
Amazon
VPC
amazon
web services

VPC

- Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.

- You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

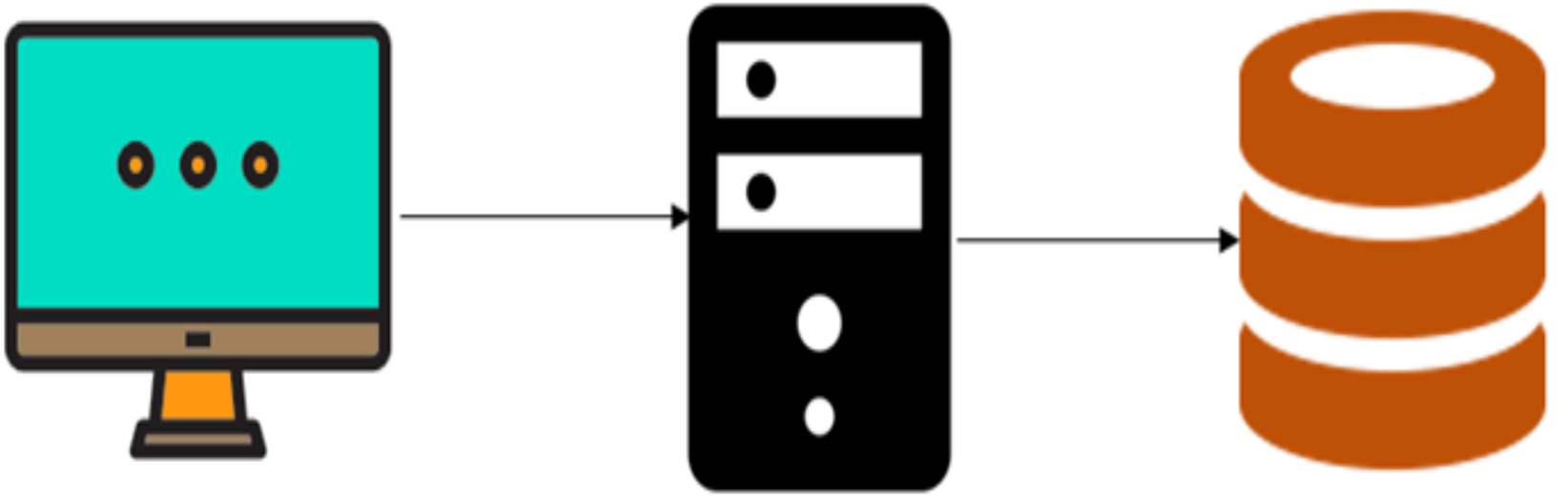
- You can easily customize the network configuration of your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the internet. You can also place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. You can use multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

VPC components

- **Virtual private cloud (VPC)** — A virtual network dedicated to your AWS account.
- **Subnet** — A range of IP addresses in your VPC.
- **Route table** — A set of rules, called routes, that are used to determine where network traffic is directed.
- **Internet gateway** — A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.
- **VPC endpoint** — Enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by Private Link without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Parameter	Default VPC	Custom / nondefault VPC
Explanation	Virtual network which is automatically created for customer AWS account the very 1st time EC2 resources are provisioned	A nondefault (also called Customer VPC) is not automatically created when EC2 resources are provisioned. Customer needs to create own VPC.
Created by	AWS	Customer
VPC assigned when an instance is launched without allocating subnet	Default VPC is assigned	NA
IPv4 address on instance launch	private IPv4 address and a public IPv4 address	a private IPv4 address, but no public IPv4 address
Access to Internet by default	Yes	No
Internet gateway	Included	No
Ready to use	Yes	Partially
Number of VPC per region	One	5 by default

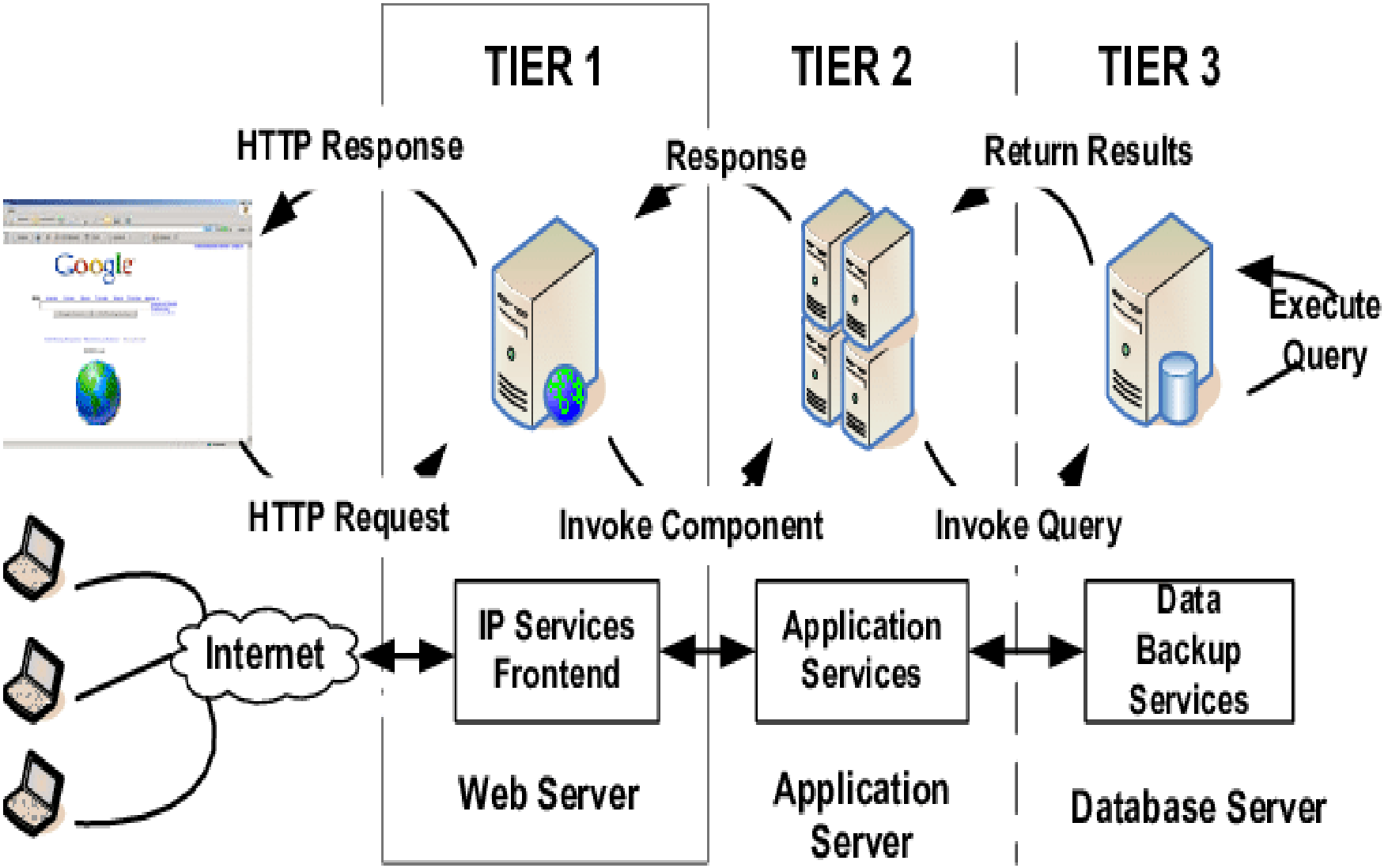
Three Tier Architecture



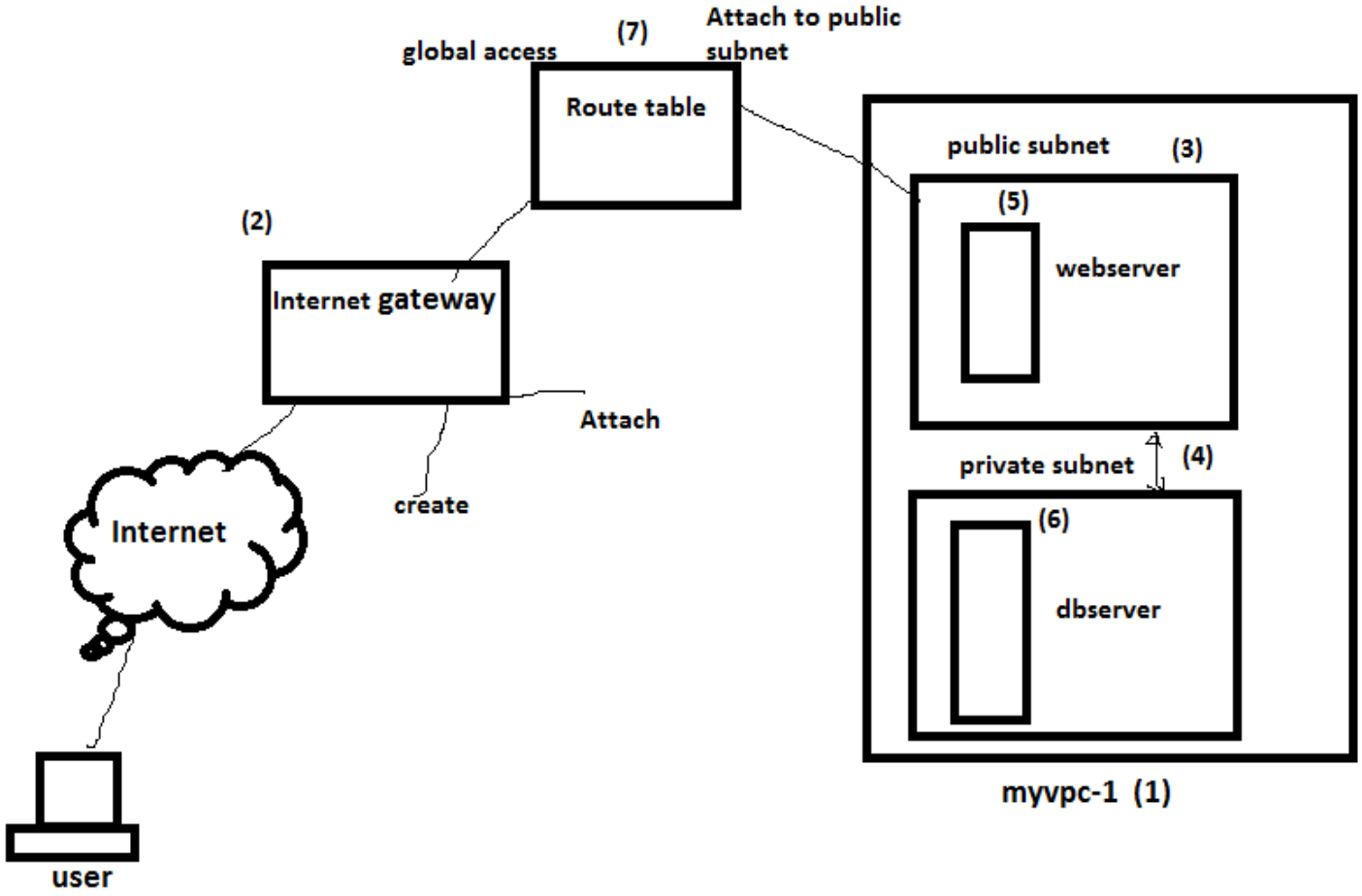
Client

Server

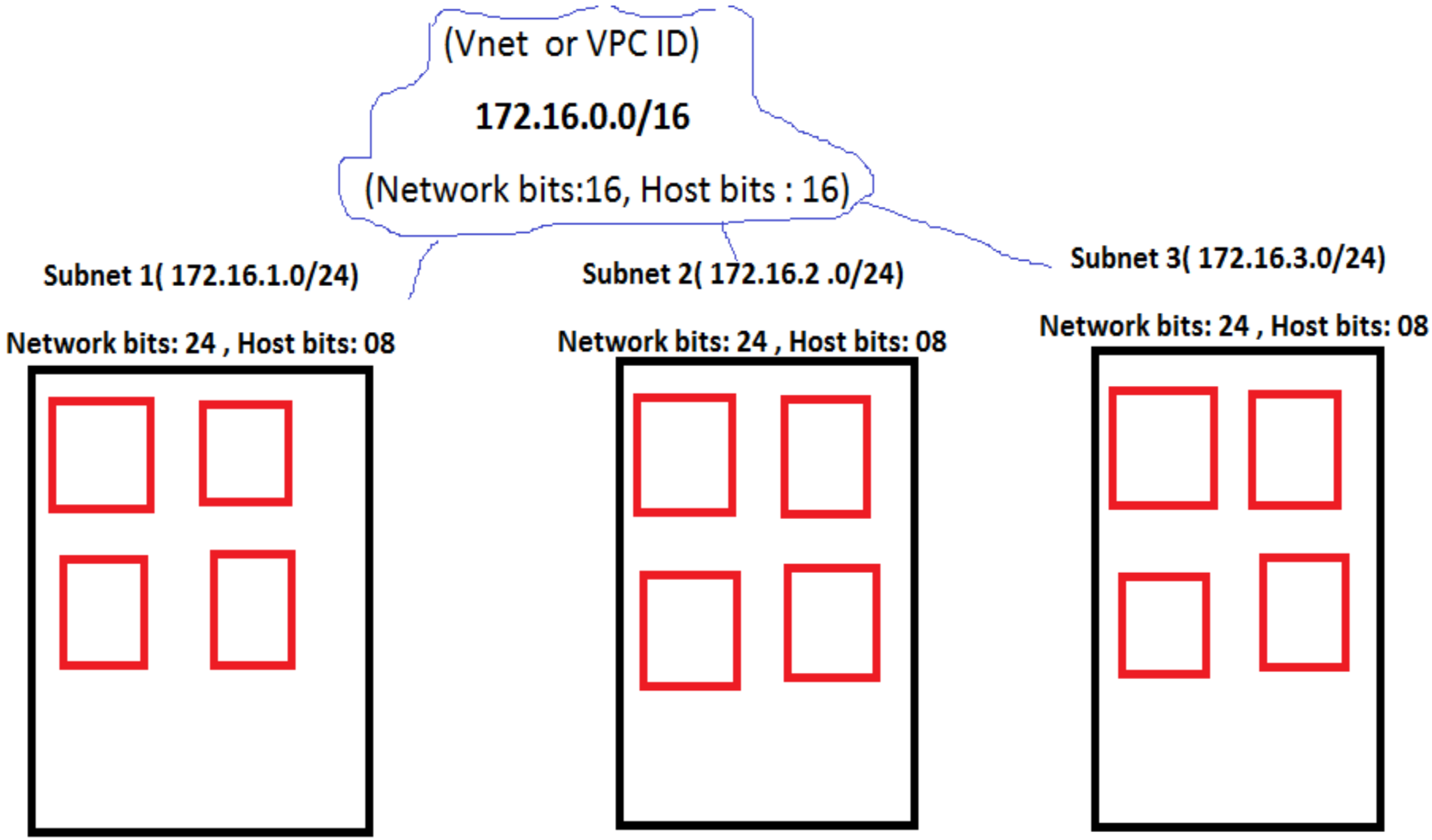
Database


TIER 1
TIER 2
TIER 3
HTTP Response
Response
Return Results
Google
Execute Query
HTTP Request
Invoke Component
Invoke Query
Internet
IP Services Frontend
Application Services
Data Backup Services
Web Server
Application Server
Database Server

Hands on – Configure custom VPC with public and private network



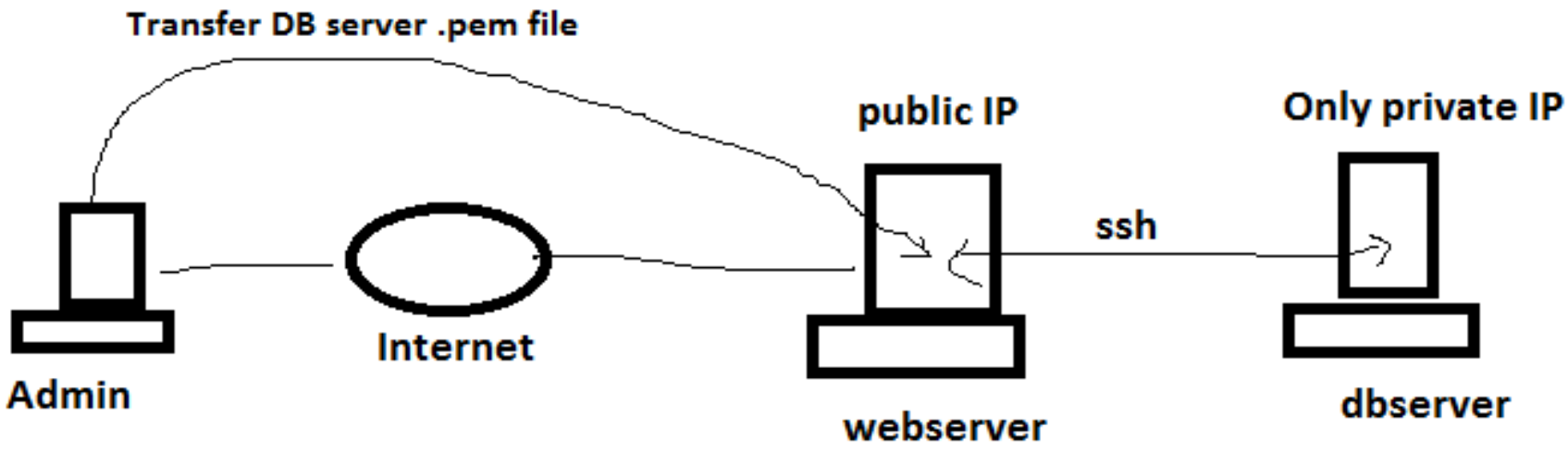
Private IP address range		
Class	Starting	Ending
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255


(Vnet or VPC ID)
172.16.0.0/16
(Network bits:16, Host bits : 16)
Subnet 1(172.16.1.0/24)
Network bits: 24 , Host bits: 08
Subnet 2(172.16.2 .0/24)
Network bits: 24 , Host bits: 08
Subnet 3(172.16.3.0/24)
Network bits: 24 , Host bits: 08

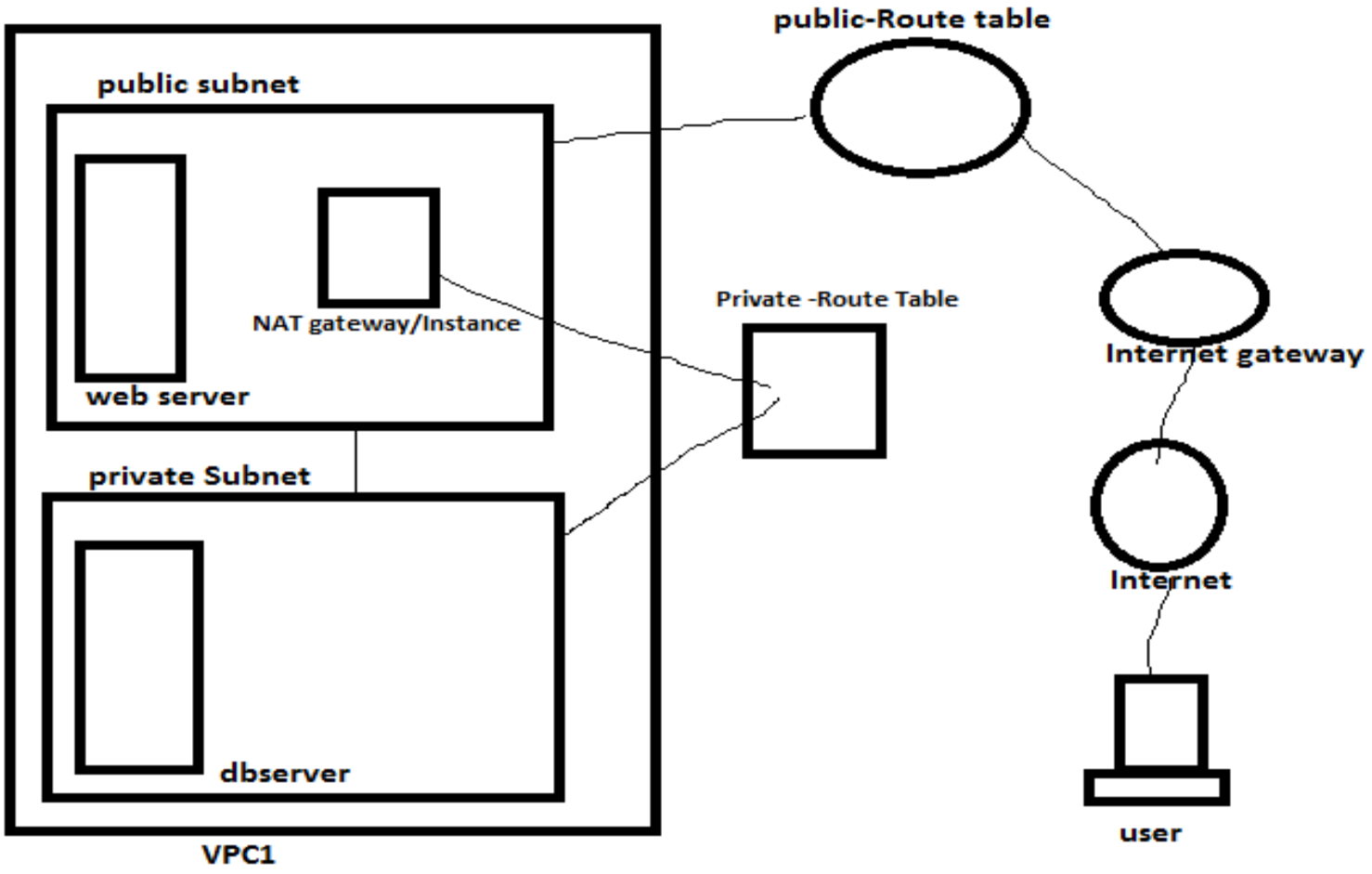
DB Server Security

1) No public IP
2) Security group--SSH –mapped—webserver-SG
3) No route table configuration

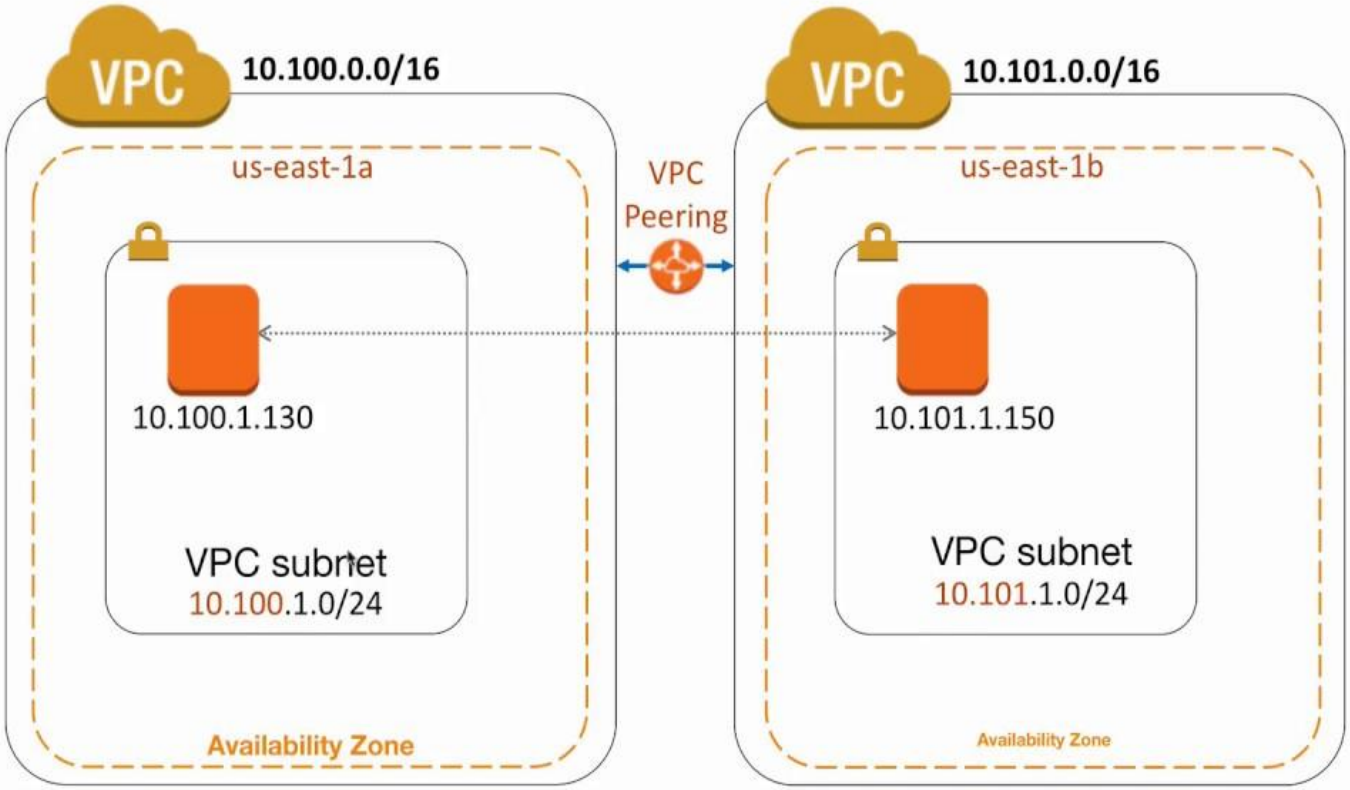
Connecting Dbserver through Webserver



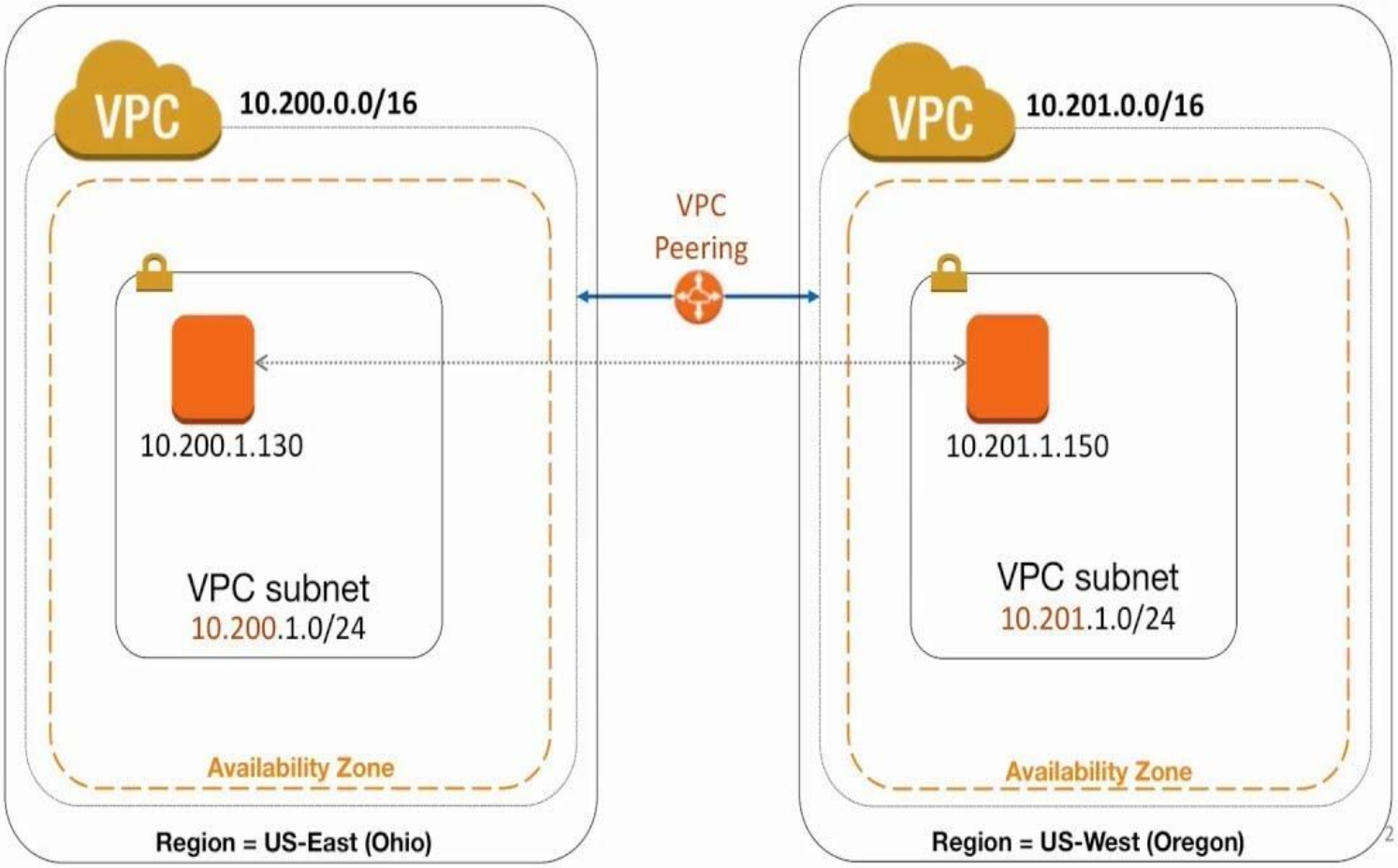
Provide Internet Connectivity (Outbound) to Private Subnet



Set up VPC Peering b/w VPCs in the same Region



Set up VPC Peering b/w VPCs in the different Regions



VPC peering

Term	VPC1	VPC2
VPC	Project1vpc	Project2vpc
VPC-ID	172.16.0.0./16	172.17.0.0/16
Subnet1	Project1publicsubnet (172.16.1.0/24)	Project2publicsubnet (172.17.1.0/24)
Subnet2	Project1privatesubnet (172.16.2.0/24)	Project2privatesubnet (172.17.2.0/24)
Route Table	Project1-public-rt	Project2-public-rt
Internet gateway	Internet gatewayproject1	Internet gatewayproject2

VPC peering Steps

1) Create 2 VPC with all detail –RT, IG, Subnet etc.

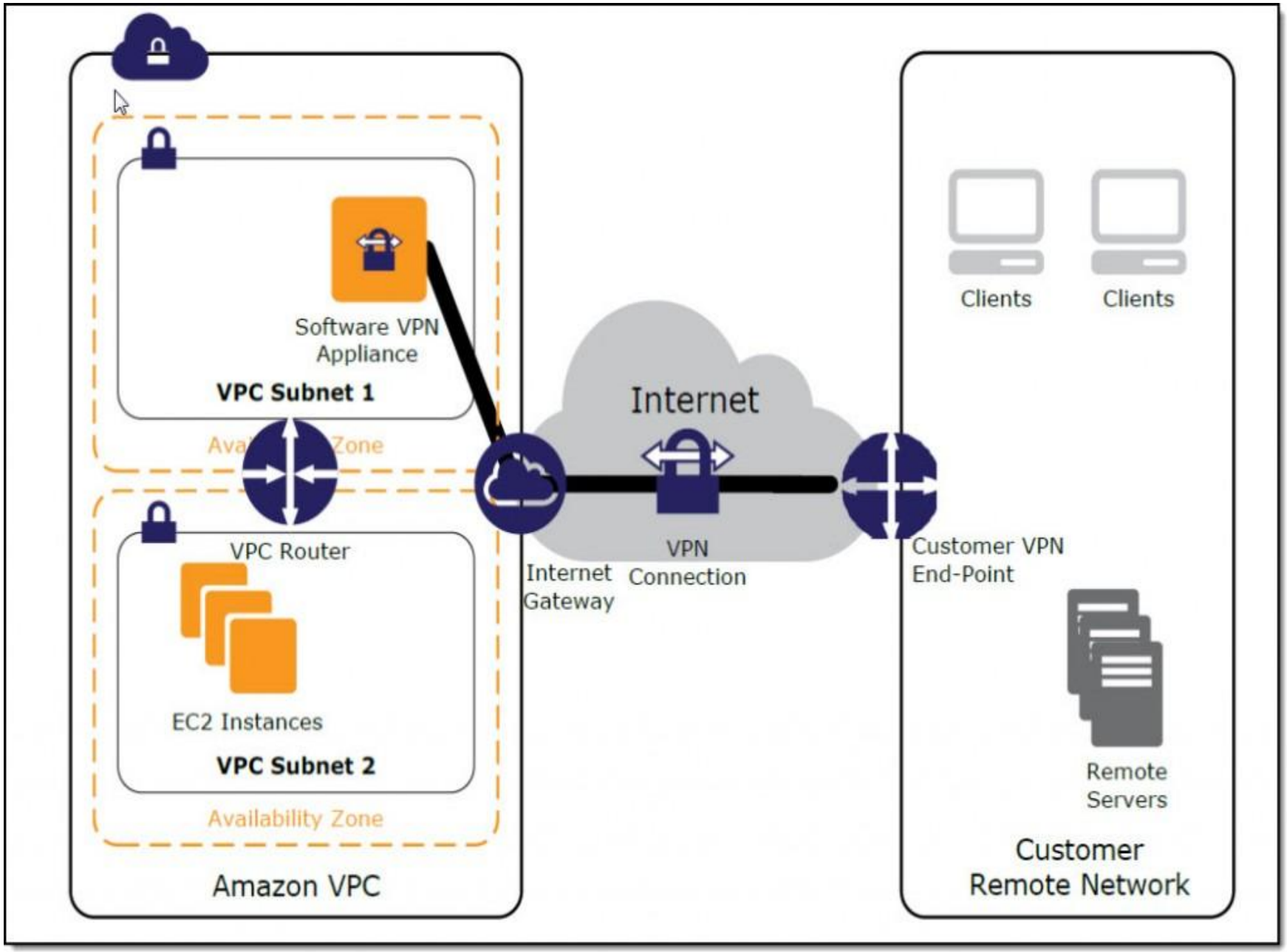
2) Peering Connection –New Peering –Fill the detail—name—vpc1-vpc2 –vpc , Requester –vpc1, Accepter –vpc2

--same account –same region—ok

3) Select created VPC peering –Action –Accept –ok

4) Route Table –select vpc1 route table—routes—edit routes—add route– vpc2 IP –target—peering connection---select: vpc1-vpc2 –ok

5) Route Table –select vpc2 route table—routes—edit routes—add route– vpc1 IP –target—peering connection---select: vpc1-vpc2 –ok


Software VPN
Appliance
VPC Subnet 1
VPC Router
EC2 Instances
VPC Subnet 2
Availability Zone
Amazon VPC
Internet
Internet
Gateway
VPN
Connection
Customer VPN
End-Point
Clients
Clients
Remote
Servers
Customer
Remote Network