Network Service

- VPC
- Connectivity
- Availability

Virtual Private Cloud

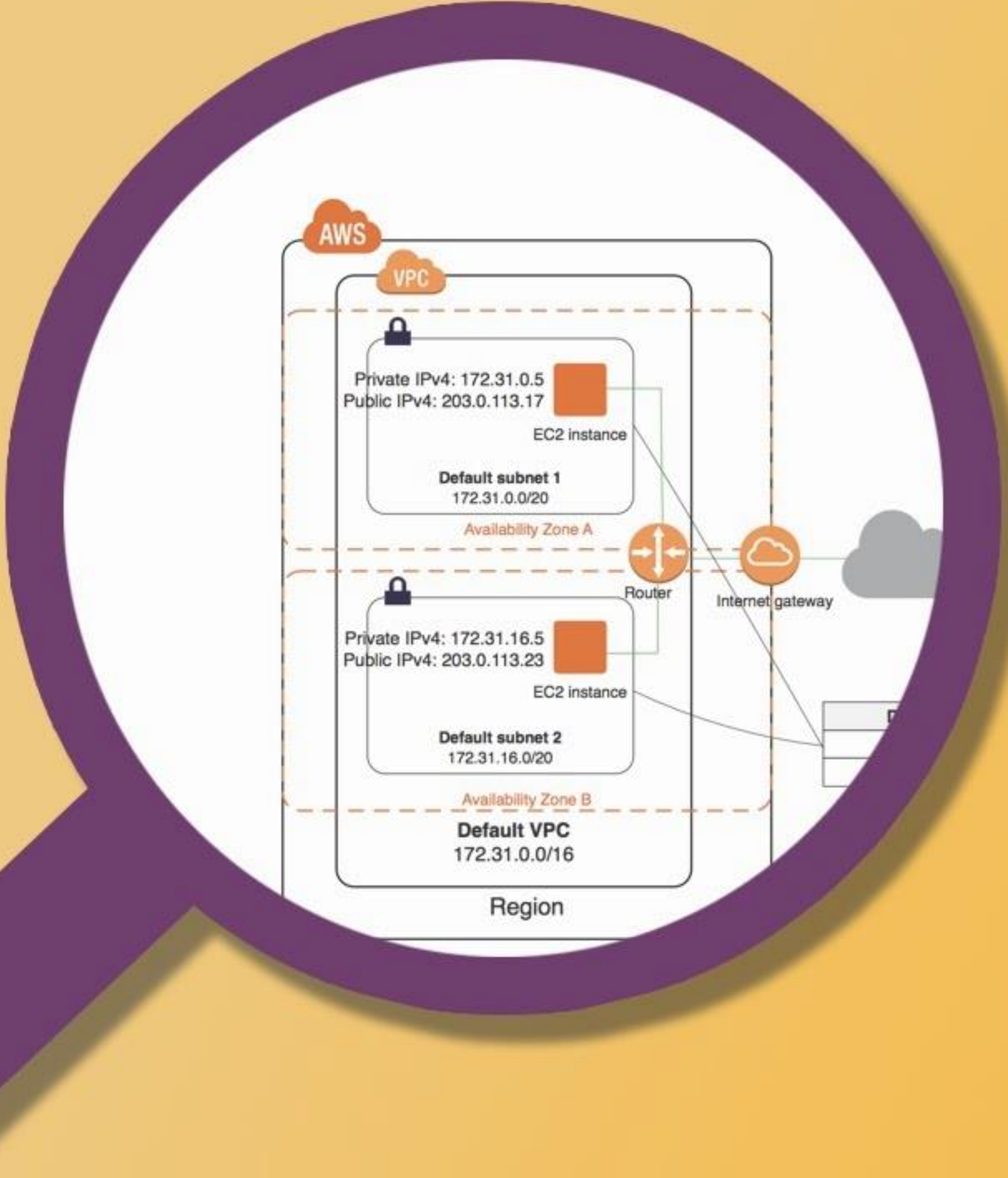
Network On-Prem

Network Architecture

Network Protocols

Network Devices

AWS VPC


AWS
VPC
Private IPv4: 172.31.0.5
Public IPv4: 203.0.113.17
EC2 instance
Default subnet 1
172.31.0.0/20
Availability Zone A
Router
Internet gateway
Private IPv4: 172.31.16.5
Public IPv4: 203.0.113.23
EC2 instance
Default subnet 2
172.31.16.0/20
Availability Zone B
Default VPC
172.31.0.0/16
Region

VPC Basic

- VPC is SDN
- VPC in a region
- Subnets are created in a VPC to break up network range
- VMs are placed in a subnet with NIC
- All VM can communication in a subnet

VPC Tips

- VPC has more than 1 CIDR
- Subnet: Private/Public (AWS)
- Each VPC has some remained IPs
- Not support L2 feature
- No multicast/broadcast/GRE/IPIP
- Network ACL/Security Group

Routing Table

- Main RT for all subnets
- Custom RT for special subnets
- RT can bind the following:

✓ Gateway Endpoint(IGW VGW NATGW EIGW)

✓ VPC Endpoint

✓ VPC Peering

✓ ENI

- Route Priority

Connectivity

Connectivity

VPC Peer

- AWS Backbone
- Not Transit

Endpoint

- Bypass internet
- Limited Service

Connectivity

Public Internet

- NIC Public IP
- Elastic IP

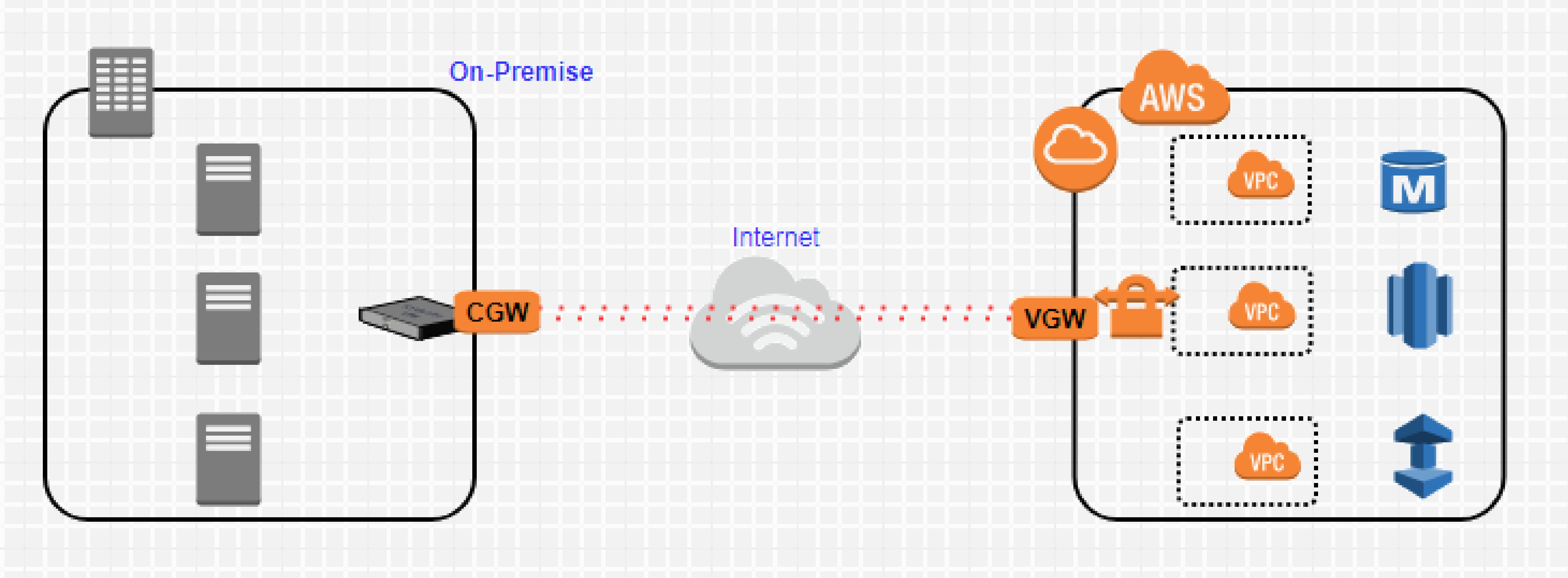
VPN

- AWS Managed VPN
- Software VPN

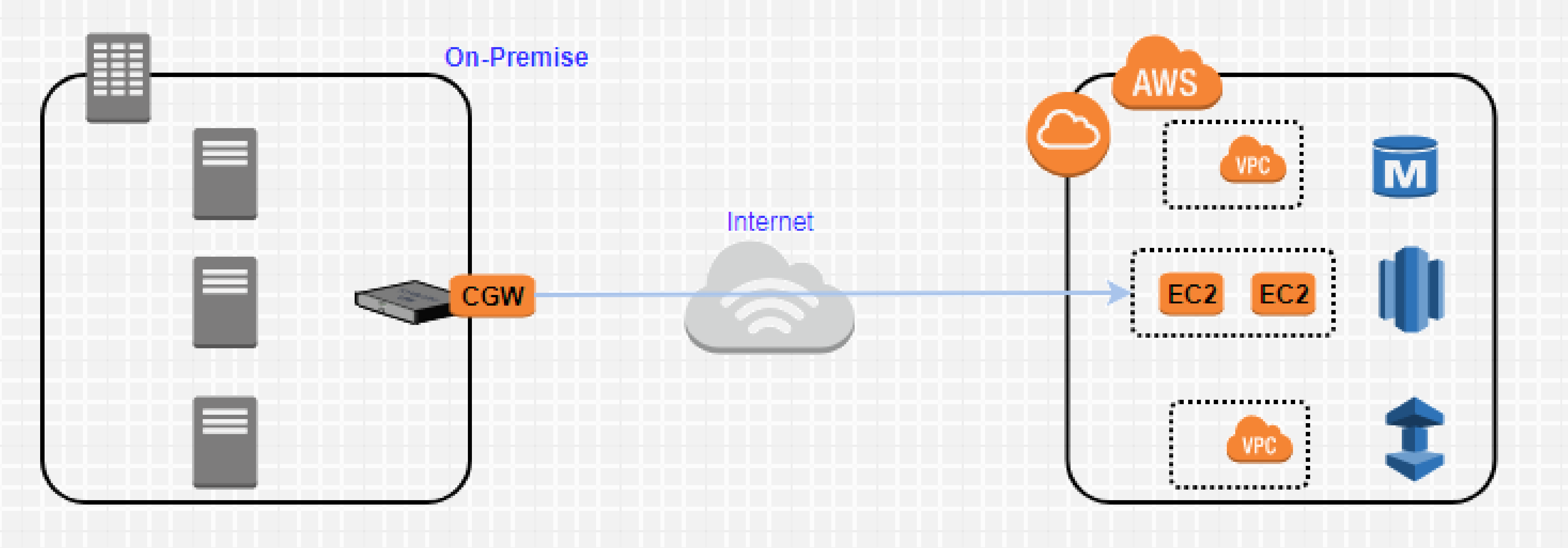
Direct Connect

- Private Connection
- Except China

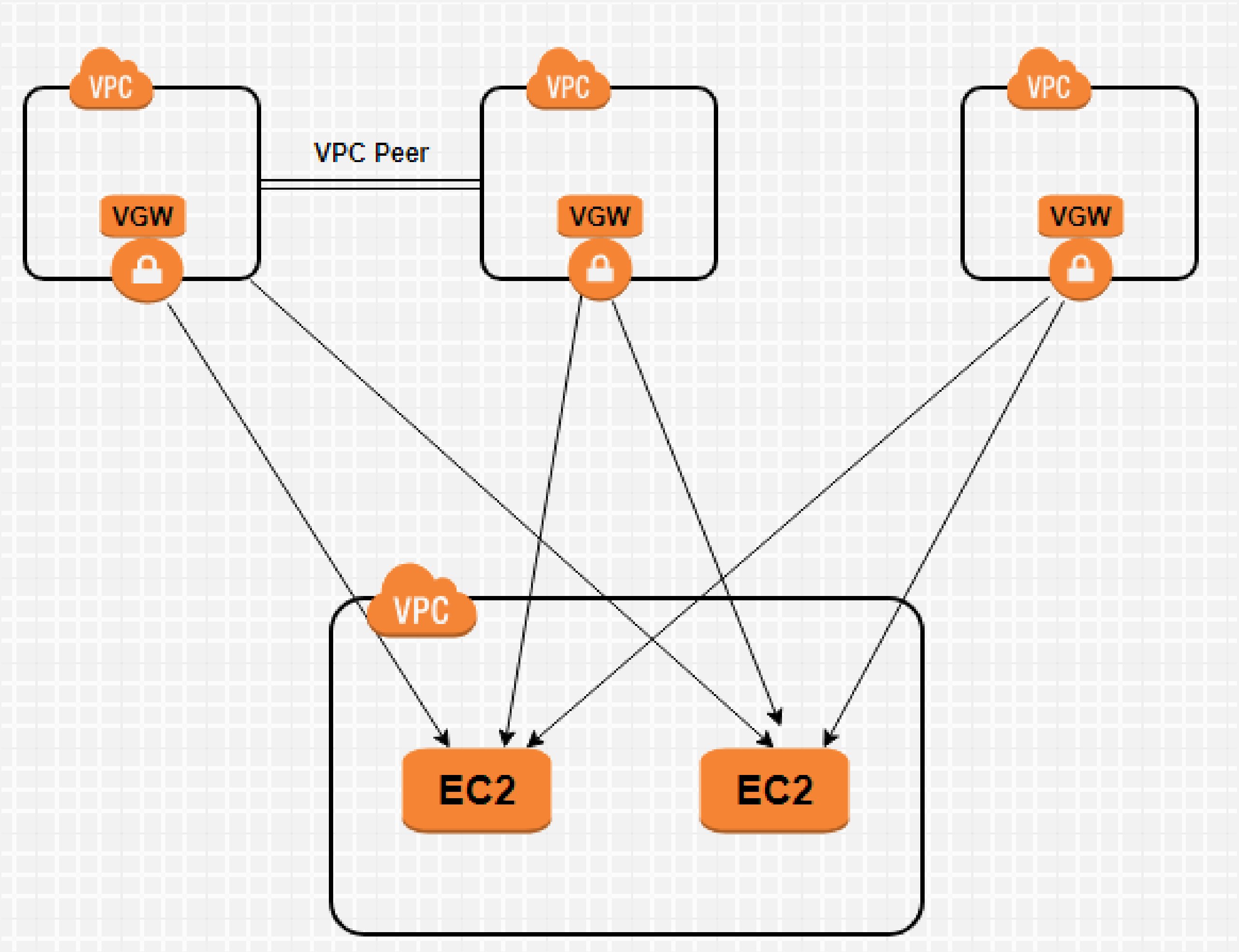
AWS Managed VPN



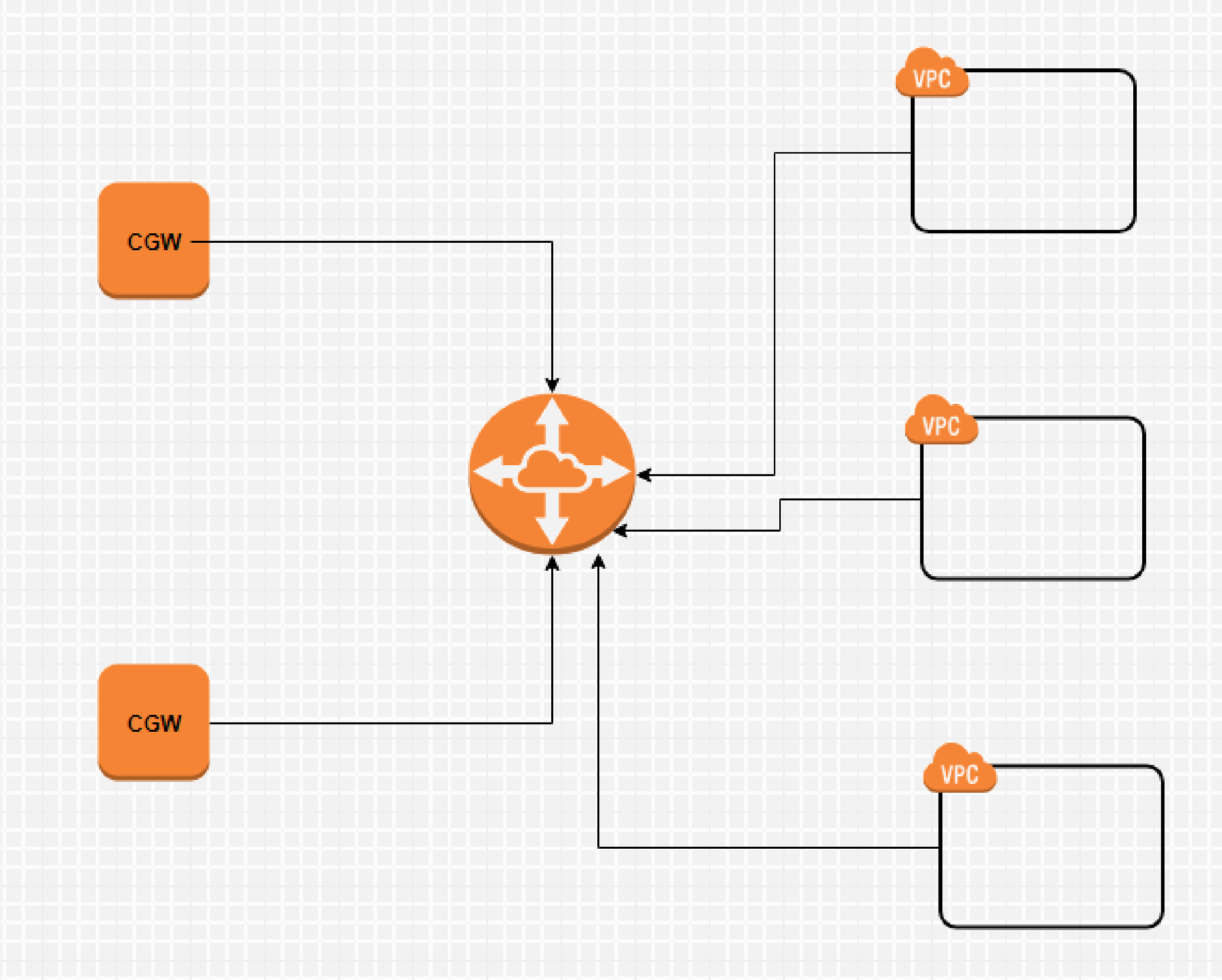
Software VPN



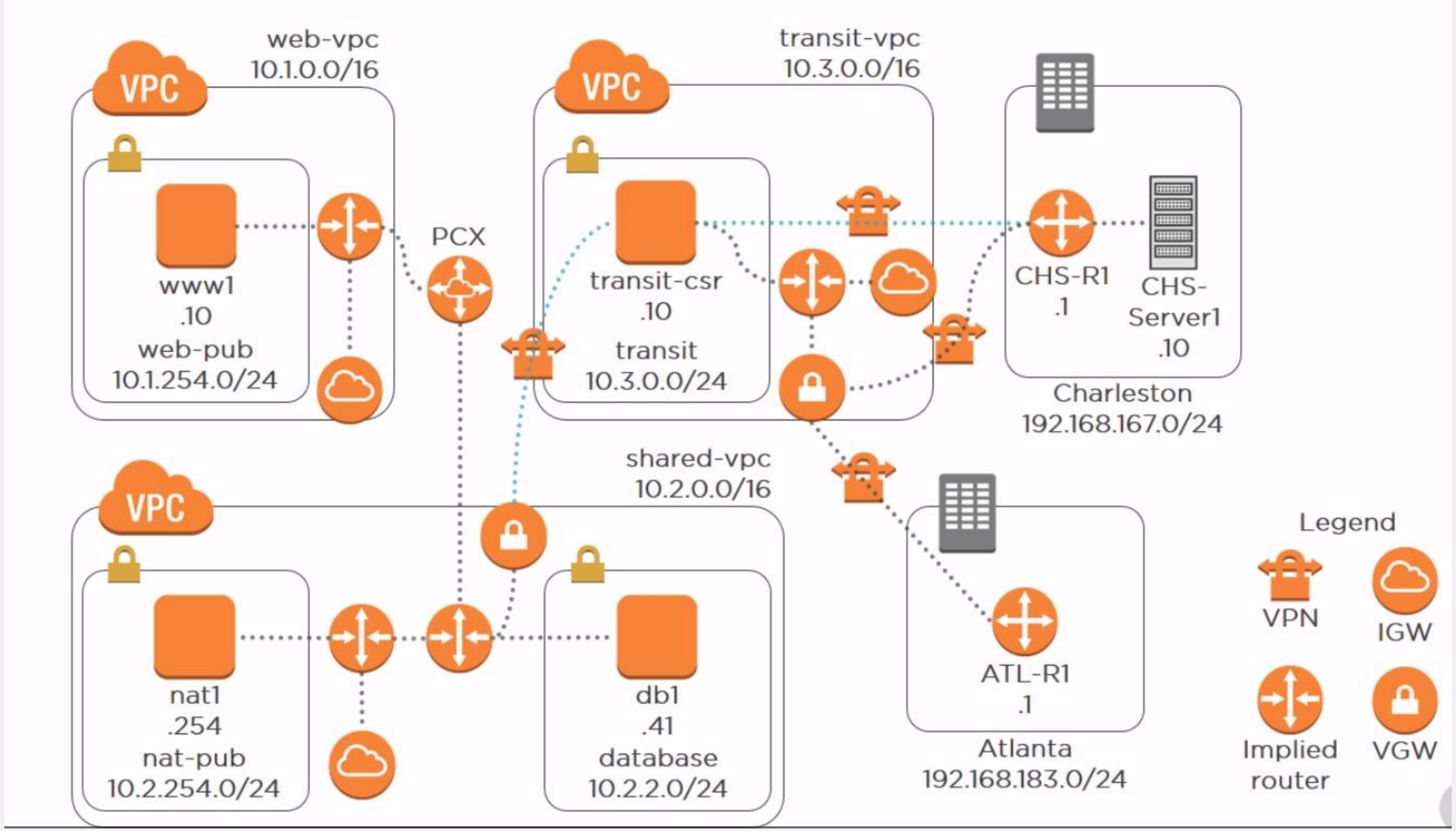
Transit VPC



Transit Gateway



Network Topo



Gateway

IPv4	IPv6
IGW for Public Subnet	IGW for Public Subnet
NAT GW for Private Subnet	Egress-Only IGW for Private Subnet
NAT instance for Private Subnet	
VGW for VPN connection	VGW for VPN connection

Network Connection

AWS	Azure
VPC Peering	Virtual Network Peering
VPC Endpoint	Azure Endpoint
AWS VPC Gateway	Site-Site VPN Gateway
Direct Connect	Express Route

Availability

Availability

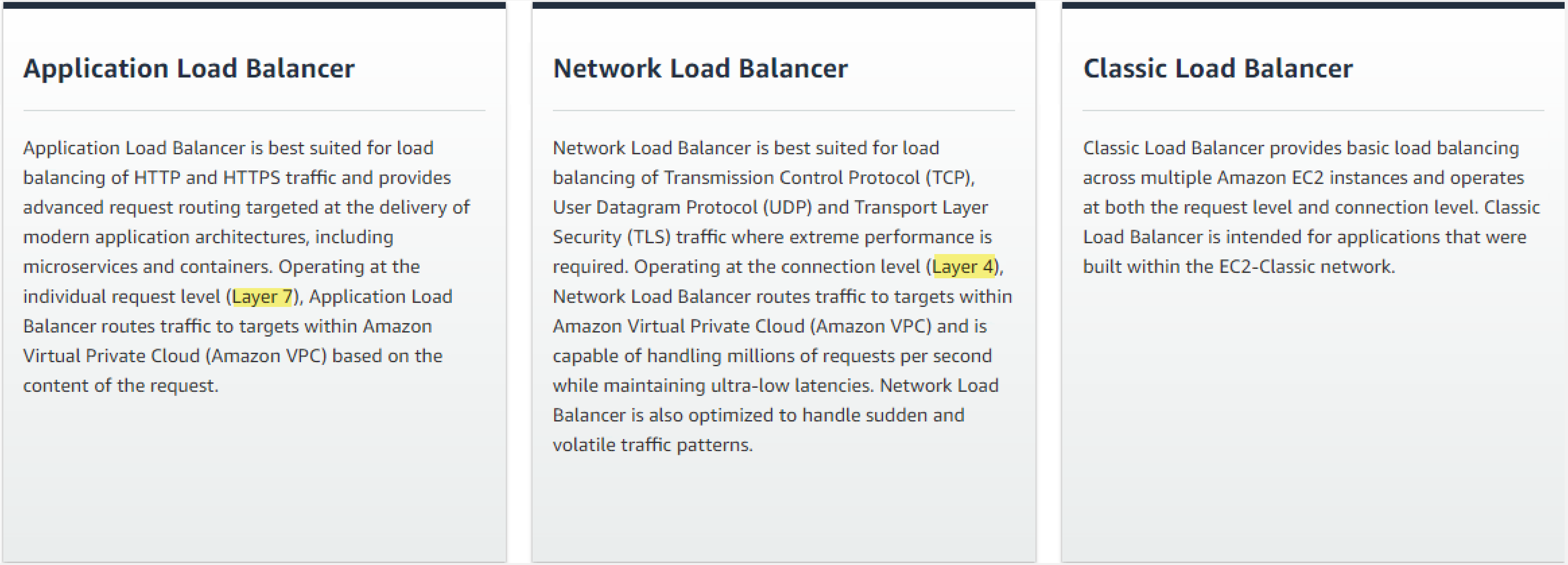
Load Balancer

- Public & Private
- LB Service Type

Router 53

- DNS Function
- DNS Method

LB Service



Application Load Balancer

Application Load Balancer is best suited for load balancing of HTTP and HTTPS traffic and provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers. Operating at the individual request level (Layer 7), Application Load Balancer routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) based on the content of the request.

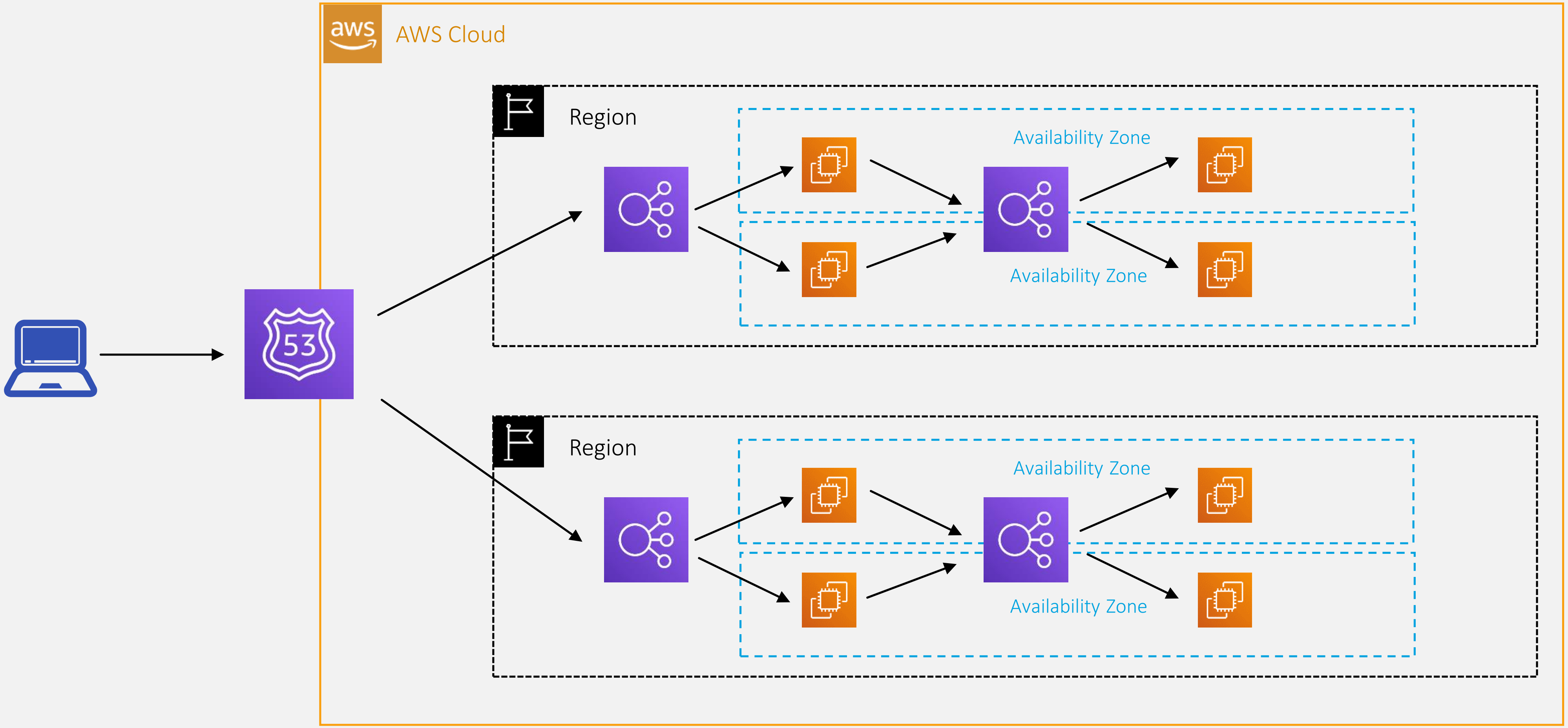
Network Load Balancer

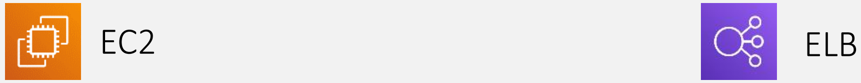
Network Load Balancer is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Transport Layer Security (TLS) traffic where extreme performance is required. Operating at the connection level (Layer 4), Network Load Balancer routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) and is capable of handling millions of requests per second while maintaining ultra-low latencies. Network Load Balancer is also optimized to handle sudden and volatile traffic patterns.

Classic Load Balancer

Classic Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and connection level. Classic Load Balancer is intended for applications that were built within the EC2-Classic network.

LB Scenario





CiTRiX

DNS in AWS

Instance DNS

- Run on instance
- 3rd DNS server

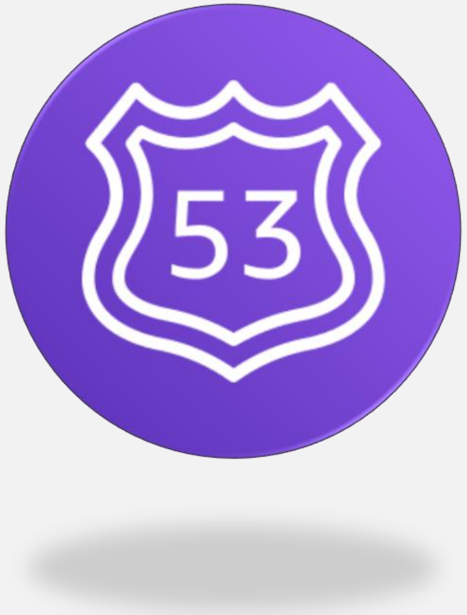
EC2 DNS

- AWS Managed DNS
- enableDnsSupport
- enableHostnames
- DHCP Option Set

Route 53

- All the DNS
- Health Check

Route53 Policy



Simple

Health Check

Failover

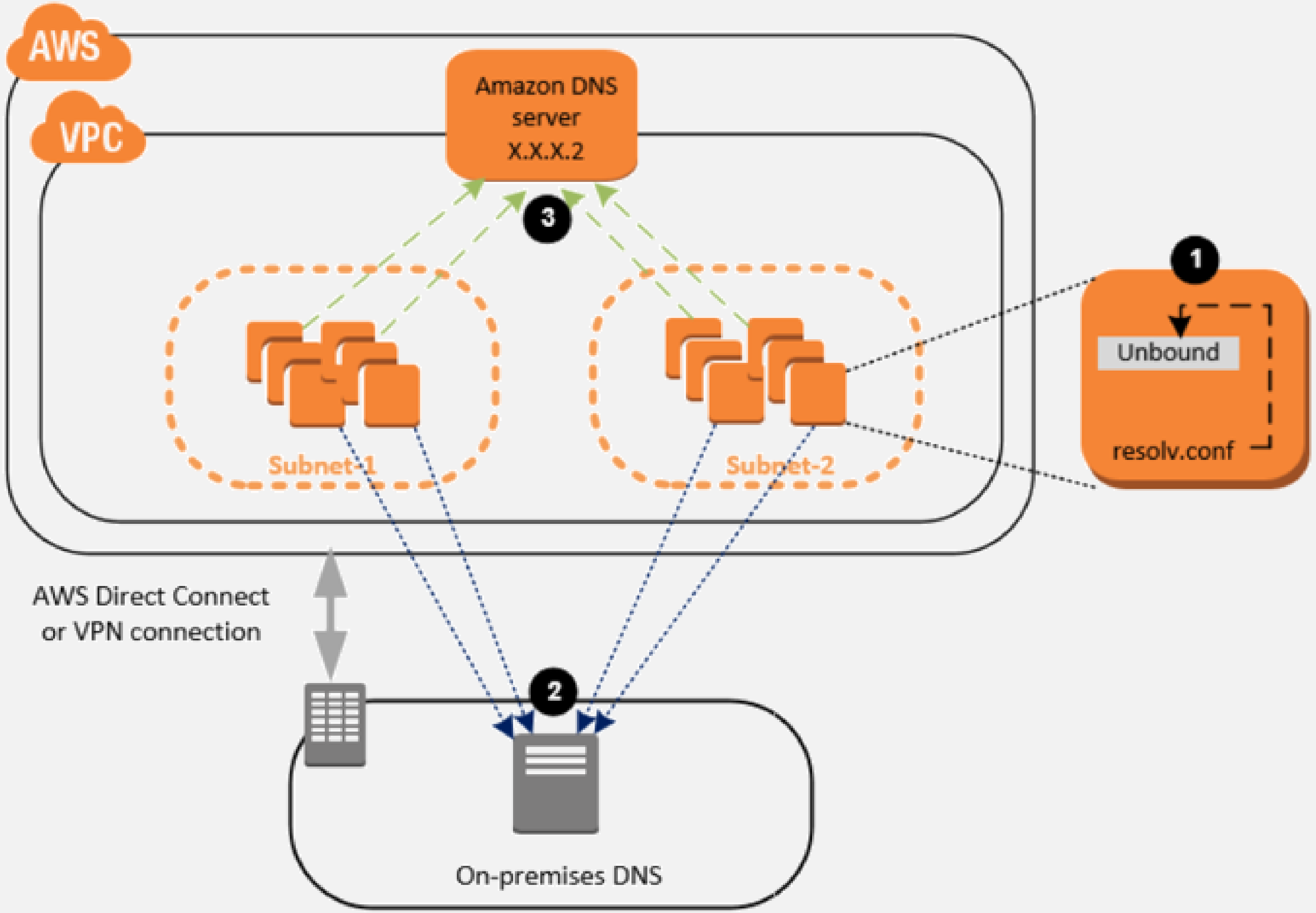
Weighted

Geolocation

latency records

Multi-Value Answer

DNS Forwarder


AWS
VPC
Amazon DNS server X.X.X.2
3
1
Unbound
resolv.conf
Subnet-1
Subnet-2
AWS Direct Connect or VPN connection
2
On-premises DNS

Network Available

AWS	Azure
ELB/ALB	Azure LB/Application Gateway
Route 53	Azure Traffic Manager/Azure DNS

Group Discussion

- VPC peering can communication between different region?
- VPC peering can do transit packets for different VPC