

VIRTUAL PRIVATE CLOUD (VPC)

- A virtual private cloud is a virtual network that closely resembles a traditional networking that you operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
- VPC is a virtual network of data center inside AWS for one client.
- It is logically isolated from other virtual network in the AWS cloud.
- Maximum 5 VPC can be created in one region and 200 subnets in 1 VPC.
- We can allocate maximum 5 Elastic IP.
- Once we created VPC, DHCP, NACL and security group will automatically created.
- A VPC is confined to an AWS region and does not extend between regions.
- Once the VPC is created you cannot change its CIDR block range.
- If you need a different CIDR size create a new VPC.
- The different subnets within a VPC cannot overlap.
- You can however expand your VPC CIDR by adding new/extra IP address ranges (except GovCloud and AWS China)

Components of VPC:

- A. CIDR and IP address subnets
- B. Implied Router and Routing table
- C. Internet Gateway
- D. Security Group
- E. NACL
- F. Virtual Private Gateway
- G. Peering Connectors
- H. Elastic IP

Types of VPC:

VPC is of 2 types:

- i. Default VPC
- ii. Custom VPC

i. Default VPC:

- Created in each AWS region when an AWS account is created.
- Has default CIDR, security group, NACL and route table settings.
- Has an internet gateway by default.

ii. Custom VPC:

- It is a VPC and AWS account owner creates.
- AWS user creating the Custom VPC can decide the CIDR.
- It has its own default security group, NACL and route tables.

- It doesn't have an internet gateway by default, one needs to be created if needed.

Public Subnet: if a subnet's traffic is routed to an internet gateway, the subnet is known as public subnet. If you want your instance in a public subnet to communicate with the internet over IPV4, it must have a public IPV4 address or an Elastic IP address.

Private Subnet: if a subnet doesn't have a route to the internet gateway, the subnet is known as private subnet. When you create a VPC you must specify an IPV4 CIDR block for the VPC. The allowed blocks size is between /16 to /28 networks. The first four and last IP address of subnet cannot be assigned.

The instances in the public subnet can send outbound traffic directly to the internet, but instances in private subnet can't.

For e.g: 10.0.0.0- network address

10.0.0.1- reserved by AWS for the VPC router

10.0.0.2- reserved by AWS the IP address of DNS server

10.0.0.3- reserved for future use

10.0.0.255- broadcast address

Note: AWS do not support broadcast in a VPC but reserve this address.

B. Implied Router and Routing Table:

- It is the central routing function.
- It connects the different AZ together and connects the VPC to the internet gateway.
- You can have up to 200 route tables per VPC.
- You can have up to 50 routes entries per route table.
- Each subnet must be associated with only one route table at any given time only.
- If you don't specify a subnet to route table association, the subnet will be associated with the default VPC route table.
- You can also edit the main route table if you need but you cannot delete the main route table.
- However you can make a custom route table manually become the main route table then you can delete the former main as it is no longer a main route table.
- You can associate multiple subnets with the same route table.

C. Internet Gateway:

- An internet gateway is a virtual router that connects a VPC to the internet.
- Default VPC is already attached with an internet gateway.

- If you create a new VPC then you must attach the internet gateway in order to access the internet.
- Ensure that your subnet's route table points to the internet gateway.
- It performs NAT between your private and public IPV4 address.
- It supports both IPV4 and IPV6.

NAT Gateway:

- You can use a network address translation gateway to enable instances in a private subnet to connect to the internet or other AWS services but prevent the internet from initiating a connection with those instances.
- You are charged for creating and using a NAT gateway in your account. NAT gateway hourly usage and data processing rates apply. Amazon EC2 charges for data transfer also apply.
- To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside.
- You must also specify an elastic IP address to associate with NAT gateway when you create it.
- No need to assign public IP address to your private instance.
- After you have created a NAT gateway you must update the route table associated with one or more of your private subnets to point internet bound traffic to the NAT gateway. This enables instances in your private subnet to communicate with the internet.
- Deleting a NAT gateway, disassociates its elastic IP address, but does not release the address from your account.

D. Security Group:

- It is a virtual firewall works at ENI level.
- Up to 5 security groups per EC2 instance interface can be applied.
- Can only have permit rules, cannot have deny rules.
- Stateful, return traffic of allowed inbound traffic is allowed even if there are no rules to allow it.

E. NACL:

- It is a function performed on the implied router.
- NACL 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.
- Your VPC automatically comes with a modifiable default NACL. By default, it allows all inbound and outbound IPV4 traffic and if applicable IPV6 traffic.
- You can create a custom NACL and associate it with a subnet. By default each NACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a NACL. If you don't explicitly associate a subnet with a NACL, the Subnet is automatically associated with the default NACL.

- You can associate a NACL with multiple subnets; however a subnet can be associated with only one NACL at a time. When you associate a NACL with a subnet the previous association is removed.
- A NACL contains a numbered list of rules that we evaluate in order starting with the lowest numbered rule.
- The highest number that you can use for a rule is 32766. Recommended that you start by creating rules with rule numbers that a multiple of 100, so that you can insert new rules where you need later.
- It functions at the subnet level.
- NACL are stateless, outbound traffic for an allowed inbound traffic must be explicitly allowed too.
- You can have permit and deny rules in a NACL.

VPC Peering:

- A VPC peering connection is a network connection between two VPC that enables you to route traffic between them using private IPV4 addresses or IPV6 addresses.
- Instances in either VPC can communicate with each other as if they are within the same network.
- You can create a VPC peering connection between your own VPC or with a VPC in another AWS account. The VPC can be in different region.

VPC EndPoint: A VPC endpoint enables you to privately connect your VPC to supported AWS services, instances in your VPC do not require public IP address to communicate with resources in the service. Endpoints are virtual devices.

Difference between security group and NACL.

Security Group	NACL
<ul style="list-style-type: none"> ➤ Operate at instance level. ➤ Supports allow rules only. ➤ Stateful, return traffic is automatically allowed. ➤ Applies to an instance only. 	<ul style="list-style-type: none"> ➤ Operates at the subnet level. ➤ It permits allow as well as deny rules. ➤ Stateless, return traffic must be explicitly allowed by rules. ➤ Applies to all instances in the subnet.