VPC

1. VPC – Virtual Private Cloud (Your Private Cloud)
2. We have Regions, Availability Zones,
   1. We can think of AZ as data centers.
   2. Region can have multiple data centers.
   3. We can launch EC2 instances, RDS instances in these availability zones.
   4. To protect against failures, fault tolerances, we can create multiple instances in different availability zones, so if 1 AZ goes does we can provide services from other AZ.
   5. Different AZ
3. Each AWS account you create, comes with default VPC.
4. VPC is ur data center in the cloud.
5. Ip subset range can be divide among multiple AZ using subnet.

Subnet

1. Internal IP Range inside VPC
2. Public IP can help us to communicate to internal ip range.

Public vs Private Subnet

1. Public subnet can host webservers that can be accessible by outside network
2. Database and internal apps can be available in private subnet.

Internet Gateway

1. To communicate with outside world from inside VPC we can use Internet Gateway

Security Group

1. You can assign instances in VPC with security groups.
2. Security Groups can be shared across AZ.
3. Security Groups allows to control
   1. Which access is allowed to instances
   2. Which traffic can leave instances
   3. Acts as Firewall
   4. More granular as applied to instances

Network Access Control List (NACL)

1. Applies at subnet level
2. Which traffic can access subnet

NAT Gateway

1. Ability to route private subnet traffic to access outside world (for updates etc)
2. Nat Gateway has public ip
3. Instances in private subnet don’t have public ip but they can access outside world using NAT gateway
4. NAT is private to public routing.

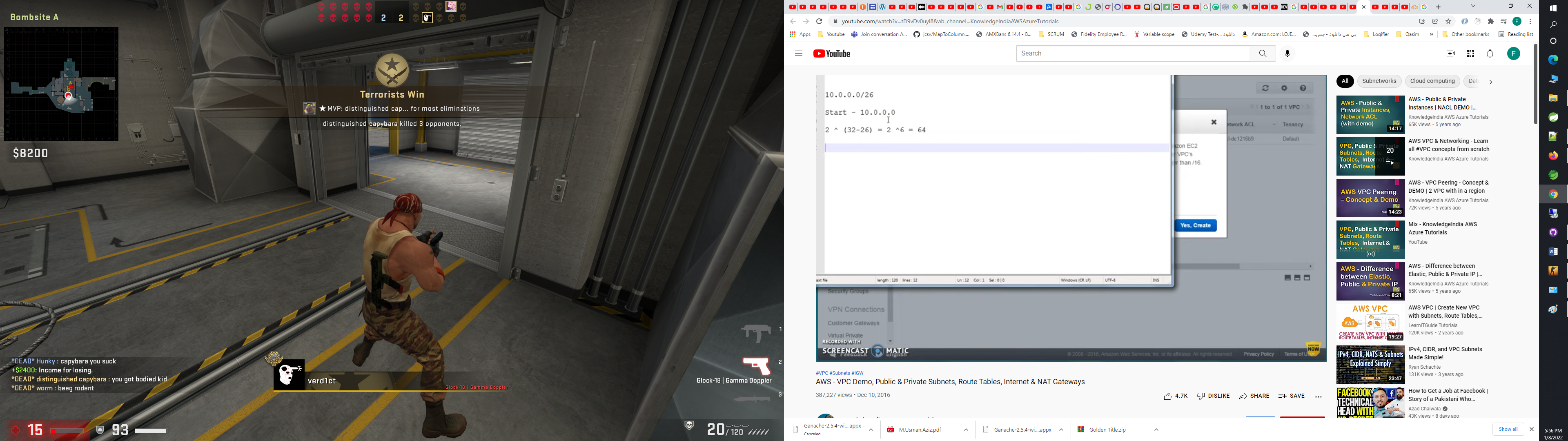
How many valid Ips

1. Subnet mask = 26
2. 2 ^ (32-26) = 2 ^ 8 => 64 Valid ips in CIDR
3. We will divide in 4 subnets of 16
4. Deploy VPC
5. Create subnets

Luanch VPC and aws work

<https://www.youtube.com/watch?v=tD9vDv0uyI8&ab_channel=KnowledgeIndiaAWSAzureTutorials>

Range



Route Table

1. How network is routed when it leaves VPC
2. Is traffic allowed to leave/enter VPC
3. Controls routing of out-going network requests

Public IP

1. If the instance launch in the subnet will receive Public IP
2. So we can create two subnets, one can be accessible by public ip and other for internal use only.

VPC span multiple AZ

Subnet is tied to a specific AZ.

CIDR Block

1. Ip Ranges

Why do we want to isolate our network under a region?

For

1. Compliance Perspective
2. PROD/UAT/QA/DEV
3. Maybe to connect cloud network with on premise data center.

Resources

<https://www.youtube.com/watch?v=bGDMeD6kOz0&ab_channel=Academind>

Create VPC with subnets

<https://www.youtube.com/watch?v=tD9vDv0uyI8&ab_channel=KnowledgeIndiaAWSAzureTutorials>

FAQ:

What is VPC

Amazon VPC provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define

1. IP Address range
2. Creation of subnets
3. Route Table configuration
4. Network Gateway
5. Enable us to VPN , on-premise data center with AWS VPC.
6. Layers of security
   1. Security Groups
   2. Network Access control lists.
   3. etc

Components of VPC

1. Virtual Private Cloud
2. Subnet
3. Internet Gateway: Amazon VPC side of connect to public internet
4. NAT Gateway: A highly available, managed Network Address Translation (NAT) service for your resources in private subnet to access the internet.
5. Virtual Private Gateway: The Amazon VPC side of a VPN connection
6. Peering connection: A peering connection enables you to route traffic via private IP addresses between two peered VPCs.
7. VPC Endpoints: Enables private connectivity to services hosted in AWS, from within your VPC without using an Internet Gateway, VPN, Network Address Translation (NAT) devices, or firewall proxies.
8. Egress-only Internet Gateway: A stateful gateway to provide egress only access for IPv6 traffic from the VPC to the Internet.

Notes;

1. Whenever we create subnet in AWS, 5 are reserved.
2. For each VPC, one route table is created by default. That route table is marked as Main and will be used as default route table for all subnets. Unless changed
3. 1-1 relationship b/w subnet and route table.
4. 1 route table can be associated with multiple subnets.
5. 1 -1 relationship b/w Internet Gateway and VPC.
6. Custom route tables are not set with any subnet, unless u assigned them.
7. NAT Gateway allows internal traffics to get response from outside (Public) networks.
   1. Those instances who don’t have Public IP , can use NAT gateway to communicate with external world.
   2. Act as forward proxy
   3. NAT Gateway use 1 IP from Available public ip range