Amazon Virtual Private Cloud (Amazon VPC) is a web service provided by Amazon Web Services (AWS) that allows you to launch and manage a logically isolated section of the AWS Cloud. Within an Amazon VPC, you have control over your virtual networking environment, including IP address ranges, subnets, and the configuration of route tables and network gateways. Here are the key components of Amazon VPC:

1. VPC (Virtual Private Cloud):**
A logically isolated section of the AWS Cloud where you can launch AWS resources.
You can think of it as a private, isolated network within the AWS infrastructure.

2.Subnet:
A range of IP addresses in your VPC.
You can divide your VPC IP address range into subnets to host your resources.
Subnets are associated with availability zones, helping distribute resources across multiple data centers for fault tolerance.

3. Route Tables
Contain a set of rules, called routes, that are used to determine where network traffic is directed.
Each subnet in a VPC must be associated with a route table, which controls the traffic routing for the subnet.

4. Internet Gateway
A horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet.
It enables instances to connect to the internet and vice versa.

5. NAT Gateway:
Network Address Translation (NAT) gateway allows instances in a private subnet to connect to the internet, while keeping them private.
It helps in outbound internet traffic for instances in private subnets.

6. Elastic IP Address:
A static IP address designed for dynamic cloud computing.
You can associate an Elastic IP address with an instance in your VPC to ensure that it keeps the same public IP address, even if the instance is stopped and restarted.

7. VPC Peering
Allows you to connect one VPC with another VPC via a direct network route using private IP addresses.
Instances in either VPC can communicate with each other as if they are within the same network.

8. VPC Endpoint:

Enables you to privately connect your VPC to supported AWS services without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

Helps to keep traffic within the AWS network.

9. Security Groups:

Act as a virtual firewall for your instances to control inbound and outbound traffic.

You can define rules that allow or deny traffic based on protocols, ports, and source/destination IP addresses.

10. Network ACLs (Access Control Lists):

An optional layer of security for your VPC that acts as a stateless firewall.

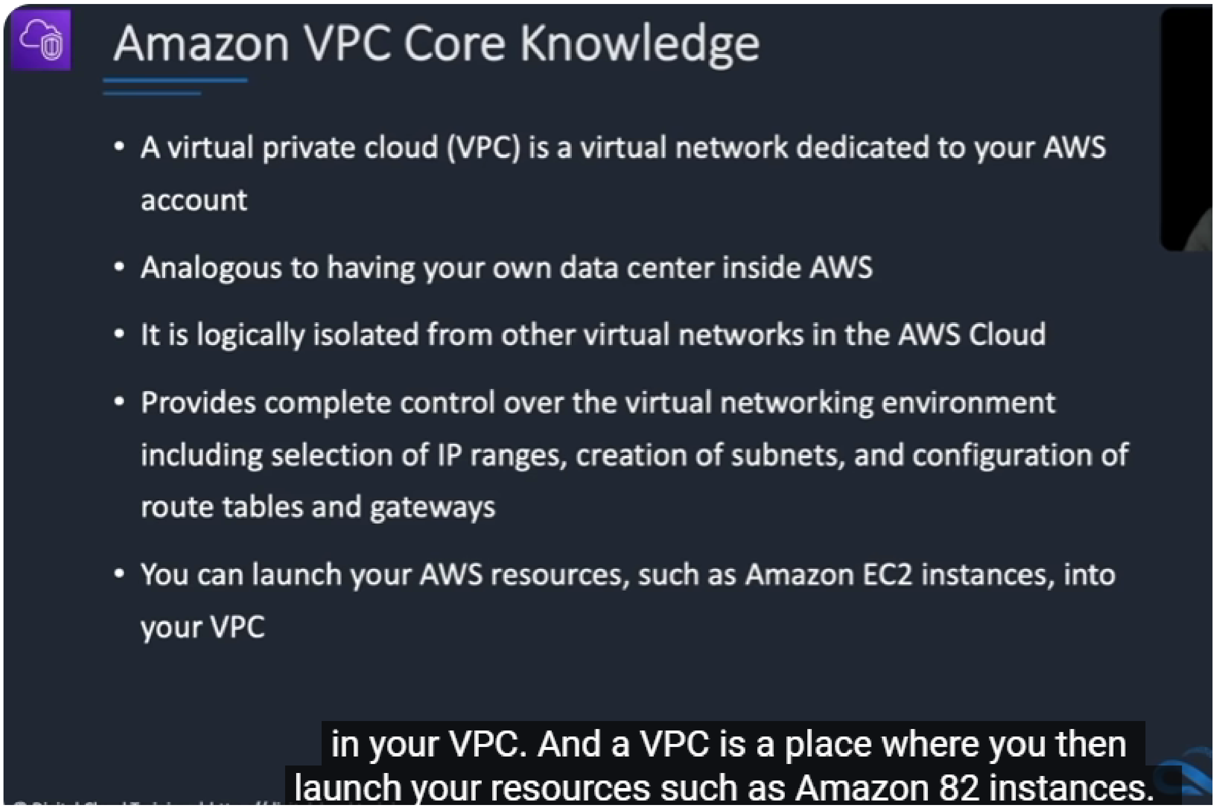
You can use network ACLs to control traffic at the subnet level by defining rules for inbound and outbound traffic.

11. VPN Connection:

Allows you to establish a secure connection between your on-premises data center and your VPC.

Utilizes IPSec VPN tunnels over the internet.

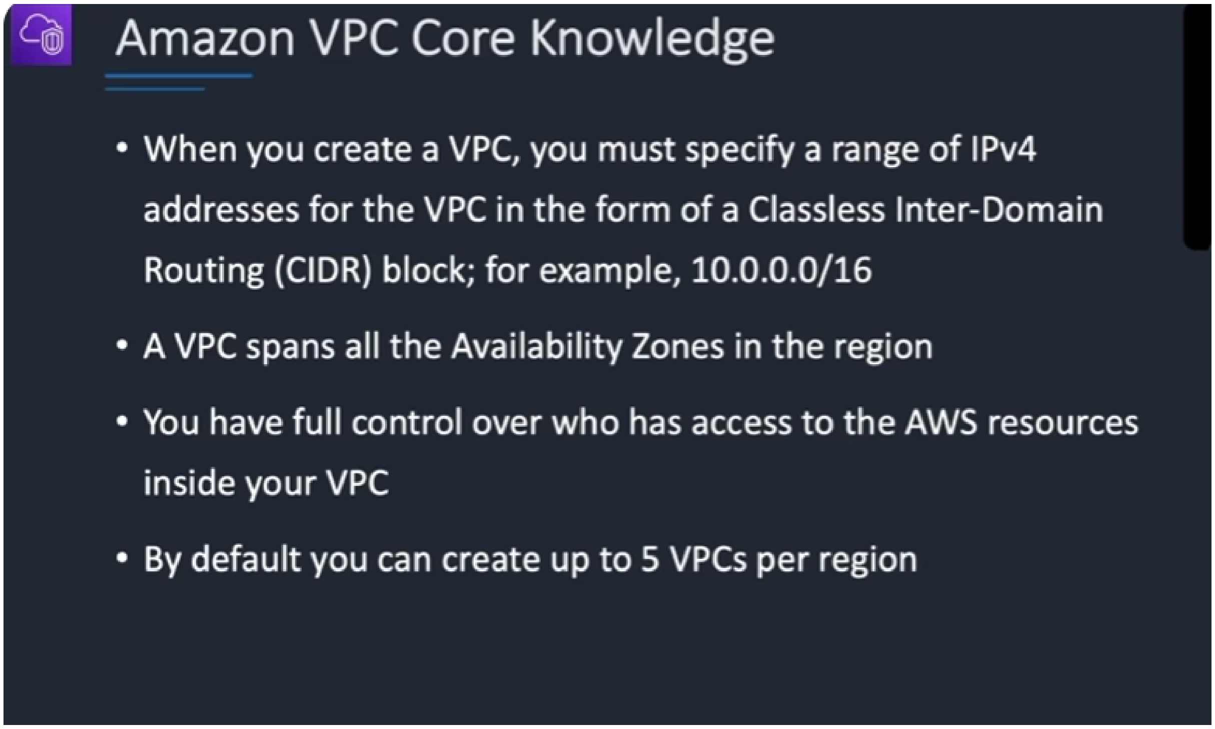
These components work together to provide a flexible and secure networking environment within AWS, allowing you to build and manage your infrastructure as needed.



Amazon VPC Core Knowledge

- A virtual private cloud (VPC) is a virtual network dedicated to your AWS account
- Analogous to having your own data center inside AWS
- It is logically isolated from other virtual networks in the AWS Cloud
- Provides complete control over the virtual networking environment including selection of IP ranges, creation of subnets, and configuration of route tables and gateways
- You can launch your AWS resources, such as Amazon EC2 instances, into your VPC

in your VPC. And a VPC is a place where you then
launch your resources such as Amazon 82 instances.



Amazon VPC Core Knowledge

- When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16
- A VPC spans all the Availability Zones in the region
- You have full control over who has access to the AWS resources inside your VPC
- By default you can create up to 5 VPCs per region

Classless inter domain routing (CIDR)

is a method for allocating IP addresses and routing Internet Protocol packets. It allows for more efficient use of IP address space and more flexible allocation of addresses. CIDR replaces the older class-based addressing system with a system that allows for variable-length subnet masking. This means that blocks of IP addresses can be allocated and divided more efficiently, reducing the amount of wasted address space. CIDR also allows for more efficient routing of IP packets, as it allows for aggregation of routes and reduces the size of routing tables. Overall, CIDR has helped to improve the scalability and efficiency of the Internet.