**VPC**

Amazon VPC (Amazon Virtual Private Cloud) is a service that allows you to launch AWS resources in a logically isolated virtual network that you identify. You have full control over your virtual networking environment, including IP address range selection, subnet construction, and route table and network gateway configuration. For most resources in your network, you can use both IPv4 and IPv6. For web servers that have internet connectivity, you can build a public-facing subnet. It also allows you to put your backend structures, such as databases or application servers, in a private-facing subnet that is not accessible from the internet. To help manage access to Amazon EC2 instances in ea, Amazon VPC allows you to use several layers of protection, such as security groups and network access control lists.

**SUBNETS**

**Subnetwork or subnet** is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.AWS provides two types of subnetting one is Public which allow the internet to access the machine and another is private which is hidden from the internet.

AWS provides two types of subnetting one is Public which allow the internet to access the machine and another is private which is hidden from the internet. Instance is a virtual server in the AWS cloud.

**ROUTE TABLES**

Each route in a table specifies a destination and a target. Every route table contains a local route for communication within the VPC. This route is added by default to all route tables. If your VPC has more than one IPv4 CIDR block, your route tables contain a local route for each IPv4 CIDR block. If you've associated an IPv6 CIDR block with your VPC, your route tables contain a local route for the IPv6 CIDR block. You cannot modify or delete these routes in a subnet route table or in the main route table. When you create a VPC, it automatically has a main route table. The main route table controls the routing for all subnets that are not explicitly associated with any other route table. On the Route Tables page in the Amazon VPC console, you can view the main route table for a VPC by looking for Yes in the Main column.

By default, when you create a non-default VPC, the main route table contains only a local route. When you use the VPC wizard in the console to create a non-default VPC with a NAT gateway or virtual private gateway, the wizard automatically adds routes to the main route table for those gateways.

**INTERNET GATEWAY**

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. For more information, see [Enabling internet access](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html#vpc-igw-internet-access).

An internet gateway supports IPv4 and IPv6 traffic. It does not cause availability risks or bandwidth constraints on your network traffic. There's no additional charge for having an internet gateway in your account.

**SECURITY GROUPS**

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups.

If you launch an instance using the Amazon EC2 API or a command line tool and you don't specify a security group, the instance is automatically assigned to the default security group for the VPC. If you launch an instance using the Amazon EC2 console, you have an option to create a new security group for the instance.

For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic. This section describes the basic things that you need to know about security groups for your VPC and their rules.

**NETWORK ACLs**

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set additional layer of security to your VPC. The default network ACL is configured to allow all traffic to flow in and out of the subnets with which it is associated. Each network ACL also includes a rule whose rule number is an asterisk. This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied. You can't modify or remove this rule up network ACLs with rules similar to your security groups.

