Module 4

Amazon Virtual Private Cloud(Amazon VPC)

A networking service that you can use to establish **boundaries around your AWS resources** is Amazon Virtual Private Cloud (Amazon VPC).

1. It enables an isolated section of the AWS cloud.
    a. In this isolated system, you can launch resources in a virtual network that you define.
    b. Withing a virtual private cloud, you can organize your resources into subnets.
2. A **subnet** is a section of a VPC that can contain resources such as Amazon EC2 instances.

To allow public traffic from the internet to access your VPC, you attack an **internet gateway** to the VPC.

An **internet gateway** is a connection between a VPC and the internet. Without an internet gateway, no one can access the resources within your VPC.

Virtual private gateway

To access private resources in VPC, you can use a virtual private gateway.

- The virtual private gateway is the component that allows protected internet traffic to enter into the VPC.
- A virtual private gateway enables you to establish a virtual private network(VPN) connection between your VPC and a private network, such as on-premises data center or internal corporate network.
- A virtual private gateway allows traffic into the VPC only if it is coming from an approved network.

AWS Direct Connect

It is a service that enables you to establish a dedicated private connection between your data center and a VPC.

The private connection that AWS Direct connect provides helps you to reduce network costs and increase the amount of bandwidth that can travel through your network.

Subnets:

A **subnet** is a section of a VPC that can contain resources such as Amazon EC2 instances.

Subnets can be public or private

a. Public subnet: It contains resources that need to be accessible by the public, such as an online store website.
b. Private subnets: It contain resource that should be accessible only through your private network, such as a database that contains customer’s personal information and order histories.

Network traffic in a VPC

When a customer requests data from an application hosted in AWS cloud, this request is sent as a packet.

A **packet** is a unit of data sent over the internet or a network.

It enters into a VPC through an internet gateway. Before a packet can enter into a subnet or exit from a subnet, it checks for permission.

These permission indicate who sent the packet and how the packet is trying to communicate with resources in a subnet.

The VPC component that checks packet permissions for subnets is a network access control list (ACL).

Network access control lists(ACLs)

A network access control list is a virtual firewall that controls inbound and outbound traffic at the subnet level.

Security groups

A security group is a virtual firewall that controls inbound and outbound traffic for an Amazon EC2 instance.

Domain name System (DNS)

Customers enter the web address into their browser, and they are able to access the website.

This happens because of DNS resolution. DNS resolution involves a customer DNS resolver communicating with a company DNS server.

Amazon Route 53

It is a DNS web server. It gives developers and businesses a reliable way to route end users to internet applications hosted in AWS.

Amazon route 54 connects user request to infrastructure running in AWS. It can route users to infrastructure outside of AWS.

- Another feature of Route 53 is the ability to manage the DNS records for domain names. You can register new domain names directly in route 53. You can also transfer DNS records for existing domain names managed by other domain registrars.