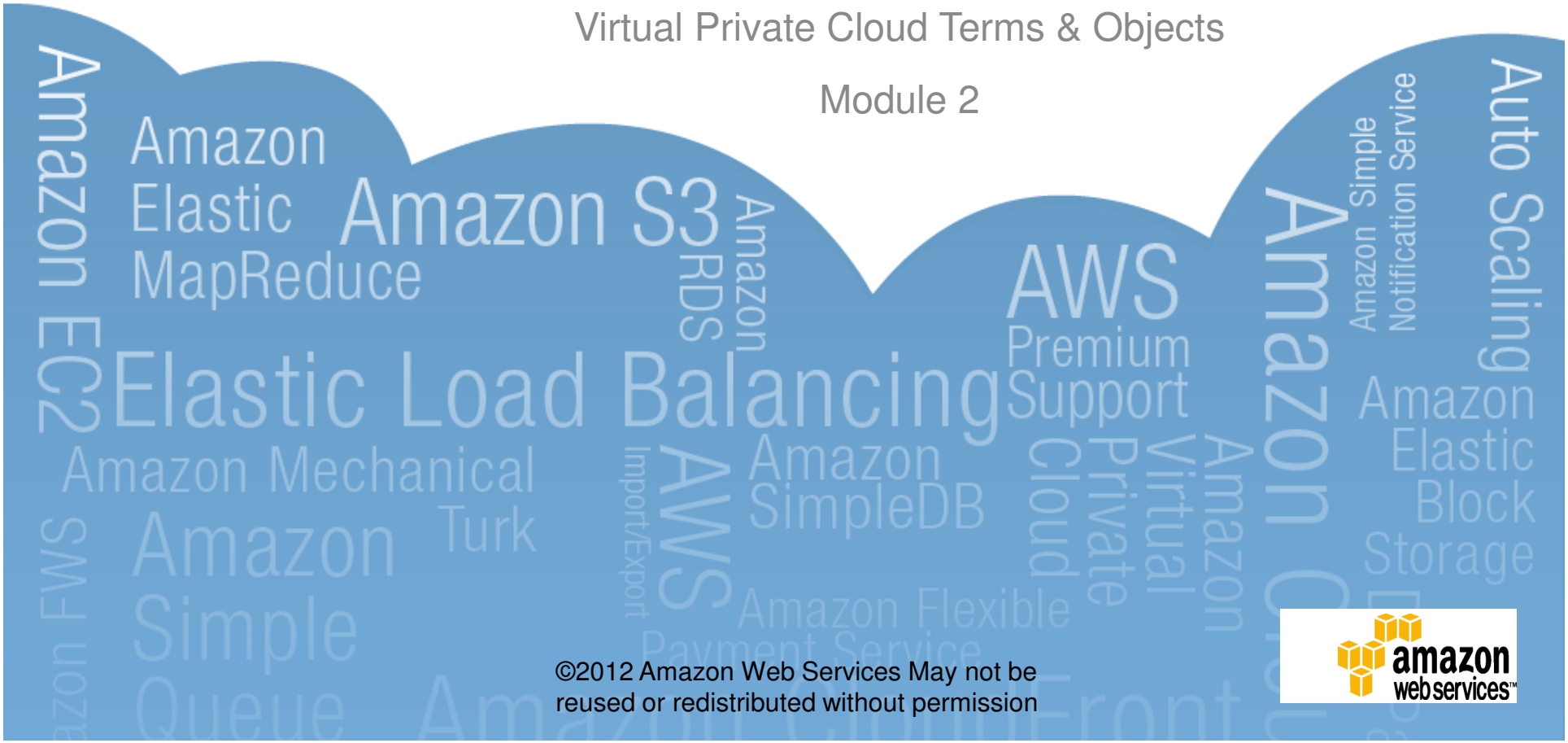


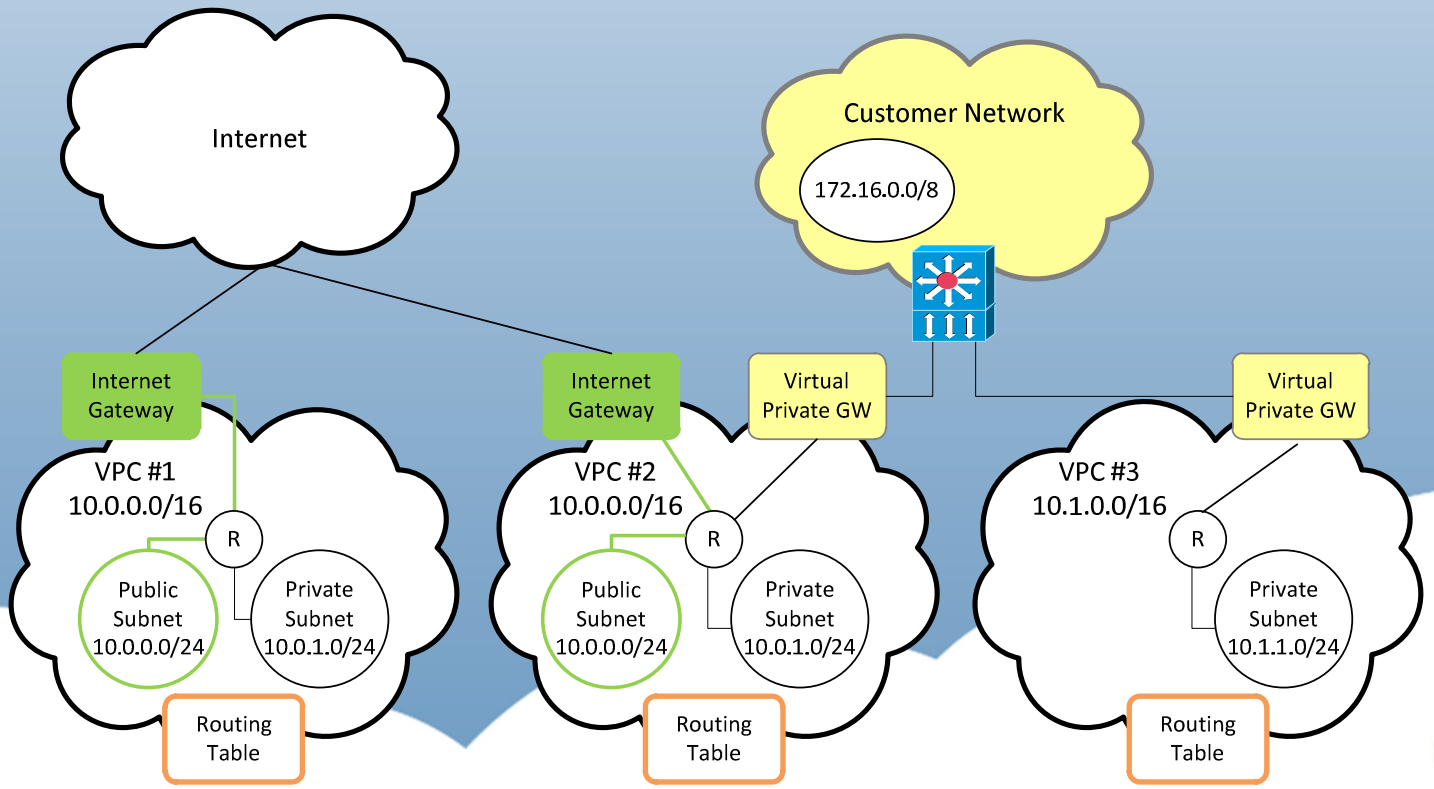
AWS Architecture Training - VPC

Virtual Private Cloud Terms & Objects

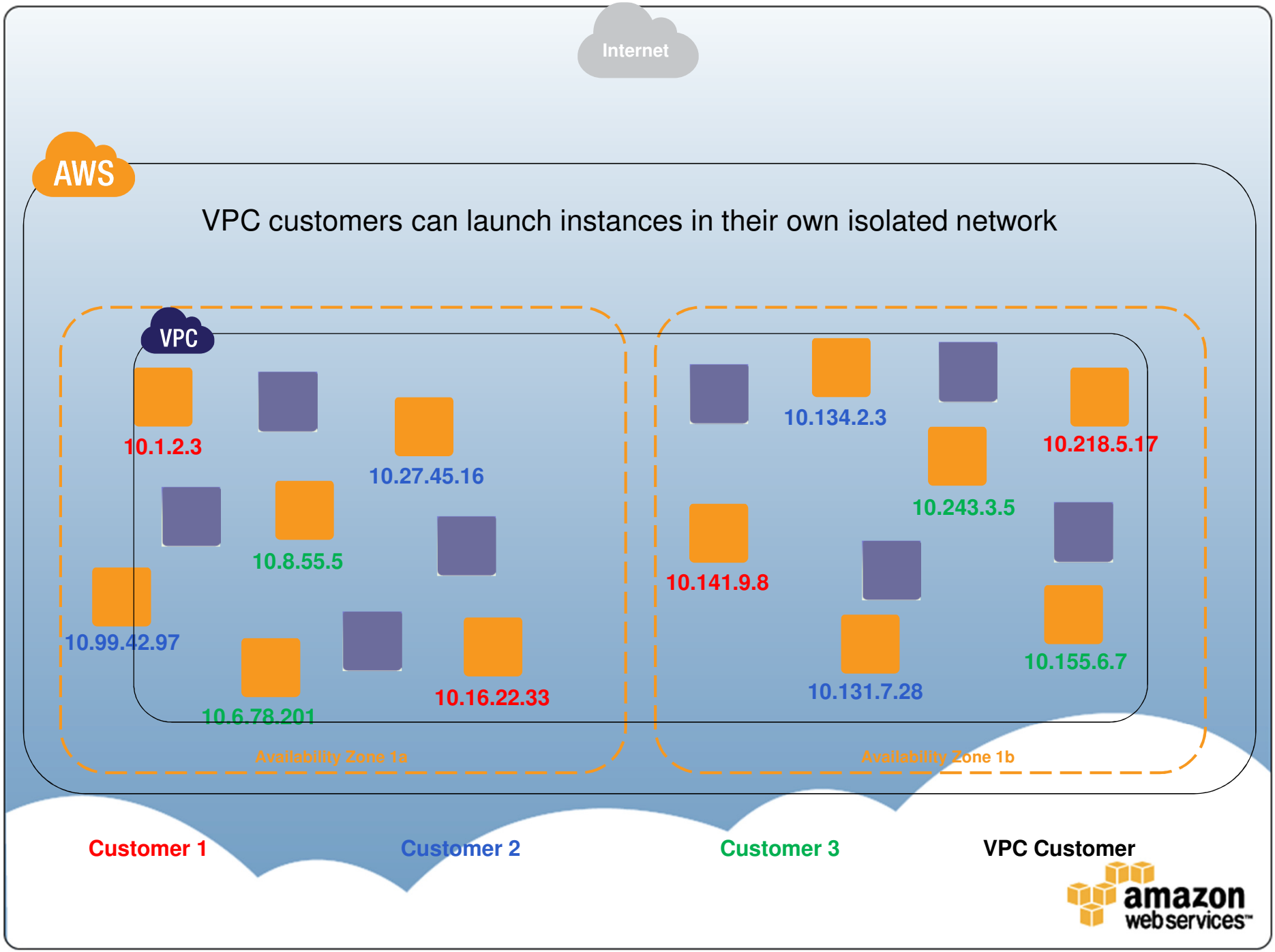
Module 2

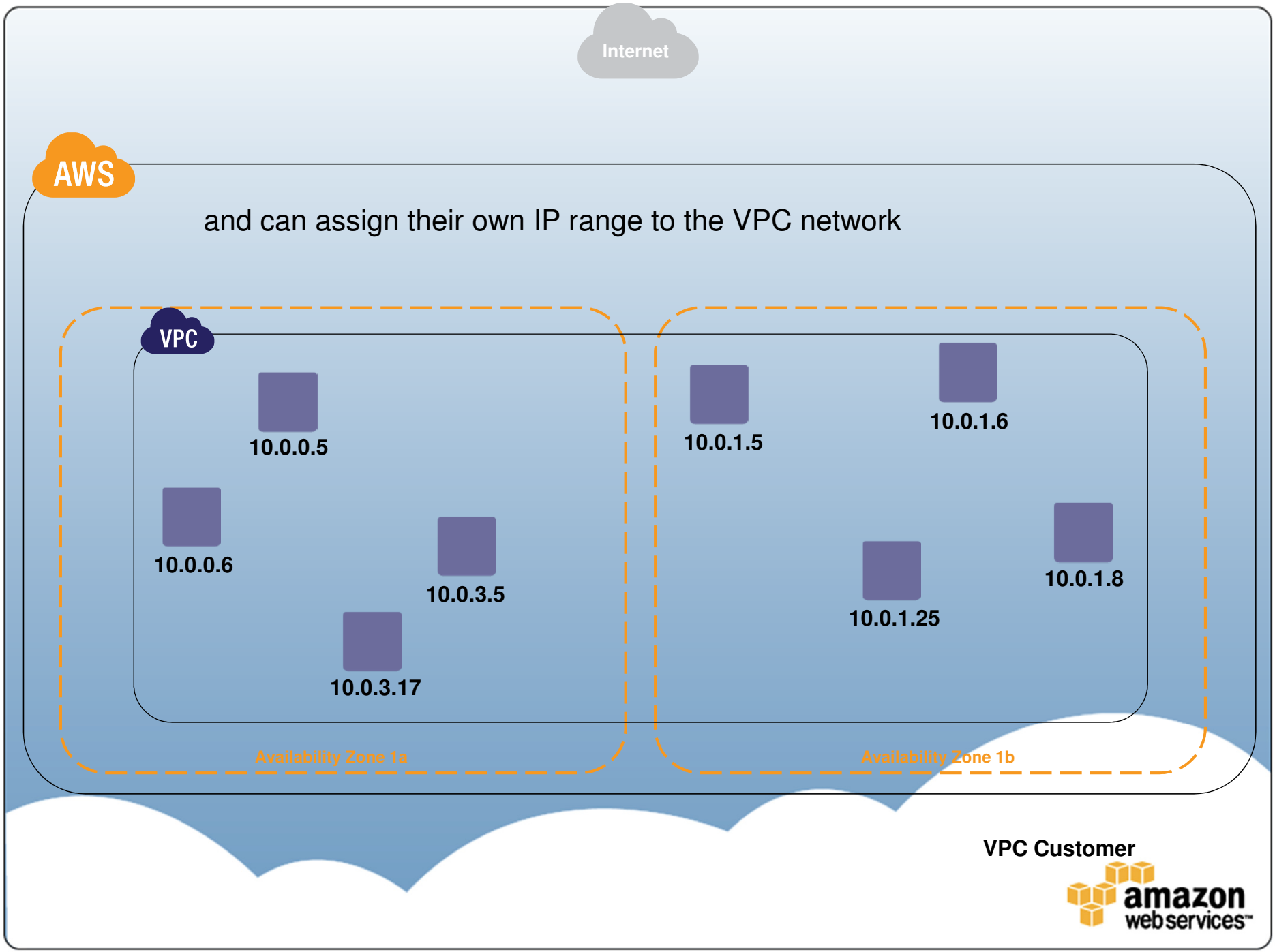
Amazon Virtual Private Cloud (VPC)

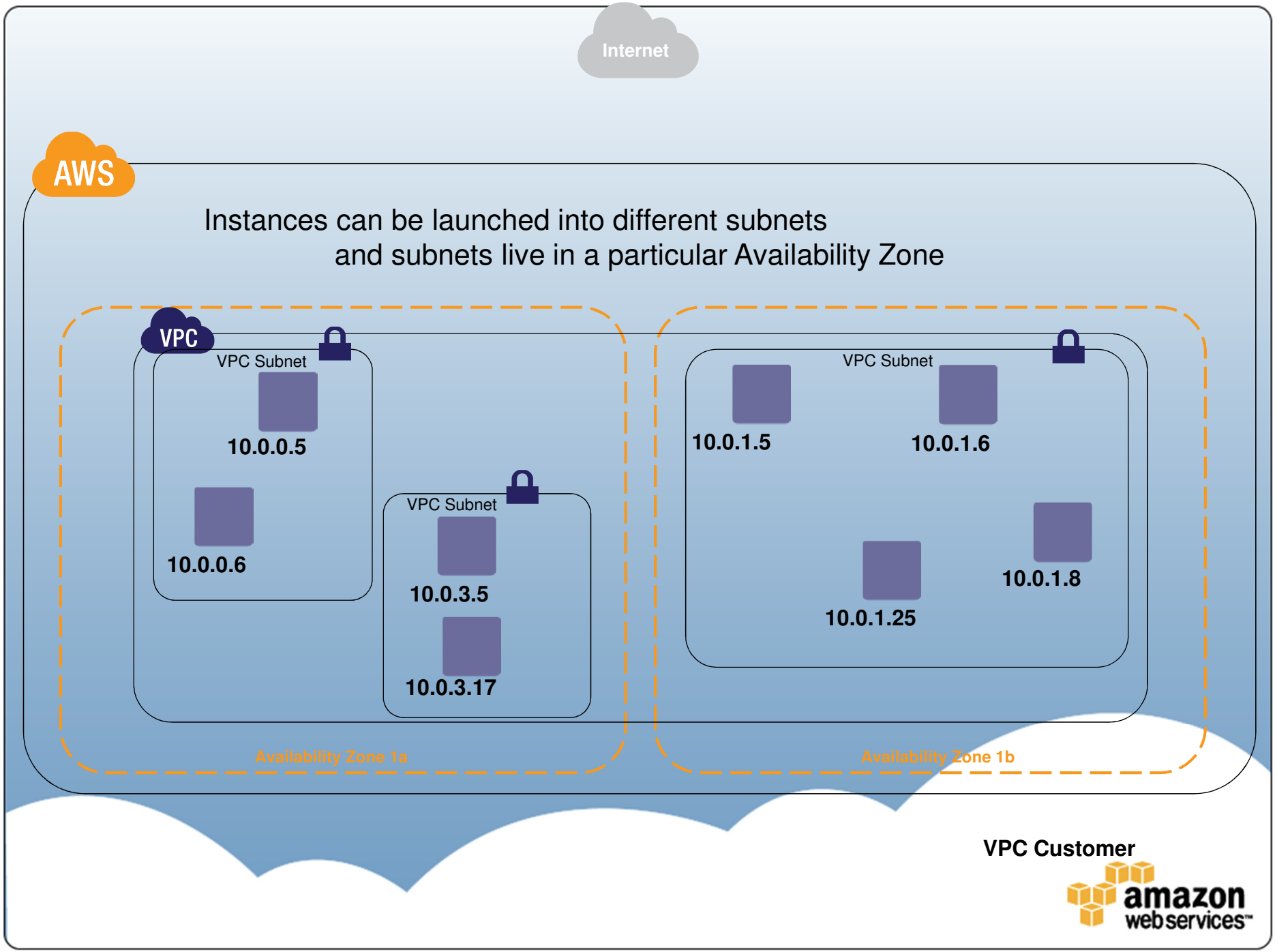
- L**ogically isolated** environment
- Your **private IP** range
- Internet or Hardware VPN connectivity options

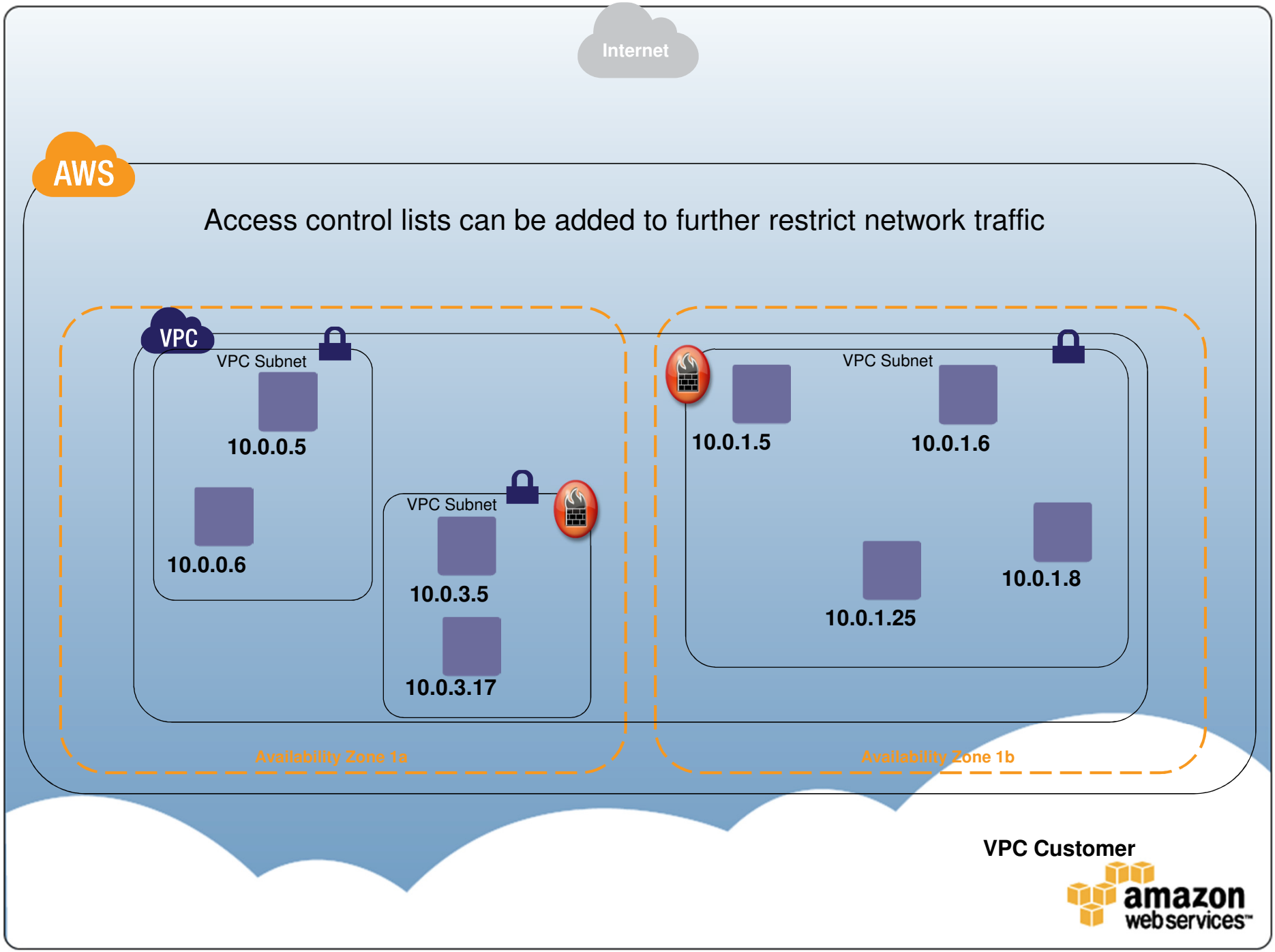


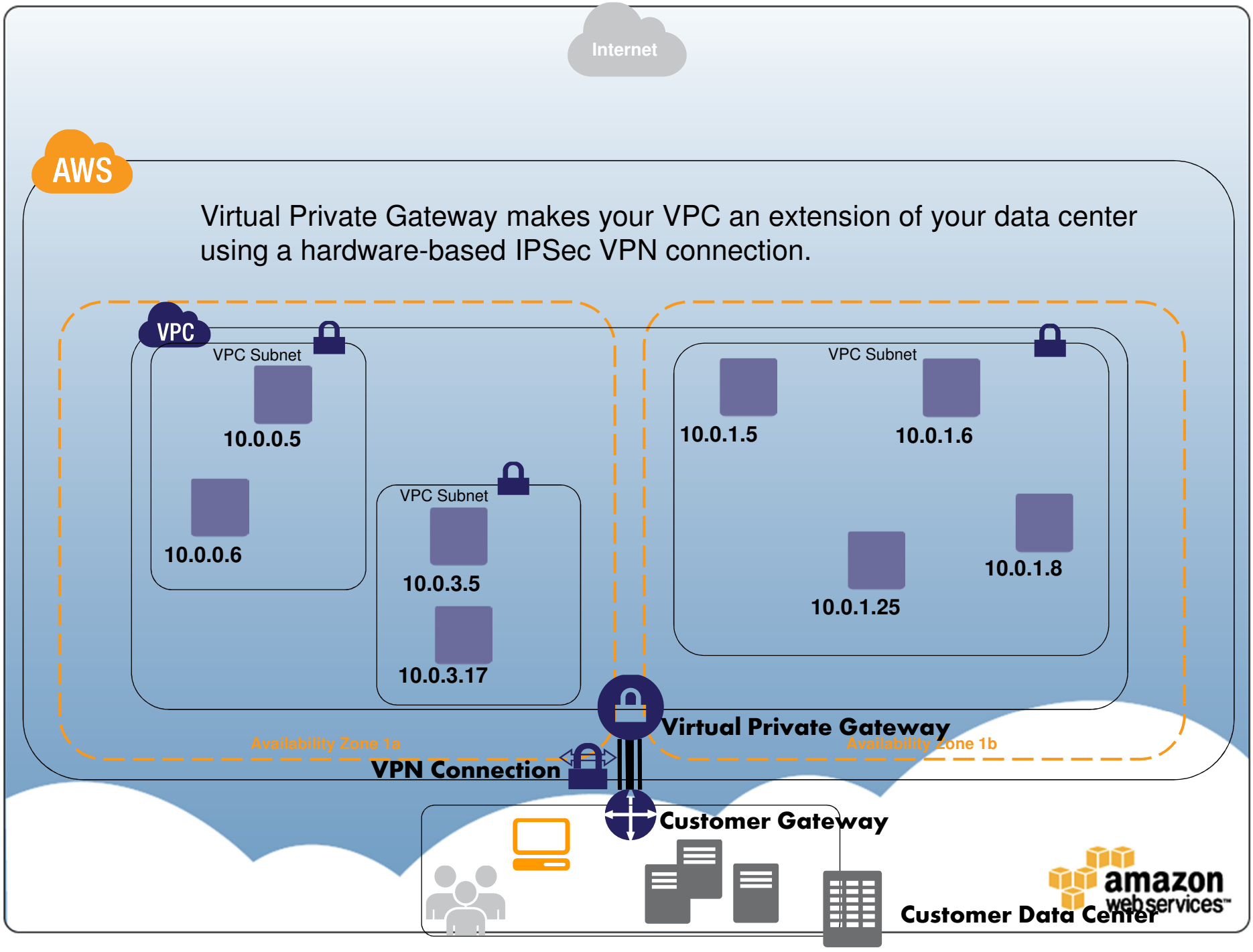
amazon web services™

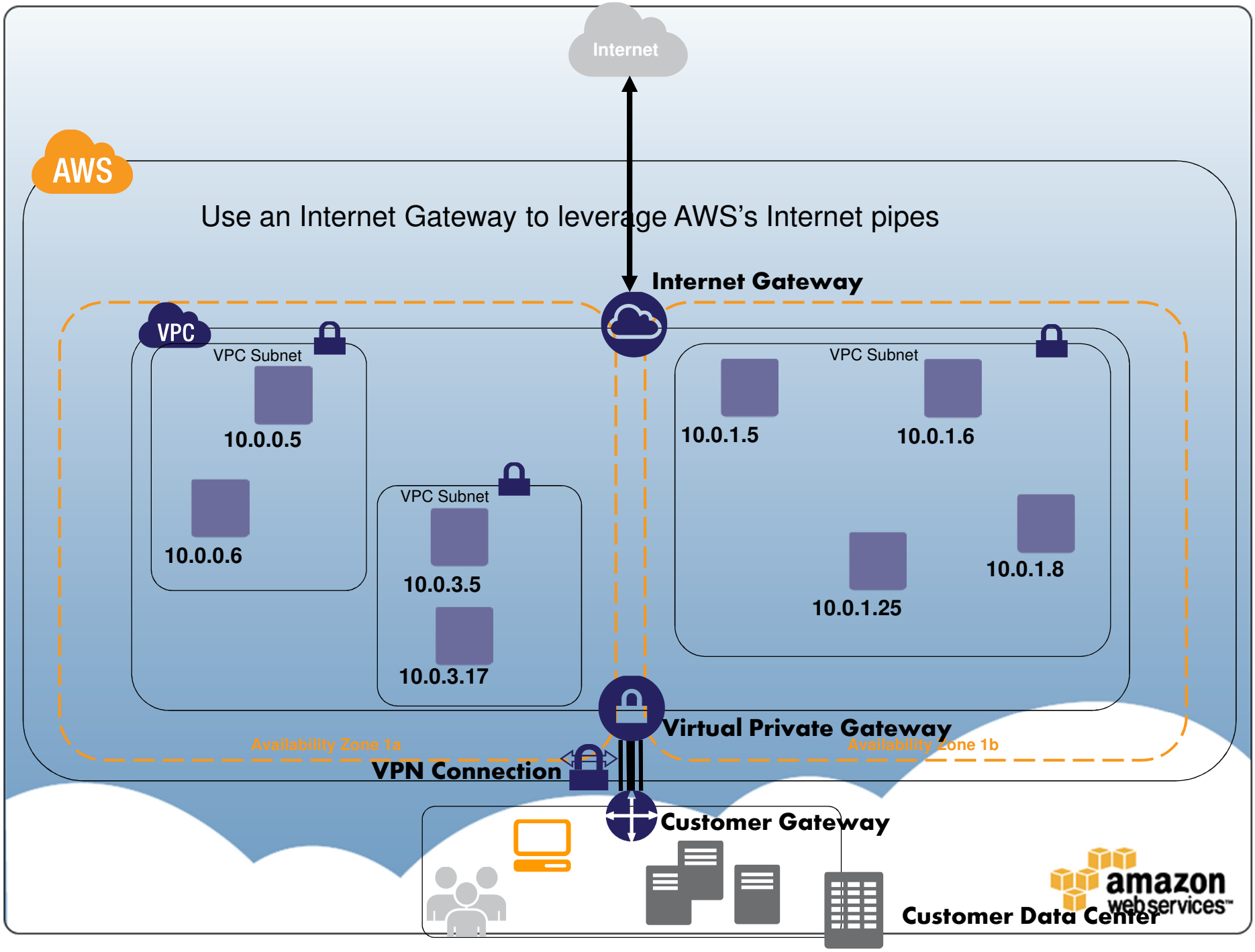

Internet
AWS
VPC customers can launch instances in their own isolated network
VPC
10.1.2.3
10.27.45.16
10.8.55.5
10.99.42.97
10.6.78.201
10.16.22.33
Availability Zone 1a
10.134.2.3
10.218.5.17
10.243.3.5
10.141.9.8
10.131.7.28
10.155.6.7
Availability Zone 1b
Customer 1
Customer 2
Customer 3
VPC Customer
amazon web services


Internet
AWS
and can assign their own IP range to the VPC network
VPC
10.0.0.5
10.0.0.6
10.0.3.5
10.0.3.17
10.0.1.5
10.0.1.6
10.0.1.8
10.0.1.25
Availability Zone 1a
Availability Zone 1b
VPC Customer
amazon
web services


Internet
AWS
Instances can be launched into different subnets
and subnets live in a particular Availability Zone
VPC
VPC Subnet
10.0.0.5
10.0.0.6
VPC Subnet
10.0.3.5
10.0.3.17
VPC Subnet
10.0.1.5
10.0.1.6
10.0.1.8
10.0.1.25
Availability Zone 1a
Availability Zone 1b
VPC Customer
amazon
web services


Internet
AWS
Access control lists can be added to further restrict network traffic
VPC
VPC Subnet
10.0.0.5
10.0.0.6
VPC Subnet
10.0.3.5
10.0.3.17
VPC Subnet
10.0.1.5
10.0.1.6
10.0.1.8
10.0.1.25
Availability Zone 1a
Availability Zone 1b
VPC Customer
amazon web services


Internet
AWS
Virtual Private Gateway makes your VPC an extension of your data center using a hardware-based IPSec VPN connection.
VPC
VPC Subnet
10.0.0.5
10.0.0.6
VPC Subnet
10.0.3.5
10.0.3.17
VPC Subnet
10.0.1.5
10.0.1.6
10.0.1.8
10.0.1.25
Availability Zone 1a
Availability Zone 1b
Virtual Private Gateway
VPN Connection
Customer Gateway
Customer Data Center
amazon web services


Internet
AWS
Use an Internet Gateway to leverage AWS's Internet pipes
Internet Gateway
VPC
VPC Subnet
10.0.0.5
10.0.0.6
VPC Subnet
10.0.3.5
10.0.3.17
VPC Subnet
10.0.1.5
10.0.1.6
10.0.1.8
10.0.1.25
Virtual Private Gateway
Availability Zone 1a
Availability Zone 1b
VPN Connection
Customer Gateway
Customer Data Center
amazon web services

VPC Capabilities Summary

- User-defined address space up to /16
- Up to 20* user-defined, per AZ subnets up to /16
- User-defined:
  - Virtual Routing, DHCP options, and NAT instances
  - Internet Gateways, Private/Customer Gateways, and VPN tunnels
- Private IPs stable once assigned
- Elastic Network Interfaces

Enhanced Security Capabilities

- Network topology, routing, and subnet ACLs
- Security group enhancements
  - Egress control; dynamic (re)assignment; richer protocol support
- Multiple network interfaces per instance
- Completely private networking via VPN
- Support for dedicated instances

Common Use Cases

- Mixing public and private resources
  - *E.g.*, web-facing hosts with DMZ subnets, control plane subnets
- Workloads that expect fixed IPs and/or multiple NICs
- AWS cloud as private extension of on-premises network
  - Accessible from on-premises hosts
  - No change to addressing
  - No change to Internet threat/risk posture

DirectConnect: Private X-Connect to AWS

- Dedicated bandwidth to AWS border network in 1gbps or 10gbps chunks
- Full access to public endpoints, EC2 standard, VPCs
  - VLAN tagging maps to public side or VPCs
- Benefits:
  - Faster / more consistent throughput
  - Increased isolation and control
- Great companion technology to VPC

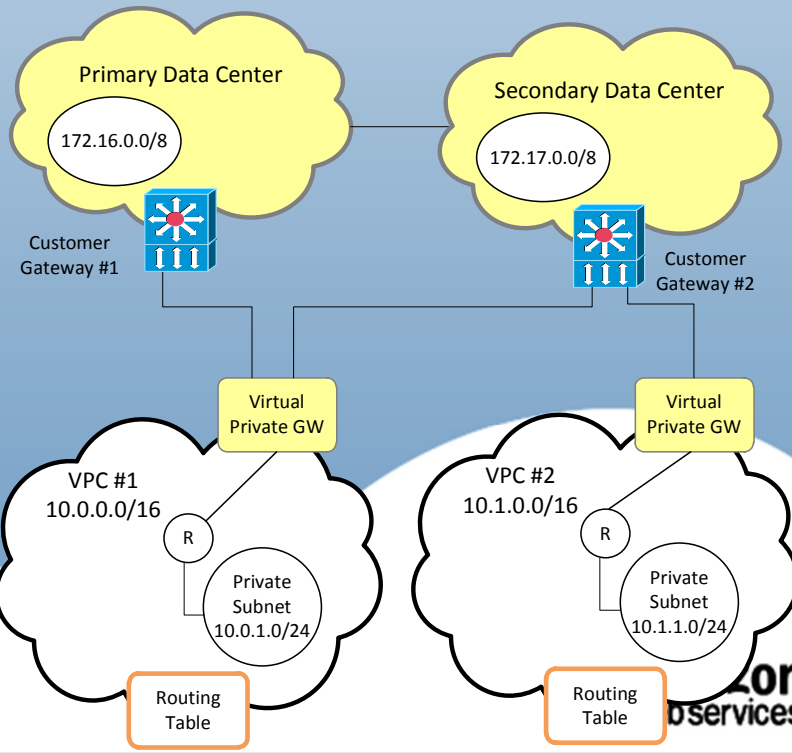
VPC Limits

- VPC Soft Limits
  - 5 VPCs per Region
  - 20 Subnets per VPC
  - 10 Network ACLs per VPC
    - 20 rules/ACL
  - 10 Route Tables per VPC
    - 20 entries/Route Table
  - 50 Security Groups per VPC
    - 50 rules/Security Group

http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html

VPC Constraints

- CGWs require unique public IP addresses
- Non-overlapping IP Ranges w/ internal networks
- Inability to change CIDR/Subnet address ranges
- Moving instances from one subnet to another
  - ENIs in same VPC/AZ
  - Image & relaunch for different VPC or AZ



amazon web services™