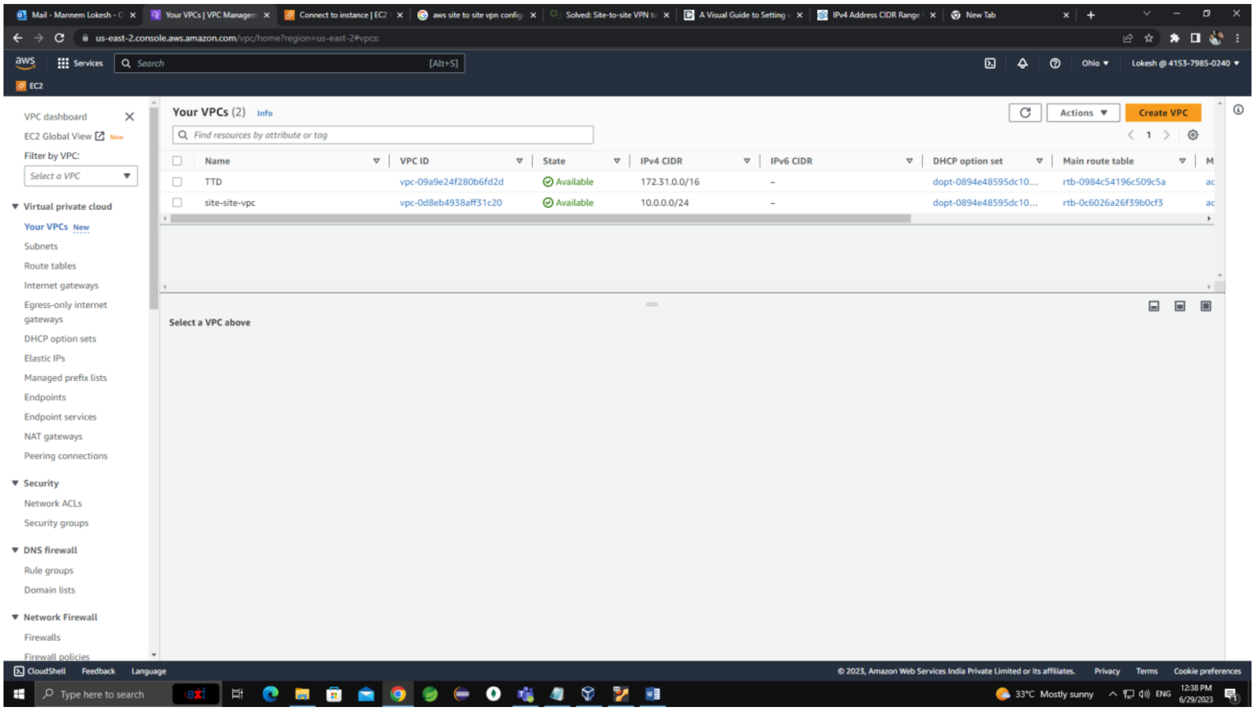
1. Site to Site Connectivity between AWS to On premises

Step 1: Create a VPC



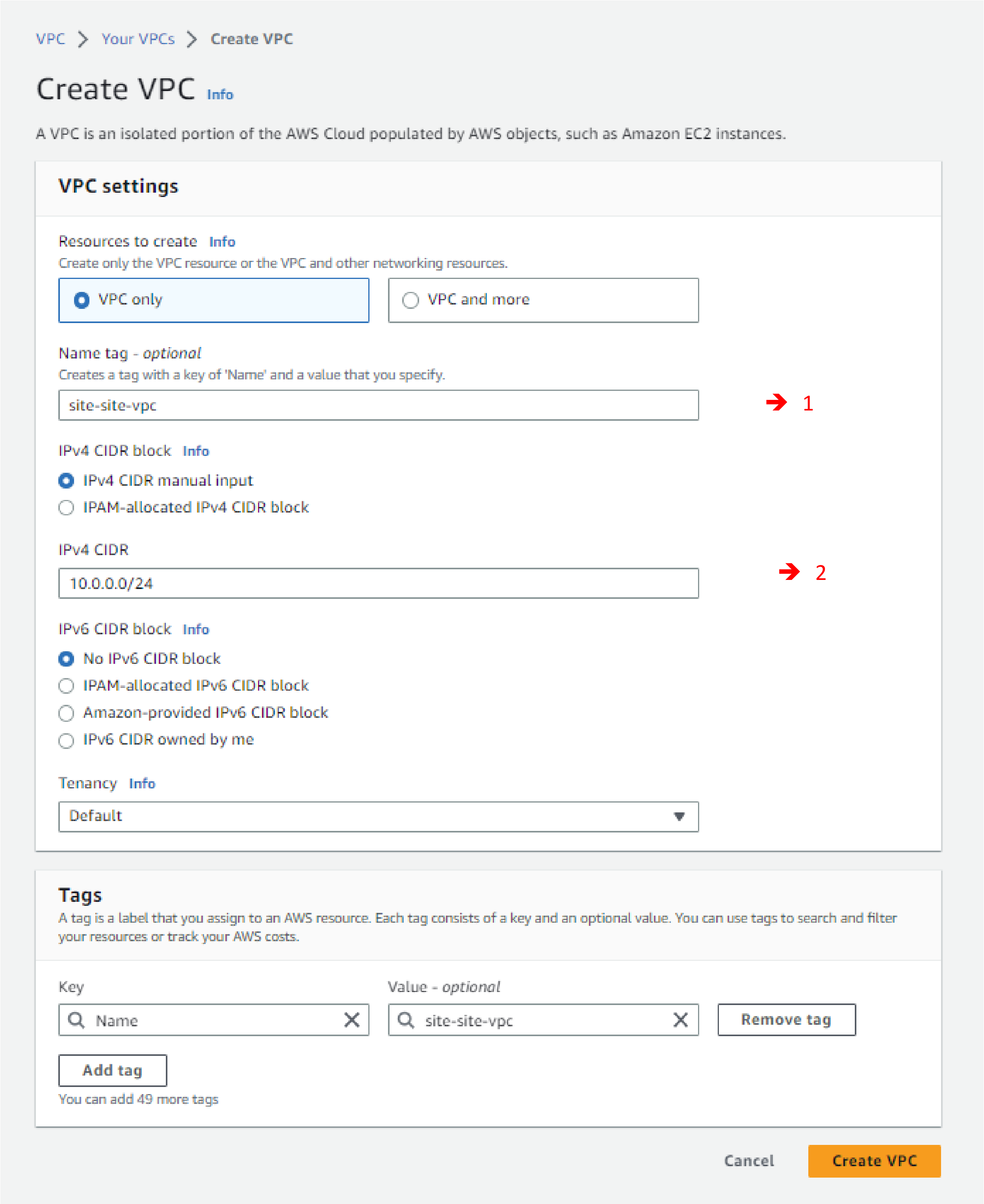
Your VPCs (2) Info

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table
TTD	vpc-09a9e24f280b6fd2d	Available	172.31.0.0/16	–	dopt-0894e48595dc10...	rtb-0984c54196c509c5a
site-site-vpc	vpc-0d8eb4938aff31c20	Available	10.0.0.0/24	–	dopt-0894e48595dc10...	rtb-0c6026a26f39b0cf3

Select a VPC above

Click on Create VPC Button

Do the Configuration as mentioned in below image



VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

● VPC only ○ VPC and more

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

site-site-vpc

IPv4 CIDR block Info

● IPv4 CIDR manual input

○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/24

IPv6 CIDR block Info

● No IPv6 CIDR block

○ IPAM-allocated IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

○ IPv6 CIDR owned by me

Tenancy Info

Default

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

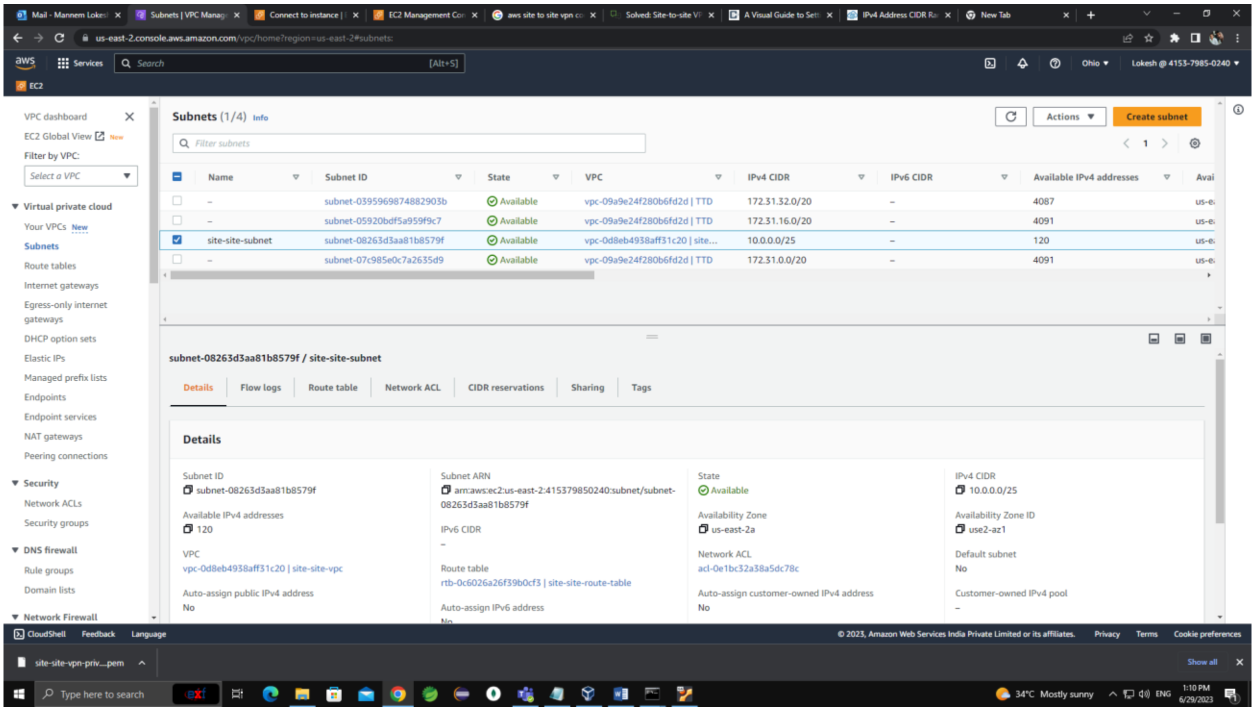
Key	Value - *optional*	
Name	site-site-vpc	Remove tag

Add tag

You can add 49 more tags

1. Enter the name of the VPC under Name tag – optional
2. Enter IPv4 CIDR range. It’s your choice. I had entered 10.0.0.0/24

Step 2: Create a Subnet



us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#subnets:

Subnets (1/4) Info

	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Avai
□	–	subnet-0395969874882903b	Available	vpc-09a9e24f280b6fd2d | TTD	172.31.32.0/20	–	4087	us-e
□	–	subnet-05920bdf5a959f9c7	Available	vpc-09a9e24f280b6fd2d | TTD	172.31.16.0/20	–	4091	us-e
☑	site-site-subnet	subnet-08263d3aa81b8579f	Available	vpc-0d8eb4938aff31c20 | site...	10.0.0.0/25	–	120	us-e
□	–	subnet-07c985e0c7a2635d9	Available	vpc-09a9e24f280b6fd2d | TTD	172.31.0.0/20	–	4091	us-e

subnet-08263d3aa81b8579f / site-site-subnet

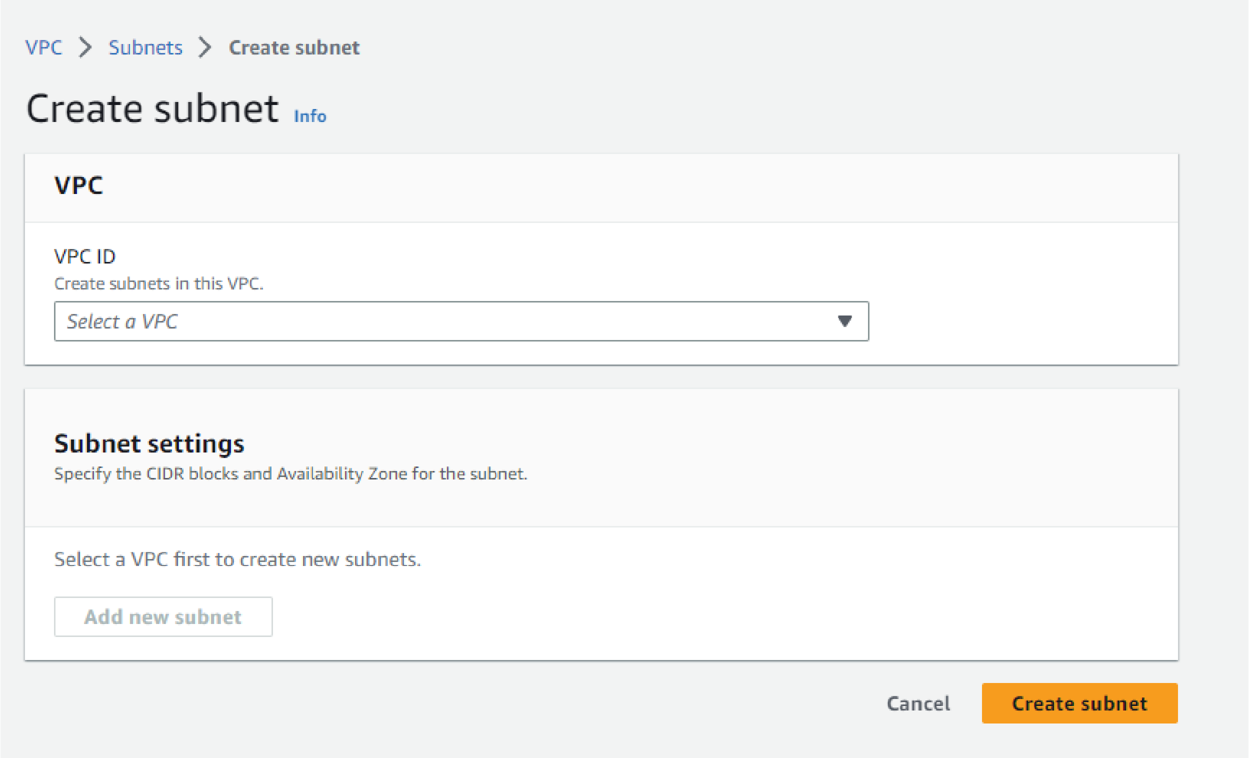
Details | Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Details

Subnet ID: subnet-08263d3aa81b8579f
Subnet ARN: arn:aws:ec2:us-east-2:415379850240:subnet/subnet-08263d3aa81b8579f
State: Available
IPv4 CIDR: 10.0.0.0/25
Available IPv4 addresses: 120
IPv6 CIDR: –
Availability Zone: us-east-2a
Availability Zone ID: use2-az1
VPC: vpc-0d8eb4938aff31c20 | site-site-vpc
Route table: rtb-0c6026a26f39b0cf3 | site-site-route-table
Network ACL: acl-0e1bc32a38a5dc78c
Default subnet: No
Auto-assign public IPv4 address: No
Auto-assign IPv6 address: No
Auto-assign customer-owned IPv4 address: No
Customer-owned IPv4 pool: –

© 2023, Amazon Web Services India Private Limited or its affiliates.

Click on Create Subnet Button



Create subnet

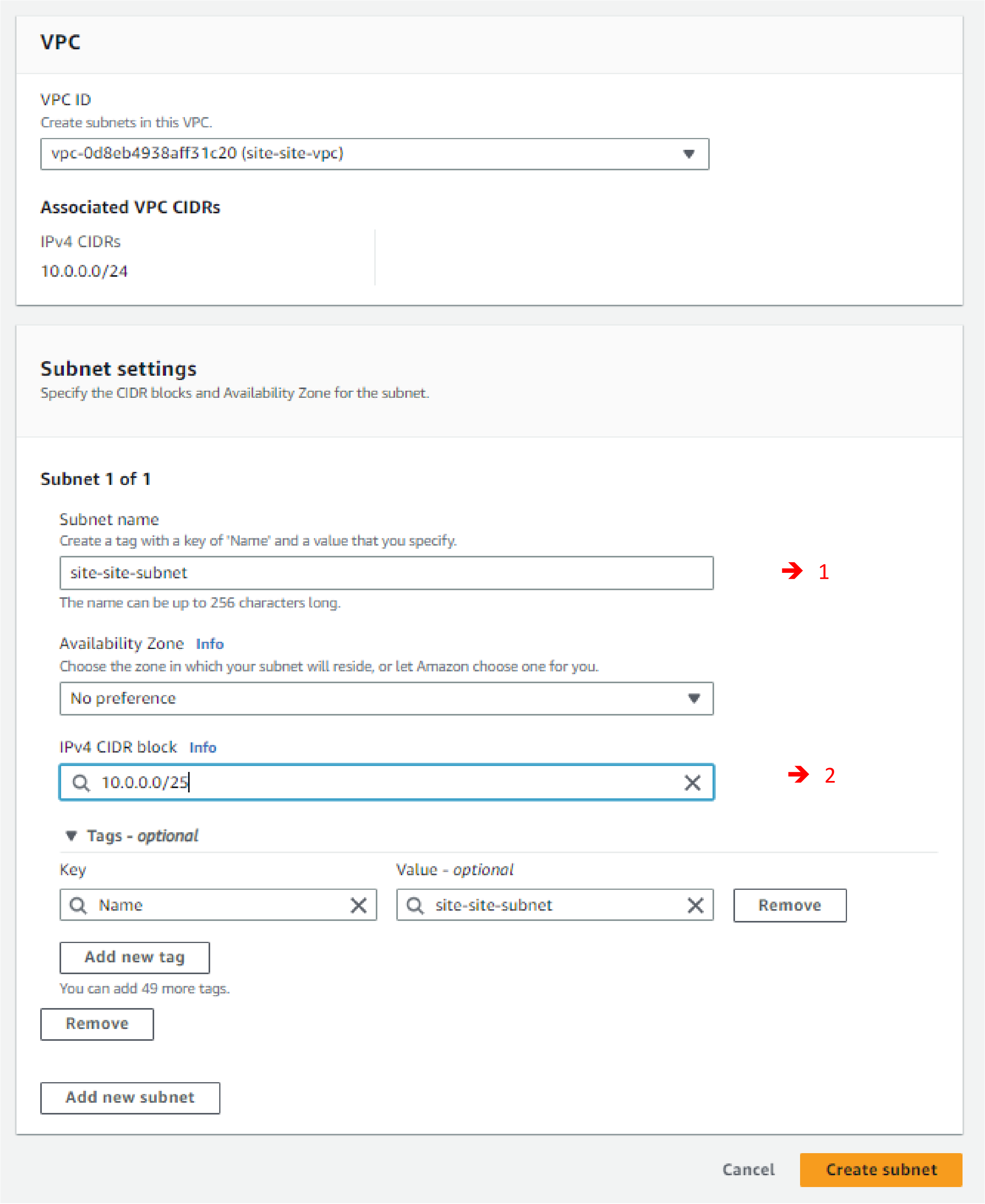
VPC

VPC ID
Create subnets in this VPC.
Select a VPC

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Select a VPC first to create new subnets.

Attach VPC which we had create earlier (site-site-vpc) to the subnet



VPC

VPC ID
Create subnets in this VPC.
vpc-0d8eb4938aff31c20 (site-site-vpc) ▼

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/24

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
site-site-subnet
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference ▼

IPv4 CIDR block Info
10.0.0.0/25

▼ Tags - *optional*

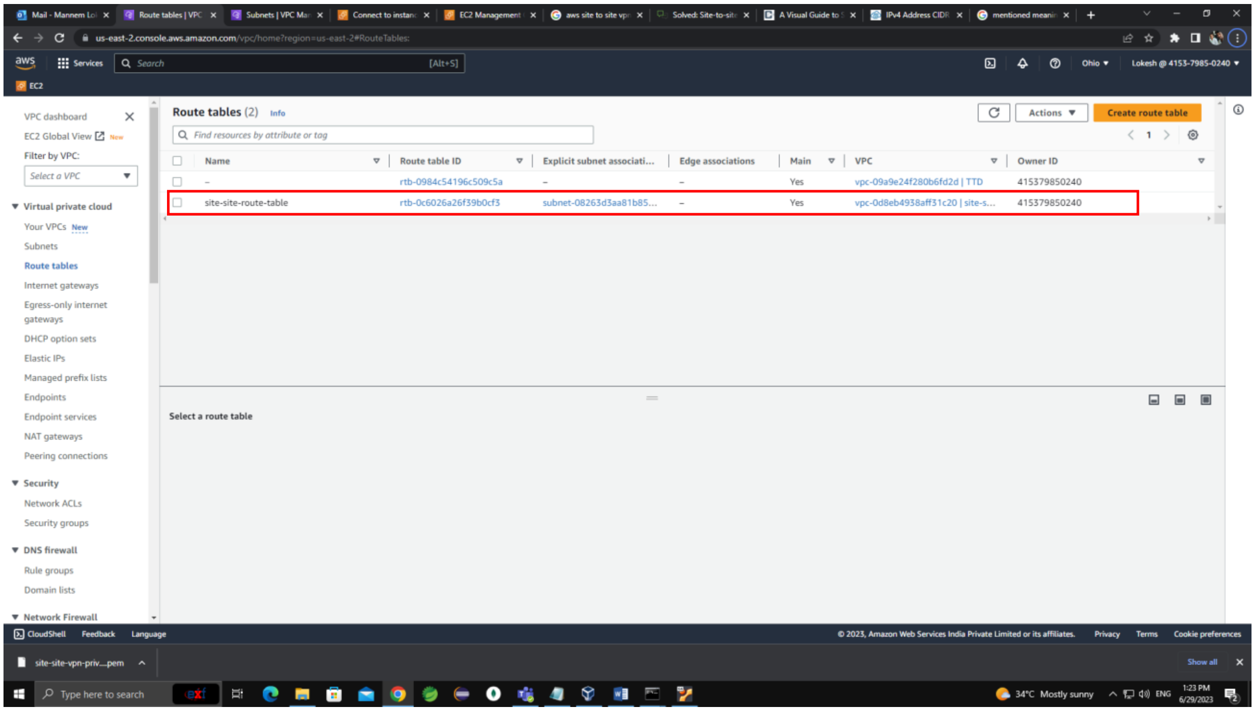
Key	Value - *optional*	
Name	site-site-subnet	Remove

Add new tag
You can add 49 more tags.

1. Enter Subnet name of your choice. I had named it as (site-site-subnet)
2. Inside IPv4 CIDR block, Enter CIDR range for your preference. (i.e, you can also enter the same CIDR range while you create VPC (10.0.0.0/24) also. Or else you can give different CIDR range. In my case I had given a CIDR range as 10.0.0.0/25

Step 3: Route Table

When you create a subnet, route table is automatically created as mentioned below.

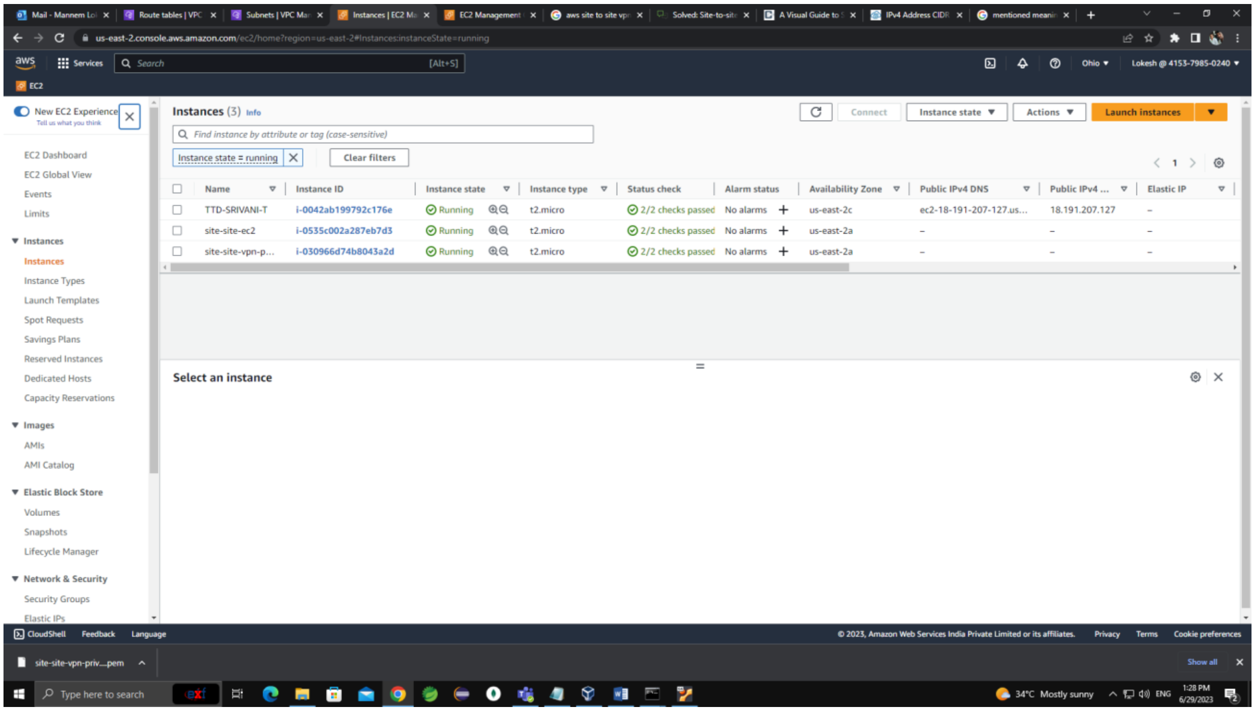


Route tables (2)

Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC	Owner ID
–	rtb-0984c54196c509c5a	–	–	Yes	vpc-09a9e24f280b6fd2d | TTD	415379850240
site-site-route-table	rtb-0c6026a26f39b0cf3	subnet-08263d3aa81b85...	–	Yes	vpc-0d8eb4938aff31c20 | site-s...	415379850240

Initially no name is there, So I had named it as site-site-route-table

Step 4: Create an instance in EC2

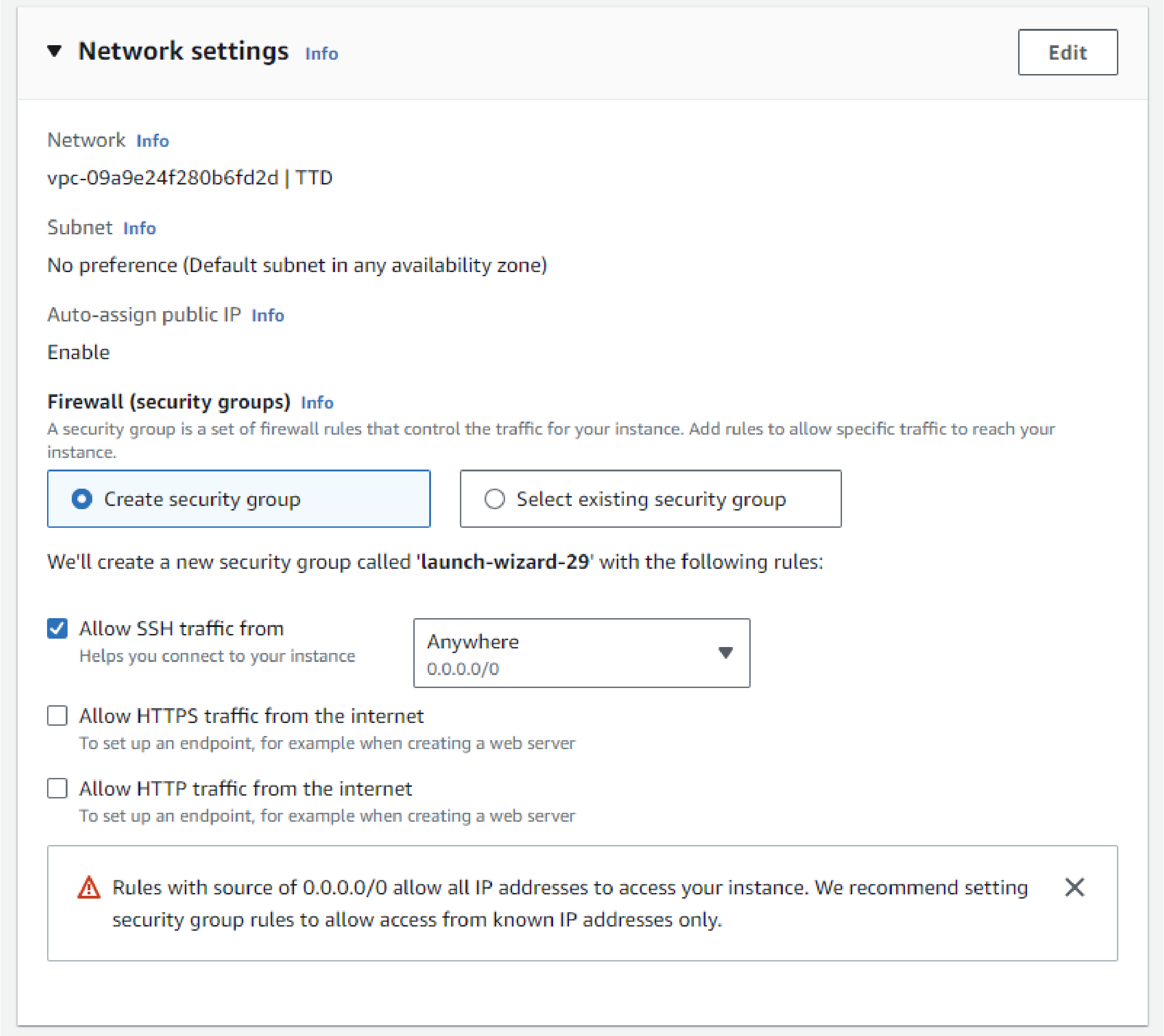


Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
TTD-SRIVANI-T	i-0042ab199792c176e	Running	t2.micro	2/2 checks passed	No alarms	us-east-2c	ec2-18-191-207-127.us...	18.191.207.127	–
site-site-ec2	i-0535c002a287eb7d3	Running	t2.micro	2/2 checks passed	No alarms	us-east-2a	–	–	–
site-site-vpn-p...	i-030966d74b8043a2d	Running	t2.micro	2/2 checks passed	No alarms	us-east-2a	–	–	–

Click on Launch instances Button

Create instance based on your needs and also you can able to choose OS of your choice.

Note: Make sure to create a new key pair of the instance.



Network Info
vpc-09a9e24f280b6fd2d | TTD

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-29**' with the following rules:

☑ Allow SSH traffic from — Anywhere 0.0.0.0/0
Helps you connect to your instance

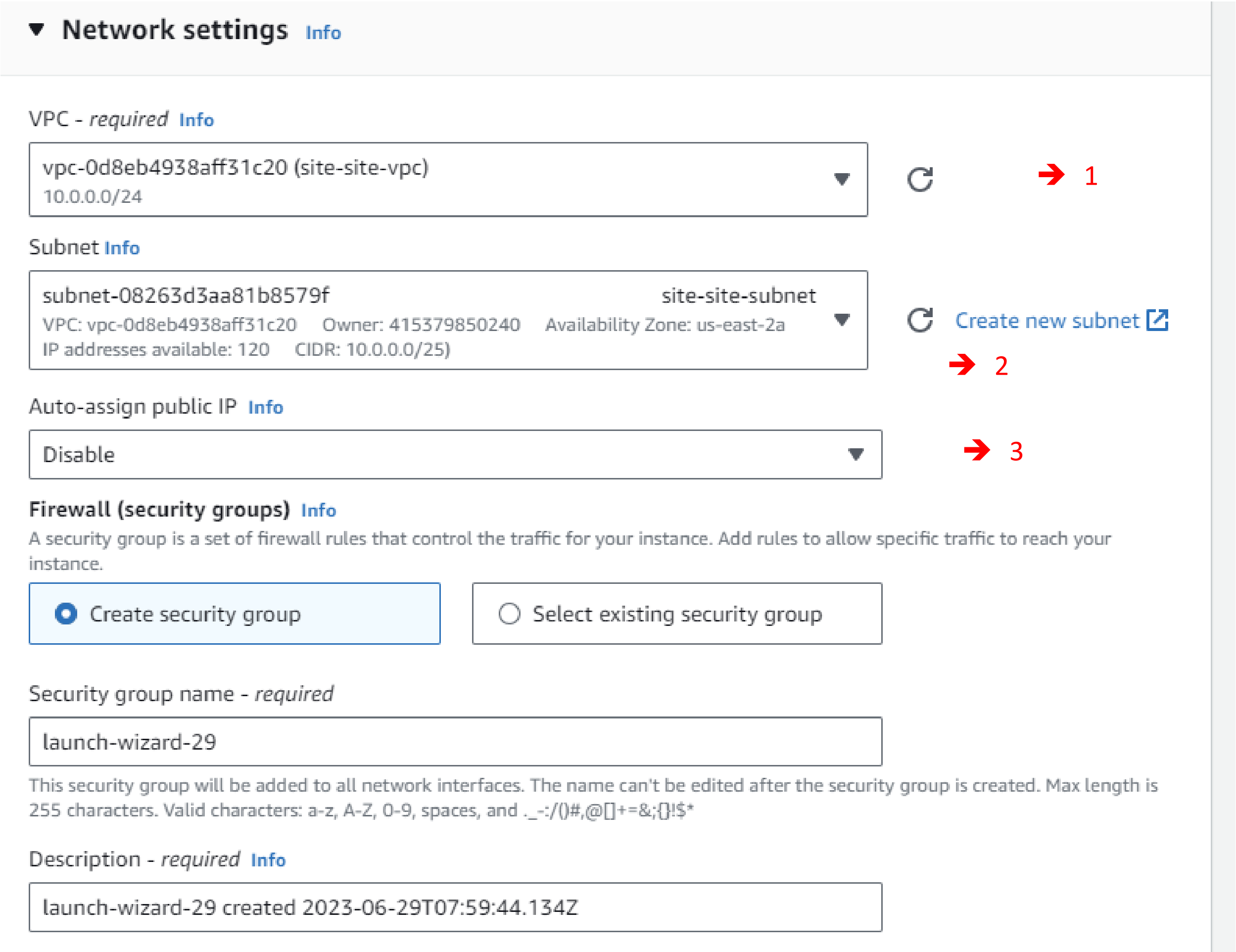
□ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

We have change these network settings.

So click on edit.


▼ Network settings Info

VPC - *required* Info

vpc-0d8eb4938aff31c20 (site-site-vpc)
10.0.0.0/24

Subnet Info

subnet-08263d3aa81b8579f site-site-subnet
VPC: vpc-0d8eb4938aff31c20 Owner: 415379850240 Availability Zone: us-east-2a
IP addresses available: 120 CIDR: 10.0.0.0/25)

Auto-assign public IP Info

Disable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*

launch-wizard-29

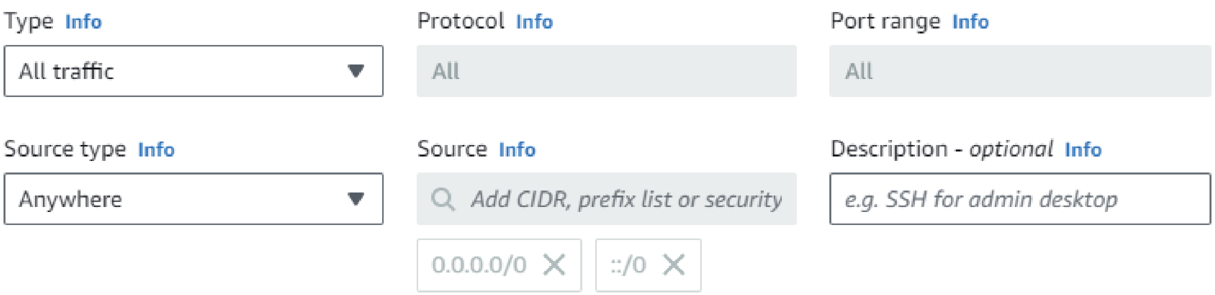
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

launch-wizard-29 created 2023-06-29T07:59:44.134Z

1. Attach VPC which we had created earlier. In my case (site-site-vpc)
2. Attach Subnet which we had created earlier. In my case (site-site-subnet)
3. Make sure to disable Auto-assign public IP

Note: Under inbound Security Group Rules Allow all traffic from anywhere.


Type Info: All traffic

Protocol Info: All

Port range Info: All

Source type Info: Anywhere

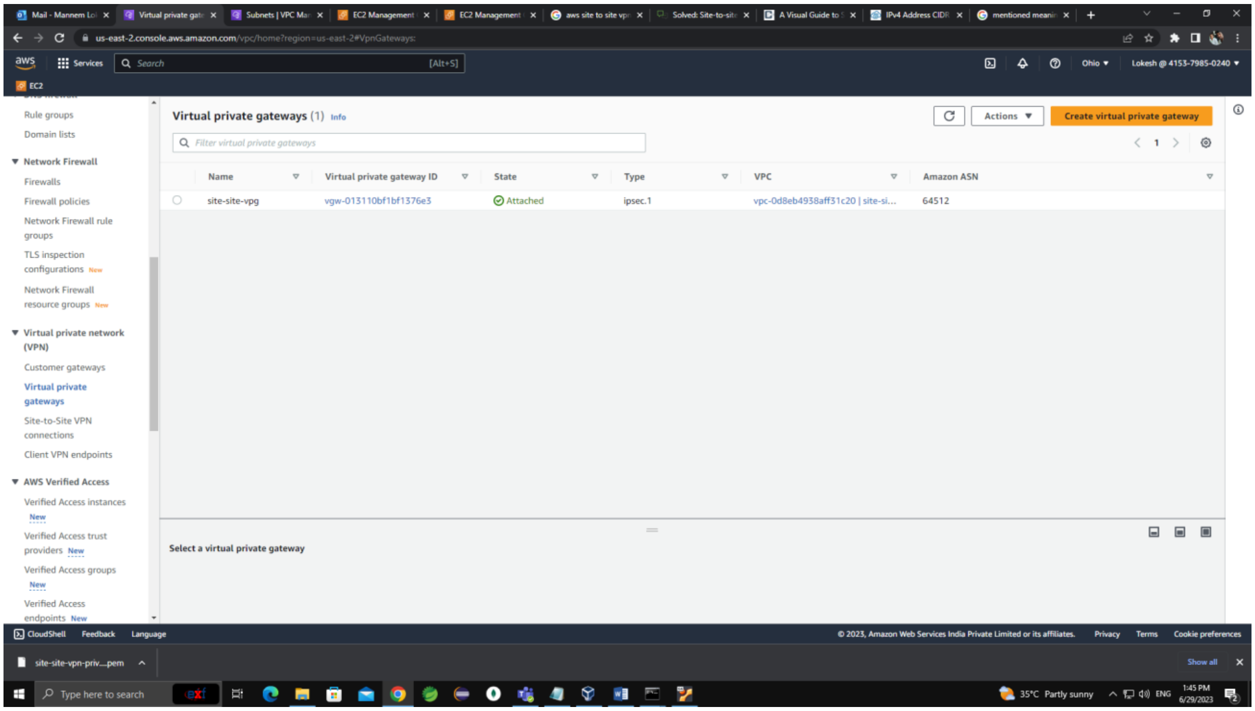
Source Info: *Add CIDR, prefix list or security*
0.0.0.0/0 ✕ ::/0 ✕

Description - *optional* Info: *e.g. SSH for admin desktop*

Now Click on Launch instance.

Note: If you want multiple instances at AWS site you can able create multiple instances with same vpc attached under Network Settings.

Step 4: Create Virtual Private Gateway

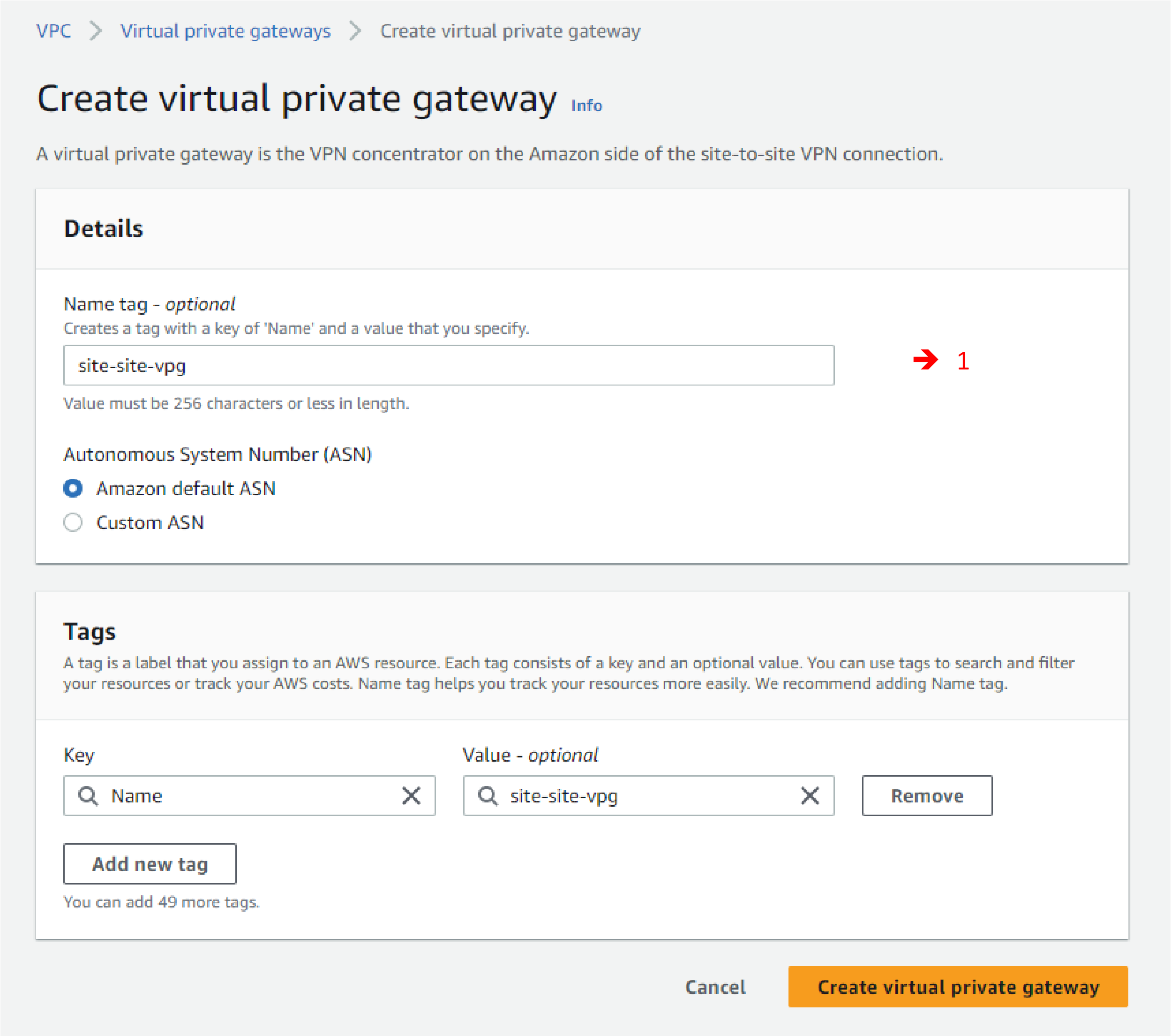


Rule groups
Domain lists
Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
TLS inspection configurations New
Network Firewall resource groups New
Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN connections
Client VPN endpoints
AWS Verified Access
Verified Access instances New
Verified Access trust providers New
Verified Access groups New
Verified Access endpoints New
Actions
Create virtual private gateway
Select a virtual private gateway

Virtual private gateways (1)

Name	Virtual private gateway ID	State	Type	VPC	Amazon ASN
site-site-vpg	vgw-013110bf1bf1376e3	Attached	ipsec.1	vpc-0d8eb4938aff31c20 | site-si...	64512

Click on Create virtual private gateway



VPC > Virtual private gateways > Create virtual private gateway

Create virtual private gateway Info

A virtual private gateway is the VPN concentrator on the Amazon side of the site-to-site VPN connection.

Details

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
site-site-vpg
Value must be 256 characters or less in length.

Autonomous System Number (ASN)
● Amazon default ASN
○ Custom ASN

Tags

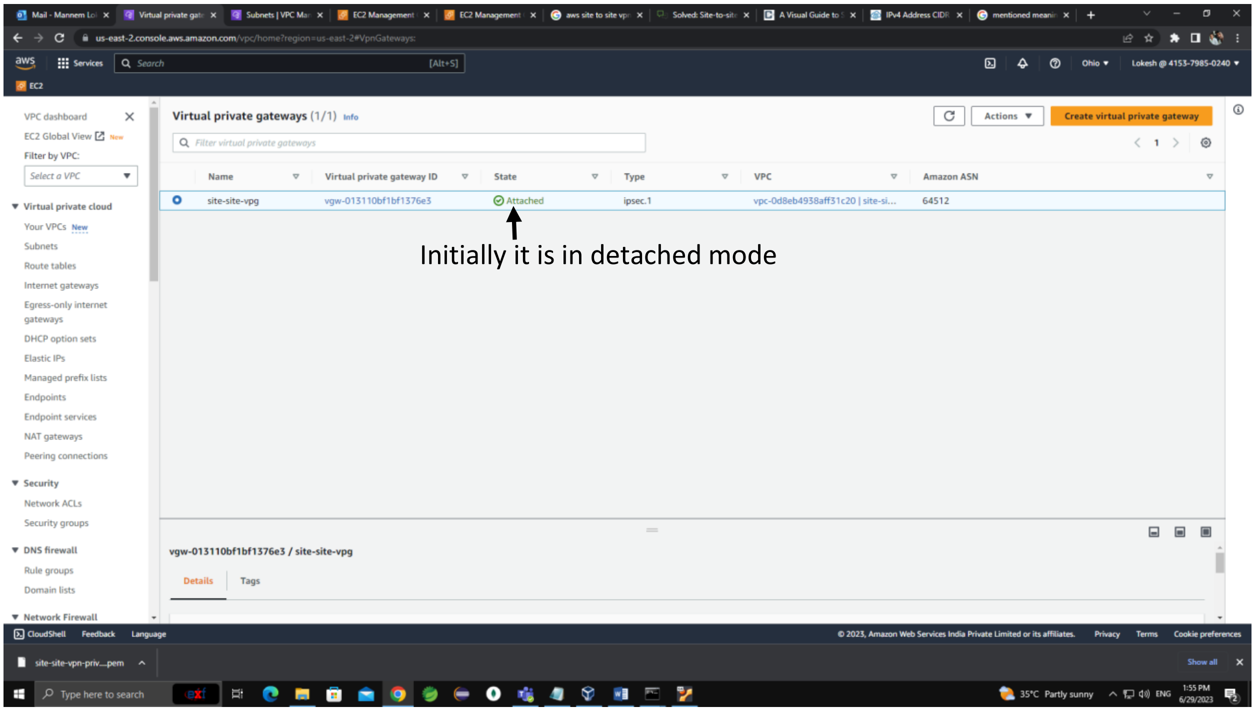
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key	Value - *optional*
Name	site-site-vpg

You can add 49 more tags.

1. Enter the Name of VPG. In my case I had named it as site-site-vpg

Click on virtual private gateway button to create VPG



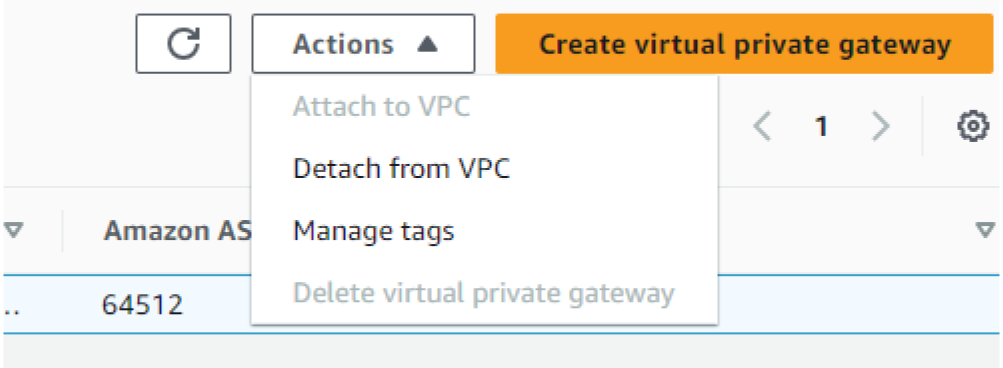
Virtual private gateways (1/1)

Name	Virtual private gateway ID	State	Type	VPC	Amazon ASN
site-site-vpg	vgw-013110bf1bf1376e3	Attached	ipsec.1	vpc-0d8eb4938aff31c20 | site-si...	64512

Initially it is in detached mode

Click on the VPG (site-site-vpg).

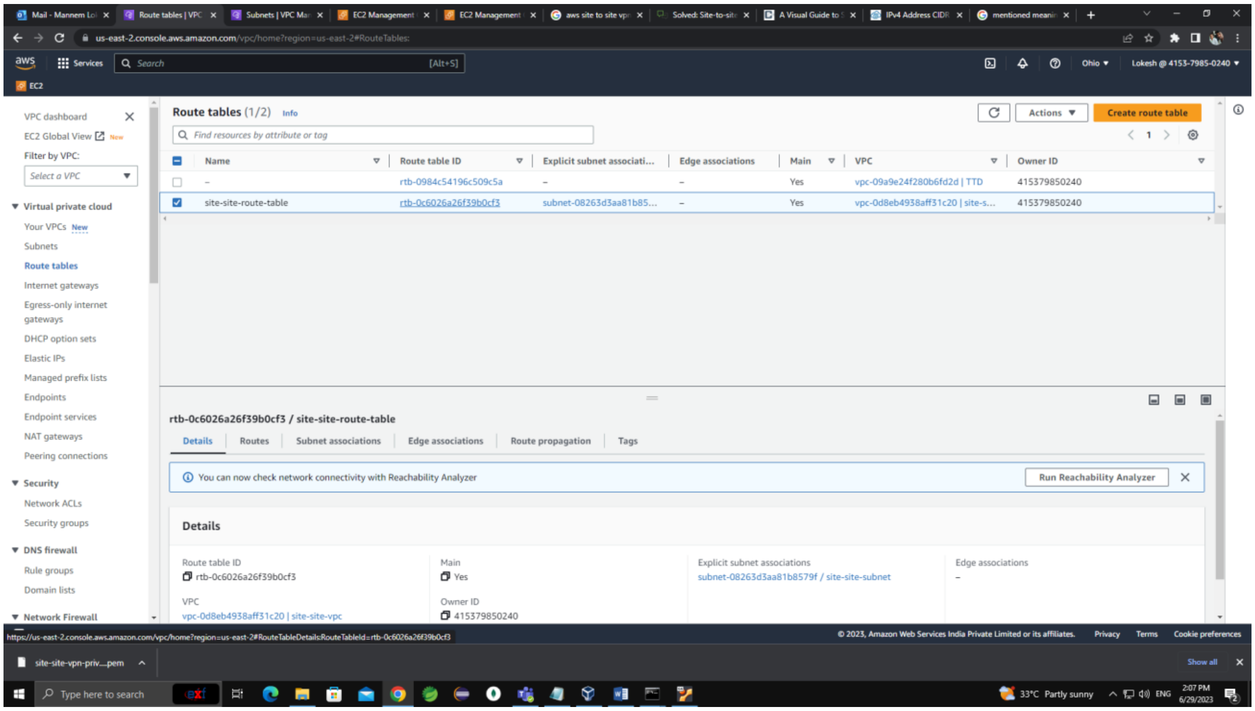
Click on Actions.



Click on Attach to VPC (in my case I had already attached to VPC).

Step 5: Create Customer Gateway and site-to-site connection [follow this page.]

Step 6: Go to Route table and do the configuration mentioned below.


us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#RouteTables:
Create route table
Actions
Run Reachability Analyzer

Route tables (1/2)

☐	Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC	Owner ID
☐	–	rtb-0984c54196c509c5a	–	–	Yes	vpc-09a9e24f280b6fd2d | TTD	415379850240
☑	site-site-route-table	rtb-0c6026a26f39b0cf3	subnet-08263d3aa81b85...	–	Yes	vpc-0d8eb4938aff31c20 | site-s...	415379850240

rtb-0c6026a26f39b0cf3 / site-site-route-table

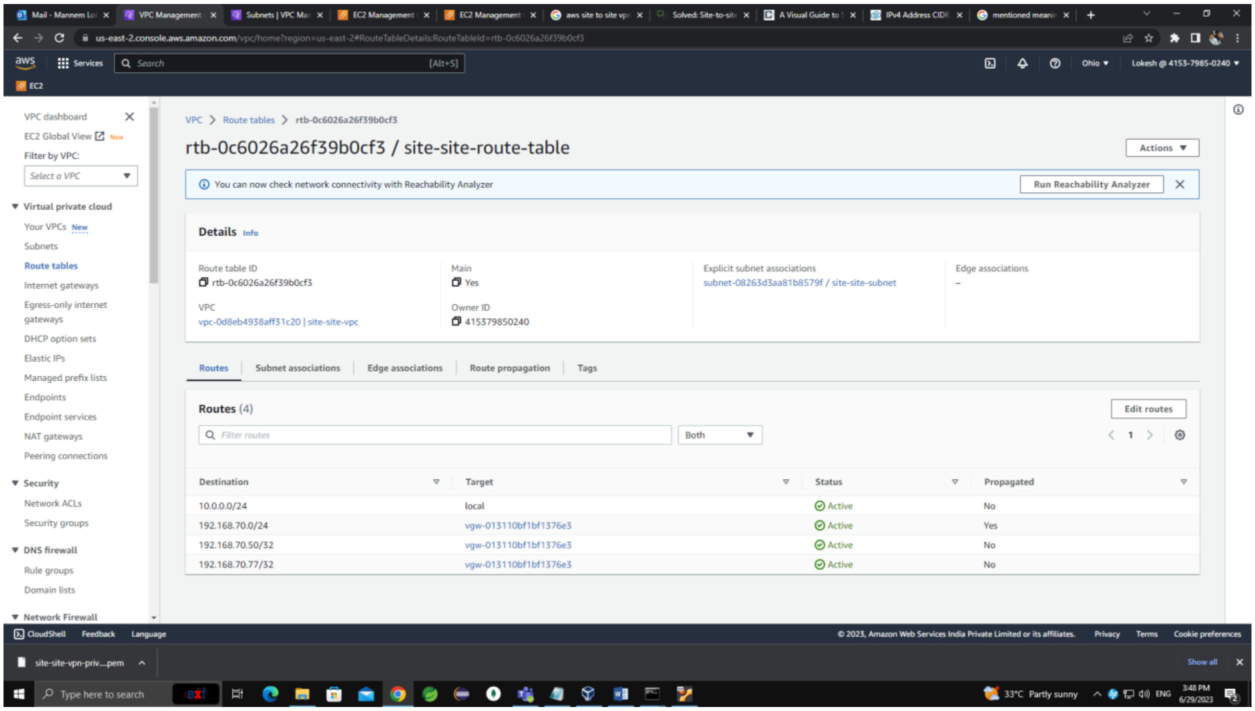
Details | Routes | Subnet associations | Edge associations | Route propagation | Tags

You can now check network connectivity with Reachability Analyzer

Details

Route table ID: rtb-0c6026a26f39b0cf3
Main: Yes
Explicit subnet associations: subnet-08263d3aa81b8579f / site-site-subnet
Edge associations: –
VPC: vpc-0d8eb4938aff31c20 | site-site-vpc
Owner ID: 415379850240

Click on Route table id


us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#RouteTableDetails:RouteTableId=rtb-0c6026a26f39b0cf3
VPC > Route tables > rtb-0c6026a26f39b0cf3
Actions
Run Reachability Analyzer
Edit routes

rtb-0c6026a26f39b0cf3 / site-site-route-table

You can now check network connectivity with Reachability Analyzer

Details

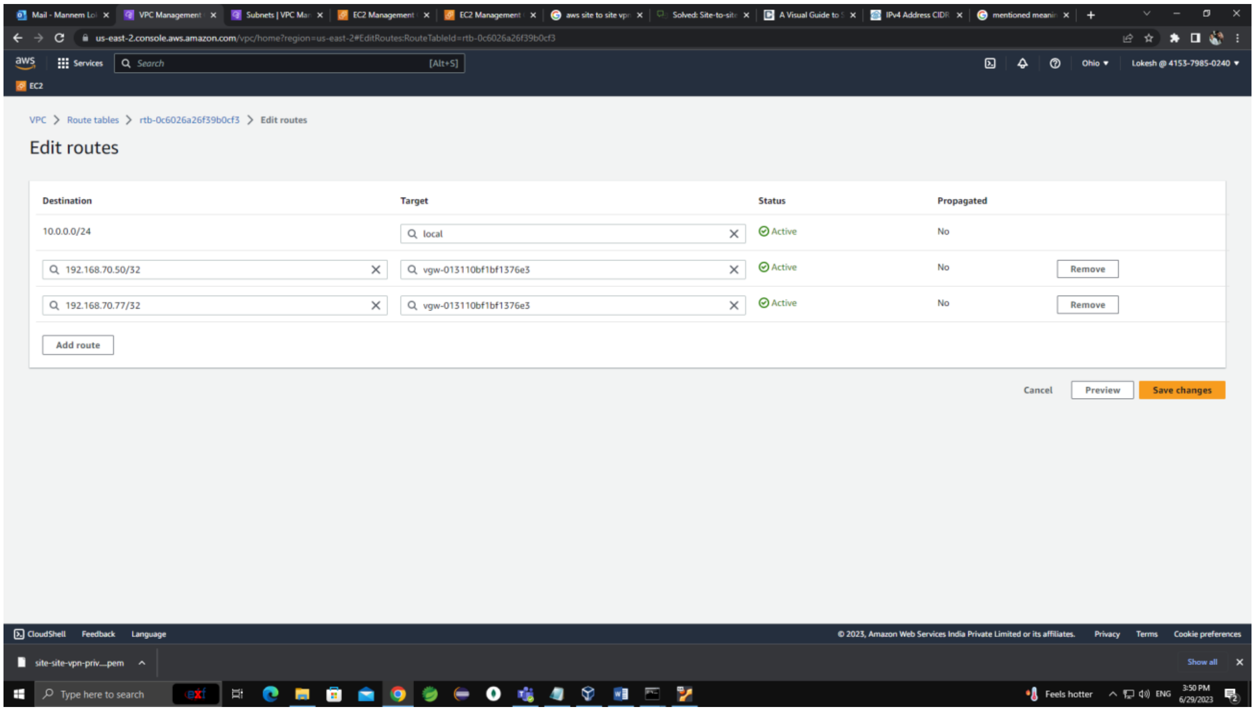
Route table ID: rtb-0c6026a26f39b0cf3
Main: Yes
Explicit subnet associations: subnet-08263d3aa81b8579f / site-site-subnet
Edge associations: –
VPC: vpc-0d8eb4938aff31c20 | site-site-vpc
Owner ID: 415379850240

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (4)

Destination	Target	Status	Propagated
10.0.0.0/24	local	Active	No
192.168.70.0/24	vgw-013110bf1bf1376e3	Active	Yes
192.168.70.50/32	vgw-013110bf1bf1376e3	Active	No
192.168.70.77/32	vgw-013110bf1bf1376e3	Active	No

Click on edit routes



Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/24	local	Active	No	
192.168.70.50/32	vgw-013110bf1bf1376e3	Active	No	Remove
192.168.70.77/32	vgw-013110bf1bf1376e3	Active	No	Remove

Click on Add route

Under destination you have to add IP address of the device in On Premises and Select target as Virtual Private Gateway and select (site-site-VPG).

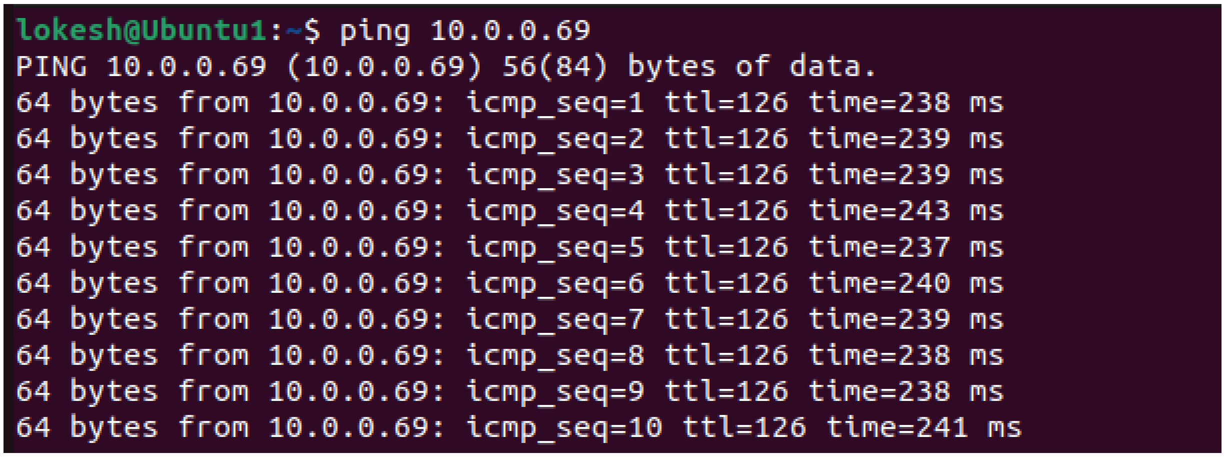
Finally Click on Save changes.

In my case I want to allow 2 systems from on premises so I had added 2 IP address.

Testing

Connecting AWS instance from On Premises

1. Open command prompt or terminal in your PC.
2. Ping the private IP of instance in AWS.
   Example: private IP of instance is 10.0.0.69
   ping 10.0.0.69

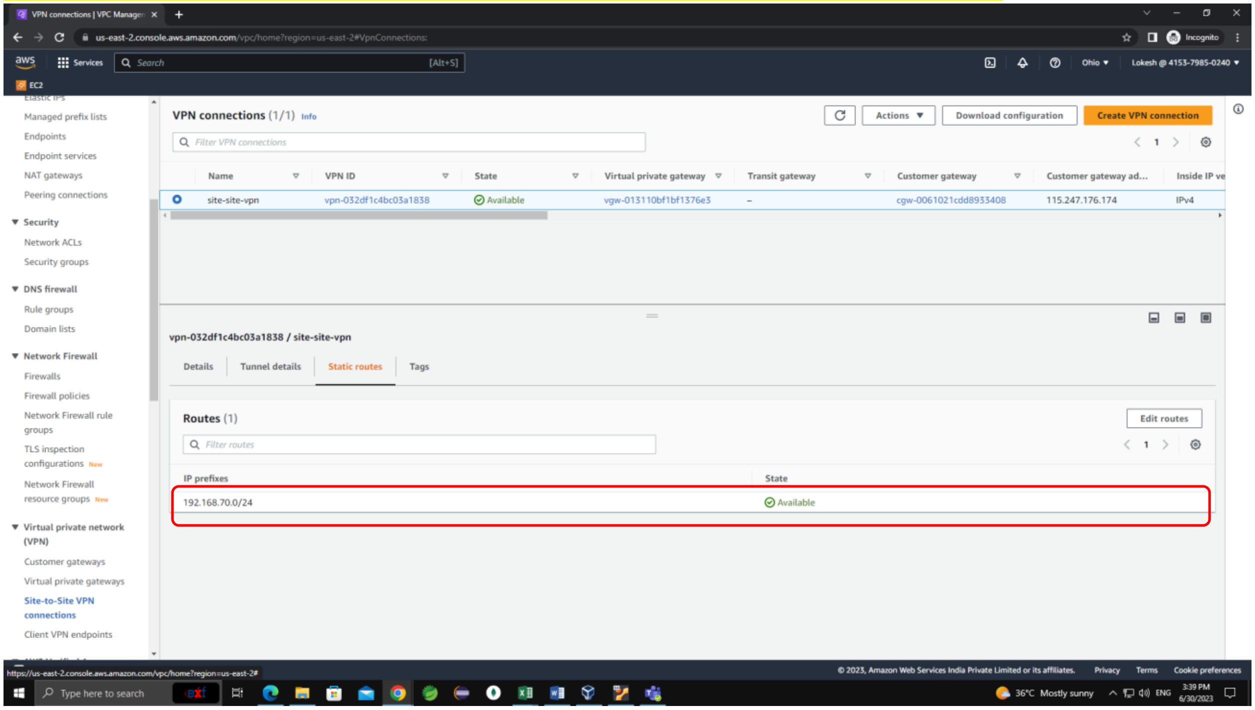


```
lokesh@Ubuntu1:~$ ping 10.0.0.69
PING 10.0.0.69 (10.0.0.69) 56(84) bytes of data.
64 bytes from 10.0.0.69: icmp_seq=1 ttl=126 time=238 ms
64 bytes from 10.0.0.69: icmp_seq=2 ttl=126 time=239 ms
64 bytes from 10.0.0.69: icmp_seq=3 ttl=126 time=239 ms
64 bytes from 10.0.0.69: icmp_seq=4 ttl=126 time=243 ms
64 bytes from 10.0.0.69: icmp_seq=5 ttl=126 time=237 ms
64 bytes from 10.0.0.69: icmp_seq=6 ttl=126 time=240 ms
64 bytes from 10.0.0.69: icmp_seq=7 ttl=126 time=239 ms
64 bytes from 10.0.0.69: icmp_seq=8 ttl=126 time=238 ms
64 bytes from 10.0.0.69: icmp_seq=9 ttl=126 time=238 ms
64 bytes from 10.0.0.69: icmp_seq=10 ttl=126 time=241 ms
```

If you see info like above, you have no problem in the configuration at AWS side.

Note: If you didn't receive messages like above than you have a problem in configuration at AWS side. Please check the configuration by following the given steps.

1. Make sure that IP prefix is allowed in the static routes under Site-to-Site VPN



VPN connections (1/1)

	Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway	Customer gateway ad...	Inside IP ve
●	site-site-vpn	vpn-032df1c4bc03a1838	✓ Available	vgw-013110bf1bf1376e3	–	cgw-0061021cdd8933408	115.247.176.174	IPv4

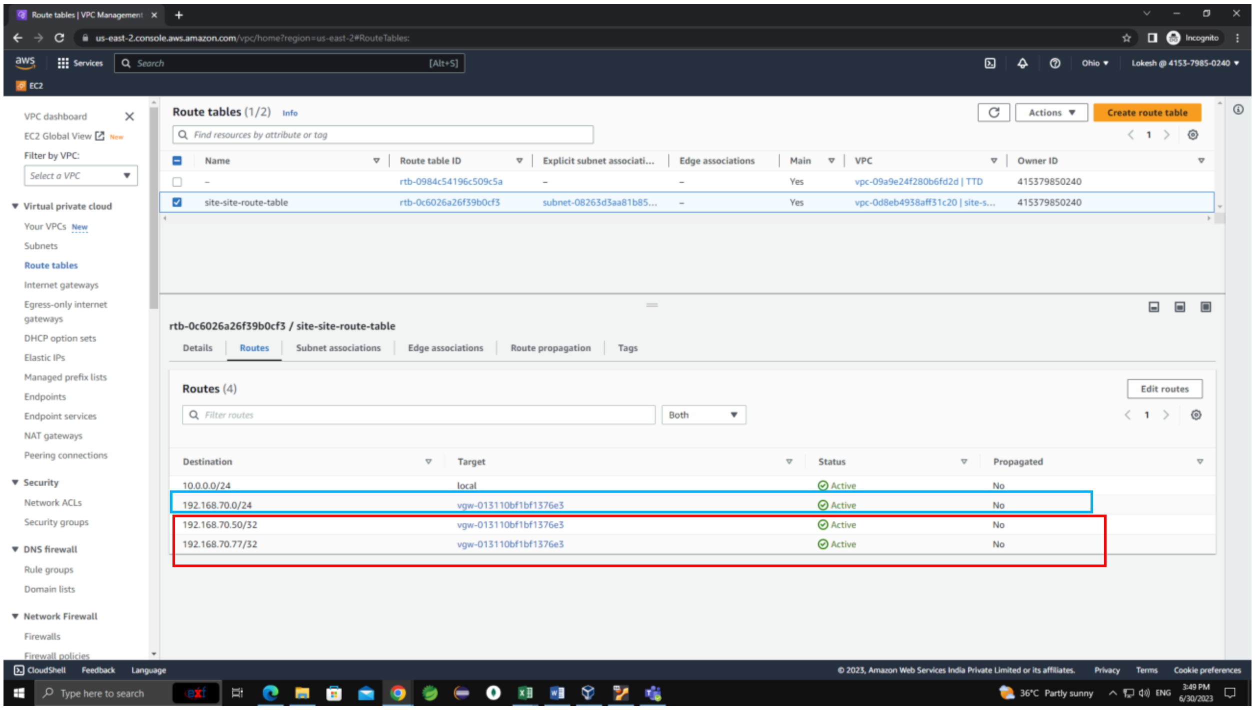
vpn-032df1c4bc03a1838 / site-site-vpn

Routes (1)

IP prefixes	State
192.168.70.0/24	✓ Available

I had allowed IP prefix of my On Premises PC as mentioned in the above (192.168.70.0/24)

2. Make sure that private IP address of your system is allowed in routes under Route table.



Route tables (1/2)

Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC	Owner ID
–	rtb-0984c54196c509c5a	–	–	Yes	vpc-09a9e24f280b6fd2d | TTD	415379850240
site-site-route-table	rtb-0c6026a26f39b0cf3	subnet-08263d3aa81b85...	–	Yes	vpc-0d8eb4938aff31c20 | site-s...	415379850240

rtb-0c6026a26f39b0cf3 / site-site-route-table

Routes (4)

Destination	Target	Status	Propagated
10.0.0.0/24	local	Active	No
192.168.70.0/24	vgw-013110bf1bf1376e3	Active	No
192.168.70.50/32	vgw-013110bf1bf1376e3	Active	No
192.168.70.77/32	vgw-013110bf1bf1376e3	Active	No

Red Color → Private IP address of On Premises PC’s

Or Enable Route Propagation.

I had enabled route propagation. (192.168.70.0/24) so that all the PC’s inside On Premises with that range will communicate to AWS instance.

Blue Color → Private IP address range of On Premises.

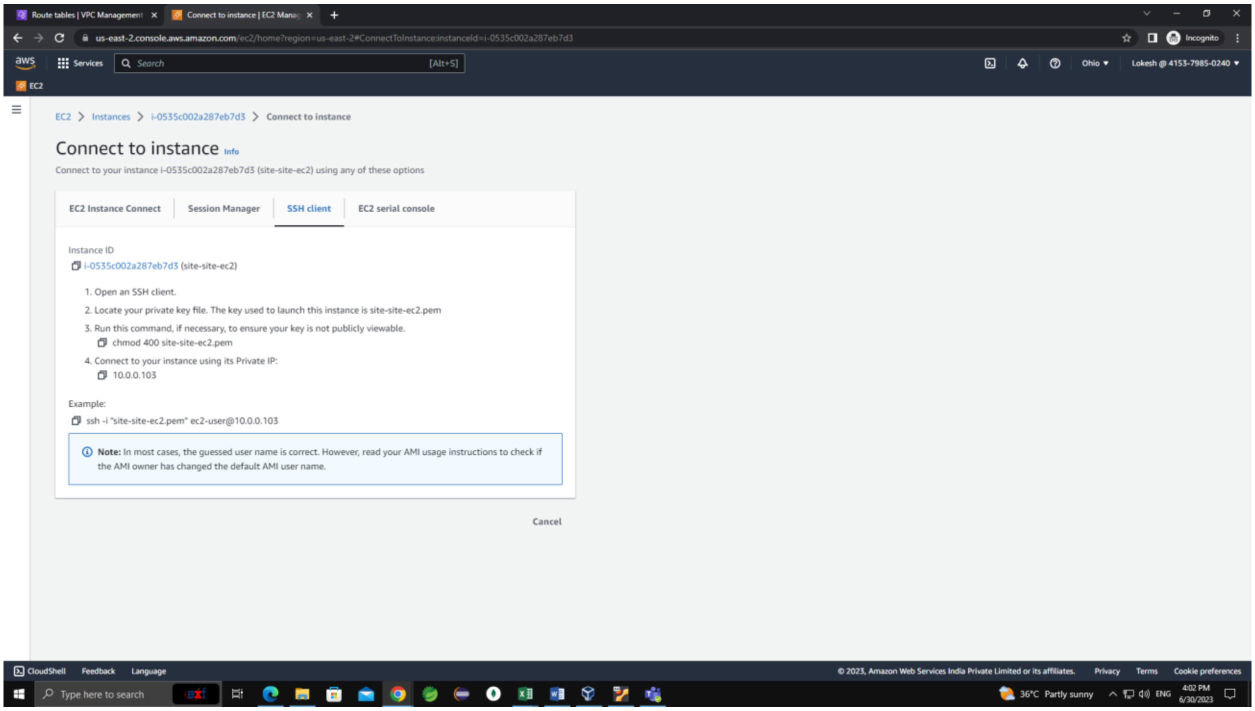
3. All Traffic is allowed under inbound rules at AWS instance.

Trying to Connect instance using ssh from on premises to AWS instance

Open Command Prompt or terminal.

Go to the directory where you are having pem key for the AWS instance.

Now go SSH Client in EC2 instance at AWS side.


Route tables | VPC Management
Connect to instance | EC2 Manag
us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#ConnectToInstance:instanceId=i-0535c002a287eb7d3
aws
Services
Search
[Alt+S]
EC2
EC2 > Instances > i-0535c002a287eb7d3 > Connect to instance

Connect to instance Info

Connect to your instance i-0535c002a287eb7d3 (site-site-ec2) using any of these options

EC2 Instance Connect
Session Manager
SSH client
EC2 serial console

Instance ID

i-0535c002a287eb7d3 (site-site-ec2)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is site-site-ec2.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   chmod 400 site-site-ec2.pem
4. Connect to your instance using its Private IP:
   10.0.0.103

Example:

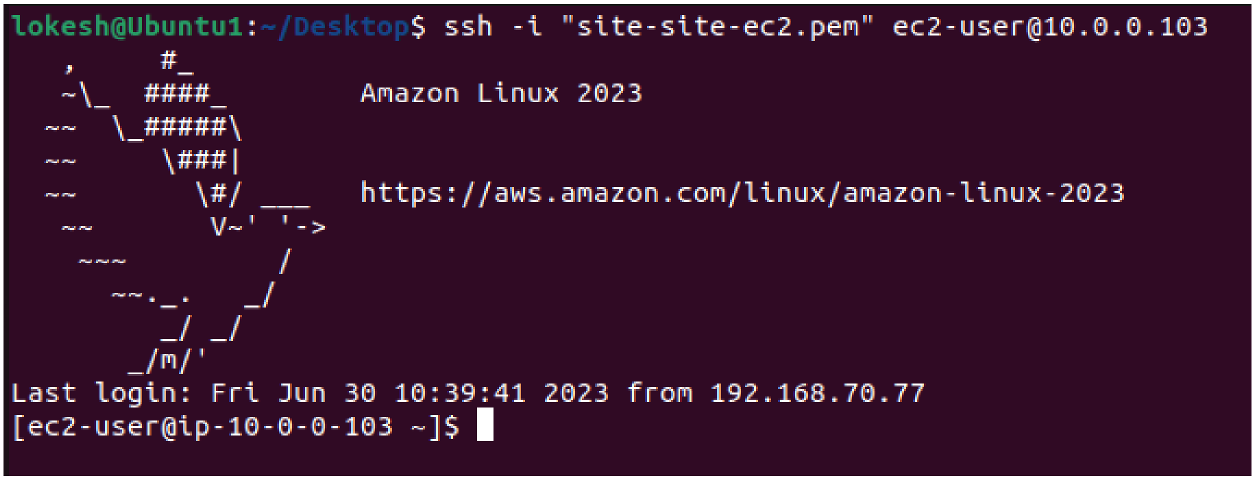
ssh -i "site-site-ec2.pem" ec2-user@10.0.0.103

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Now copy and paste ssh –i “pem_key” ec2-user@Private_IP_Of_AWS_Instance

In my case

ssh -i "site-site-ec2.pem" ec2-user@10.0.0.103



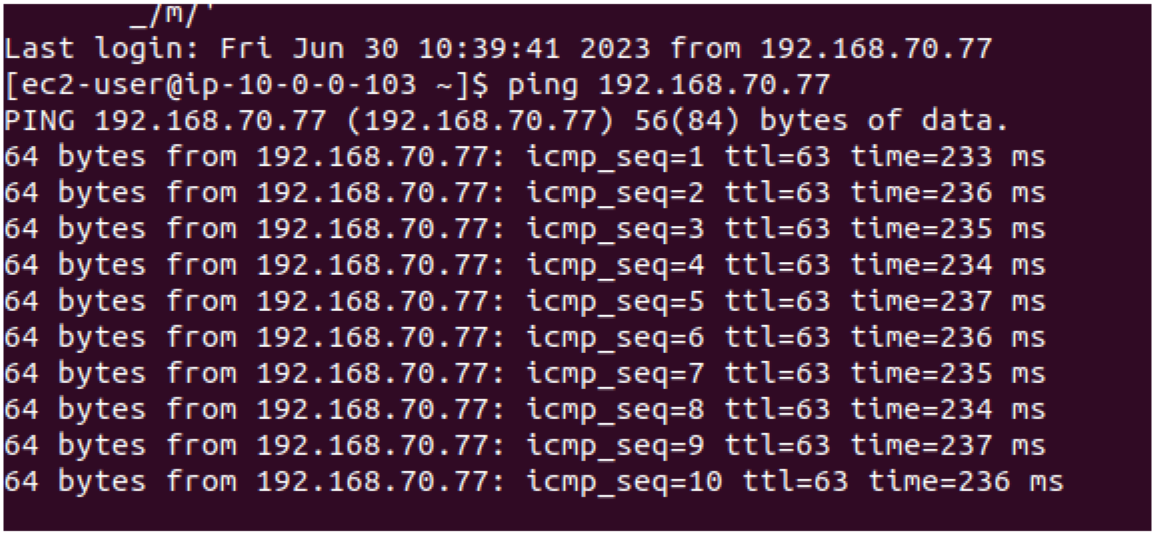
```
lokesh@Ubuntu1:~/Desktop$ ssh -i "site-site-ec2.pem" ec2-user@10.0.0.103
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Jun 30 10:39:41 2023 from 192.168.70.77
[ec2-user@ip-10-0-0-103 ~]$
```

I had successfully connected to the instance from On Premises.

Now I will ping to my On Premises PC (192.168.70.77)

Enter command in the terminal

ping 192.168.70.77



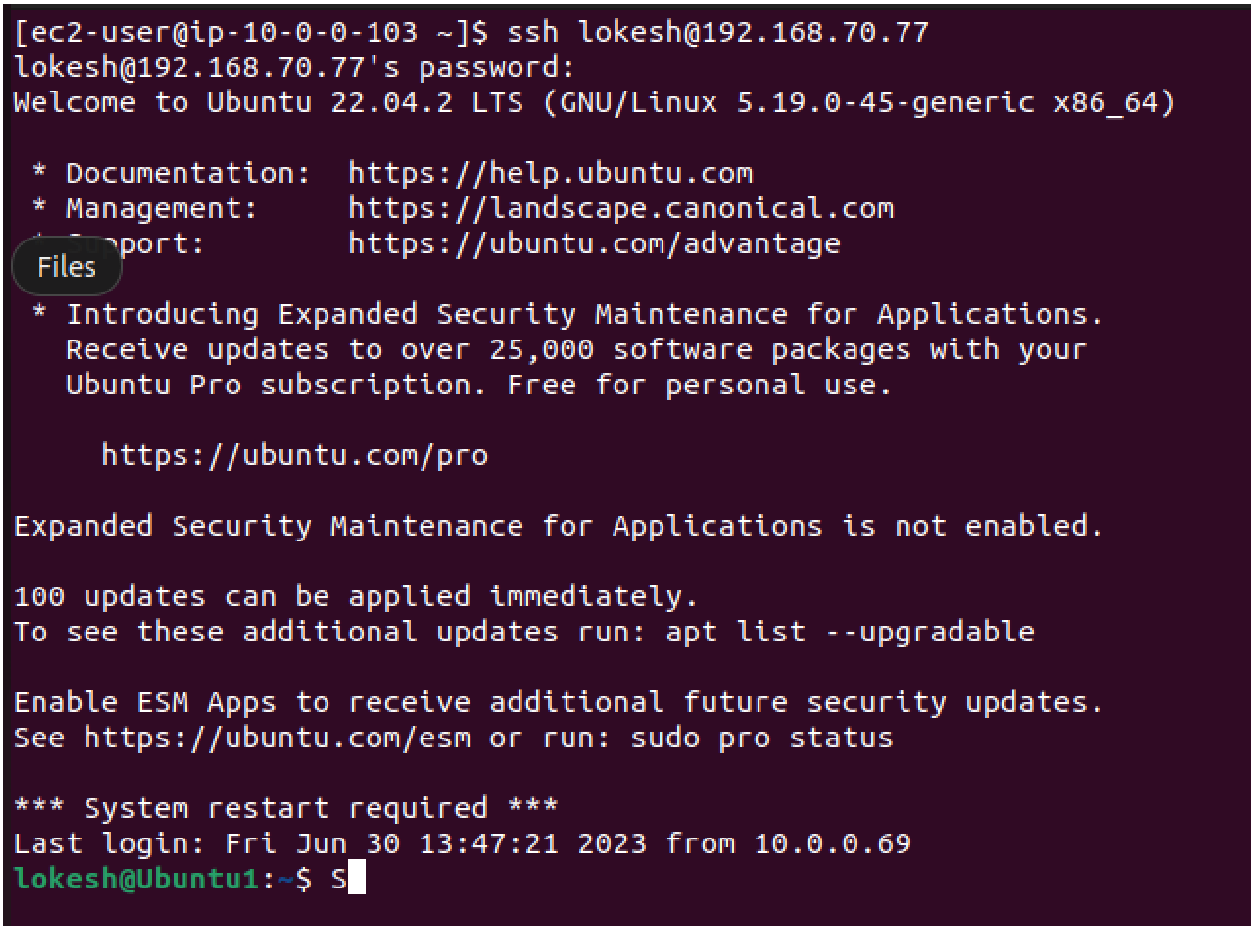
```
       _/m/'
Last login: Fri Jun 30 10:39:41 2023 from 192.168.70.77
[ec2-user@ip-10-0-0-103 ~]$ ping 192.168.70.77
PING 192.168.70.77 (192.168.70.77) 56(84) bytes of data.
64 bytes from 192.168.70.77: icmp_seq=1 ttl=63 time=233 ms
64 bytes from 192.168.70.77: icmp_seq=2 ttl=63 time=236 ms
64 bytes from 192.168.70.77: icmp_seq=3 ttl=63 time=235 ms
64 bytes from 192.168.70.77: icmp_seq=4 ttl=63 time=234 ms
64 bytes from 192.168.70.77: icmp_seq=5 ttl=63 time=237 ms
64 bytes from 192.168.70.77: icmp_seq=6 ttl=63 time=236 ms
64 bytes from 192.168.70.77: icmp_seq=7 ttl=63 time=235 ms
64 bytes from 192.168.70.77: icmp_seq=8 ttl=63 time=234 ms
64 bytes from 192.168.70.77: icmp_seq=9 ttl=63 time=237 ms
64 bytes from 192.168.70.77: icmp_seq=10 ttl=63 time=236 ms
```

Ping is working.

If Ping is not working than, please follow instructions in this video to install ssh in On Premises PC and to allow port 22 to connect.

Now trying to connect On Premises PC from AWS instance.

1. Enter command like below
   ssh user_name@Private_IP_Of_On_Premises_PC
2. If your login for the first time it will ask yes or no. enter yes and hit enter.
3. Enter Password of On Premises PC to Connect.



```
[ec2-user@ip-10-0-0-103 ~]$ ssh lokesh@192.168.70.77
lokesh@192.168.70.77's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

100 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***
Last login: Fri Jun 30 13:47:21 2023 from 10.0.0.69
lokesh@Ubuntu1:~$ S
```

I had Connected to On Premises PC.

If your facing port 22 not allowed issue than, please follow instructions in this video to install ssh and allow port 22.