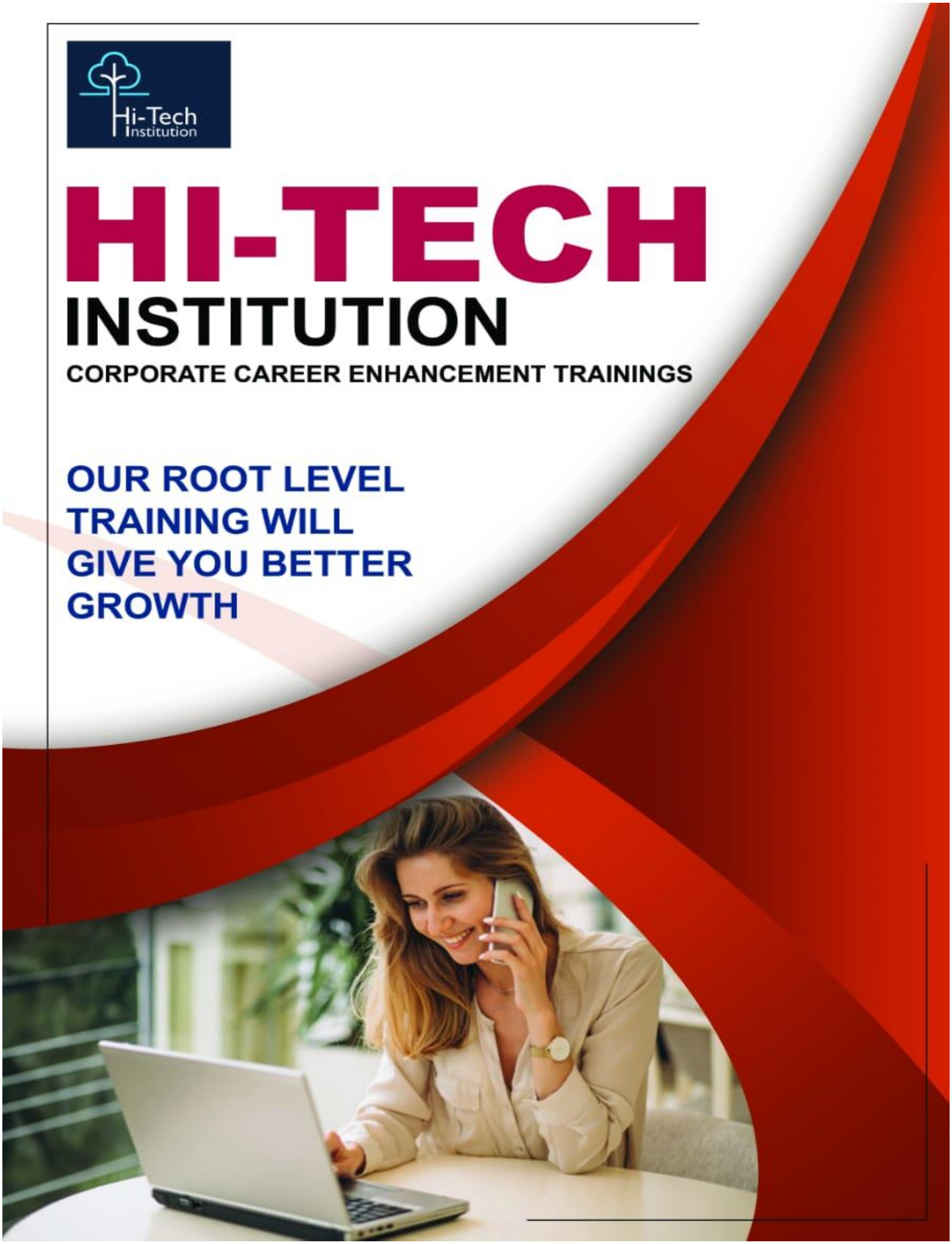


HI-TECH INSTITUTION

CORPORATE CAREER ENHANCEMENT TRAININGS

OUR ROOT LEVEL TRAINING WILL GIVE YOU BETTER GROWTH

ABOUT US

Our Vision:

To provide better training by full filing the requirements of our trainee.

Our Mission:

We always ensure to give practical based training. And we make the candidates to get good hands-on experience on any platform.

Philosophy:

Our Root Level Training Will give you Better Growth.

We successfully survived around 5 years in the IT field. Started this is as small Training room. But now we are having 5 branches across India.

Certified Trainers taking the session on various domain with any level of doubts clarification.

For More Details: www.hitechins.in

Write feedback to operations@hitechins.in

Virtual Private Cloud

What Is Amazon VPC?

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 center, with the benefits of using the scalable infrastructure of AWS.

Amazon VPC Concepts

As you get started with Amazon VPC, you should understand the key concepts of this virtual network, and how it is similar to or different from your own networks. This section provides a brief description of the key concepts for Amazon VPC.

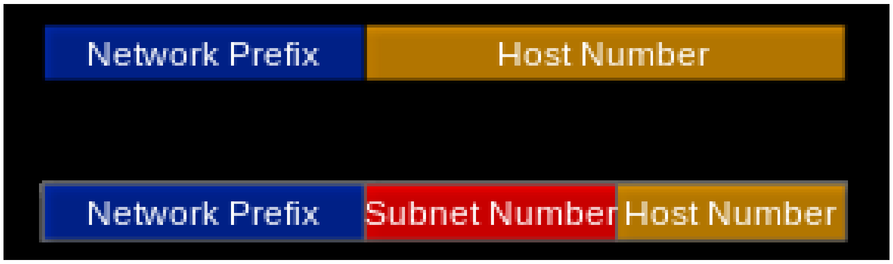
Amazon VPC is the networking layer for Amazon EC2.

Major topic:

- Subnetting
- Route table
- Internet Gateway
- NAT
- ACL
- Security Group
- Peering connection
- VPN

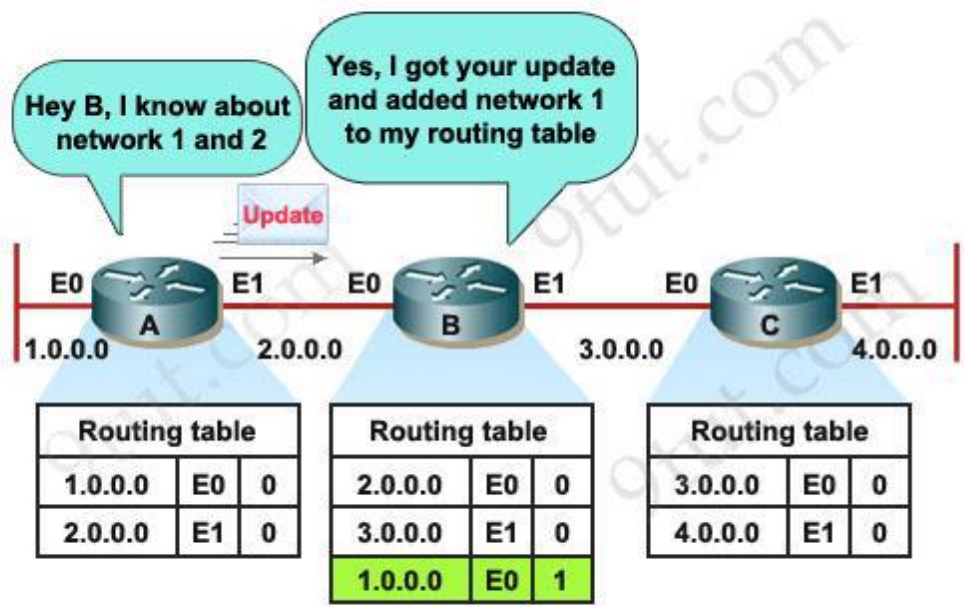
Subnetting

- Subnetting is the process of dividing a network into two or more subnets.
- An IP address has numbers that identify the network ID and the host ID.
- A subnet address borrows some of the bits from the host ID of the IP address.
- Subnetting is largely invisible to computer users who aren't also network administrators



Routing table

- Routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables.


Hey B, I know about network 1 and 2
Yes, I got your update and added network 1 to my routing table
Update
E0
E1
E0
E1
E0
E1
A
B
C
1.0.0.0
2.0.0.0
3.0.0.0
4.0.0.0

Routing table		
1.0.0.0	E0	0
2.0.0.0	E1	0

Routing table		
2.0.0.0	E0	0
3.0.0.0	E1	0
1.0.0.0	E0	1

Routing table		
3.0.0.0	E0	0
4.0.0.0	E1	0

Internet Gateway

- An **Internet gateway** is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the **Internet**. It therefore imposes no availability risks or bandwidth constraints on your network traffic.

Enabling Internet Access

To enable access to or from the Internet for instances in a VPC subnet, you must do the following:

- Attach an Internet gateway to your VPC.
- Ensure that your subnet's route table points to the Internet gateway.
- Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
- Ensure that your network access control and security group rules allow the relevant traffic to flow to and from your instance.

NAT Gateway

- We can use a network address translation (*NAT*) *gateway* to enable instances in a private subnet to connect to the internet or other *AWS* services
- We can prevent the internet from initiating a connection with those instances

Network ACLs

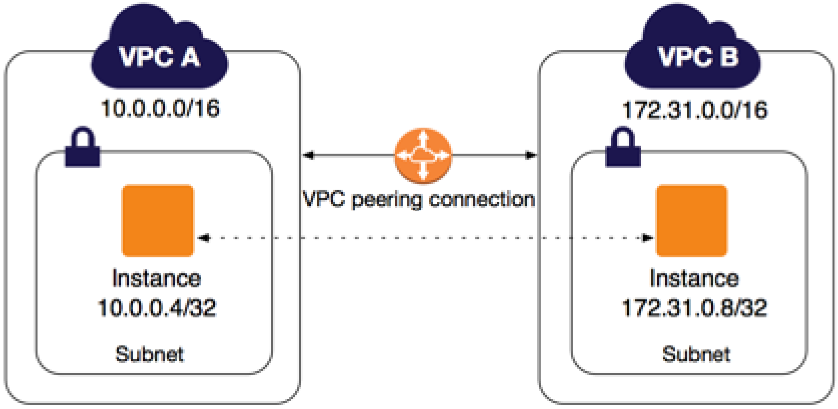
- A *network access control list (ACL)* is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.
- You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC

Security Groups for Your VPC

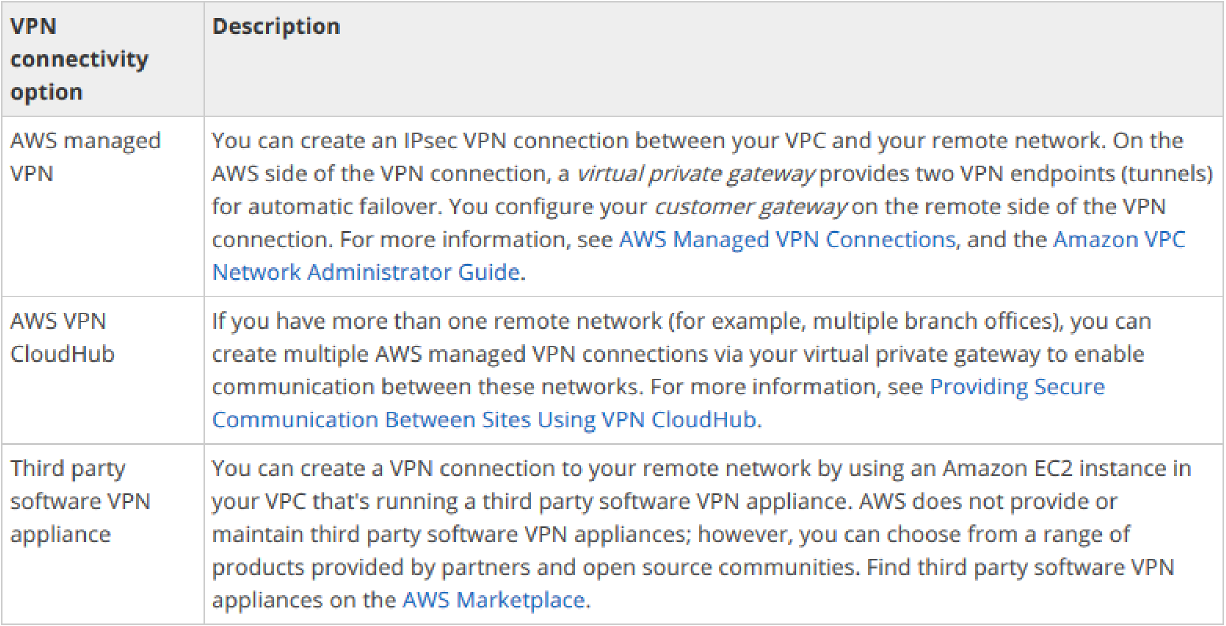
- A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic.
- When you launch an instance in a VPC, you can assign up to **five security groups** to the instance.
- Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups.
- If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.

VPC Peering

- 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).

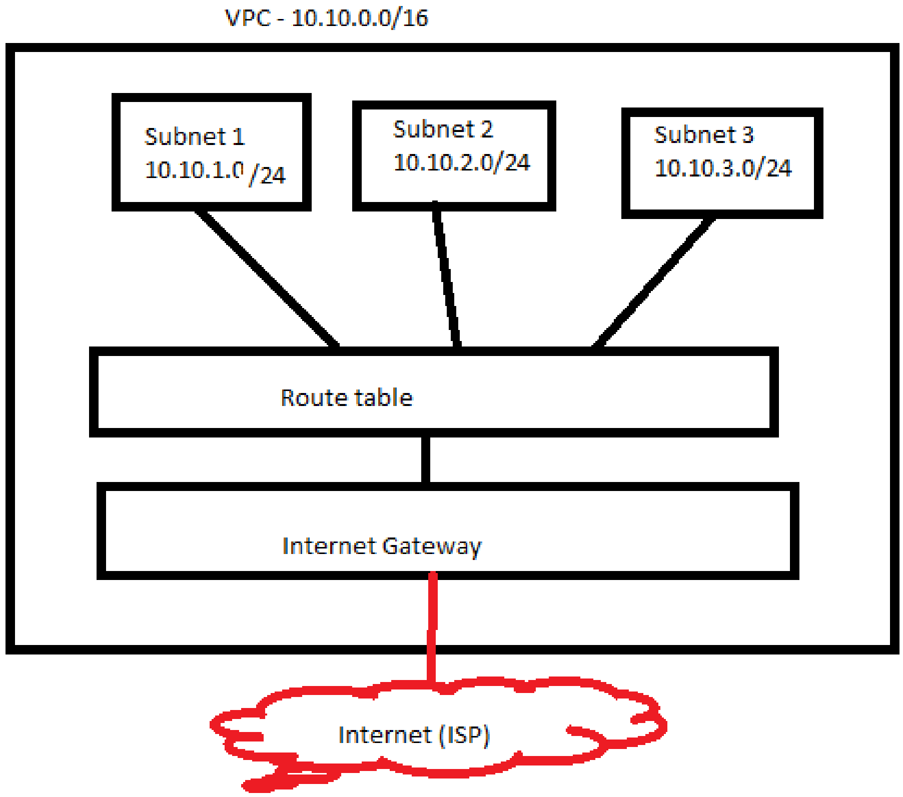


VPN Connections



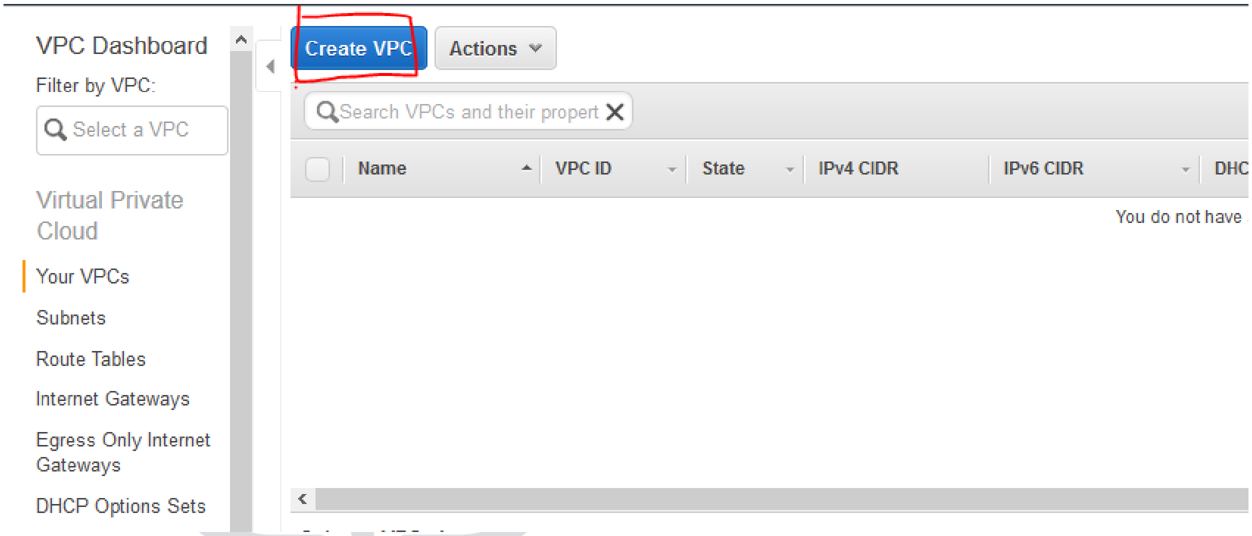
VPN connectivity option	Description
AWS managed VPN	You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a *virtual private gateway* provides two VPN endpoints (tunnels) for automatic failover. You configure your *customer gateway* on the remote side of the VPN connection. For more information, see AWS Managed VPN Connections, and the Amazon VPC Network Administrator Guide.
AWS VPN CloudHub	If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS managed VPN connections via your virtual private gateway to enable communication between these networks. For more information, see Providing Secure Communication Between Sites Using VPN CloudHub.
Third party software VPN appliance	You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a third party software VPN appliance. AWS does not provide or maintain third party software VPN appliances; however, you can choose from a range of products provided by partners and open source communities. Find third party software VPN appliances on the AWS Marketplace.

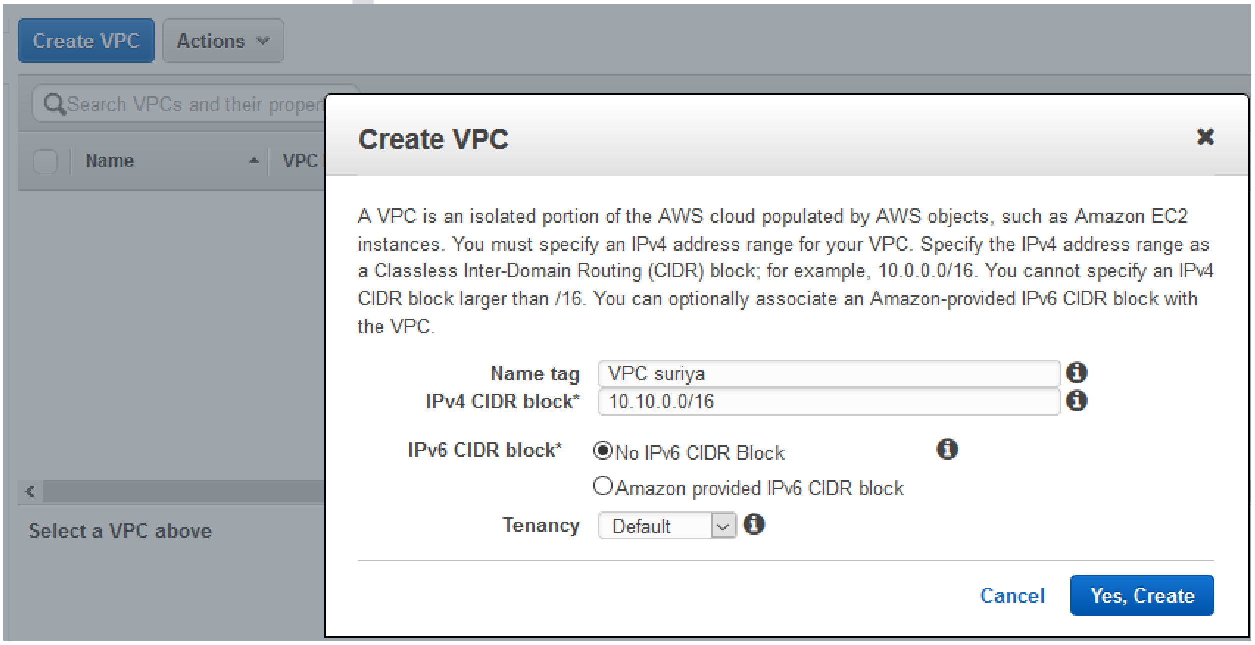
Scenarios and Examples of VPC



To create a VPC

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the dashboard, choose **Start VPC Wizard**.





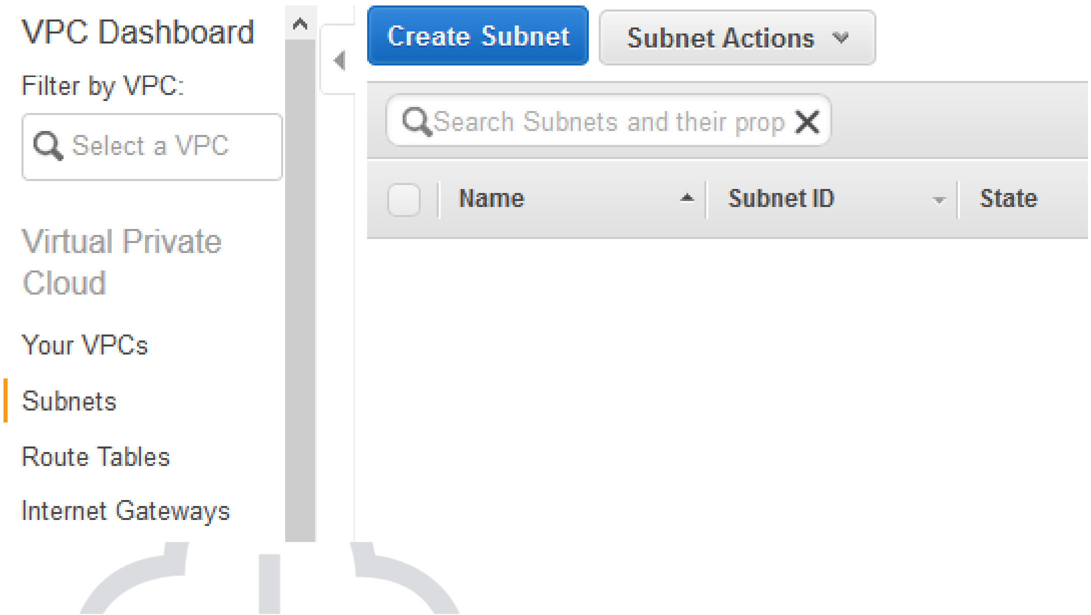
Create VPC

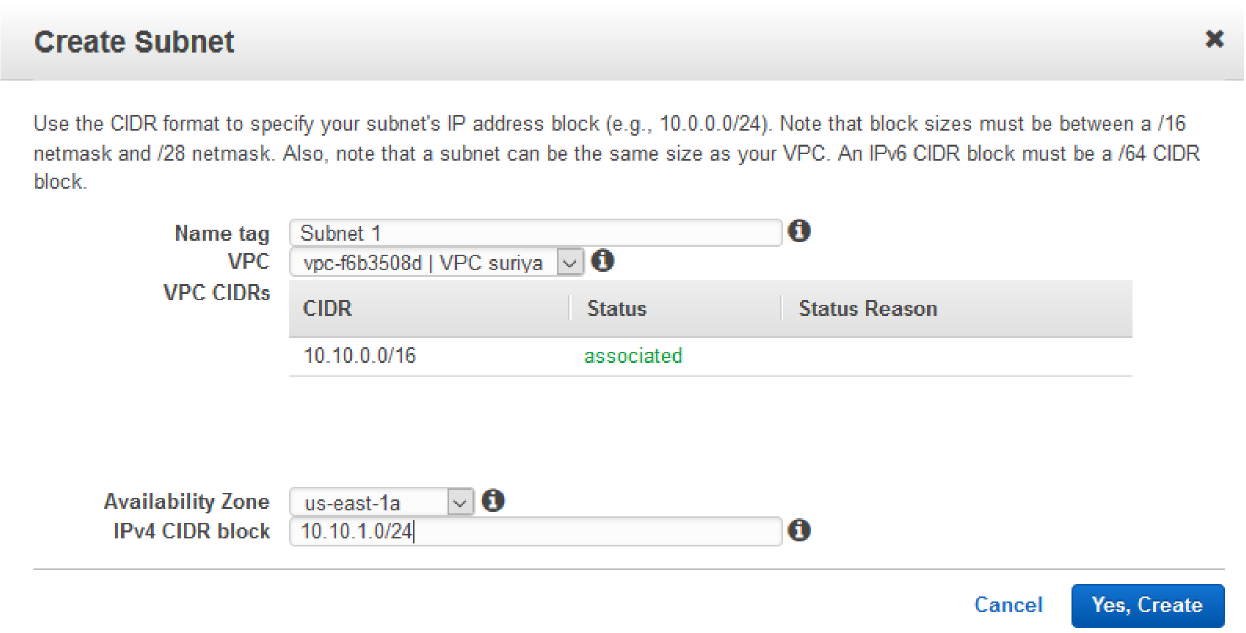
A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag: VPC suriya
IPv4 CIDR block*: 10.10.0.0/16
IPv6 CIDR block*: ● No IPv6 CIDR Block
○ Amazon provided IPv6 CIDR block
Tenancy: Default

Cancel | Yes, Create

3. Select the first option, **VPC with a Single Public Subnet**, and then choose **Select**.





Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag Subnet 1

VPC vpc-f6b3508d | VPC suriya

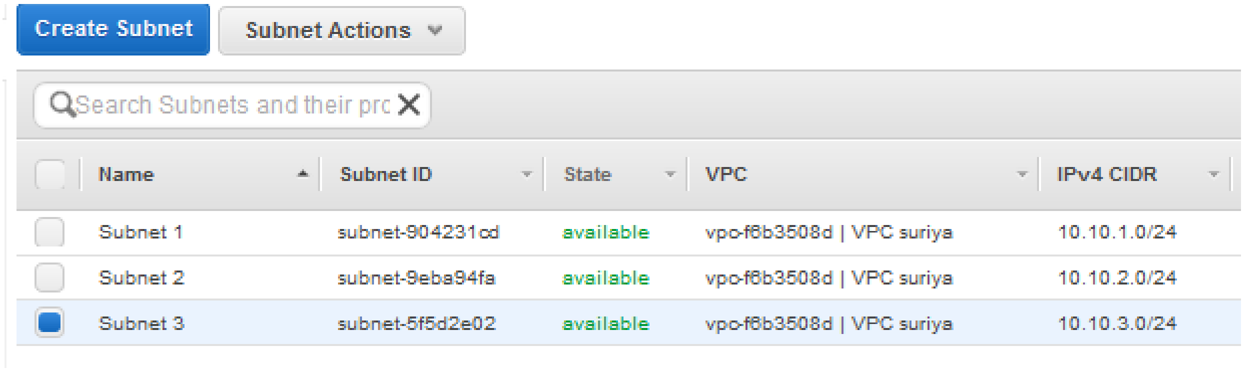
VPC CIDRs

CIDR	Status	Status Reason
10.10.0.0/16	associated	

Availability Zone us-east-1a

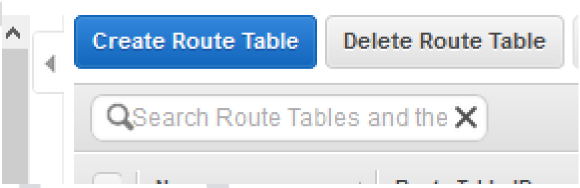
IPv4 CIDR block 10.10.1.0/24

- For **VPC name** and **Subnet name**, you can name your VPC and subnet to help you to identify them later in the console. You can specify your own IPv4 CIDR block range for the VPC and subnet, or you can leave the default values (10.0.0.0/16 and 10.0.0.0/24 respectively).

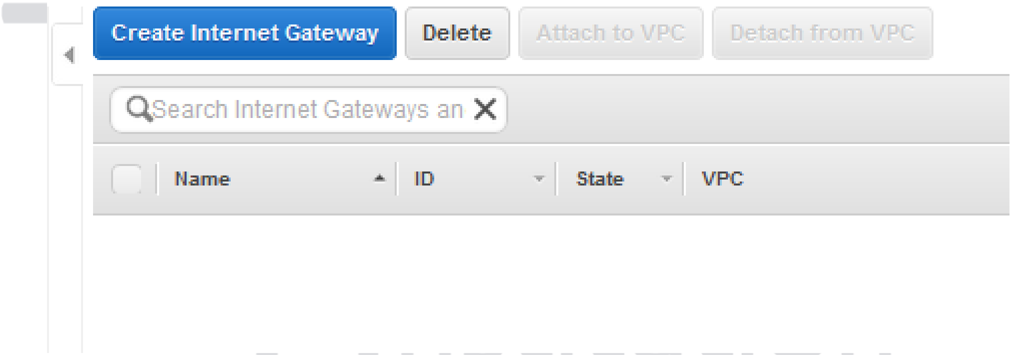


□	Name	Subnet ID	State	VPC	IPv4 CIDR
□	Subnet 1	subnet-904231cd	available	vpc-f6b3508d | VPC suriya	10.10.1.0/24
□	Subnet 2	subnet-9eba94fa	available	vpc-f6b3508d | VPC suriya	10.10.2.0/24
☑	Subnet 3	subnet-5f5d2e02	available	vpc-f6b3508d | VPC suriya	10.10.3.0/24

5. Create **route table**



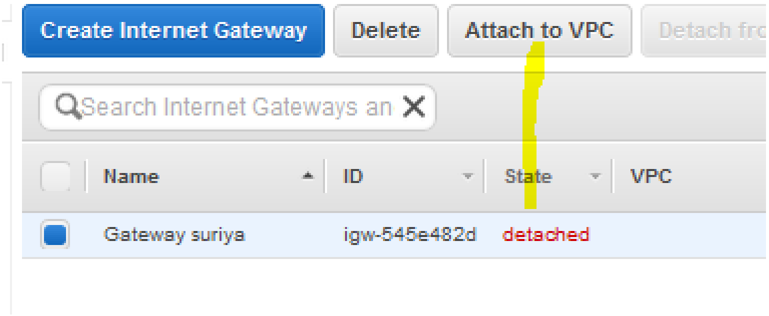
6. Creating and Attaching an Internet Gateway



□	Name	ID	State	VPC

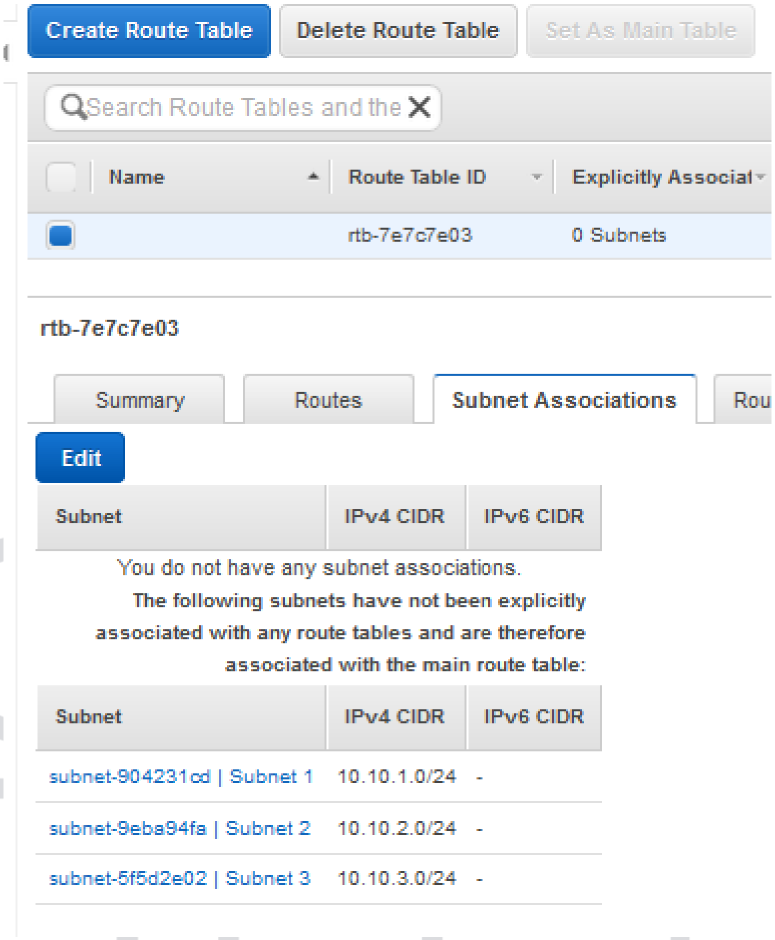
7. Select the Internet gateway that you just created, and then choose **Attach to VPC**.

In the **Attach to VPC** dialog box, select your VPC from the list, and then choose **Yes, Attach**.



□	Name	ID	State	VPC
☑	Gateway suriya	igw-545e482d	detached	

8. In Subnet Association, Attach the created Subnet and save



	Name	Route Table ID	Explicitly Associat
■		rtb-7e7c7e03	0 Subnets

rtb-7e7c7e03

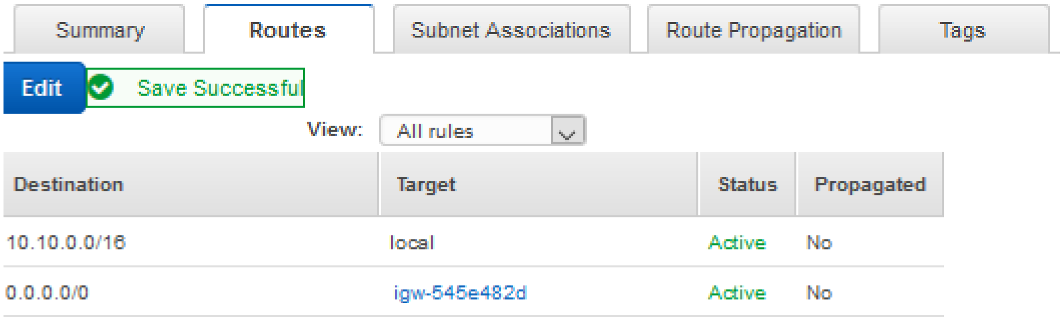
Subnet	IPv4 CIDR	IPv6 CIDR

You do not have any subnet associations.

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-904231cd | Subnet 1	10.10.1.0/24	-
subnet-9eba94fa | Subnet 2	10.10.2.0/24	-
subnet-5f5d2e02 | Subnet 3	10.10.3.0/24	-

9. In the Route table, Choose Routes and Edit and add the Internet gateway in it and Save



Save Successful

View: All rules

Destination	Target	Status	Propagated
10.10.0.0/16	local	Active	No
0.0.0.0/0	igw-545e482d	Active	No

To create a new security group and associate it with your instances

- Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
- In the navigation pane, choose **Security Groups**, and then choose **Create Security Group**.
- In the **Create Security Group** dialog box, specify a name for the security group and a description. Select the ID of your VPC from the **VPC** list, and then choose **Yes, Create**.
- Select the security group. The details pane displays the details for the security group, plus tabs for working with its inbound rules and outbound rules.
- On the **Inbound Rules** tab, choose **Edit**. Choose **Add Rule**, and complete the required information. For example, select **HTTP** or **HTTPS** from the **Type** list, and enter the **Source** as 0.0.0.0/0 for IPv4 traffic, or ::/0 for IPv6 traffic. Choose **Save** when you're done.
- Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
- In the navigation pane, choose **Instances** .
- Select the instance, choose **Actions**, then **Networking**, and then select **Change Security Groups**.
- In the **Change Security Groups** dialog box, clear the check box for the currently selected security group, and select the new one. Choose **Assign Security Groups**.

Adding Elastic IP Addresses

After you've launched an instance into the subnet, you must assign it an Elastic IP address if you want it to be reachable from the Internet over IPv4.

To allocate an Elastic IP address and assign it to an instance using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Elastic IPs**.
3. Choose **Allocate new address**.
4. Choose **Allocate**.

Note:

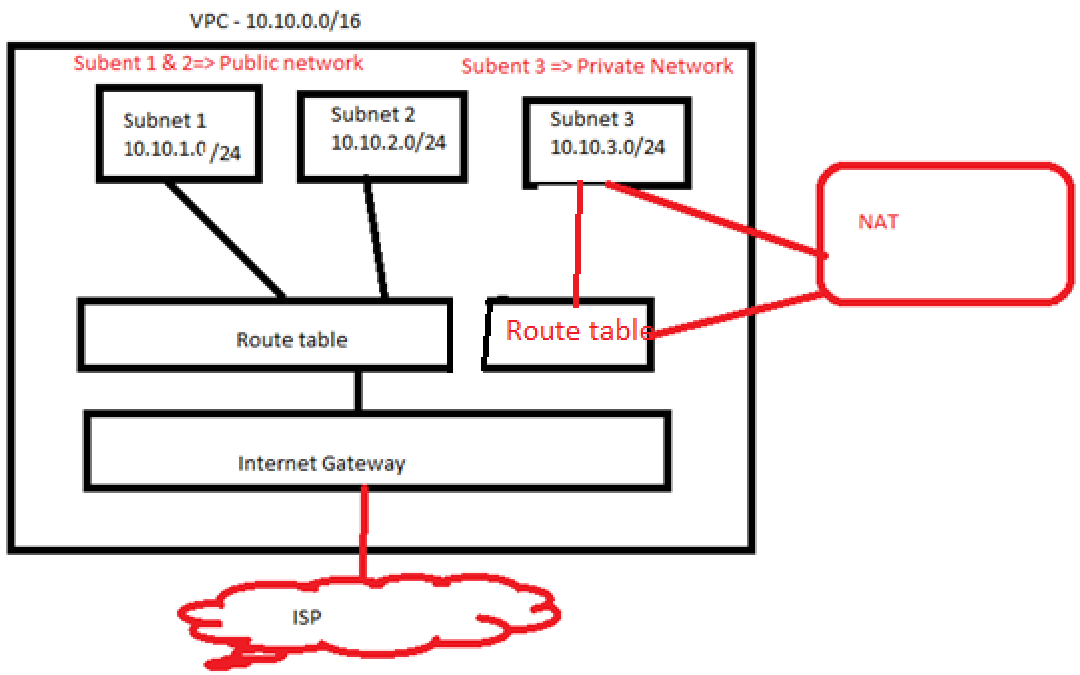
If your account supports EC2-Classic, first choose **VPC**.

5. 5. Select the Elastic IP address from the list, choose **Actions**, and then choose **Associate address**.
6. 6. Choose **Instance** or **Network interface**, and then select either the instance or network interface ID. Select the private IP address with which to associate the Elastic IP address, and then choose **Associate**.

NAT :-

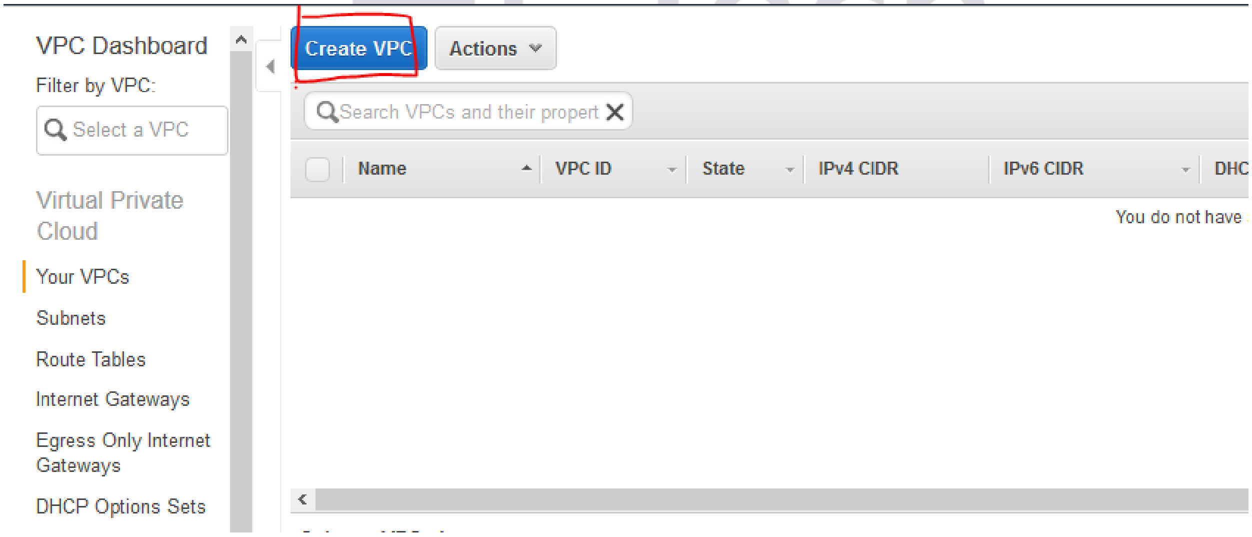
We can create a public-facing subnet for your web servers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access and can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Scenarios and Examples of NAT in VPC



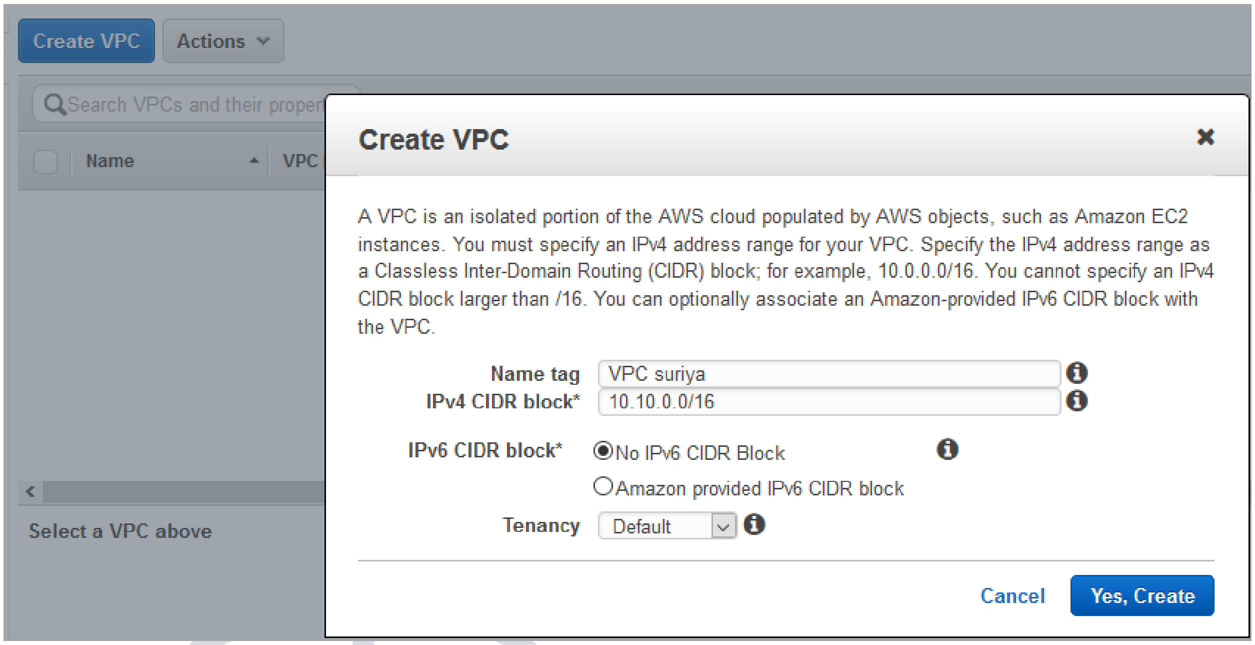
To create a NAT in VPC

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the dashboard, choose **Start VPC Wizard**.



	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHC

You do not have



Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

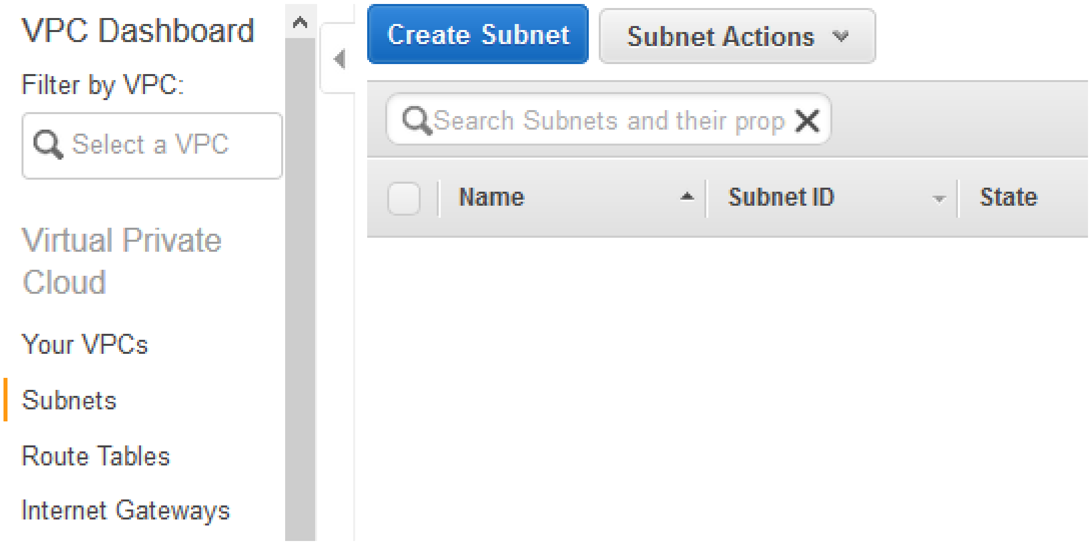
Name tag: VPC suriya

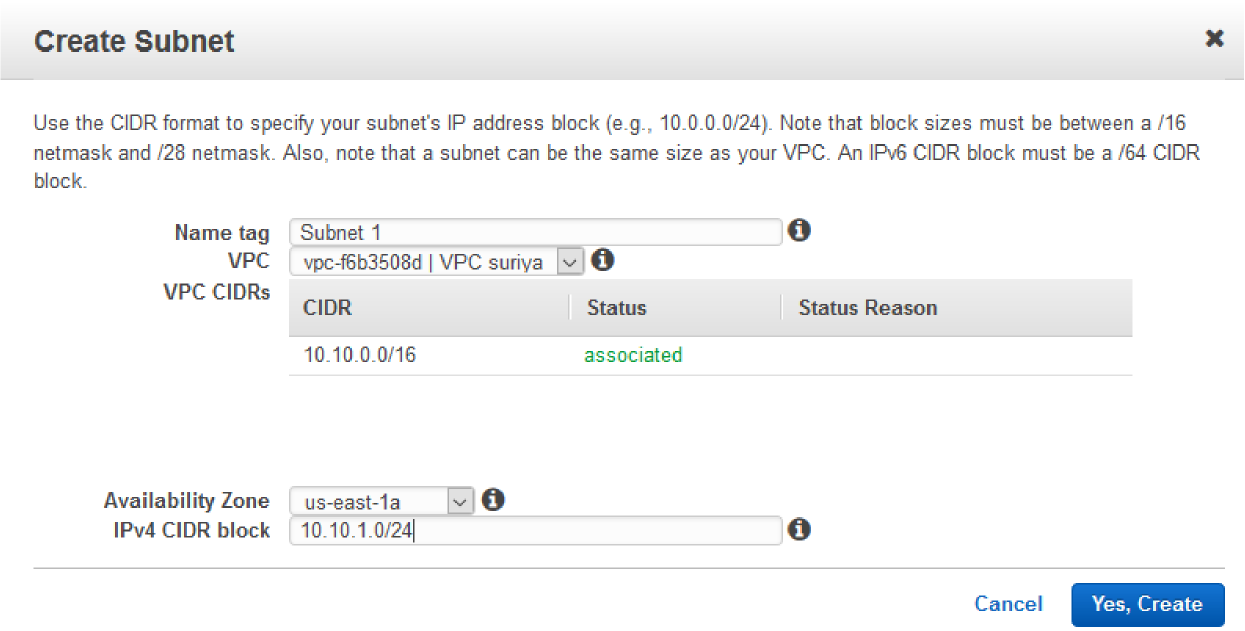
IPv4 CIDR block*: 10.10.0.0/16

IPv6 CIDR block*: ● No IPv6 CIDR Block ○ Amazon provided IPv6 CIDR block

Tenancy: Default

3. Select the first option, **VPC with a Single Public Subnet**, and then choose **Select**.





Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: Subnet 1

VPC: vpc-f6b3508d | VPC suriya

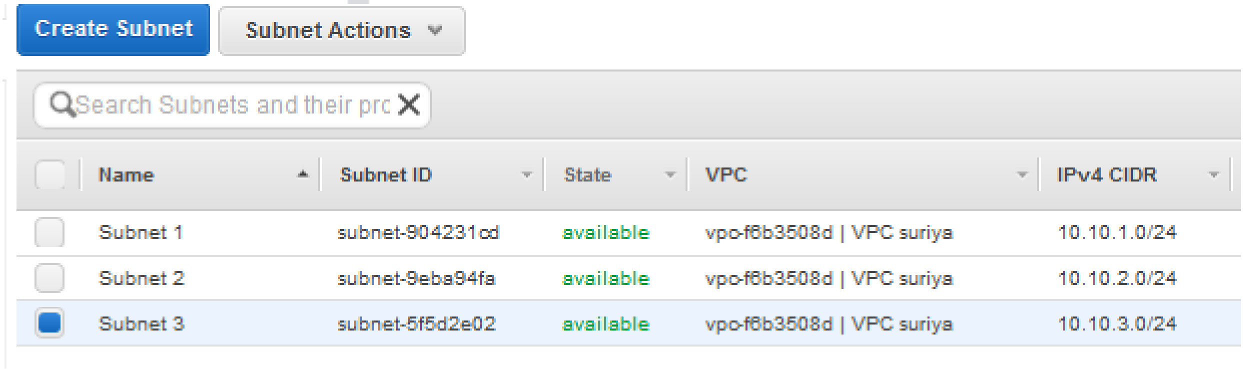
VPC CIDRs

CIDR	Status	Status Reason
10.10.0.0/16	associated	

Availability Zone: us-east-1a

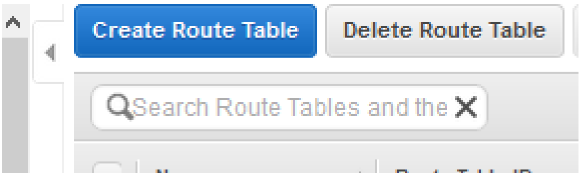
IPv4 CIDR block: 10.10.1.0/24

4. For **VPC name** and **Subnet name**, you can name your VPC and subnet to help you to identify them later in the console. You can specify your own IPv4 CIDR block range for the VPC and subnet, or you can leave the default values (10.0.0.0/16 and 10.0.0.0/24 respectively).

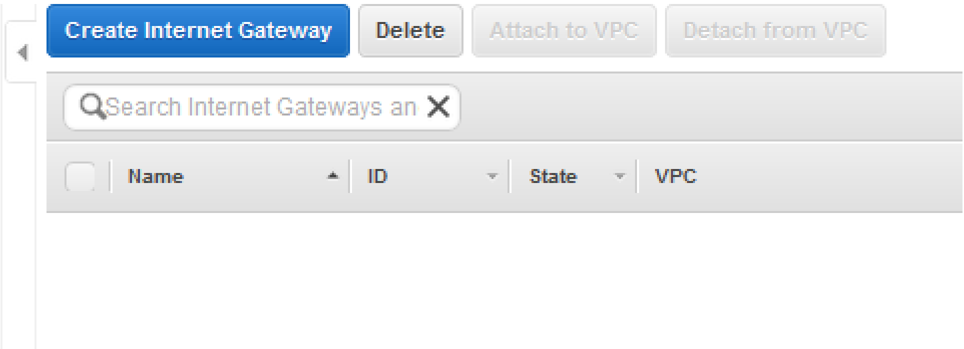


☐	Name	Subnet ID	State	VPC	IPv4 CIDR
☐	Subnet 1	subnet-904231cd	available	vpc-f6b3508d | VPC suriya	10.10.1.0/24
☐	Subnet 2	subnet-9eba94fa	available	vpc-f6b3508d | VPC suriya	10.10.2.0/24
■	Subnet 3	subnet-5f5d2e02	available	vpc-f6b3508d | VPC suriya	10.10.3.0/24

5. Create **route table**



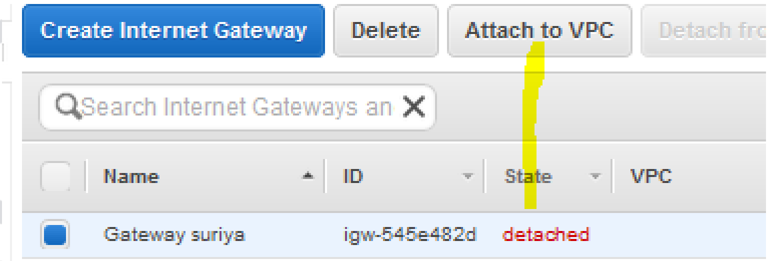
6. Creating and Attaching an Internet Gateway



☐	Name	ID	State	VPC

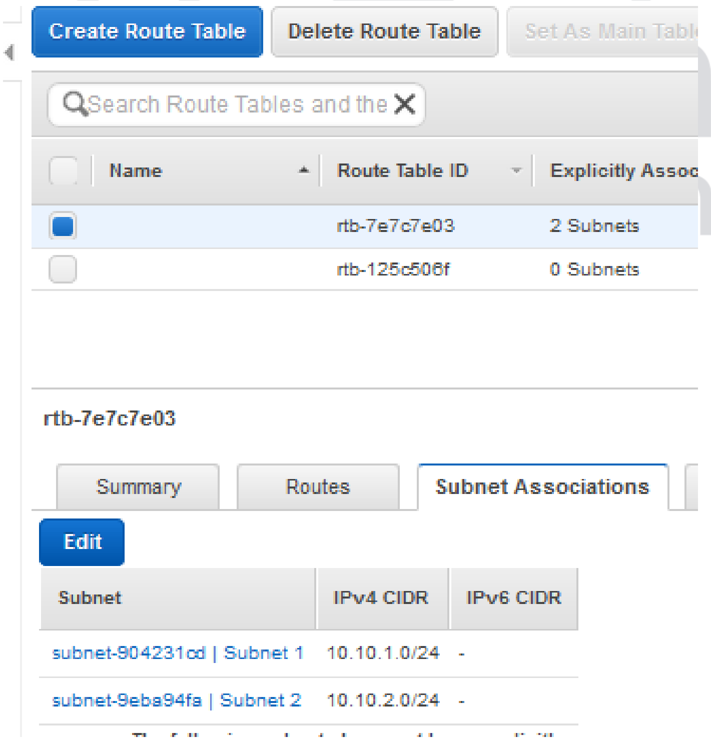
7. Select the Internet gateway that you just created, and then choose **Attach to VPC**.

In the **Attach to VPC** dialog box, select your VPC from the list, and then choose **Yes, Attach**.



☐	Name	ID	State	VPC
☑	Gateway suriya	igw-545e482d	detached	

8. In the Route Table, Subnet Association attach the created Subnet as subnet 1 and subnet 2, save it

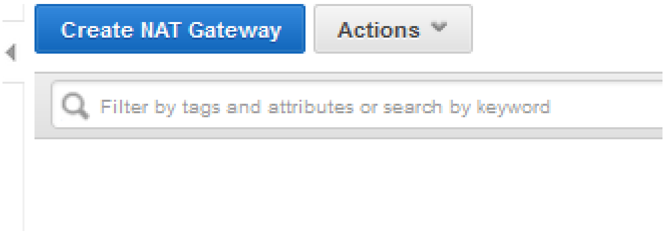


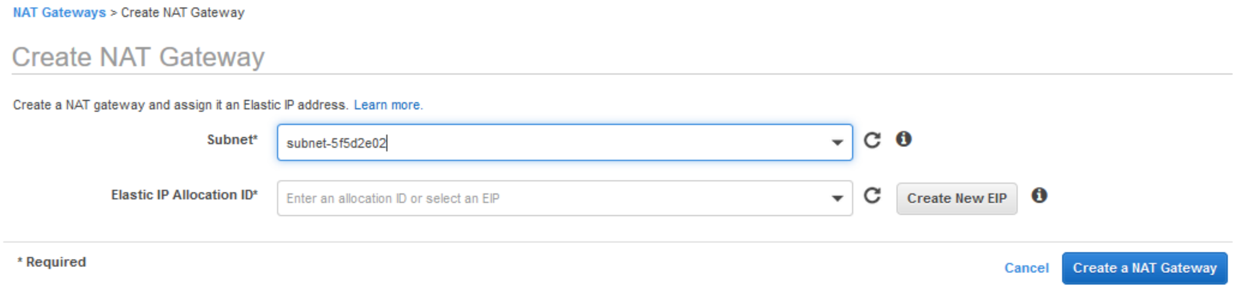
☐	Name	Route Table ID	Explicitly Assoc
☑		rtb-7e7c7e03	2 Subnets
☐		rtb-125c506f	0 Subnets

rtb-7e7c7e03

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-904231cd | Subnet 1	10.10.1.0/24	-
subnet-9eba94fa | Subnet 2	10.10.2.0/24	-

9. Create a NAT table for Subnet 3





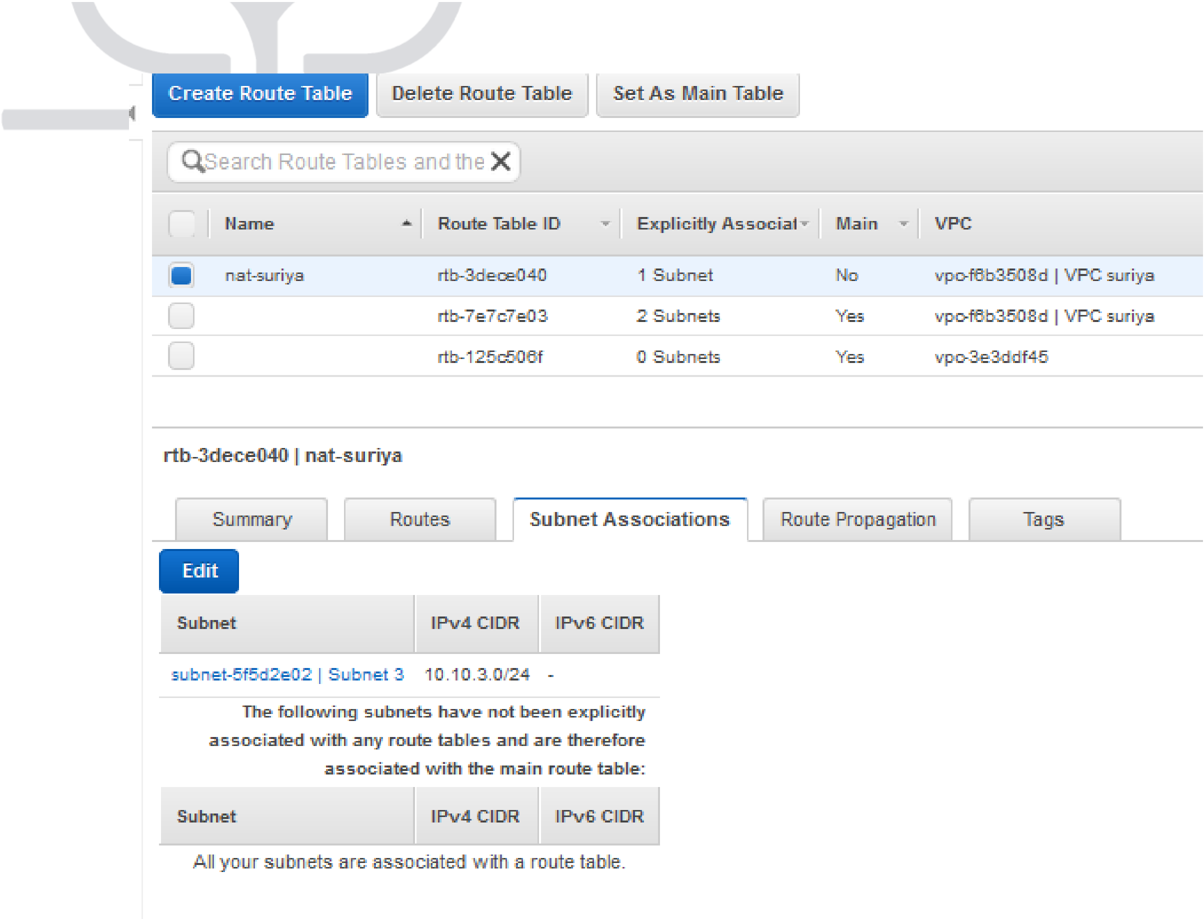
NAT Gateways > Create NAT Gateway

Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. Learn more.

Subnet*	subnet-5f5d2e02
Elastic IP Allocation ID*	Enter an allocation ID or select an EIP

* Required



	Name	Route Table ID	Explicitly Associat	Main	VPC
☑	nat-suriya	rtb-3dece040	1 Subnet	No	vpc-f6b3508d | VPC suriya
□		rtb-7e7c7e03	2 Subnets	Yes	vpc-f6b3508d | VPC suriya
□		rtb-125c506f	0 Subnets	Yes	vpc-3e3ddf45

rtb-3dece040 | nat-suriya

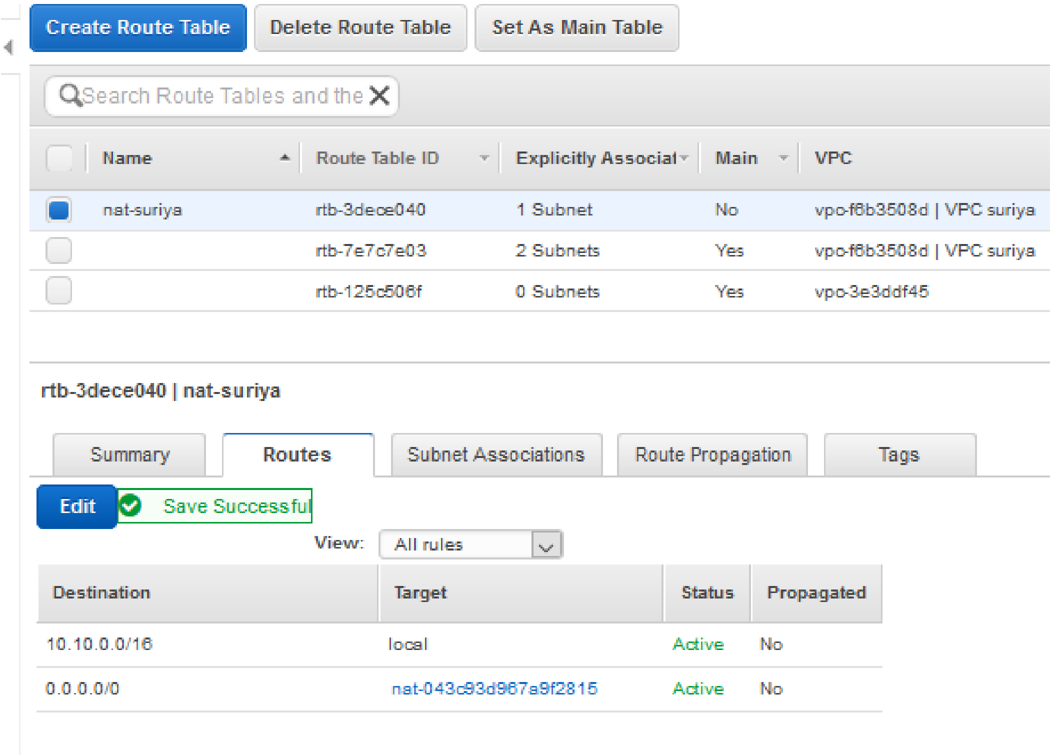
Subnet	IPv4 CIDR	IPv6 CIDR
subnet-5f5d2e02 | Subnet 3	10.10.3.0/24	-

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet	IPv4 CIDR	IPv6 CIDR

All your subnets are associated with a route table.

10. Create a route for NAT



☐	Name	Route Table ID	Explicitly Associat	Main	VPC
☑	nat-suriya	rtb-3dece040	1 Subnet	No	vpc-f6b3508d | VPC suriya
☐		rtb-7e7c7e03	2 Subnets	Yes	vpc-f6b3508d | VPC suriya
☐		rtb-125c506f	0 Subnets	Yes	vpc-3e3ddf45

rtb-3dece040 | nat-suriya

View: All rules

Destination	Target	Status	Propagated
10.10.0.0/16	local	Active	No
0.0.0.0/0	nat-043c93d967a9f2815	Active	No

11. Create a EC2 instance for Three subnet , subnet 3 will communicate a server Through NAT

12. We are unable to take a Subnet 3 server as a remote so that we can take RDP through subnet 3 by subnet 2 server.

13. We can check a NAT Elastic IP in subnet 3 instance

Network ACLs

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.

Network ACL Basics

The following are the basic things that you need to know about network ACLs:

- Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.
- You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.

- You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.
- A network ACL contains a numbered list of rules that we evaluate in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL. The highest number that you can use for a rule is 32766. We recommend that you start by creating rules with rule numbers that are multiples of 100, so that you can insert new rules where you need to later on.
- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

For more information about the number of network ACLs you can create, see Amazon VPC Limits.

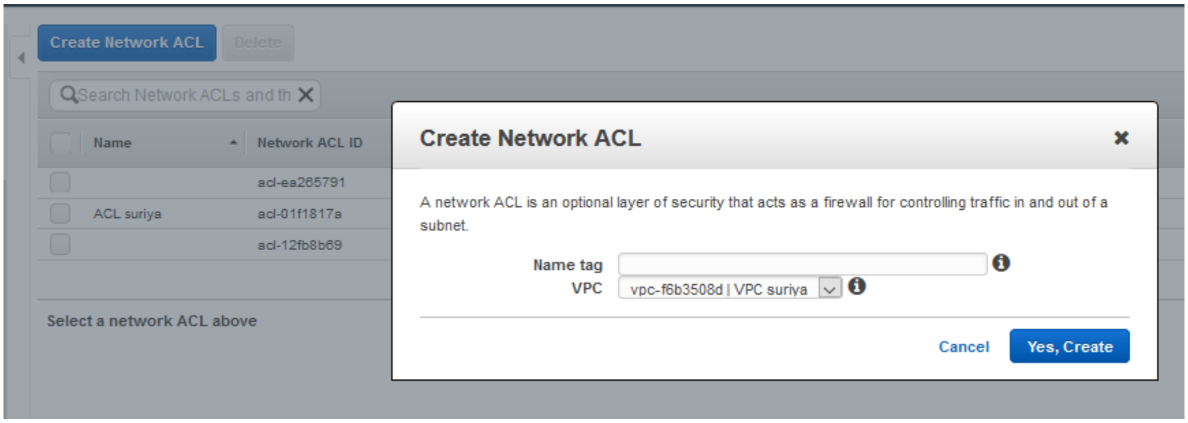
Network ACL Rules

You can add or remove rules from the default network ACL, or create additional network ACLs for your VPC. When you add or remove rules from a network ACL, the changes are automatically applied to the subnets it's associated with.

The following are the parts of a network ACL rule:

- Rule number. Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that may contradict it.
- Protocol. You can specify any protocol that has a standard protocol number. For more information, see Protocol Numbers. If you specify ICMP as the protocol, you can specify any or all of the ICMP types and codes.
- [Inbound rules only] The source of the traffic (CIDR range) and the destination (listening) port or port range.
- [Outbound rules only] The destination for the traffic (CIDR range) and the destination port or port range.
- Choice of ALLOW or DENY for the specified traffic.

1. Create a Network ACL in AWS and attach VPC for which it is connect.



Name	Network ACL ID
	acl-ea265791
ACL suriya	acl-01f1817a
	acl-12fb8b69

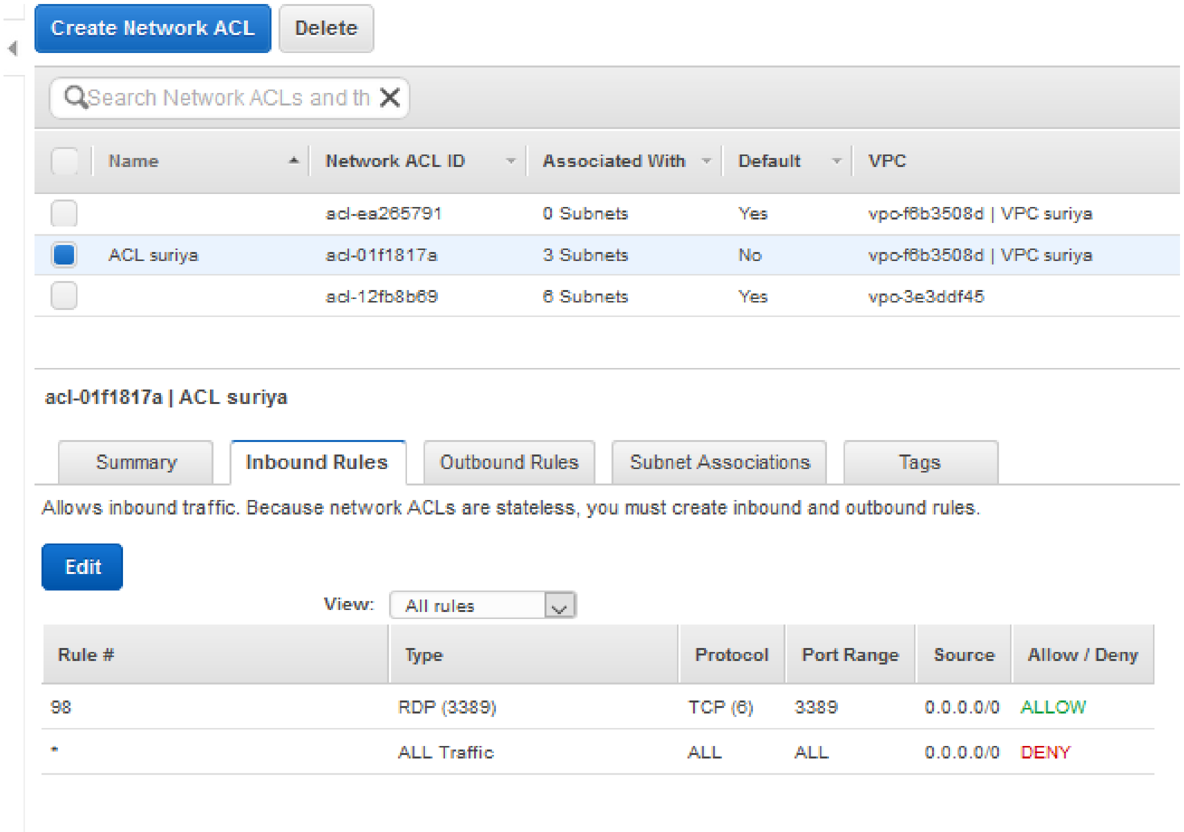
Select a network ACL above

Create Network ACL

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Name tag:
VPC: vpc-f6b3508d | VPC suriya

2. IN bound and Outbound rule can be DENY /ALLOW



	Name	Network ACL ID	Associated With	Default	VPC
□		acl-ea265791	0 Subnets	Yes	vpc-f6b3508d | VPC suriya
■	ACL suriya	acl-01f1817a	3 Subnets	No	vpc-f6b3508d | VPC suriya
□		acl-12fb8b69	6 Subnets	Yes	vpc-3e3ddf45

acl-01f1817a | ACL suriya

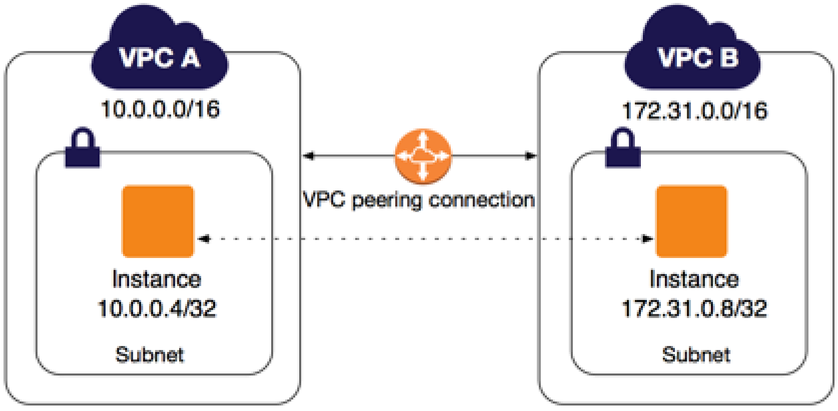
Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

View: All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
98	RDP (3389)	TCP (6)	3389	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Peering Connection:-

- 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.
- We 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).



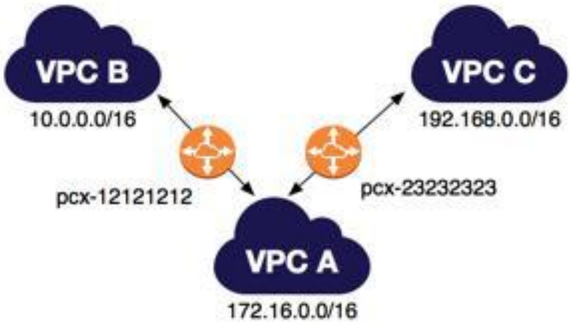
AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

A VPC peering connection helps you to facilitate the transfer of data. For example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.

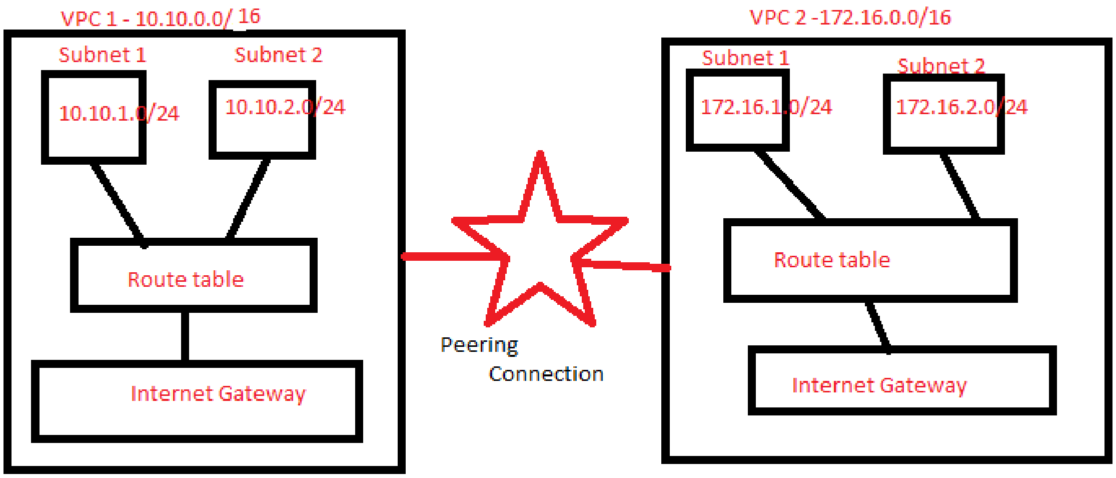
Multiple VPC Peering Connections

A VPC peering connection is a one to one relationship between two VPCs. You can create multiple VPC peering connections for each VPC that you own, but transitive peering relationships are not supported. You do not have any peering relationship with VPCs that your VPC is not directly peered with.

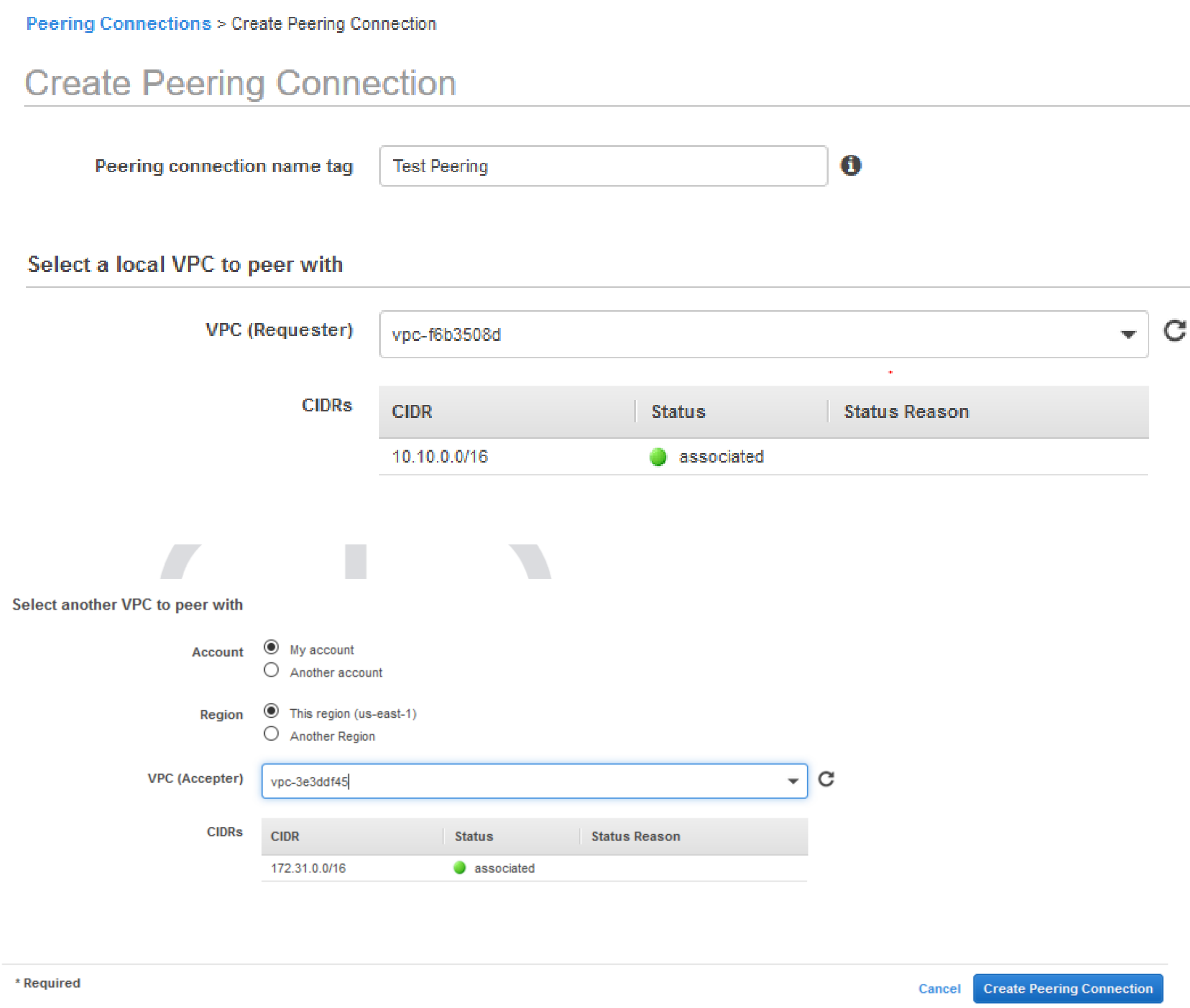
The following diagram is an example of one VPC peered to two different VPCs. There are two VPC peering connections: VPC A is peered with both VPC B and VPC C. VPC B and VPC C are not peered, and you cannot use VPC A as a transit point for peering between VPC B and VPC C. If you want to enable routing of traffic between VPC B and VPC C, you must create a unique VPC peering connection between them.



Scenarios and Examples of Two VPC Through Peering connection



1. Create a Peering connection in AWS



Peering Connections > Create Peering Connection

Create Peering Connection

Peering connection name tag: Test Peering

Select a local VPC to peer with

VPC (Requester): vpc-f6b3508d

CIDRs

CIDR	Status	Status Reason
10.10.0.0/16	● associated	

Select another VPC to peer with

Account: ● My account ○ Another account

Region: ● This region (us-east-1) ○ Another Region

VPC (Accepter): vpc-3e3ddf45

CIDRs

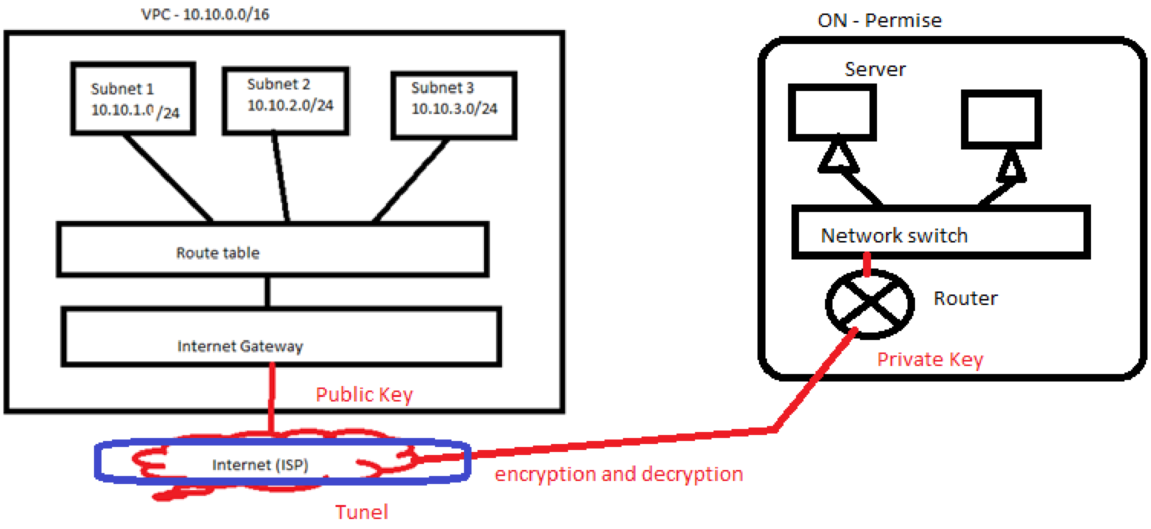
CIDR	Status	Status Reason
172.31.0.0/16	● associated	

* Required

VPN:-

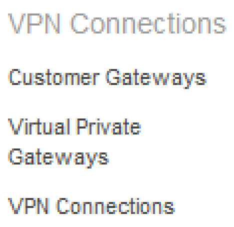
- A **virtual private network** (**VPN**) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
- Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network
- A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.
- A VPN available from the public Internet can provide some of the benefits of a wide area network

Scenarios and Examples of Two VPC Through Peering connection



To set up a VPN connection, you need to complete the following steps:

Step 1: Create a Customer Gateway
Step 2: Create a Virtual Private Gateway
Step 3: Enable Route Propagation in Your Route Table
Step 4: Update Your Security Group
Step 5: Create a VPN Connection and Configure the Customer Gateway


VPN Connections

Customer Gateways

Virtual Private Gateways

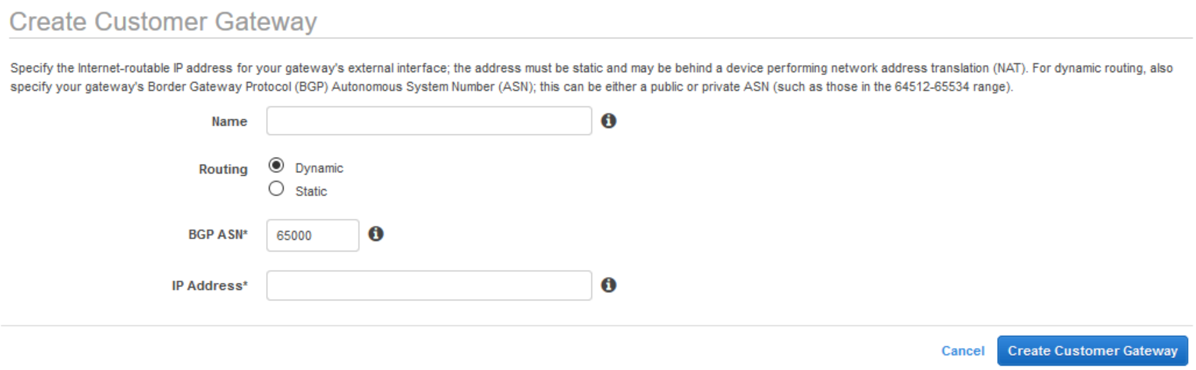
VPN Connections

To create a customer gateway using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Customer Gateways**, and then **Create Customer Gateway**.
3. Complete the following and then choose **Create Customer Gateway**:

- (Optional) For **Name**, type a name for your customer gateway. Doing so creates a tag with a key of Name and the value that you specify.
- For **Routing**, select the routing type.
- For dynamic routing, for **BGP ASN**, type the Border Gateway Protocol (BGP) Autonomous System Number (ASN).

- For **IP Address**, type the static, internet-routable IP address for your customer gateway device. If your customer gateway is behind a NAT device that's enabled for NAT-T, use the public IP address of the NAT device.



Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

Name

Routing ● Dynamic ○ Static

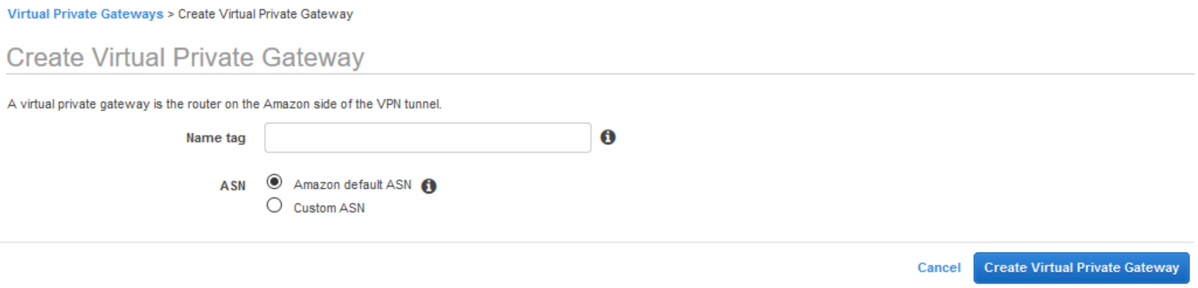
BGP ASN* 65000

IP Address*

Cancel | Create Customer Gateway

To create a virtual private gateway and attach it to your VPC

1. In the navigation pane, choose **Virtual Private Gateways**, **Create Virtual Private Gateway**.
2. (Optional) Type a name for your virtual private gateway. Doing so creates a tag with a key of Name and the value that you specify.
3. For **ASN**, leave the default selection to use the default Amazon ASN. Otherwise, choose **Custom ASN** and type a value. For a 16-bit ASN, the value must be in the 64512 to 65534 range. For a 32-bit ASN, the value must be in the 4200000000 to 4294967294 range.
4. Choose **Create Virtual Private Gateway**.
5. Select the virtual private gateway that you created, and then choose **Actions**, **Attach to VPC**.
6. Select your VPC from the list and choose **Yes, Attach**.



Virtual Private Gateways > Create Virtual Private Gateway

Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag

ASN ● Amazon default ASN ○ Custom ASN

Cancel | Create Virtual Private Gateway

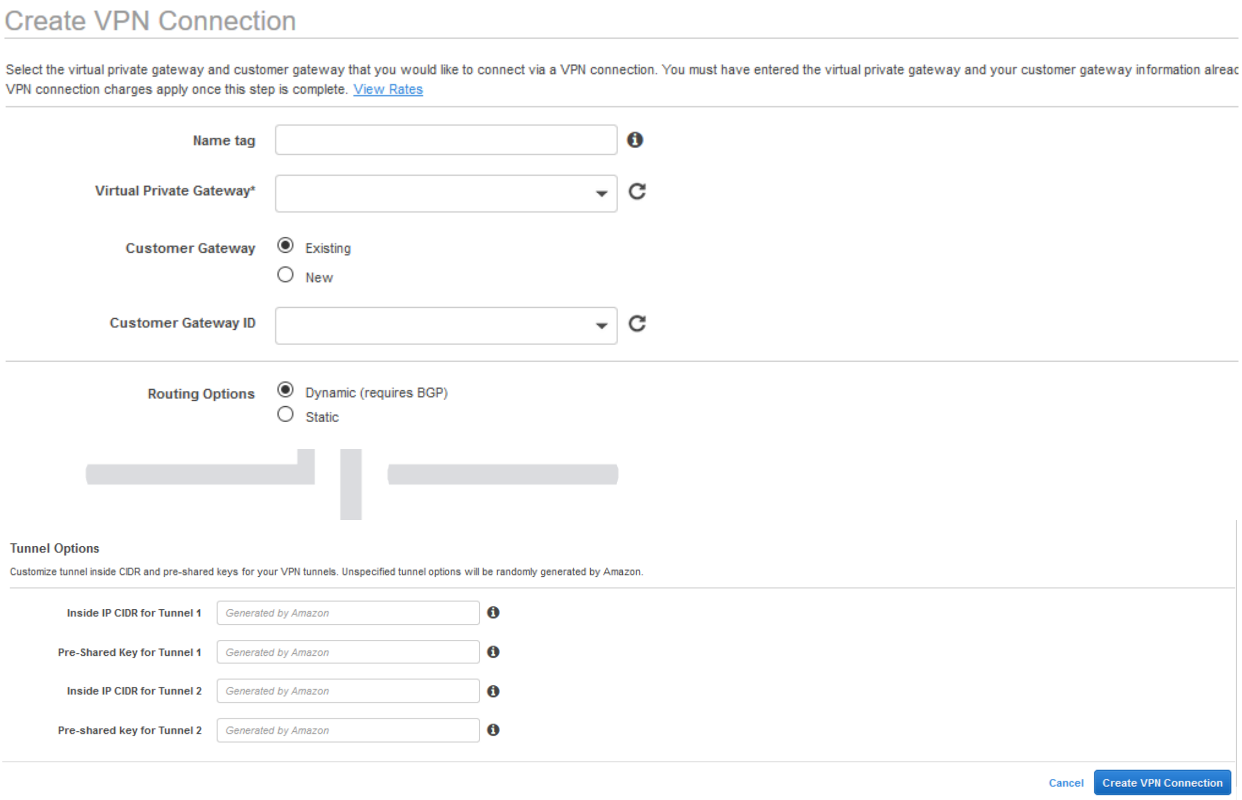
To enable route propagation using the console

1. In the navigation pane, choose **Route Tables**, and then select the route table that's associated with the subnet; by default, this is the main route table for the VPC.
2. On the **Route Propagation** tab in the details pane, choose **Edit**, select the virtual private gateway that you created in the previous procedure, and then choose **Save**.

To add rules to your security group to enable inbound SSH, RDP and ICMP access

1. In the navigation pane, choose **Security Groups**, and then select the default security group for the VPC.
2. On the **Inbound** tab in the details pane, add rules that allow inbound SSH, RDP, and ICMP access from your network, and then choose **Save**. For more information about adding inbound rules, see Adding, Removing, and Updating Rules.

To create a VPN connection and configure the customer gateway



Create VPN Connection

Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information alreac
VPN connection charges apply once this step is complete. View Rates

Name tag

Virtual Private Gateway*

Customer Gateway ● Existing ○ New

Customer Gateway ID

Routing Options ● Dynamic (requires BGP) ○ Static

Tunnel Options

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IP CIDR for Tunnel 1: Generated by Amazon

Pre-Shared Key for Tunnel 1: Generated by Amazon

Inside IP CIDR for Tunnel 2: Generated by Amazon

Pre-shared key for Tunnel 2: Generated by Amazon

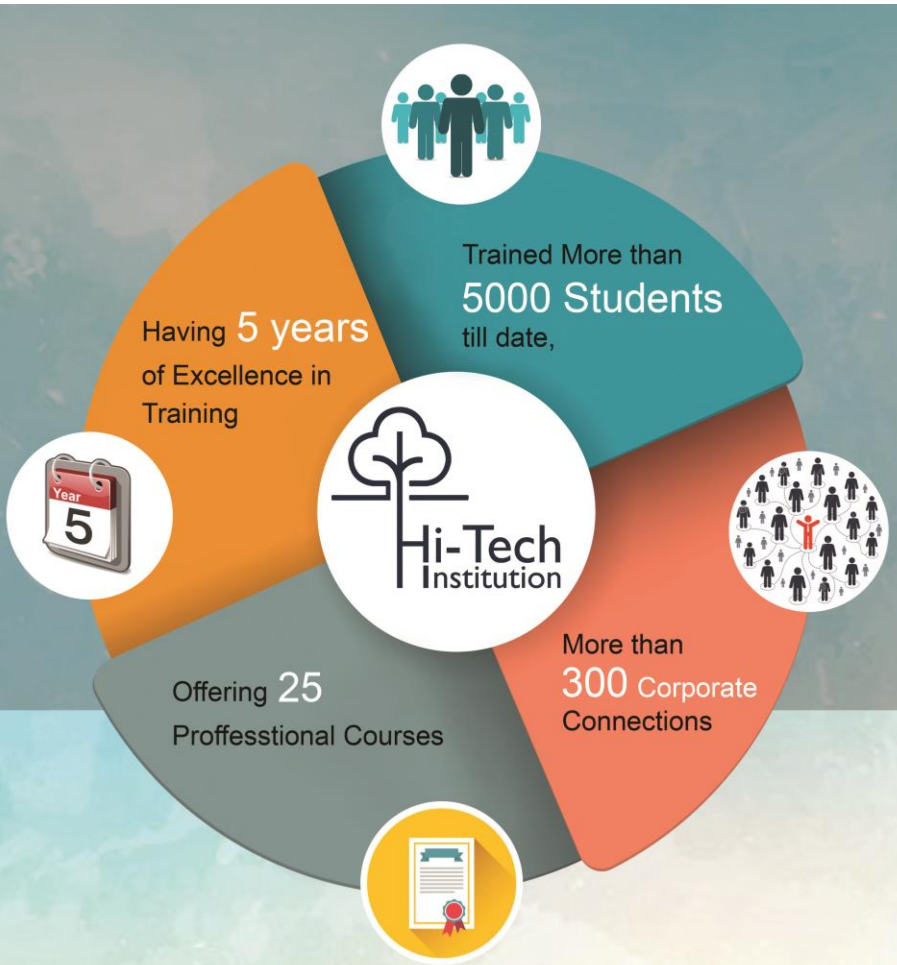
1. In the navigation pane, choose **VPN Connections**, **Create VPN Connection**.
2. Complete the following information, and then choose **Create VPN Connection**:
    - (Optional) For **Name tag**, type a name for your VPN connection. Doing so creates a tag with a key of Name and the value that you specify.
    - Select the virtual private gateway that you created earlier.
    - Select the customer gateway that you created earlier.
    - Select one of the routing options based on whether your VPN router supports Border Gateway Protocol (BGP):
        - If your VPN router supports BGP, choose **Dynamic (requires BGP)**.
        - If your VPN router does not support BGP, choose **Static**. For **Static IP Prefixes**, specify each IP prefix for the private network of your VPN connection.

Under **Tunnel Options**, you can optionally specify the following information for each tunnel:

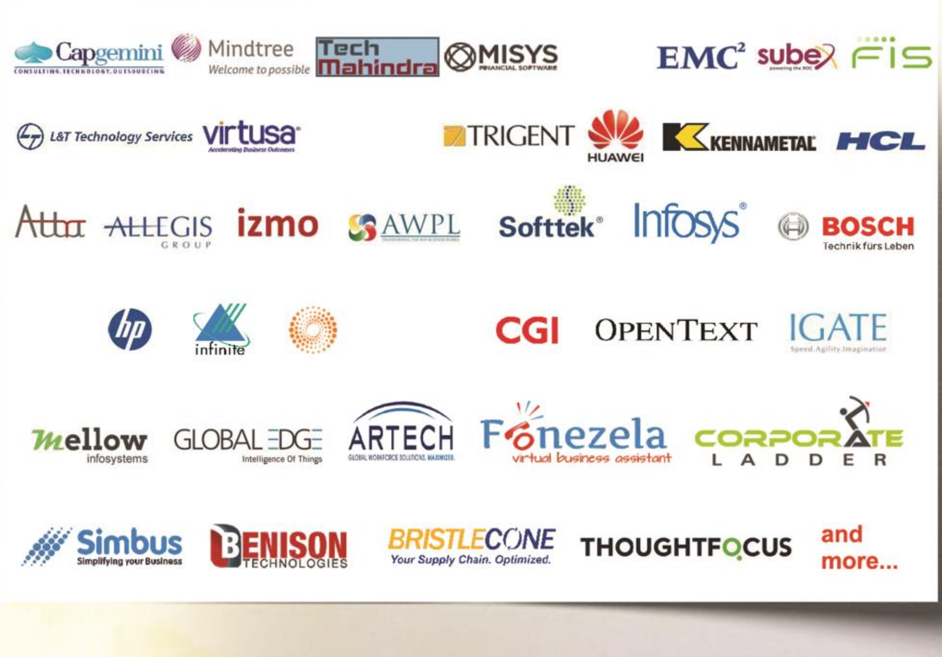
- A size /30 CIDR block from the 169.254.0.0/16 range for the inside tunnel IP addresses.
- The IKE pre-shared key (PSK).

For more information about these options, see Configuring the VPN Tunnels for Your VPN Connection.

3. It may take a few minutes to create the VPN connection. When it's ready, select the connection and choose **Download Configuration**.
4. In the **Download Configuration** dialog box, select the vendor, platform, and software that corresponds to your customer gateway device or software, and then choose **Yes, Download**.
5. Give the configuration file to your network administrator, along with this guide: Amazon VPC Network Administrator Guide. After the network administrator configures the customer gateway, the VPN connection is operational.


Hi-Tech Institution
Having 5 years of Excellence in Training
Year 5
Trained More than 5000 Students till date,
More than 300 Corporate Connections
Offering 25 Proffesstional Courses

TOP RECRUITERS



Hi-Tech Institution

Candidate Eligibilities

☑ IT Employees

☑ Any Degree

☑ Any Diploma

☑ 12th or 10th

☑

☑

50% offer for School or College students

30% offer for IT Employees

Above offer applicable only technical courses. Terms and conditions apply

Email Us

operations@hitechins.in

Search Us

www.hitechins.in

CONTACT US

7092 90 91 92 / 82 20 21 7640

PONDICHERRY
No.32, 100 feet road,
Ellaipillaichavady,
Pondicherry – 605 005,
Nearby Rajiv Gandhi Hospital

TAMBARAM
No.24, Chithi Vinayagar Kovil street,
KamarajNagar, Tambaram Sanatorium,
Chennai – 600 047,
Nearby Sanatorium Railway Station

VELACHERRY
No: 21, Officer Colony,
100 feet road, VijayaNagar,
Velacherry – 600 042,
Nearby Sathya Home Appliances

Locations

Chennai & Pondicherry