**Module 4**

**Introduction**

**What is Amazon Virtual Private Cloud (Amazon VPC)**

Is a network service that you can use to establish boundaries around your AWS resources

* Enables you to provision an isolated section of the AWS Cloud.
* You can organize your resources as subnets

**Internet getaway**

* Allows public traffic from the internet to access your VPC, you attach an internet gateway to VPC.
* Is a connection between a VPC and internet.

**Virtual Private Gateways**

* Used to access private resources in VPC
* Is the component that allows protected internet traffic to enter into the VPC.
* Enables you to establish a virtual private (VPN) connection between your VPC and a private network, such as an on-promises data-centre or internal corporate network.
* Allows traffic into VPC only if it’s coming from an approved network.

**Virtual Private Networks**

* Connection that encrypts (or protects) your internet traffic from all other request around it.

**What are AWS Direct Connect**

* Is a service that enables you to establish a dedicated private connection between your data centre and a VPC.
* Helps you to reduce network costs and increase the amount of bandwidth that can travel through your network

**Subnets and network access control list**

**What is subnet**

* Is a section of a VPC that can contain resources such as Amazon EC2 instances.
* Is a section of a VPC in which you can group resources on security or operational needs.
* Subnets can be private or public.

**Public Subnets**

* Contain resources that needs to be accessible by the network, such as an online store’s website

**Private subnets**

* Contain resources that should be accessible only through your private network, such as database that contains customers personal information and order histories

**Network Traffic in VPC**

* When customer request data from an application hosted in the AWS Cloud, this request is sent as packet.

**What is packet**

* Is a unit of data sent over the internet or network.
* It enters a VPC through an internet gateway. Before a packet can enter into a subnet or exist from a subnet, it checks for permission.
* These permissions indicate who sent the packet and how the packet is trying to communicate with the resources in subnet

**Network access control list (ACLs)**

* Is the VPC component that checks packet permissions for subnets
* Is a virtual firewall that controls inbound and outbound traffic at the subnet level
* You can use your default network ACL or create custom network ACLs

**Account default networks ACL**

* Allows all inbound and outbound traffic, but can modify it by adding your own rules

**Custom network ACLs**

* All inbound and outbound traffic is denied until you add rules specify which traffic to allow.

All network ACLs have an explicit deny rule. This rule ensures that if a packet doesn’t match any other rules on the list, the packet is denied.

**Stateless packet filtering**

* They remember nothing and check packets that cross the subnet border each way: inbound and outbound
* When a packet response for that request comes back to the subnet, the network ACL does not remember your previous request.
* The network ACL checks the packet response against its list of rules to determine whether to allow or deny

The VPC component that checks packet permissions for an Amazon EC2 instance is a security group

**Security Group**

* A security group is a virtual firewall that controls inbound and outbound traffic for an Amazon EC2 instance
* By default, security group denies all inbound traffic and allows outbound traffic. You can add custom rules to configure which traffic to allow or deny.

**Stateful packet filtering**

* Security groups perform stateful packet filtering.
* They remember previous made for incoming packets
* When a packet response for that request return to the instance, the security group remembers your previous request.
* The security group allows the response to proceed, regardless of inbound security rules.

**Domain Name System (DNS)**

* Is the process of translating a domain name to an IP address

Example of what happens you want to visit any website

* When you enter the domain name into your browser, this request is sent to a customer DNS resolver
* The customer DNS resolver asks the company DNS server for the IP address that corresponds to AnyCompany’s websites
* The company DNS server responds by providing the IP address for AnyCompany’s website, 192.0.20

**Amazon Route 53**

* Is a DNS web service.
* It gives developers and business a reliable way to route end users to internet applications hosted AWS
* Ability to manage the DNS records for domain names.
* You can register a new domain name directly in Route 53
* You can also transfer DNS records for existing domain names managed by other domain registers
* Allows you to manage all your domain names in single location