VIRTUAL PRIVATE CLOUD

By VIGNESH S

VPC

Provides a logically isolated section of the AWS Cloud where you can launch AWS resources.

It allows you to define your own IP address range, subnets, route tables, network gateways, and security settings.

You can create multiple VPCs within an AWS account, each operating independently.

Security for you network !

SUBNET

A subnet is a segmented portion of a VPC's IP address range.

It allows you to divide the IP address space of a VPC into smaller networks, which can be helpful for organizing and securing resources.

Each subnet is associated with a specific availability zone (AZ) within a region and can be public or private.

ROUTE TABLE

A route table is a set of rules that determine how network traffic is directed within a VPC.

Each subnet must be associated with a route table, which controls the traffic flow in and out of the subnet.

Route tables define the target for traffic destined for various IP ranges, such as the internet gateway, virtual private gateway, NAT gateway, VPC peering connection, or local subnet.

NACL

A NACL is an optional Stateless firewall that controls inbound and outbound traffic at the subnet level.

It operates at the protocol and port level and can allow or deny traffic based on rules you define.

Each rule in a NACL is evaluated sequentially, starting from the lowest rule number, until a matching rule is found.

STATELESS FIREWALL

NACLs operate at the subnet level and are considered stateless firewalls.

Stateless means that each network packet is evaluated independently, without considering the state of previous packets.

In the case of NACLs, inbound and outbound rules need to be explicitly defined for desired traffic flow.

For example, if you have an inbound rule to allow incoming SSH (Secure Shell) traffic on port 22, it won't automatically allow the response traffic. You need to create a separate outbound rule explicitly allowing the response traffic.

SECURITY GROUP

A security group acts as a virtual firewall for EC2 instances within a VPC.

It controls inbound and outbound traffic at the instance level, operating based on the allow rules.

Security groups are Stateful, meaning that if you allow inbound traffic, the response traffic is automatically allowed.

STATEFUL FIREWALL

Security Groups operate at the instance level and are associated with EC2 instances within a VPC.

Stateful firewalls maintain the state of established connections and automatically allow response traffic.

When a security group rule permits inbound traffic, the response traffic for that connection is automatically allowed, regardless of outbound rules.

For example, if you have a security group rule allowing inbound SSH traffic on port 22, the response traffic from the SSH session will be automatically allowed without creating a specific outbound rule.

NAT

NAT allows instances in a private subnet to communicate with the internet or other AWS services while hiding their private IP addresses.

AWS provides two types of NAT: NAT gateways and NAT instances.

NAT gateways are managed by AWS, highly available, and scalable, whereas NAT instances are EC2 instances configured to perform NAT.

ENDPOINT

An endpoint is a highly available and scalable AWS service that enables you to privately connect your VPC with AWS services without requiring internet access.

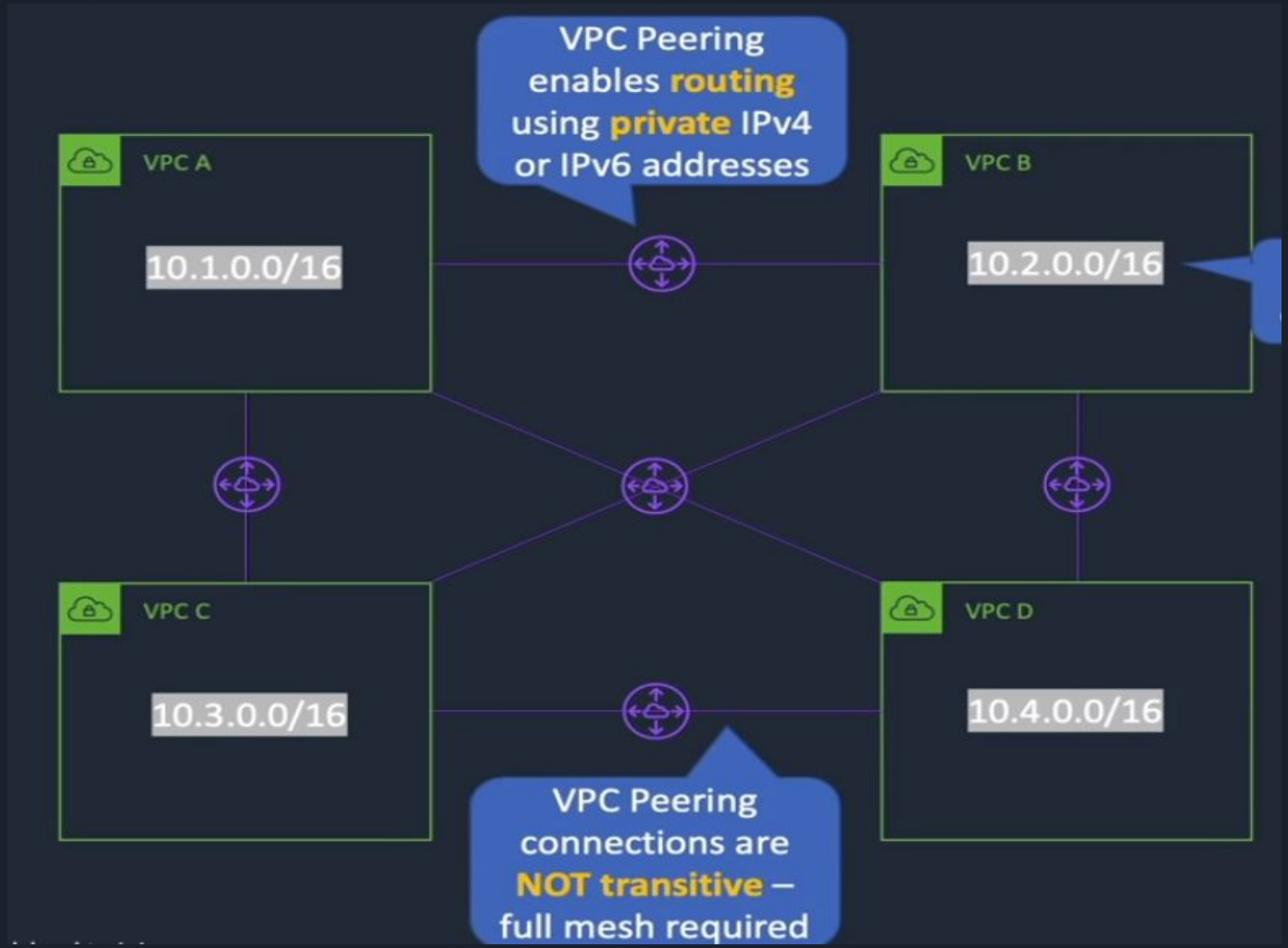
It provides a secure and efficient way to access services like Amazon S3, DynamoDB, or other AWS services without exposing them to the public internet.

PEERING

VPC peering allows you to connect two VPCs together, enabling communication between them using private IP addresses.

Peered VPCs can share resources and communicate as if they are part of the same network.

VPC peering can be established within the same AWS region or between different regions, and it supports transitive peering relationships.


VPC Peering enables routing using private IPv4 or IPv6 addresses
VPC A
10.1.0.0/16
VPC B
10.2.0.0/16
VPC C
10.3.0.0/16
VPC D
10.4.0.0/16
VPC Peering connections are NOT transitive – full mesh required