**NETWORKING**

**AMAZON VIRTUAL PRIVATE CLOUD:**

A VPC lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. These resources can be public facing so they have access to the internet, or private with no internet access, usually for backend services like databases or application servers. The public and private grouping of resources are known as subnets and they are ranges of IP addresses in your VPC.

**Connectivity to AWS**

**Amazon Virtual Private Cloud**:

A networking service that you can use to establish boundaries around your AWS resources is [**Amazon Virtual Private Cloud (Amazon VPC).**](https://aws.amazon.com/vpc/)

Amazon VPC enables you to provision an isolated section of the AWS Cloud. In this isolated section, you can launch resources in a virtual network that you define. Within a virtual private cloud (VPC), you can organize your resources into subnets. A subnet is a section of a VPC that can contain resources such as Amazon EC2 instances.

**Internet Gateway**

To allow public traffic from the internet to access your VPC, you attach an **internet gateway** to the VPC.An internet gateway is a connection between a VPC and the internet. You can think of an internet gateway as being similar to a doorway that customers use to enter the coffee shop. Without an internet gateway, no one can access the resources within your VPC.



VPC that includes only private resources

**Virtual private gateway**

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



A virtual private gateway enables you to establish a virtual private network (VPN) connection between your VPC and a private network, such as an 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**

AWS Direct Connect is a service that lets 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 and network access control list**

AWS has a wide range of tools that cover every layer of security: network hardening, application security, user identity, authentication and authorization, distributed denial-of-service or DDoS prevention, data integrity, encryption, much more

packets are messages from the internet, and every packet that crosses the subnet boundaries gets checked against something called a network access control list or network ACL. This check is to see if the packet has permissions to either leave or enter the subnet based on who it was sent from and how it's trying to communicate.

N**etwork ACLs** check traffic going into and leaving a subnet, just like passport control.

network ACL only gets to evaluate a packet if it crosses a subnet boundary, in or out. It doesn't evaluate if a packet can reach a specific EC2 instance or not.

you need instance level network security as well. To solve instance level access questions, we introduce **security groups**

Every EC2 instance, when it's launched, automatically comes with a security group. And by default, the security group does not allow any traffic into the instance at all.

Security Group : Stateful

Network ACL: Stateless

Network ACL is for subnet region and Security groups are for ec2 instances inside it.

**Subnets**:

A subnet is a section of a VPC in which you can group resources based on security or operational needs. Subnets can be public or private.

Public subnets contain resources that need to be accessible by the public, such as an online store’s website.

Private subnets contain resources that should be accessible only through your private network, such as a database that contains customers’ personal information and order histories.

In a VPC, subnets can communicate with each other. For example, you might have an application that involves Amazon EC2 instances in a public subnet communicating with databases that are located in a private subnet.



**Network Traffic in VPC**

When a customer requests data from an application hosted in the 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 permissions. These permissions indicate who sent the packet and how the packet is trying to communicate with the resources in a subnet.The VPC component that checks packet permissions for subnets is a network access control list (ACL).

**Network ACL**

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

Each AWS account includes a default network ACL. When configuring your VPC, you can use your account’s default network ACL or create custom network ACLs.

By default, your account’s default network ACL **allows** all inbound and outbound traffic, but you can modify it by adding your own rules. For custom network ACLs, all inbound and outbound traffic is denied until you add rules to specify which traffic to allow. Additionally, all network ACLs have an explicit deny rule. This rule ensures that if a packet doesn’t match any of the other rules on the list, the packet is denied.



**Stateless Packet Filtering**

Network ACLs perform stateless packet filtering. They remember nothing and check packets that cross the subnet border each way: inbound and outbound.



After a packet has entered a subnet, it must have its permissions evaluated for resources within the subnet, such as Amazon EC2 instances.

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.

a security group **denies** all inbound traffic and allows all outbound traffic



**Stateful Packet Filtering**

Security groups perform stateful packet filtering. They remember previous decisions made for incoming packets.

**Private Subnet**: isolate database containing customer’s personal informations

**Virtual Private Gateway**: Create VPN connection between VPC and internal corporate network

**Public Subnet**: Support customer facing website

**AWS Direct Connect** : Establish a dedicated connection between on-premises data center and VPC

**GLOBAL NETWORKING**

**Domain Name System**



**Amazon Route 53**

Amazon Route 53(opens in a new tab) is a DNS web service. It gives developers and businesses a reliable way to route end users to internet applications hosted in AWS.

Amazon Route 53 connects user requests to infrastructure running in AWS (such as Amazon EC2 instances and load balancers). 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 registrar

Example: **How Amazon Route 53 and Amazon CloudFront deliver content**

****

* A customer requests data from the application by going to AnyCompany’s website.
* Amazon Route 53 uses DNS resolution to identify AnyCompany.com’s corresponding IP address, 192.0.2.0. This information is sent back to the customer.
* The customer’s request is sent to the nearest edge location through Amazon CloudFront.
* Amazon CloudFront connects to the Application Load Balancer, which sends the incoming packet to an Amazon EC2 instance.