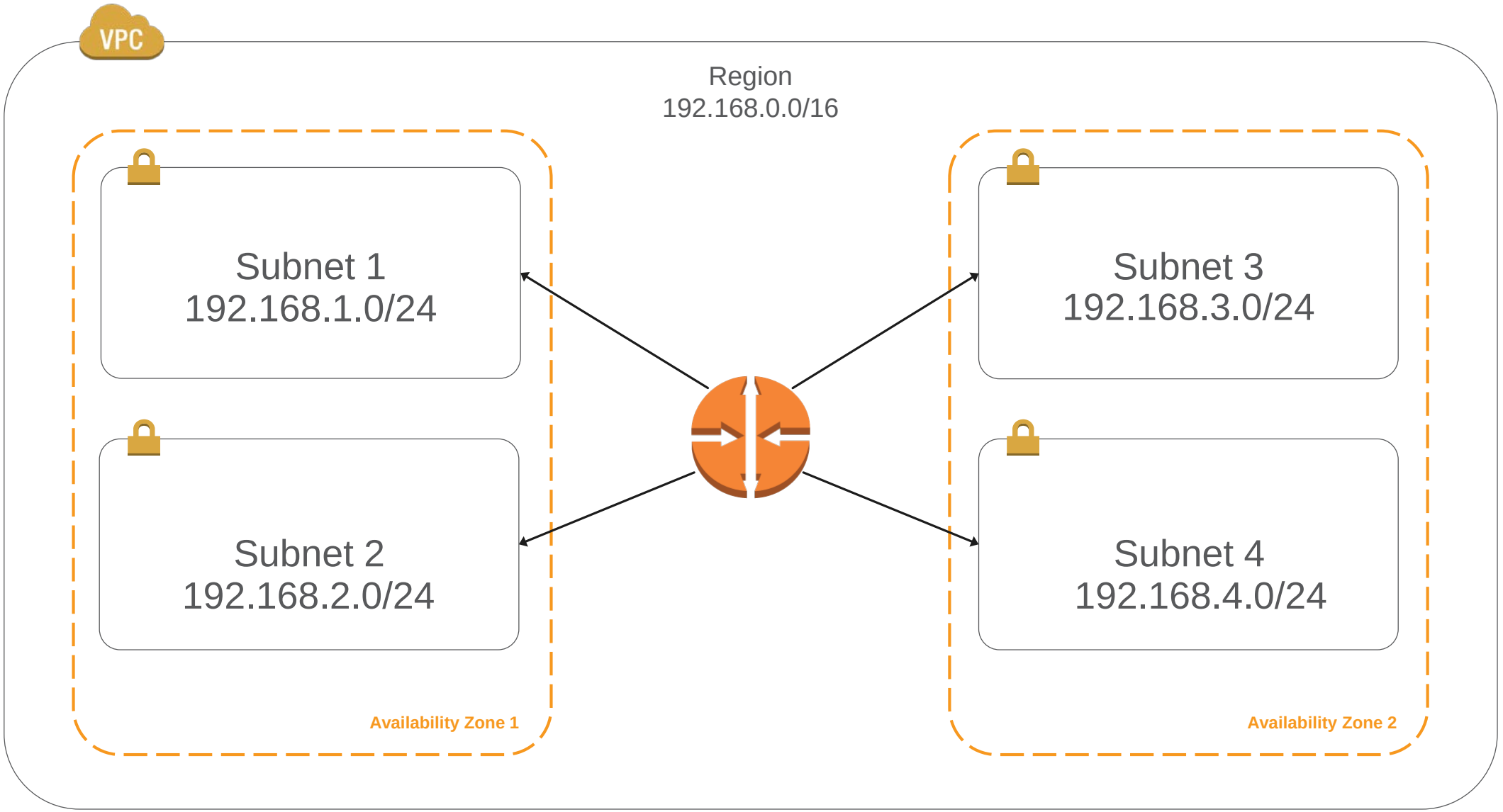




pluralsight



pluralsight



pluralsight

IP Address Blocks

- AWS reserves 5 addresses per subnet
- Single Region, multi-AZ
- CIDR 16 – 28
- Select IP prefix

pluralsight

VPC Access

Gateway

- Internet Gateway (IGW)
  - Ingress and egress
- Virtual Private Gateway (VPG)
  - AWS side of secure VPN
- Customer Gateway (CG)
  - Customer side of secure VPN

VPN

- Direct Connect
  - Dedicated and isolated
  - No internet
  - HA connectivity supported
- Hardware-based VPN
  - On-premises to AWS over internet
  - HA connectivity supported
  - 3rd party brands supported

pluralsight

VPC Security

Security Groups

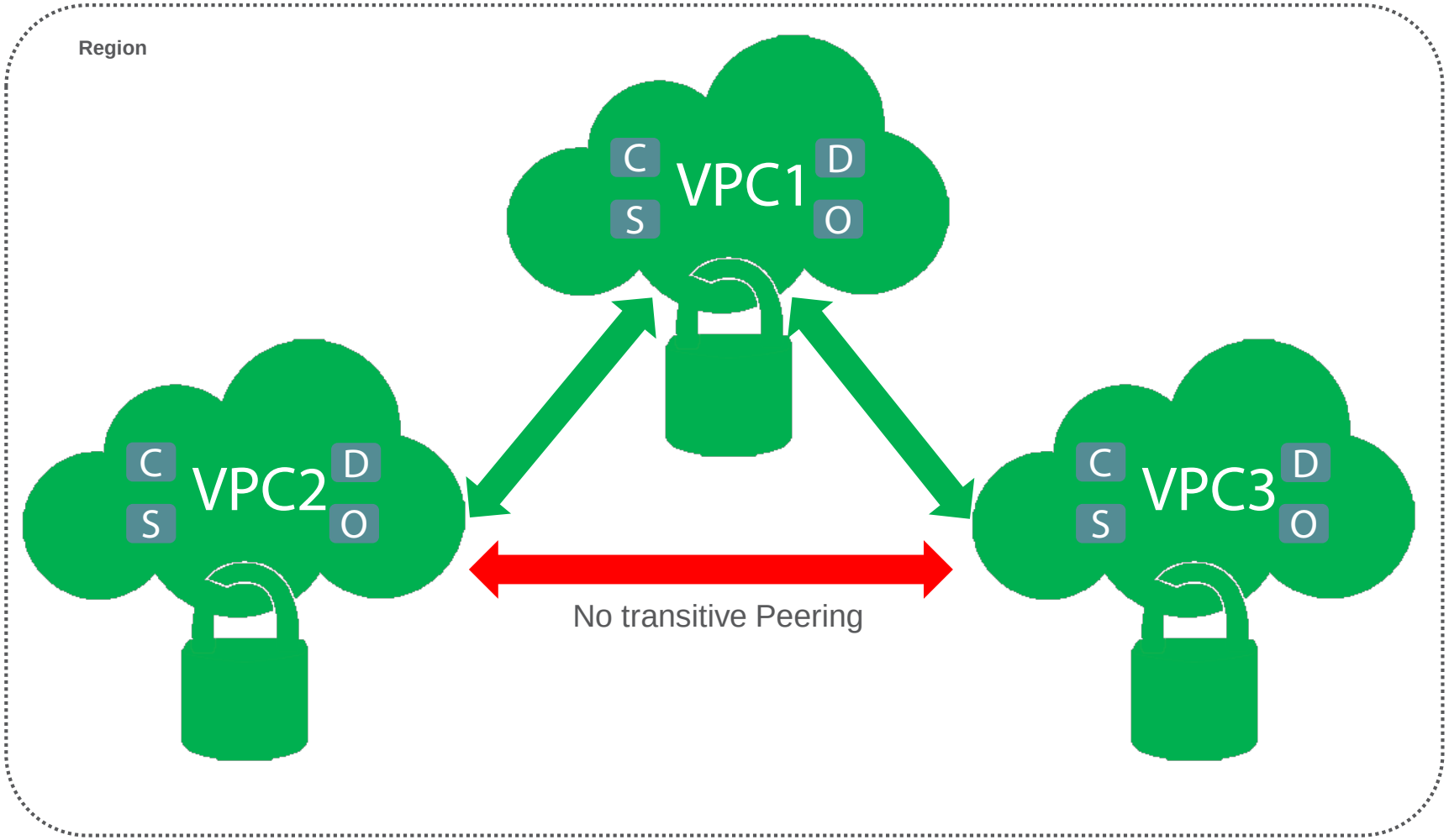
- Resource level traffic firewall
  - Instance, ELB, etc…
- Ingress and Egress
- Stateful
  - Return traffic allowed

Access Control Lists

- Source and Protocol filtering
- Subnet level traffic firewall
  - Separate inbound and outbound rule set
- Stateless
  - Traffic strictly filtered

pluralsight

VPC Peering



- Inter-VPC routing
- Same or different AWS account
- No overlapping network addresses

Wizard-driven VPC Setup

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

VPC with Private Subnet only and Hardware VPN Access

pluralsight

Summary

- What Is VPC?
- VPC Access
- VPC Security
- VPC Peering
- VPC Setup

pluralsight