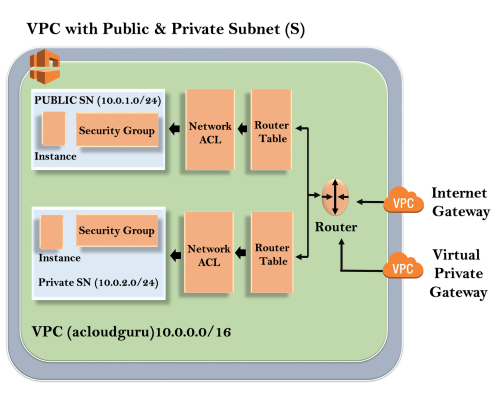
What is VPC

* VPC stands for Virtual Private Cloud.
* Amazon Virtual Private Cloud (Amazon VPC) provides a logically isolated area of the AWS cloud where you can launch AWS resources in a virtual network that you define.
* You have complete control over your virtual networking environment, including a selection of your IP address range, the creation of subnets, and configuration of route tables and network gateways.

## **Architecture of VPC**



The outer line represents the region, and the region is us-east-1. Inside the region, we have VPC, and outside the VPC, we have internet gateway and virtual private gateway. ~~Internet Gateway and Virtual Private Gateway are the ways of connecting to the VPC.~~ Both these connections go to the router in a VPC and then router directs the traffic to the route table. Route table will then direct the traffic to Network ACL. Network ACL is the firewall or much like security groups. Network ACL are statelist which allows as well as deny the roles. You can also block the IP address on your Network ACL. Now, move over to the security group that accesses another line against the EC2 instance. It has two subnets, i.e., Public and Private subnet. In public subnet, the internet is accessible by an EC2 instance, but in private subnet, an EC2 instance cannot access the internet on their own. We can connect the instances. To connect an instance, move over to the public subnet and then it SSH to the private subnet. This is known as jump boxes. In this way, we can connect an instance in public subnet to an instance in private subnet.

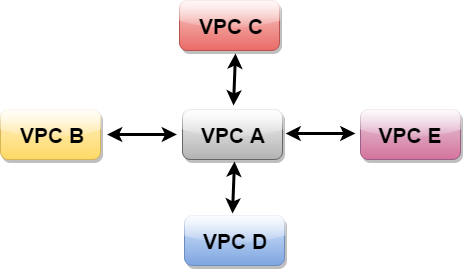
**Some ranges are reserved for private subnet:**

* 10.0.0.0 - 10.255.255.255 (10/8 prefix)
* 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
* 192.168.0.0 - 192.168.255.255 (192.108/16 prefix)

## **VPC Peering**

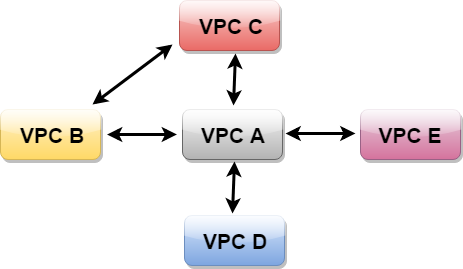
* VPC Peering is a networking connection that allows you to connect one VPC with another VPC through a direct network route using private IP addresses.
* Instances behave as if they were on the same private network.
* You can peer VPC's with other AWS accounts as well as other VPCs in the same account.
* Peering is in a star configuration, i.e., 1 VPC peers other 4 VPCs.
* It has no **Transitive Peering!!**.
* You can peer between regions. Suppose you have one VPC in one region and other VPC in another region, then you can peer the VPCs between different regions.

**Let's understand the example of non-transitive peering through an example.**



The above figure shows that VPC B has peered to the VPC A, so instance in VPC B can talk to VPC A. However, VPC B cannot talk to VPC C through VPC A. This is known as Non-Transitive Peering, i.e., both VPC C and VPC B are not directly linked so they cannot talk to each other.

o, to communicate between VPC B and VPC C, we need to peer them as shown in the below figure.

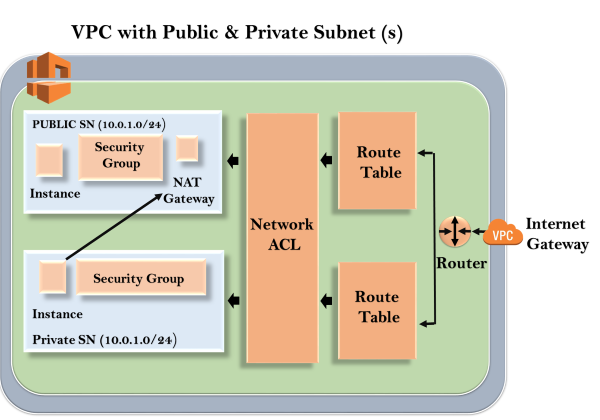


# Internet Gateway 🡪

# An internet gateway enables resources in your public subnets (such as EC2 instances) to connect to the internet if the resource has a public IPv4 address or an IPv6 address. Similarly, resources on the internet can initiate a connection to resources in your subnet using the public IPv4 address or IPv6 address. For example, an internet gateway enables you to connect to an EC2 instance in AWS using your local computer.

| **Component** | **Default VPC** | **Nondefault VPC** |
| --- | --- | --- |
| Internet gateway | Yes | No |
| Route table with route to internet gateway for IPv4 traffic (0.0.0.0/0) | Yes | No |
| Route table with route to internet gateway for IPv6 traffic (::/0) | No | No |
| Public IPv4 address automatically assigned to instance launched into subnet | Yes (default subnet) | No (nondefault subnet) |
| IPv6 address automatically assigned to instance launched into subnet | No (default subnet) | No (nondefault subnet) |

NAT Gateways

* NAT stands for **Network Address Translation**.
* If you want your EC2 instance in a private subnet can access the internet, this can be achieved only when it can communicate to the internet. However, we do not want to make a subnet public as we want to maintain the degree of control. To overcome the problem, we need to create either NAT Gateways or NAT Instances.
* In real time, NAT Gateways are highly used than NAT instances as NAT instances are an individual EC2 instances, and NAT Gateways are highly available across multiple availability zones, and they are not on a single EC2 instance.
* 

**Let's first start with NAT instance and how to create them.**

### **Important points related to NAT instance:**

* When creating a NAT instance, you need to disable source/destination check on the instance.
* NAT instances must be available in a public subnet.
* There must be some route from private subnet to NAT instance, in order to work for this.
* The amount of traffic that NAT instances can support depends upon the instance size.
* You can create high availability using Autoscaling groups, multiple subnets in different AZ's.
* NAT instance is configured with the security group.

### **Important points related to NAT Gateways:**

* It is redundant inside the availability zone.
* It is preferred by an enterprise.
* It starts at 5Gbps and scales up to 45 Gbps.
* It is not configured with the security groups.
* In NAT Gateways, there is no need to disable the source/destination checks.

# 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.

## **Some important related to Network ACL:**

* Your custom VPC automatically comes with the default Network ACL which includes all inbound and outbound ipv4 traffic.
* You can also create a custom network ACL and associates with a subnet. By default, a custom Network ACL denies all the inbound and outbound ipv4 traffic until you add rules.
* If you do not explicitly create Network ACL, then the default Network ACL automatically associated with the subnet.
* You can associate multiple subnets with a Network ACL. However, a subnet can be associated with the single Network ACL at a time.
* Network ACL is associated with both inbound and outbound rules that can either deny or allow the rules.
* A Network ACL contains numbered lists of rules that are evaluated in order, starting from the lowest numbered rule, to determine whether the traffic goes in or out of the subnet associated with the Network ACL. The highest numbered rule can be 32766. It is recommended to create new rules with increments (For example, increments of 10 or 100) so that you can easily add new rules where you need later on.

# What is a Security Group?

It adds a security layer to EC2 instances that control both inbound and outbound traffic at the instance level.

## **What is NACL?**

NACL also adds an additional layer of security associated with subnets that control both inbound and outbound traffic at the subnet level.

## **Combining Security Group and NACL**

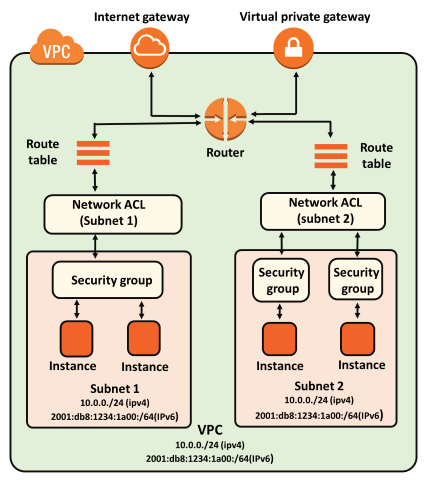
Maximum number of rules that exist per NACL: 20

Maximum number of rules that can exist per Security Group: 50

Maximum number of Security Groups that can exist per instance: 5

Maximum number of rules that can exist per instance: 5\*50 + 20 = 270

## **Differences b/w Security Group and NACL**



|  |  |
| --- | --- |
| **Security Group** | **NACL (Network Access Control List)** |
| It supports only **allow** rules, and by default, all the rules are denied(অস্বীকার). You cannot deny the rule for establishing a connection. | It supports both **allow and deny** rules, and by default, all the rules are denied. You need to add the rule which you can either allow or deny it. |
| It is a **stateful** means that any changes made in the inbound rule will be automatically reflected in the outbound rule. For example, If you are allowing an incoming port 80, then you also have to add the outbound rule explicitly. | It is a **stateless** means that any changes made in the inbound rule will not reflect the outbound rule, i.e., you need to add the outbound rule separately. For example, if you add an inbound rule port number 80, then you also have to explicitly add the outbound rule. |
| It is associated with an EC2 instance. | It is associated with a subnet. |
| All the rules are evaluated before deciding whether to allow the traffic. | Rules are evaluated in order, starting from the lowest number. |
| Security Group is applied to an instance only when you specify a security group while launching an instance. | NACL has applied automatically to all the instances which are associated with an instance. |
| It is the first layer of defense. | It is the second layer of defense. |