Assignment-17-May-22

1. What is VPC?

* Amazon Virtual Private Cloud is a commercial cloud computing service that provides users a virtual private cloud, by "provision[ing] a logically isolated section of Amazon Web Services Cloud".
* Enterprise customers are able to access the Amazon Elastic Compute Cloud over an IPsec based virtual private network.

OR

* Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.
* This virtual network closely resembles a traditional network that you'd operate in your own data centre, with the benefits of using the scalable infrastructure of AWS.

USES:

* A virtual private cloud (VPC) is a secure, isolated private cloud hosted within a public cloud.
* VPC customers can run code, store data, host websites, and do anything else they could do in an ordinary private cloud, but the private cloud is hosted remotely by a public cloud provider

2. What is Subnet in VPC?

* A subnet is a range of IP addresses in your VPC.
* You can launch AWS resources, such as EC2 instances, into a specific subnet.
* When you create a subnet, you specify the IPv4 CIDR block for the subnet, which is a subset of the VPC CIDR block.

WORK:

* Subnets would then be analogous to the different rooms in your apartment.
* They are containers within your VPC that segment off a slice of the CIDR block you define in your VPC.
* Subnets allow you to give different access rules and place resources in different containers where those rules should apply

3. What is Internet Gateway in VPC?

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

WORK:

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.

4. What is Router in VPC?

* A routing table moves the traffic inside a VPC that is coming from the gateway and divides it among subnets.
* Each VPC has a default route table that is connected to each subnet.
* On the other hand, we can create our own route table to define the flow of traffic within VPC.

WORK:

Each AWS VPC has a VPC router. The primary function of this VPC router is to take all of the route tables defined within that VPC, and then direct the traffic flow within that VPC, as well as to subnets outside of the VPC, based on the rules defined within those tables.

5. What is Peering Connection inVPC?

* A VPC peering connection is a networking connection between two VPCs 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 VPCs, or with a VPC in another AWS account.
* The VPCs can be in different regions (also known as an inter-region VPC peering connection).

WORK:

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.

6. What is VPC endpoints?

: A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by Private Link without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

WORK:

* VPC endpoint enables users to privately connect their VPC to supported AWS services. VPC Endpoint does not require a public IP address, access over the Internet, NAT device, a VPN connection or AWS Direct Connect to communicate with resources in the service.
* VPC endpoints enables you to privately access specific AWS services from your own Amazon Virtual Private Cloud (VPC), without using public IP addresses and without requiring the traffic data to travel across the Internet.

7. What is NAT instance in VPC?

* A NAT (Network Address Translation) instance is, like a bastion host, an EC2 instance that lives in your public subnet.
* A NAT instance, however, allows your private instances outgoing connectivity to the internet while at the same time blocking inbound traffic from the internet.

WORK:

* A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.
* You launch a NAT instance in a public subnet to enable instances in the private subnet to initiate outbound IPv4 traffic to the internet or other AWS services, but prevent the instances from receiving inbound traffic initiated on the internet. Your NAT instance quota depends on your instance quota for the Region.

8. What is NAT gateway in VPC?

* NAT Gateway is a highly available AWS managed service that makes it easy to connect to the Internet from instances within a private subnet in an Amazon Virtual Private Cloud (Amazon VPC).
* Previously, you needed to launch a NAT instance to enable NAT for instances in a private subnet.

PURPOSE:

A NAT gateway gives cloud resources without public IP addresses access to the internet without exposing those resources to incoming internet connections.

9. What is Virtual Private Gateway in VPC?

* A virtual private gateway is a logical, fully redundant distributed edge routing function that sits at the edge of your VPC.
* As it is capable of terminating VPN connections from your on-prem or customer environments, the VPG is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection

WORK:

You can use an AWS Direct Connect gateway to connect your AWS Direct Connect connection over a private virtual interface to one or more VPCs in any account that are located in the same or different Regions.

10. What is Customer Gateway in VPC?

: A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network. When you create a customer gateway, you provide information about your device to AWS.

VPC customer gateway: -

Image result for What is Customer Gateway in VPC at aws

A customer gateway device is a physical or software appliance that you own or manage in your on-premises network (on your side of a Site-to-Site VPN connection).

You or your network administrator must configure the device to work with the Site-to-Site VPN connection.

11. What is AWS direct Connect?

: AWS Direct Connect is a networking service that provides an alternative to using the internet to connect to AWS. Using AWS Direct Connect, data that would have previously been transported over the internet is delivered through a private network connection between your facilities and AWS.

USED:

Direct Connect is a network service that allows a customer to establish a dedicated network connection between one of Amazon's Direct Connect locations and the customer's data centre or colocation environment.

12. What is Security Group?

: A security group acts as a virtual firewall, controlling the traffic that is allowed to reach and leave the resources that it is associated with.

For example

after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.

13. What is Network ACL?

* A network access control list (ACL) is made up of rules that either allow access to a computer environment or deny it.

OR

* 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 up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

14. What is CIDR?

: When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block.

For example

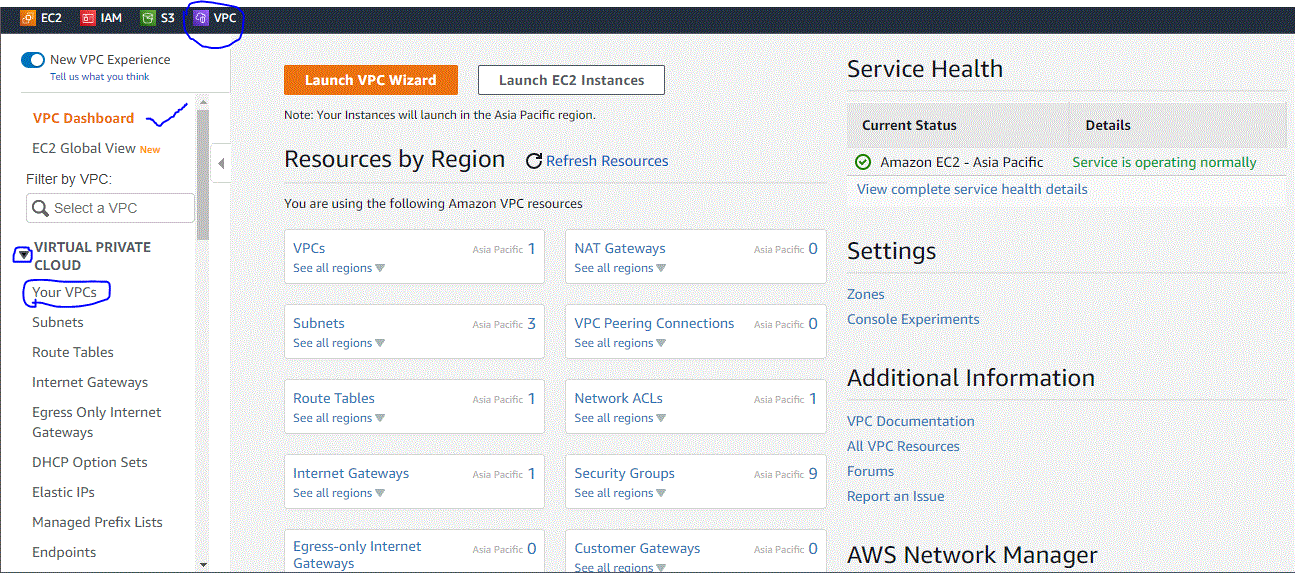
10.0. 0.0/16. This is the primary CIDR block for your VPC.

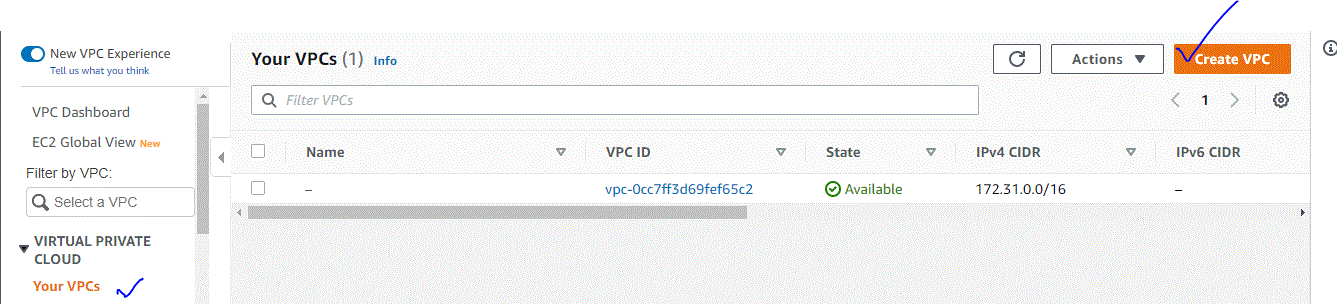
USE:

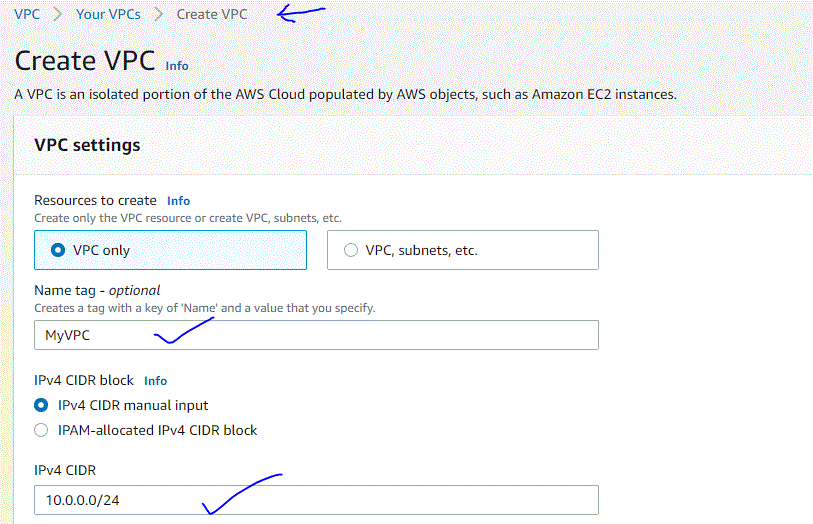
* Classless Inter-Domain Routing (CIDR) block basically is a method for allocating IP addresses and IP routing.
* When you create a network or route table, you need to specify what range are you working in. "0.0. 0.0" means that it will match to any IP address.

Assignment-18-May-22

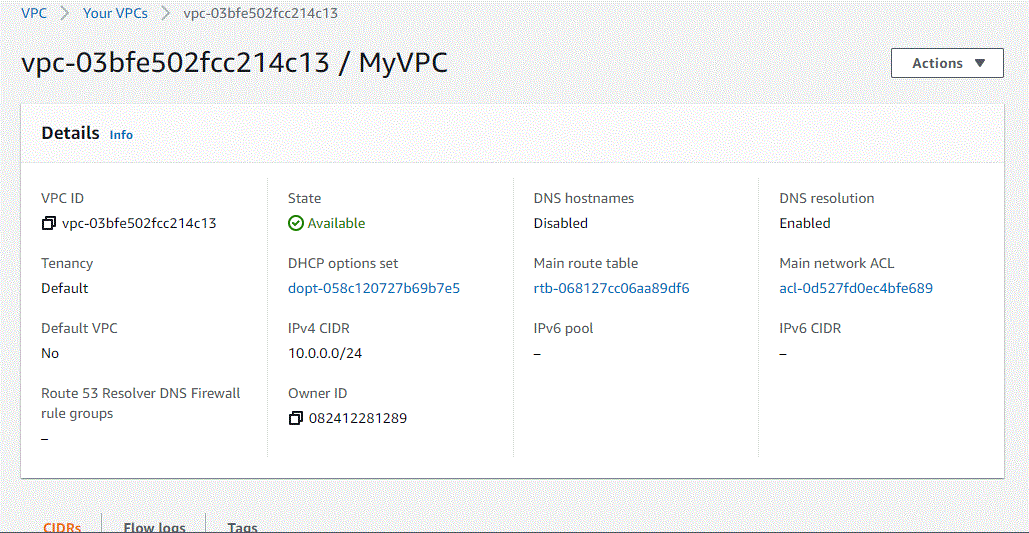
1. Create VPC 's?

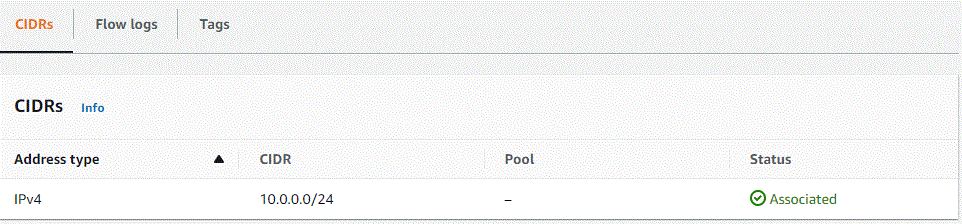




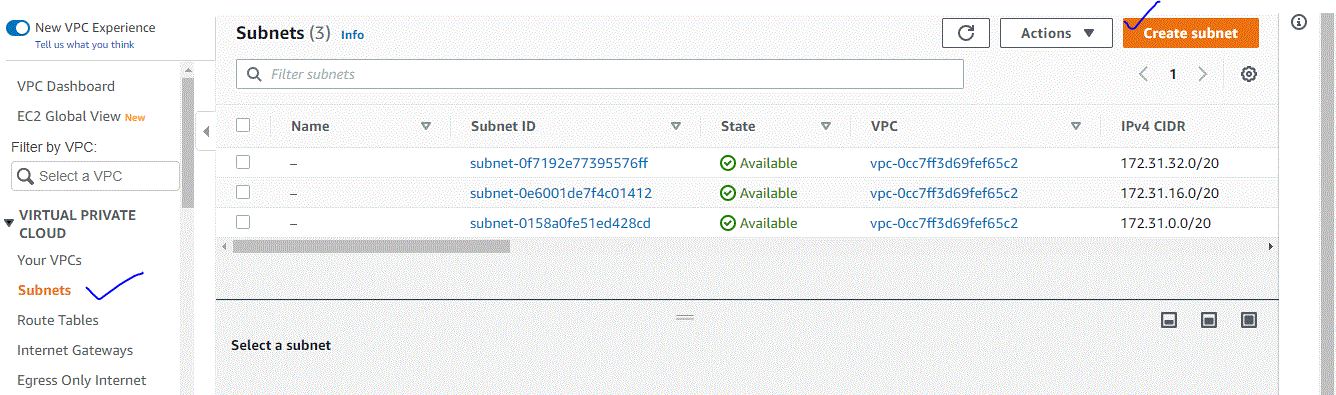


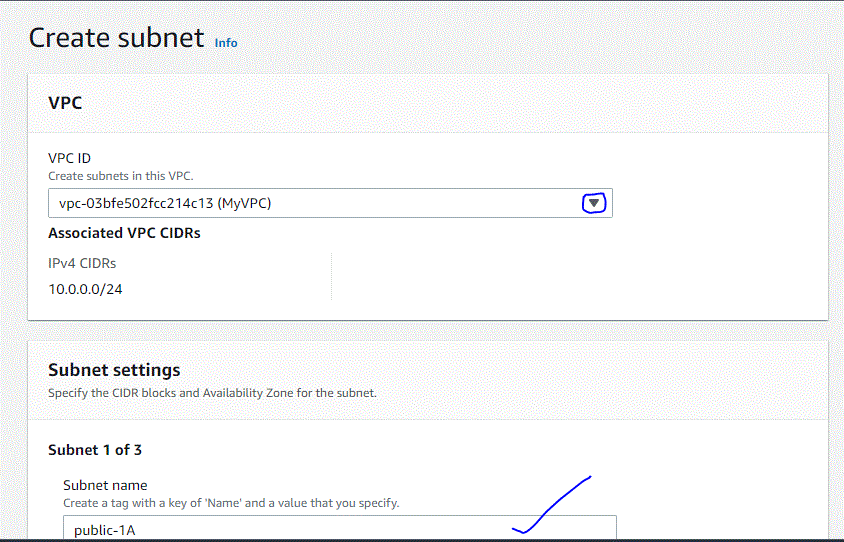


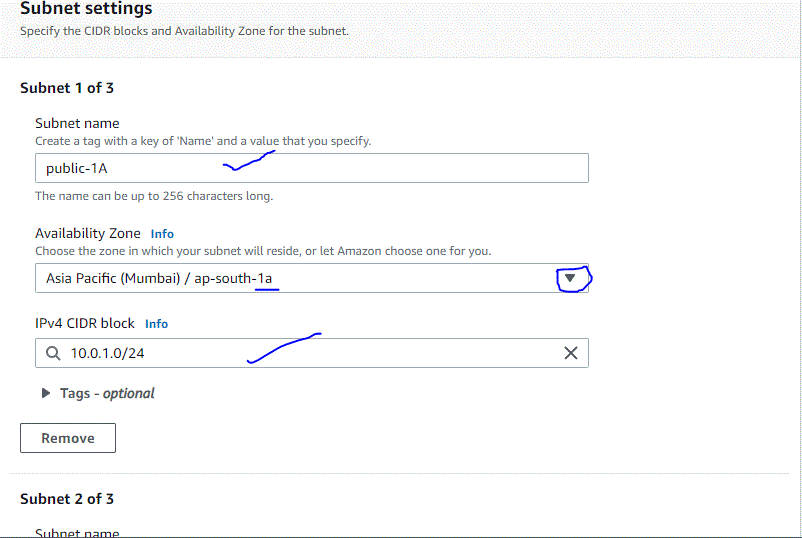


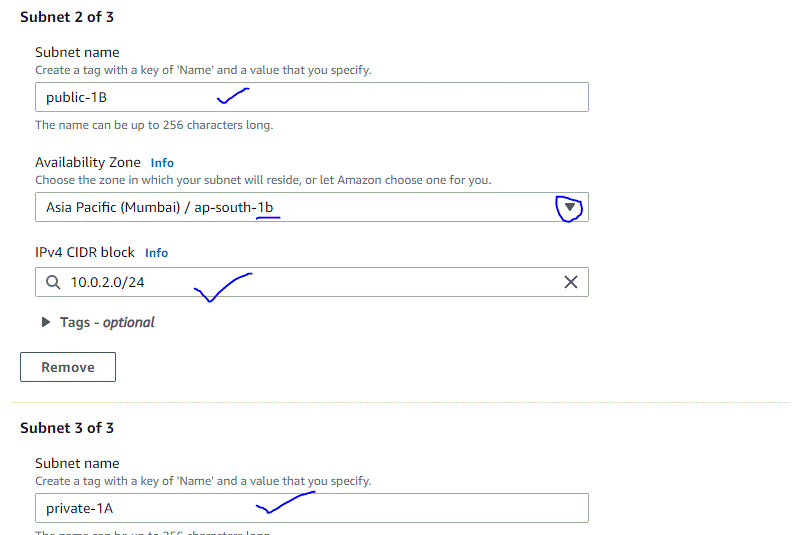


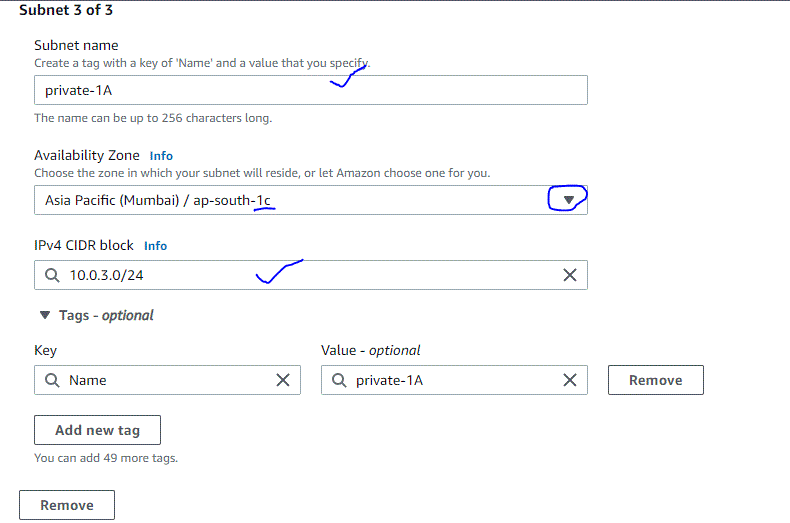
1. Create Subnet



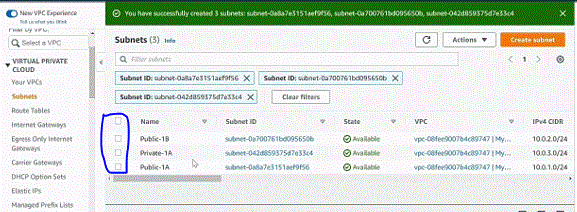




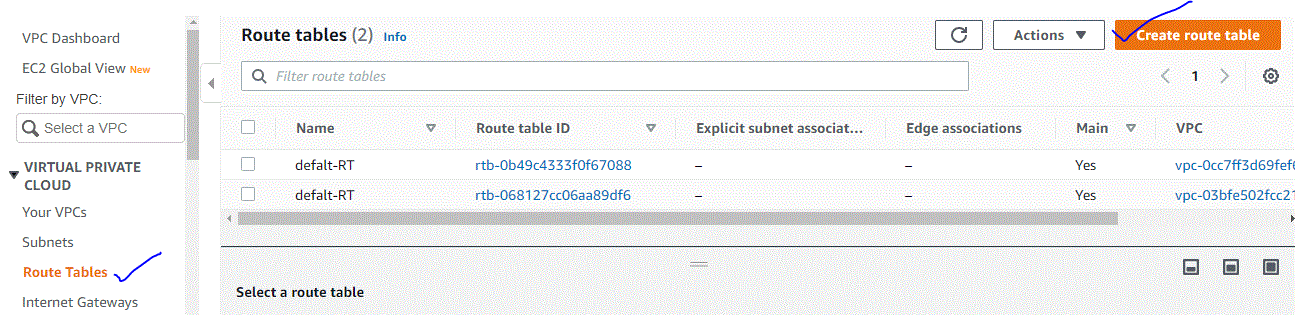


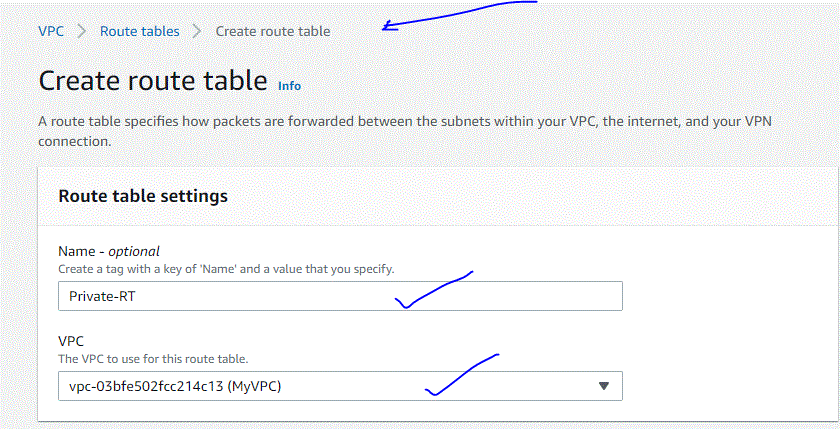




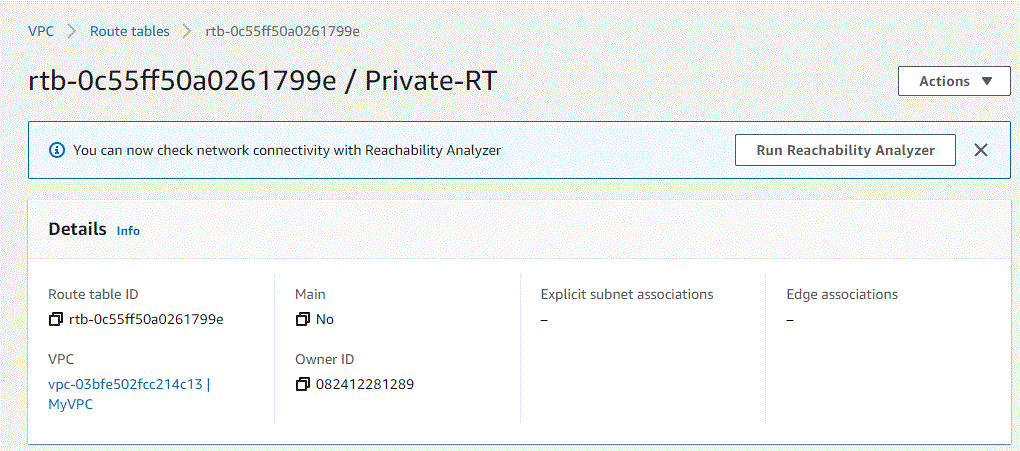


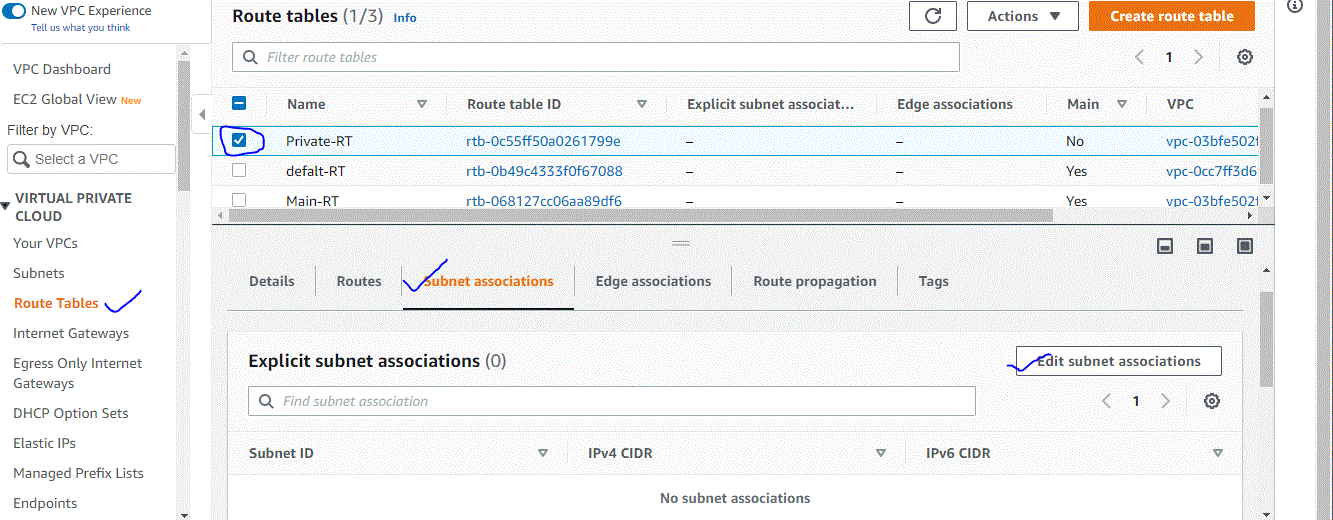
1. Create Router Table

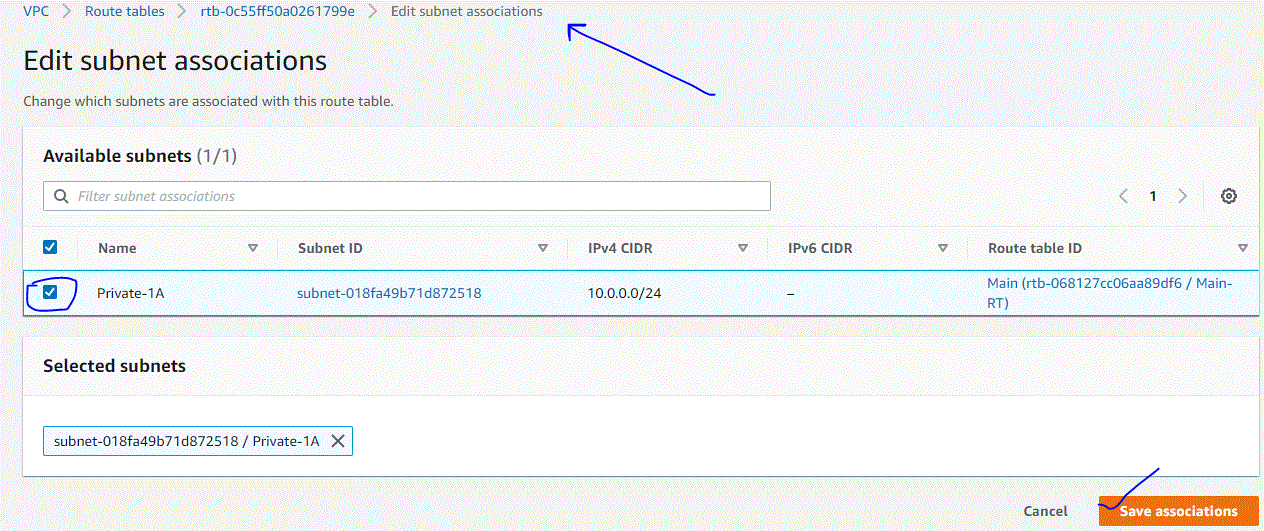


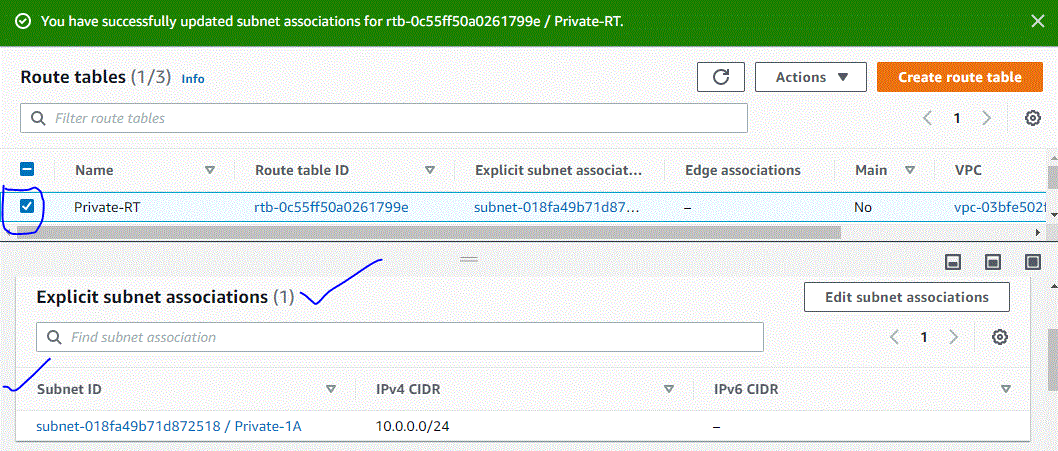




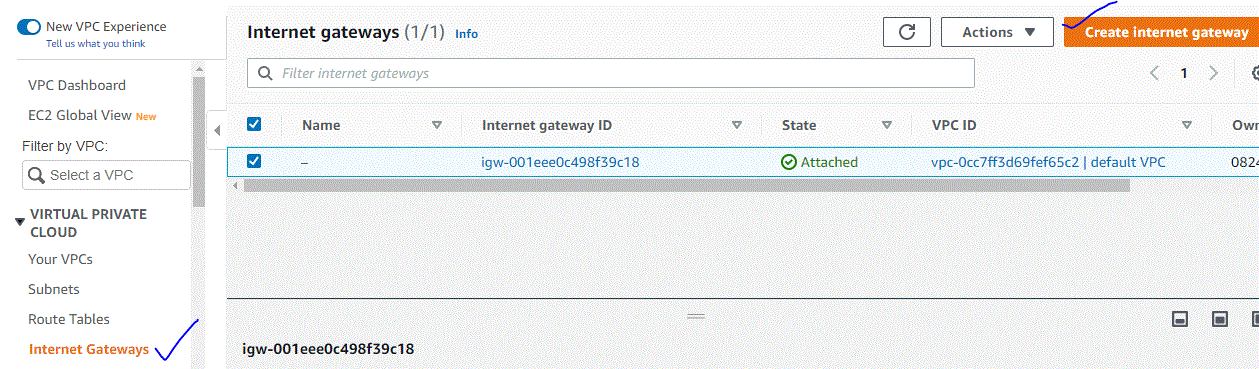


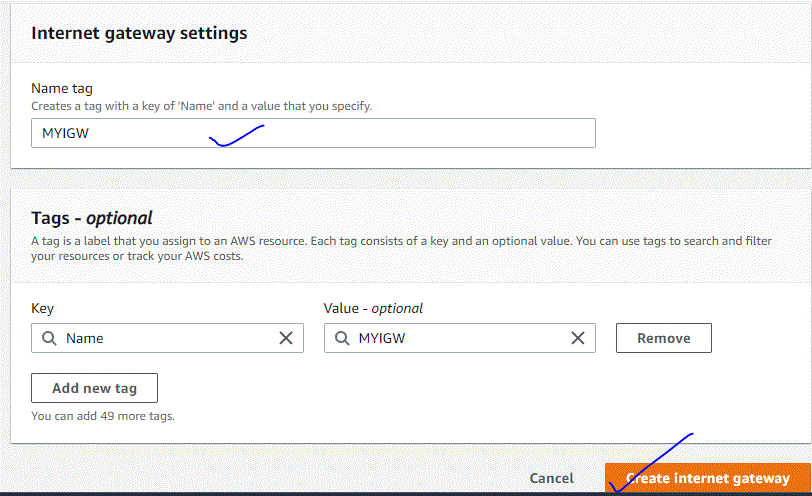


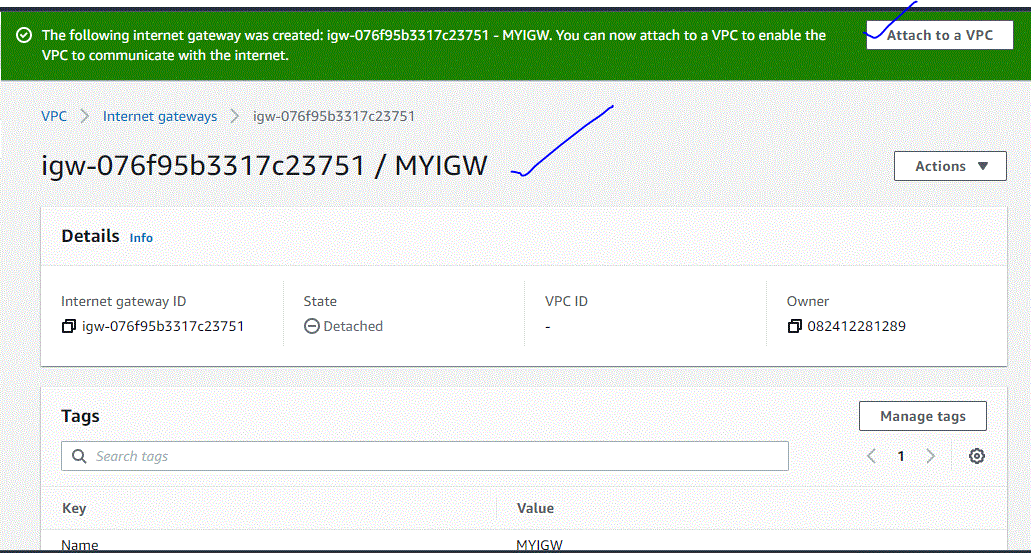


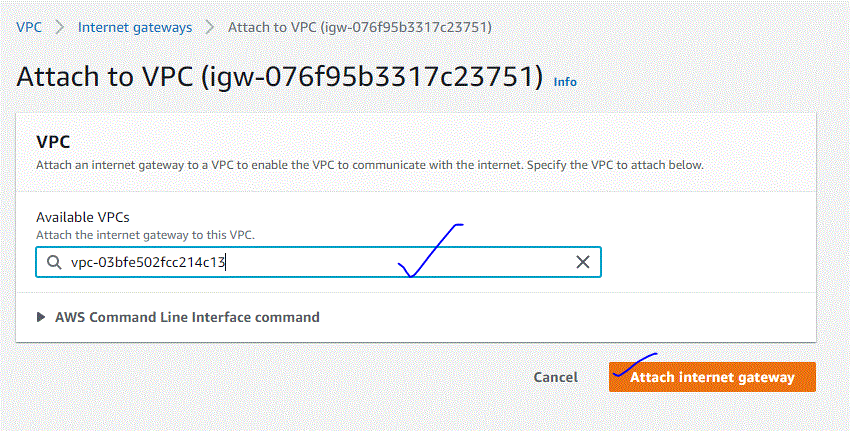


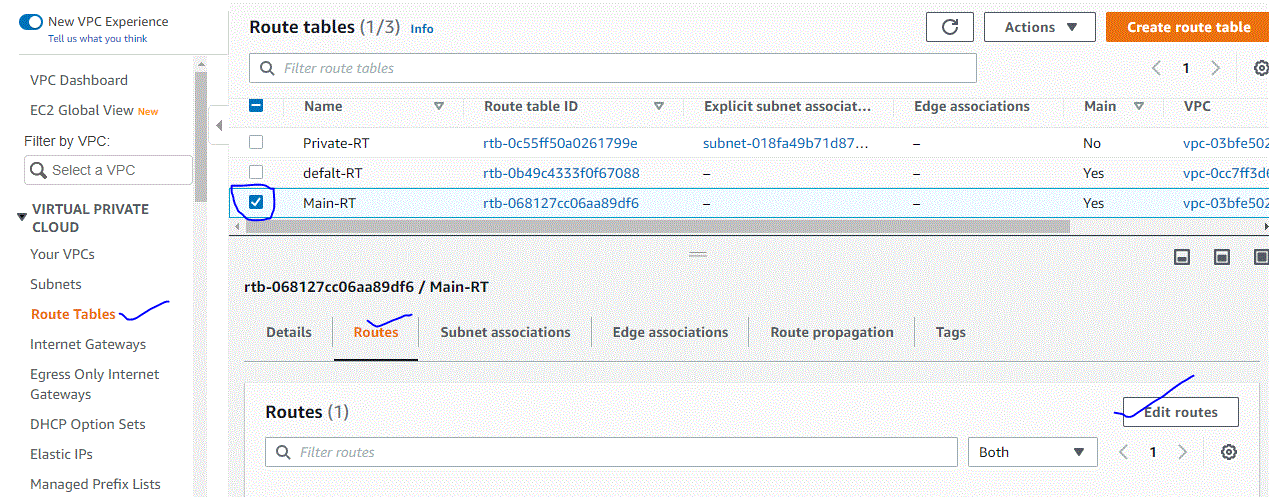
1. Create Internet Gateways

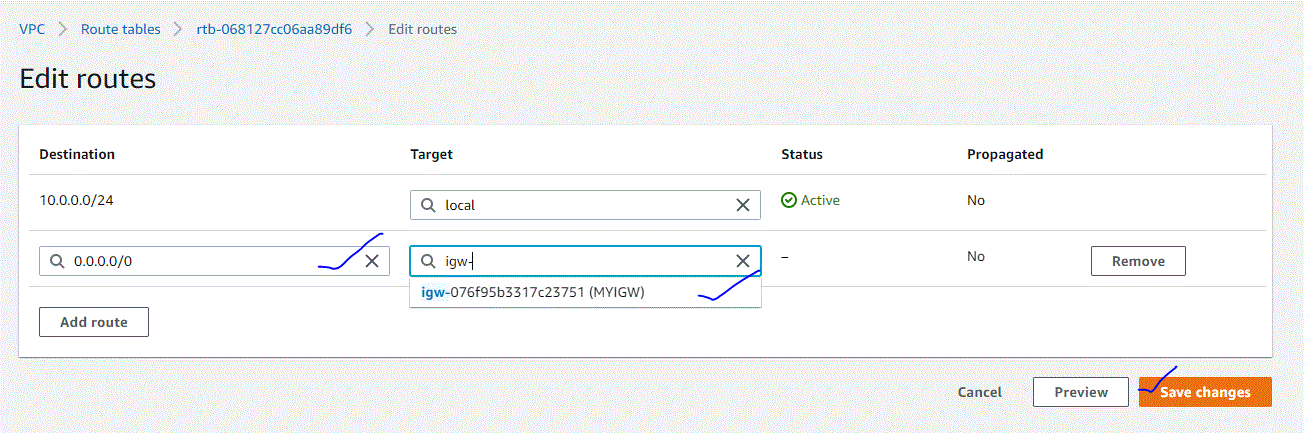


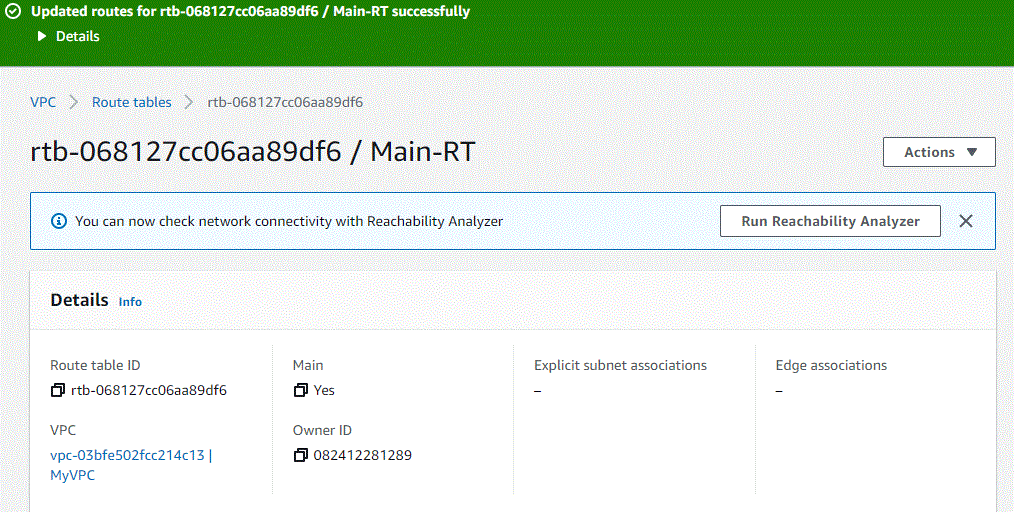


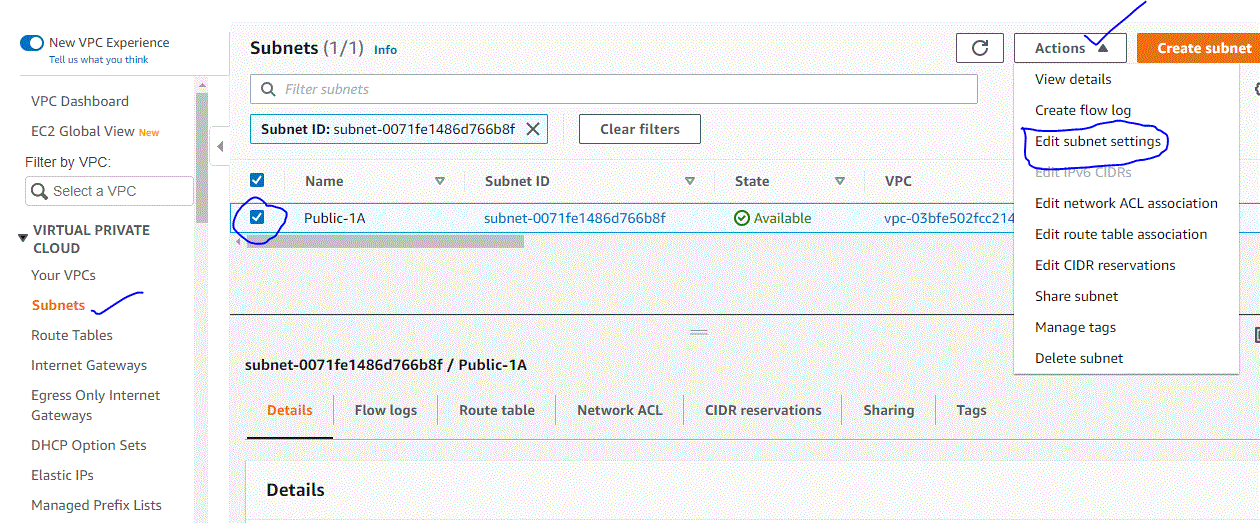


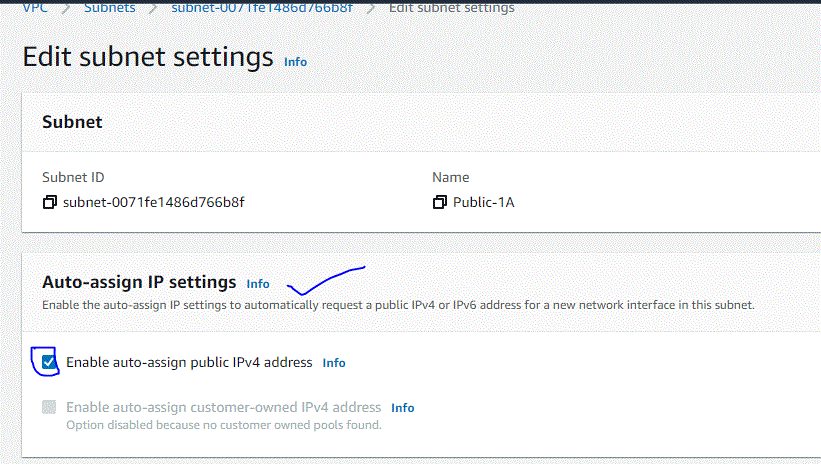










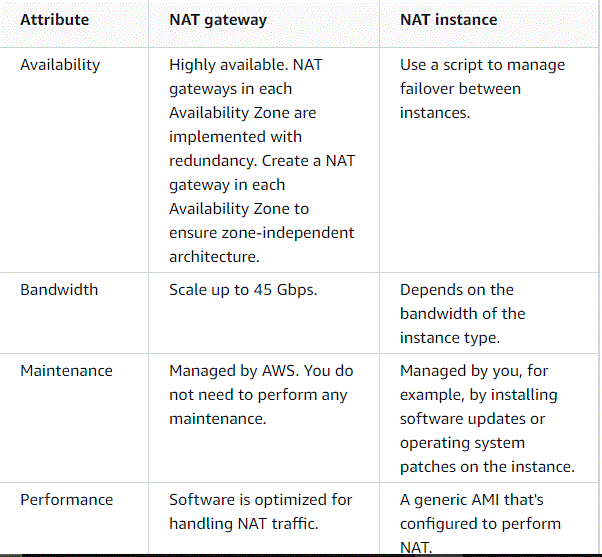


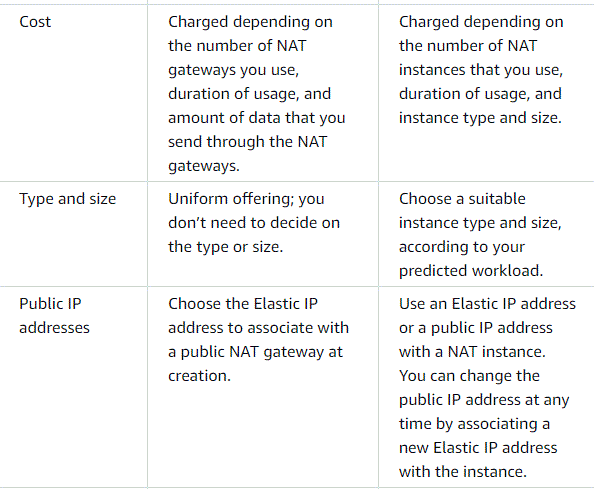


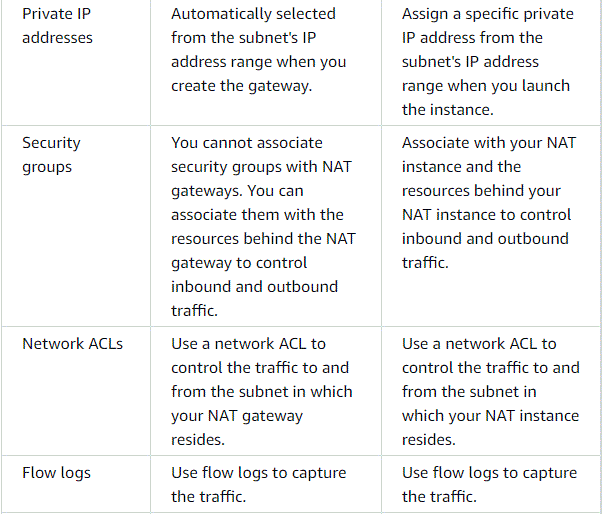
Assignment-19-May-2022

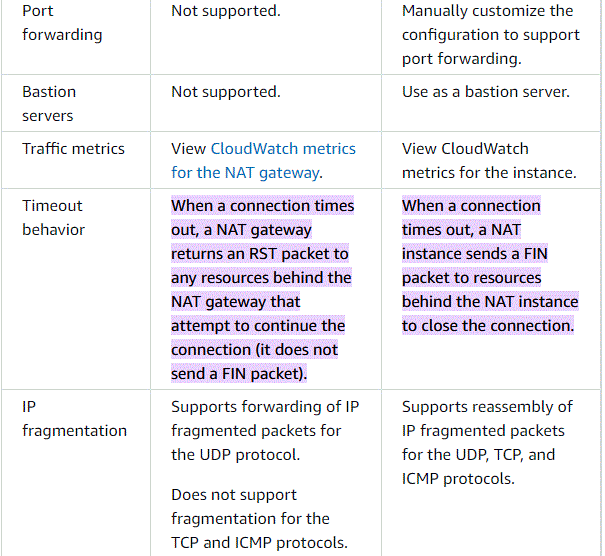
1. What is the difference between NAT Gateway and NAT instance?

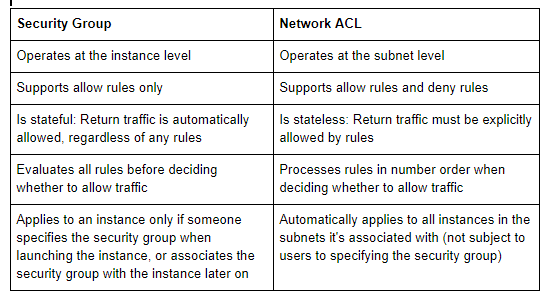
:









1. What is the difference between Security group and NACLs? 

3. What is a public IP address?

: A public IP address is an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP). Your personal device also has a private IP that remains hidden when you connect to the internet through your router's public IP

4. What is a private IP address?

: A private IP address is the address your network router assigns to your device. Each device within the same network is assigned a unique private IP address (sometimes called a private network address) — this is how devices on the same internal network talk to each other.

5. What is an elastic IP address?

: An Elastic IP address is a reserved public IP address that you can assign to any EC2 instance in a particular region, until you choose to release it. To allocate an Elastic IP address to your account in a particular region, see Allocate an Elastic IP address

6. Hands on – Allocate an Elastic IP address to an EC2 instance and release it (include steps with screen shots)?

**: To allocate an Elastic IP address**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Network & Security**, **Elastic IPs**.
3. Choose **Allocate Elastic IP address**.
4. For **Public IPv4 address pool**, choose one of the following:
   * **Amazon's pool of IPv4 addresses**—If you want an IPv4 address to be allocated from Amazon's pool of IPv4 addresses.
   * **Public IPv4 address that you bring to your AWS account**—If you want to allocate an IPv4 address from an IP address pool that you have brought to your AWS account. This option is disabled if you do not have any IP address pools.
   * **Customer owned pool of IPv4 addresses**—If you want to allocate an IPv4 address from a pool created from your on-premises network for use with an AWS Outpost. This option is disabled if you do not have an AWS Outpost.
5. (Optional) Add or remove a tag.

[Add a tag] Choose **Add new tag** and do the following:

* + For **Key**, enter the key name.
  + For **Value**, enter the key value.

[Remove a tag] Choose **Remove** to the right of the tag’s Key and Value.

1. Choose **Allocate**.

**To describe your Elastic IP addresses**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Elastic IPs**.
3. Select the Elastic IP address to view and choose **Actions**, **View details**.

**To tag an Elastic IP address**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Elastic IPs**.
3. Select the Elastic IP address to tag and choose **Actions**, **View details**.
4. In the **Tags** section, choose **Manage tags**.
5. Specify a tag key and value pair.
6. (Optional) Choose **Add tag** to add additional tags.
7. Choose **Save**.

**To associate an Elastic IP address with an instance**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Elastic IPs**.
3. Select the Elastic IP address to associate and choose **Actions**, **Associate Elastic IP address**.
4. For **Resource type**, choose **Instance**.
5. For instance, choose the instance with which to associate the Elastic IP address. You can also enter text to search for a specific instance.
6. (Optional) For **Private IP address**, specify a private IP address with which to associate the Elastic IP address.
7. Choose **Associate**.

**To associate an Elastic IP address with a network interface**

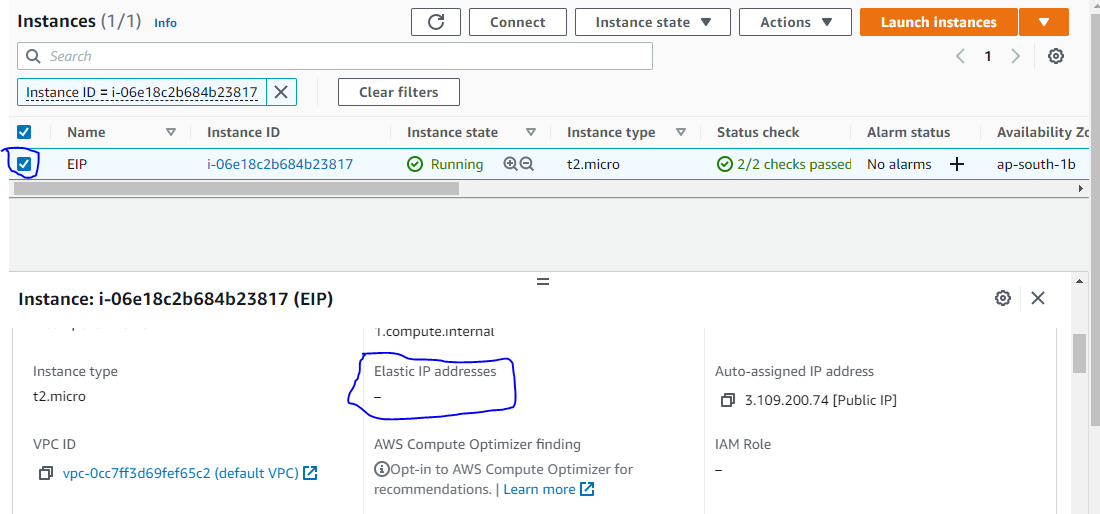
1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Elastic IPs**.
3. Select the Elastic IP address to associate and choose **Actions**, **Associate Elastic IP address**.
4. For **Resource type**, choose **Network interface**.
5. For **Network interface**, choose the network interface with which to associate the Elastic IP address. You can also enter text to search for a specific network interface.
6. (Optional) For **Private IP address**, specify a private IP address with which to associate the Elastic IP address.
7. Choose **Associate**.

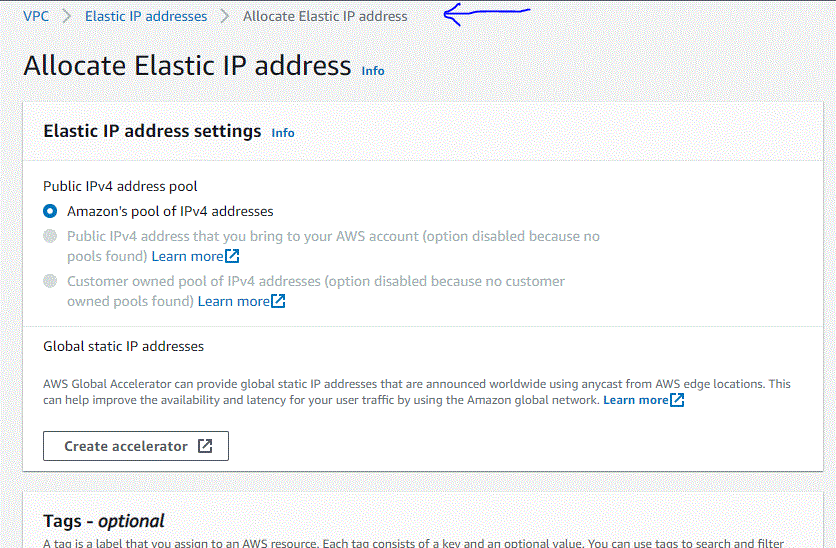
**To disassociate and reassociate an Elastic IP address**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Elastic IPs**.
3. Select the Elastic IP address to disassociate, choose **Actions**, **Disassociate Elastic IP address**.
4. Choose **Disassociate**.

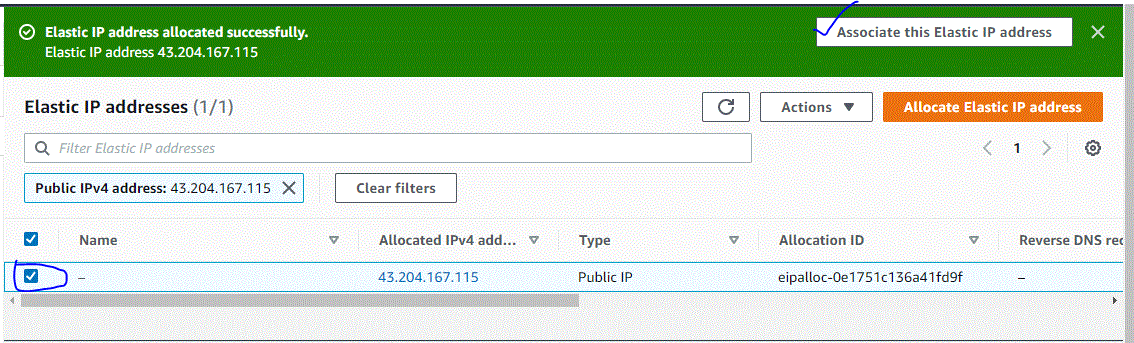
**To release an Elastic IP address**

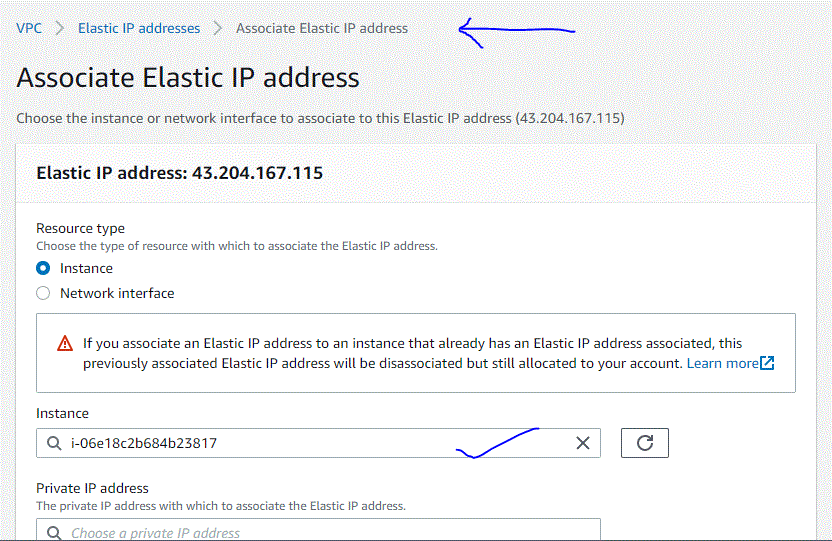
1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Elastic IPs**.
3. Select the Elastic IP address to release and choose **Actions**, **Release Elastic IP addresses**.
4. Choose **Release**.



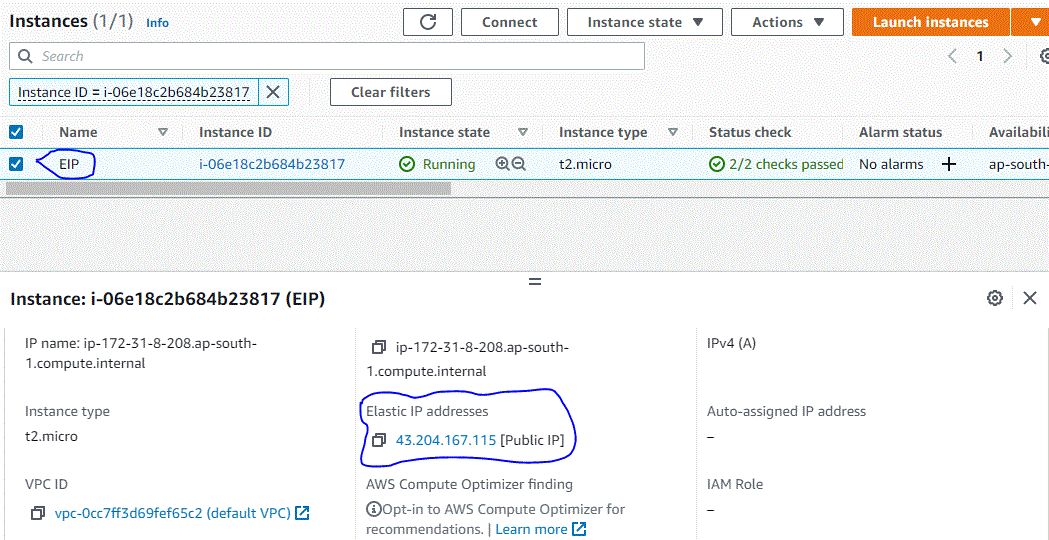


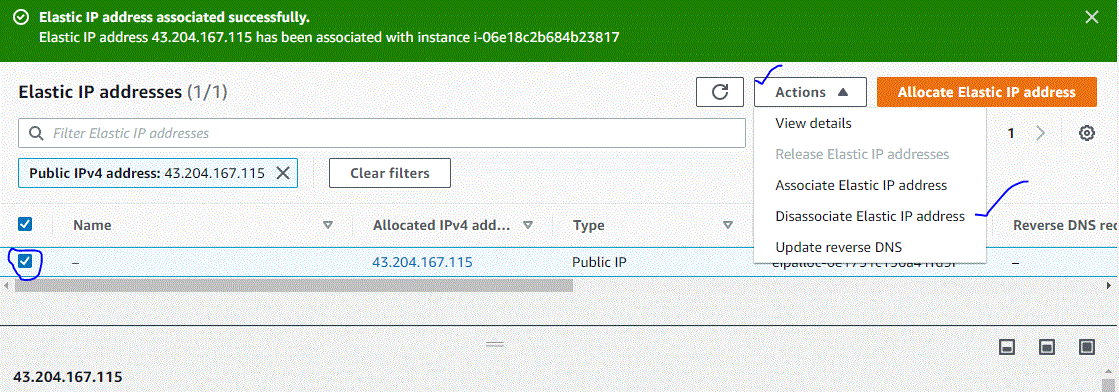


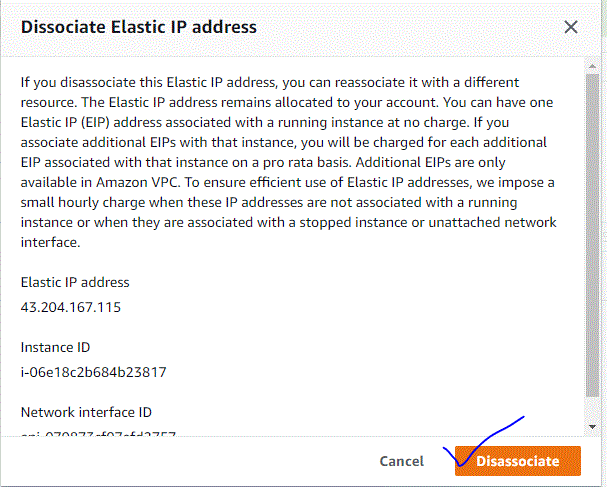


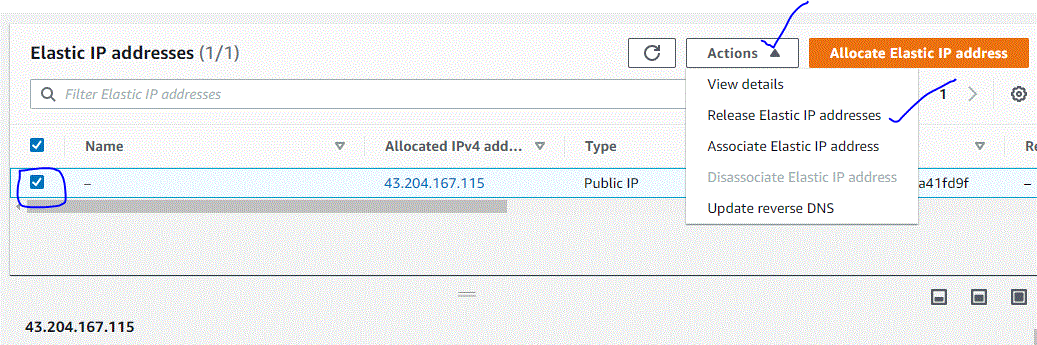


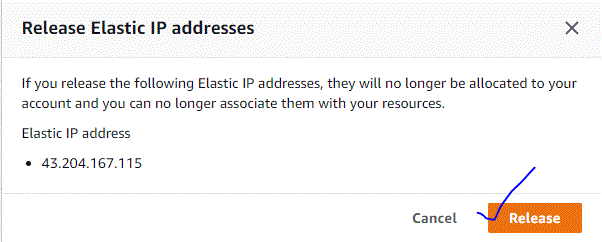


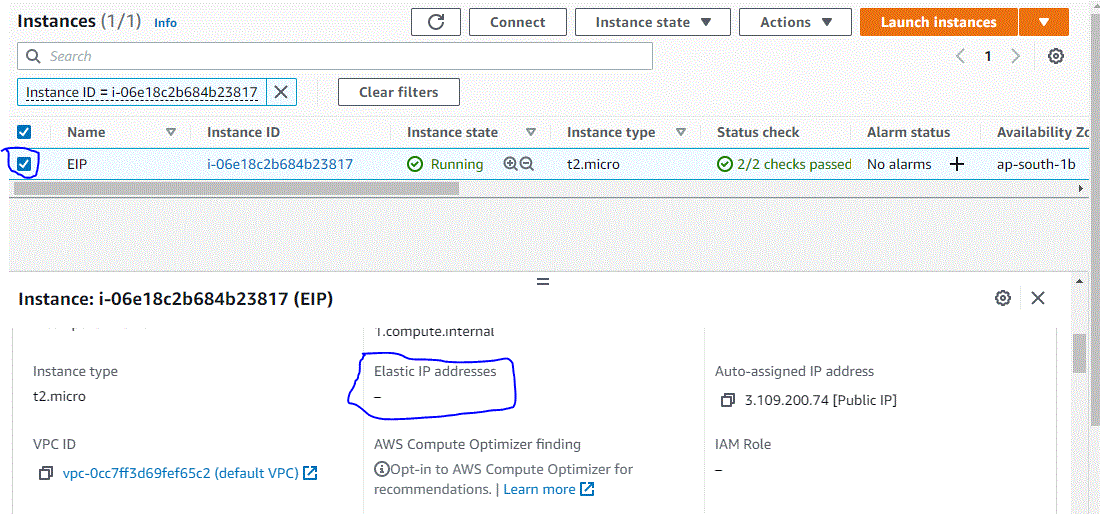










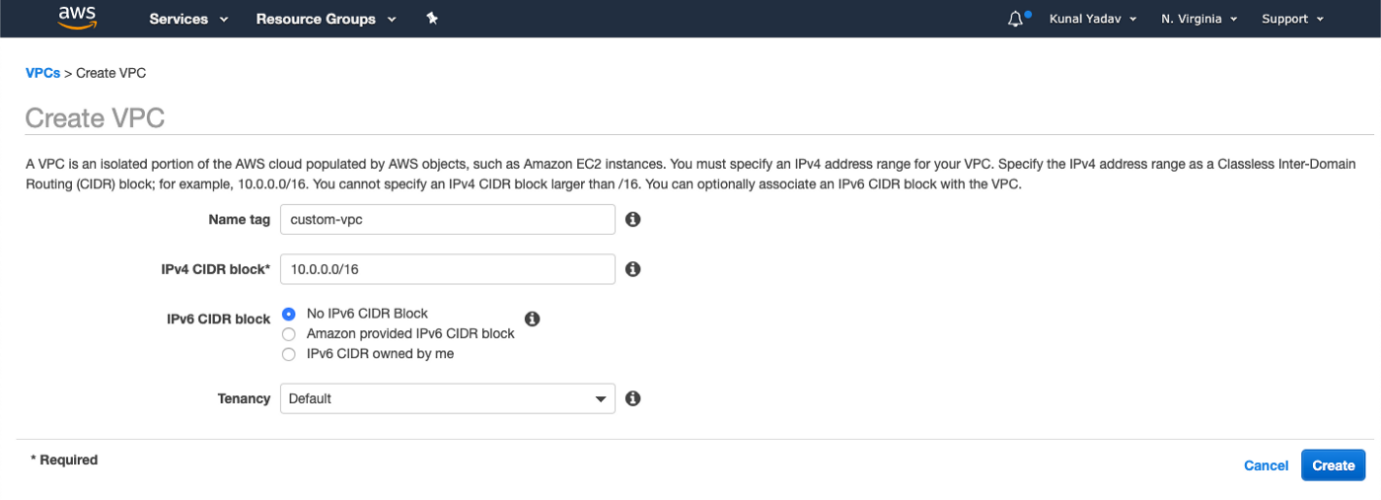


7. Hands on – Create a Custom VPC?

: Creating a Custom VPC

Log into your AWS console, select the region in which you would like to create a VPC (in this case I am using Northern Virginia) and select VPC.

Now, click on **Your VPCs**in the left sidebar and then click on **Create VPC.**



Give a name to your VPC and the IPv4 CIDR block that you would like. You can also give an IPv6 CIDR block if you want but for this example, I am going by the default selection.

You can enforce the tenancy of EC2 instances launched in this VPC. If you select **dedicated**then all your instances will be launched on dedicated tenancy instances (more cost). If you select the **Default**option then instances will use the tenancy option selected while launching them.

Click on the **Create**buttonto create your custom VPC!

Now, you can see your custom VPC along with the default VPC.

When you create a new VPC, a Network Access Control List (NACL) and the main Route Table is created by default.

8. What is Direct connect?

: AWS Direct Connect is a networking service that provides an alternative to using the internet to connect to AWS. Using AWS Direct Connect, data that would have previously been transported over the internet is delivered through a private network connection between your facilities and AWS.

USES:

AWS Direct Connect is a network service that provides an alternative to using the Internet to utilize AWS cloud services. AWS Direct Connect enables customers to have low latency, secure and private connections to AWS for workloads which require higher speed or lower latency than the internet. Q.

9. What is VPN? And its different types? (Site to site and CLoub hub)

: VPN software protects your information by masking your device's IP address, encrypting your data and routing it through secure networks to servers in faraway states or even other countries. In doing so it hides your online identity, ensuring that you are able to browse the Internet securely and anonymously.

Remote Access VPN:

Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both.

An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company’s private network and remotely access files and resources on the private network. Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users aware of Internet security also use VPN services to enhance their Internet security and privacy.

Site to Site VPN:

A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

10. What is AWS transit Gateway?

: AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once

