Amazon Virtual Private Cloud

* Amazon VPC allows us to launch **AWS resources in an isolated network** that is defined by us in a **more private and secure environment.**
* This feature enables us to **increase the security level** of the AWS resources.
* The AWS resources can be protected using **multilayered VPC** which includes **security groups** and **Network Access Control list**.
* The VPC **security group** provides security at **instance level** which acts like a firewall and controls both inbound and outbound traffic.
* The VPC **NACL** provides security at **Network Level** i.e **subnet level** which acts like a firewall for associated subnets and controls inbound and outbound traffic.

The following are the key concepts for VPCs:

* **Virtual private cloud (VPC)** — A virtual network dedicated to your AWS account.
* **Subnet** — A range of IP addresses in your VPC.
* **Route table** — A set of rules, called routes, that are used to determine where network traffic is directed.
* **Internet gateway** — A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.
* **VPC endpoint** — Enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. For more information, see [AWS PrivateLink and VPC endpoints](https://docs.aws.amazon.com/vpc/latest/userguide/endpoint-services-overview.html).
* **CIDR block** —Classless Inter-Domain Routing. An internet protocol address allocation and route aggregation methodology. For more information, see [Classless Inter-Domain Routing](http://en.wikipedia.org/wiki/CIDR_notation) in Wikipedia.
* **NACL** – NACL stands for **Network Access Control Lists**. It is a security layer for your VPC that controls the traffic in and out of one or more subnets. It is an optional layer for your VPC. You can set up a Network ACL similar to the security group that adds an additional layer of security to your VPC.
* **Nat Gateway :** If you want access your instance which is in private subnet the you have to use Nat gateway.

## Pricing for Amazon VPC

There's no additional charge for using a VPC. There are charges for some VPC components, such as NAT gateways, Reachability Analyzer, and traffic mirroring

For pricing please click on below link

<https://aws.amazon.com/vpc/pricing/>

**The main difference is the route for 0.0.0.0/0 in the associated route table.**

A private subnet sets that route to a NAT instance. Private subnet instances only need a private ip and internet traffic is routed through the NAT in the public subnet. You could also have no route to 0.0.0.0/0 to make it a truly **private** subnet with no internet access in or out.

A public subnet routes 0.0.0.0/0 through an Internet Gateway (igw). Instances in a public subnet require public IPs to talk to the internet.

The warning appears even for private subnets, but the instance is only accessible inside your vpc.