Amazon Virtual Private Cloud (VPC)

What is VPC ?

Amazon Virtual Private Cloud (Amazon 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. A VPC is a virtual data center in the cloud. You have complete control over your virtual networking environment, including selection of your own private IP address range, creation of subnets and configuration of route tables and network gateways and so on.

Important Components of VPC :

Subnets : A subnet can be thought of as dividing a large network into smaller networks. It helps to isolate the resources logically and also helps to maintain the security in a better way.

Route Table (RT) : A route table contains a set of rules called routes which determine where traffic has to be directed.

Internet Gateway (IGW) : An IGW is a horizontally scaled, redundant and highly available VPC component that allows communication between instances and the internet. Only one IGW can be attached to a VPC at a time.

Security Groups (SG) : Security groups are a set of firewall rules that controls the traffic for your instance. In Amazon Firewall the only action that can be carried out is allow. You cannot create a rule to deny.

Network Access Control Lists (NACL) : 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 up network ACLs with rules similar to your security groups in order to add an 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 to which it is associated.

Network Gateway (NAT) : NAT maps the private IP addresses to the public address on the way out and vice versa on the way in. A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet.

Virtual Private Gateway (VGW) : A virtual private gateway is the VPN concentrator on the Amazon side of the VPN connection.

Customer Gateway (CGW) : An Amazon VPC VPN connection links your data center (or network) to your Amazon VPC (virtual private cloud).

Virtual Private Network (VPN) : It is a popular internet security method which was originally designed for large organizations where employees needed to connect to a certain computer from different locations or network.

Peering Connection : it's a mechanism to route traffic via private IP addresses between two peered VPCs securely without leaving Amazon own Network.

VPC Endpoints : Enables private connectivity for your service in AWS without using an Internet Gateway, VPN, Network Address Translation (NAT) devices, or firewall proxies.

Egress-only Internet Gateway: A stateful gateway that provides egress only access for IPv6 traffic from the VPC to the Internet.

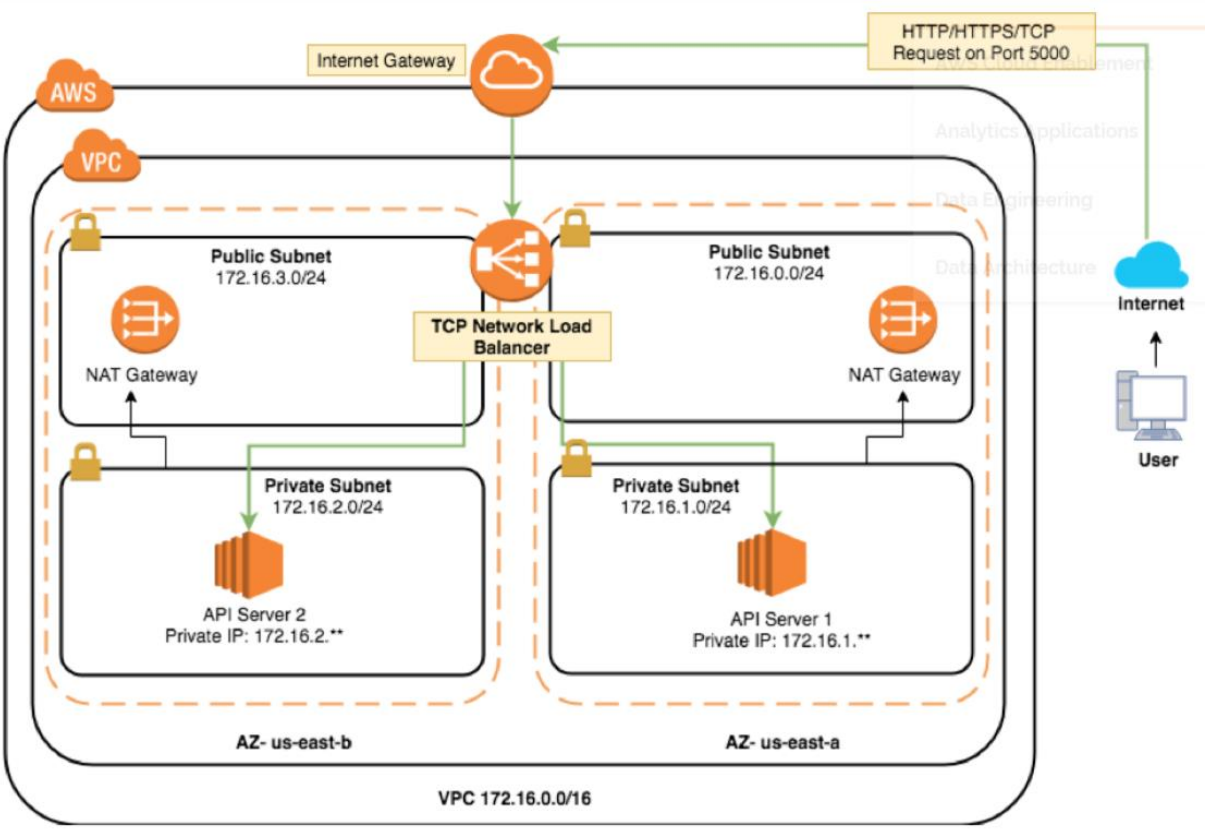
VPC and Subnet Sizing :

- The allowed block size is between /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses)
- Recommended IP CIDR ranges are below

RFC 1918 range	Example CIDR block
10.0.0.0 - 10.255.255.255 (10/8 prefix)	Your VPC must be /16 or smaller, for example, 10.0.0.0/16.
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)	Your VPC must be /16 or smaller, for example, 172.31.0.0/16.
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)	Your VPC can be smaller, for example 192.168.0.0/20.

- The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance
- **Example :** 10.0.0.0/24
    - 10.0.0.0: Network address.
    - 10.0.0.1: Reserved by AWS for the VPC router
    - 10.0.0.2: Reserved by AWS for DNS
    - 10.0.0.3: Reserved by AWS for future use.
    - 10.0.0.255: Network broadcast address.

VPC Architecture Diagram :



NOTE : VPC has no cost at all until and unless you created some resources inside the VPC and sending some data outside of the VPC. Make sure to delete the default VPC from your account and create your own VPC to get better security and control over the Network design.

VPC Limitations : (Please read the documentations for better understanding of limitations)

Link : https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html

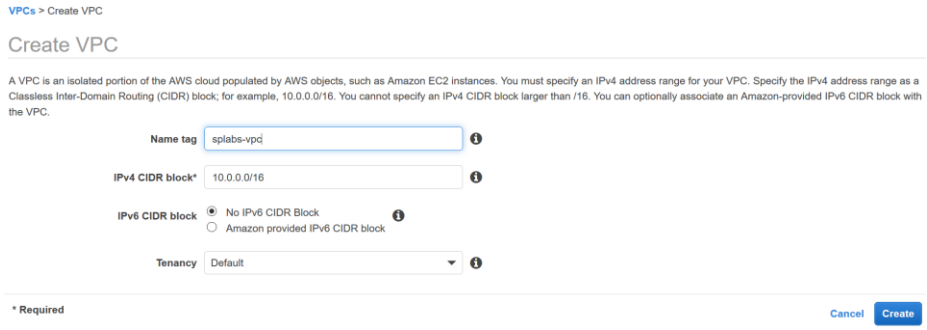
How to setup or create a VPC :

Ref Link : https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html#Create-VPC

Create Your Own New VPC :

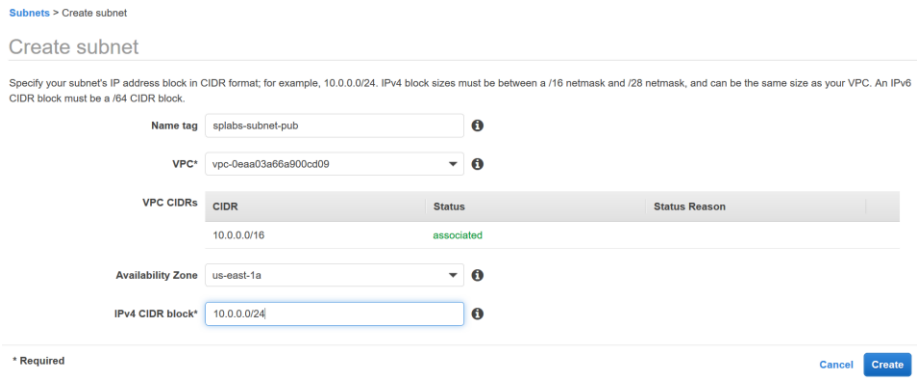
1. Go to the VPC console -> choose **Your VPCs**, **Create VPC**
2. Specify the following VPC details as necessary and choose **Create**.
    a. Name Tag : Name of the VPC
    b. IPv4 CIDR Block : Specify CIDR range for the VPC Network (Eg. 10.0.0.0/16)

c. Tenancy : Select a tenancy option. Dedicated tenancy ensures that your instances run on single-tenant hardware.
Note : Select Default, don't select Dedicated, because Dedicated one has cost.



Create Subnets for the VPC :

1. Go to VPC console -> choose **Subnets**, **Create subnet**.
2. Specify the subnet details as necessary and choose **Create**.
    a. Name Tag : Name of the Subnet
    b. VPC : Select the VPC in which you are creating the Subnet
    c. Availability Zone : Select the Subnet on which your subnet will get created.
    d. IPv4 CIDR Block : Specify the CIDR range for the Subnet (Eg. 10.0.0.0/24)
    e. Click on Create.
    f. repeat the steps above to create more subnets in your VPC.

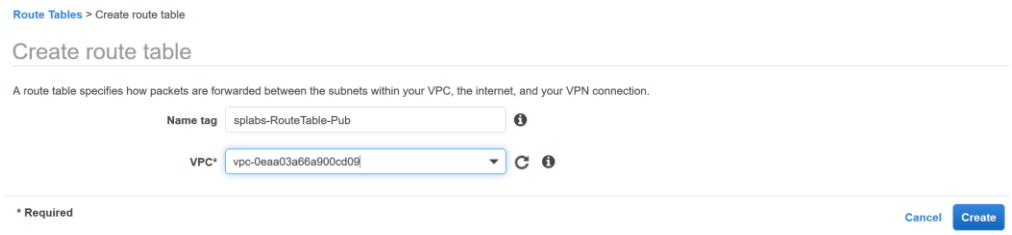


Create Internet Gateway and Attach to the VPC :

1. Go to VPC Console -> choose **Internet Gateways**, and then choose **Create internet gateway**.
2. Provide a Name Tag and click on Create.
3. Select the internet gateway that you just created, and then choose **Actions, Attach to VPC**
4. Select your VPC from the list, and then choose **Attach**.

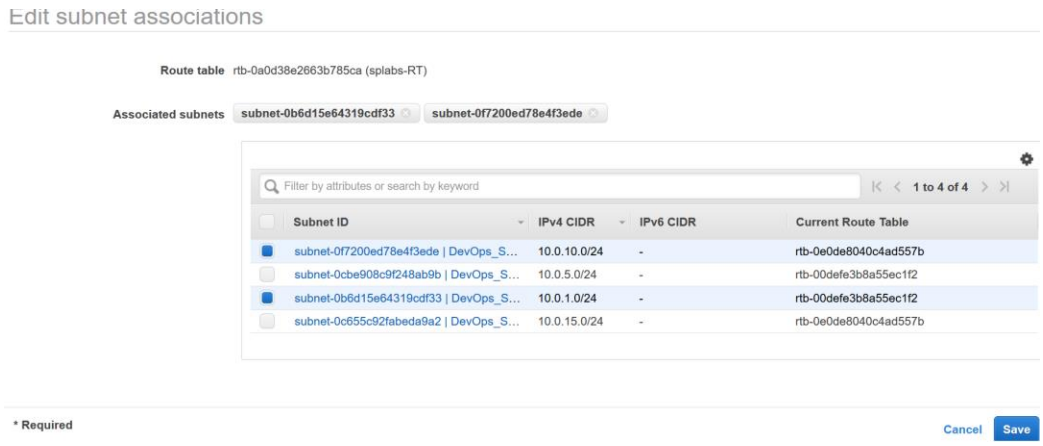
Create Route Table for the VPC :

1. Go to VPC Console -> choose **Route Tables** -> click on **Create route table**.
2. Provide a name Tag for the Route Table and select the VPC from drop down list and click on Create.



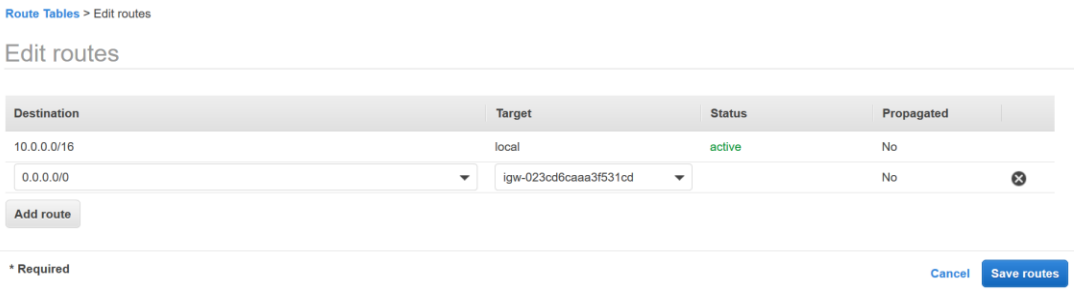
Associate Subnets to the Route Table :

1. Go to VPC Console -> Select **Route Tables** -> Select the **Route Table** from the list on which subnets has to be associated -> Click on **Subnet Association** -> Click on **Edit Subnet Association** -> Select the required **Subnets** to be associate -> Then click on **Save**.



Create Routes on the Route Table :

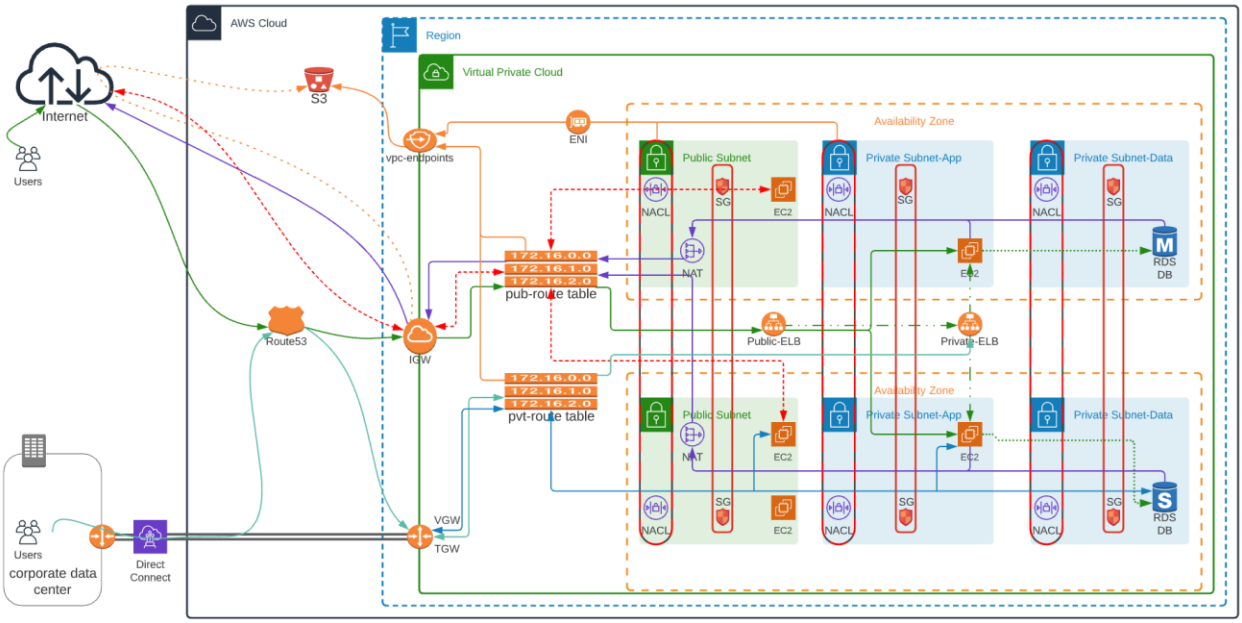
1. Go to VPC Console -> Select **Route Tables** -> Select the **Route Table** from the list on which **Routes** has to be created -> Click on **Routes** -> Click on **Edit Routes** -> Click on **Add Route** -> Provide the Source and Target information and click on **Save Routes**.

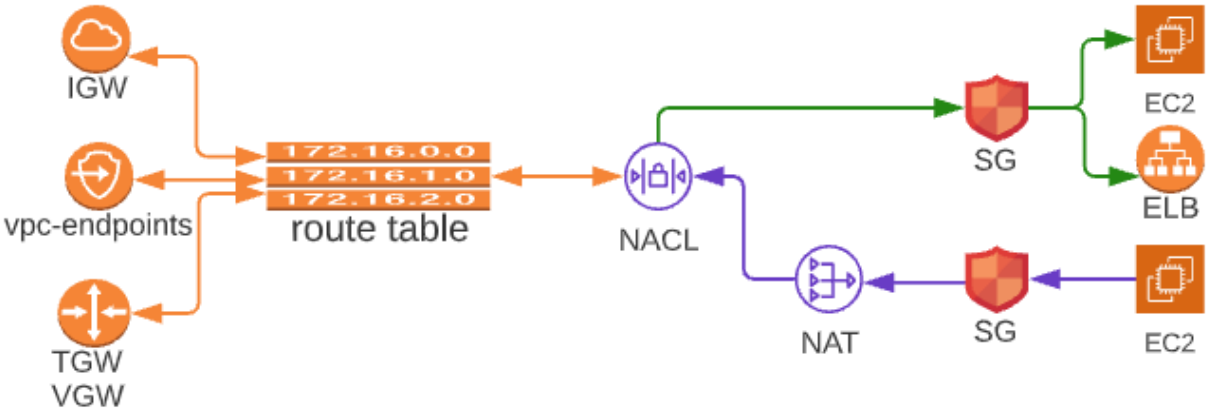


AWS VPC Routing Priority : (Route evaluation order)

Destination	Target	Priority
10.0.0.0/16	local	1
192.168.0.0/16	pcx-12345	2
172.31.0.0/16	vgw-12345 (static) or tgw-12345 (static)	2
172.31.0.0/16	vgw-12345 (propagated)	3
0.0.0.0/0	igw-12345	4

Destination	Attachment (Target)	Resource type	Route type	Priority
10.0.0.0/16	tgw-attach-123 | vpc-1234	VPC	Static or propagated	1
192.168.0.0/16	tgw-attach-789 | vpn-5678	VPN	Static	2
172.31.0.0/16	tgw-attach-456 | dxgw_id	AWS Direct Connect gateway	Propagated	3
172.31.0.0/16	tgw-attach-789 | tgw-connect-peer-123	VPN	Propagated	4
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	Propagated	5


AWS Cloud
Region
Virtual Private Cloud
Internet
Users
S3
vpc-endpoints
ENI
Availability Zone
Public Subnet
Private Subnet-App
Private Subnet-Data
NACL
SG
EC2
NAT
RDS
DB
172.16.0.0
172.16.1.0
172.16.2.0
pub-route table
pvt-route table
Route53
IGW
Public-ELB
Private-ELB
VGW
TGW
Direct
Connect
corporate data
center


IGW
vpc-endpoints
TGW
VGW
172.16.0.0
172.16.1.0
172.16.2.0
route table
NACL
NAT
SG
SG
EC2
ELB
EC2