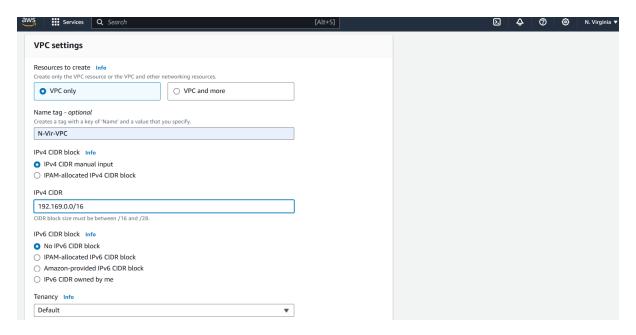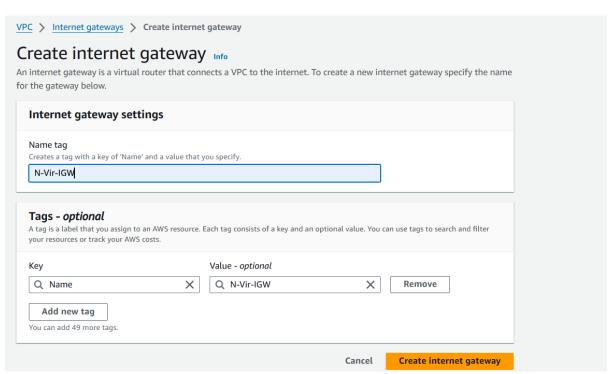# VPC – PEERING

PLEASE CHECK THIS TO CREATE A BOSTION SERVER IN MUMBAI REGION

[AWS/VPC.pdf at main · varshithnathani/AWS (github.com)](github.com)
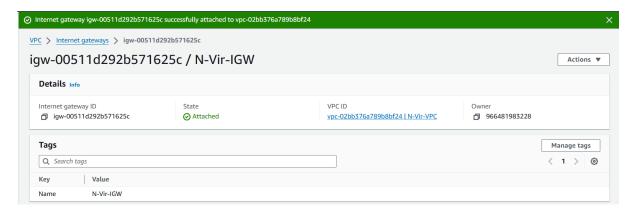
VPC – N. VIRGINIA
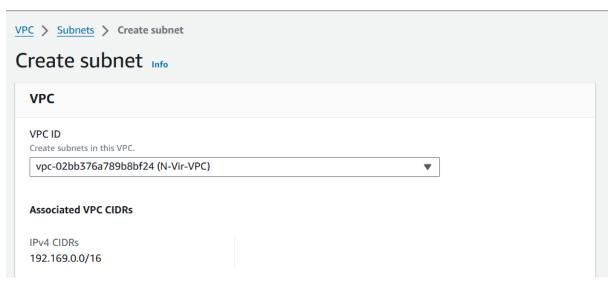
INTERNET GATEWAY

ATTACH VPC TO INTERNET GATEWAY

⊘ Internet gateway igw-00511d292b571625c successfully attached to vpc-02bb376a789b8bf24 ✕

VPC > Internet gateways > igw-00511d292b571625c

igw-00511d292b571625c / N-Vir-IGW

Actions ▼

Details Info

Internet gateway ID	State	VPC ID	Owner
🗐 igw-00511d292b571625c	⊘ Attached	vpc-02bb376a789b8bf24 | N-Vir-VPC	🗐 966481983228

Tags

Manage tags

🔍 Search tags

⟨ 1 ⟩ ⚙

Key	Value
Name	N-Vir-IGW

CREATING SUBNETS

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

vpc-02bb376a789b8bf24 (N-Vir-VPC) ▼

Associated VPC CIDRs

IPv4 CIDRs
192.169.0.0/16

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

PUBLIC-SUBNET-NV

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.

US East (N. Virginia) / us-east-1a ▼

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

192.169.0.0/16 ▼

IPv4 subnet CIDR block

192.169.1.0/24   256 IPs

⟨ ⟩ ∧ ∨

Subnet name

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

PRIVATE-SUBNET-NV

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.

US East (N. Virginia) / us-east-1b ▼

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

192.169.0.0/16 ▼

IPv4 subnet CIDR block

192.169.2.0/24   256 IPs

< > ^ ∨

▼ Tags - *optional*

CREATING NAT GATEWAY

⊘ Elastic IP address 98.80.84.222 (eipalloc-0448ced6bf13054dd) allocated.

VPC > NAT gateways > Create NAT gateway

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - *optional*

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

NAT-GW-NV

The name can be up to 256 characters long.

Subnet

Select a subnet in which to create the NAT gateway.

subnet-011ddb39db3a24f41 (PUBLIC-SUBNET-NV) ▼

Connectivity type

Select a connectivity type for the NAT gateway.

🔘 Public
⚪ Private

Elastic IP allocation ID Info

Assign an Elastic IP address to the NAT gateway.

eipalloc-0448ced6bf13054dd ▼   **Allocate Elastic IP**

CREATING ROUTE TABLE

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.

```
PUBLIC-RT-NV
```

VPC
The VPC to use for this route table.

```
vpc-02bb376a789b8bf24 (N-Vir-VPC)                          ▼
```

Edit routes

Destination	Target	Status	Propagated	
192.169.0.0/16	local ▼	⊘ Active	No	
	🔍 local ✕			
🔍 0.0.0.0/0 ✕	Internet Gateway ▼	–	No	Remove
	🔍 igw-00511d292b571625d ✕			

Add route

Cancel   Preview   **Save changes**

Edit subnet associations
Change which subnets are associated with this route table.

Available subnets (1/2)

🔍 Filter subnet associations   〈 1 〉 ⚙

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	PUBLIC-SUBNET-NV	subnet-011ddb39db3a24f41	192.169.1.0/24	–	Main (rtb-02580dfb0135eeb20)
☐	PRIVATE-SUBNET-NV	subnet-0457b62500e15abba	192.169.2.0/24	–	Main (rtb-02580dfb0135eeb20)

Selected subnets

subnet-011ddb39db3a24f41 / PUBLIC-SUBNET-NV ✕

Cancel   **Save associations**

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*
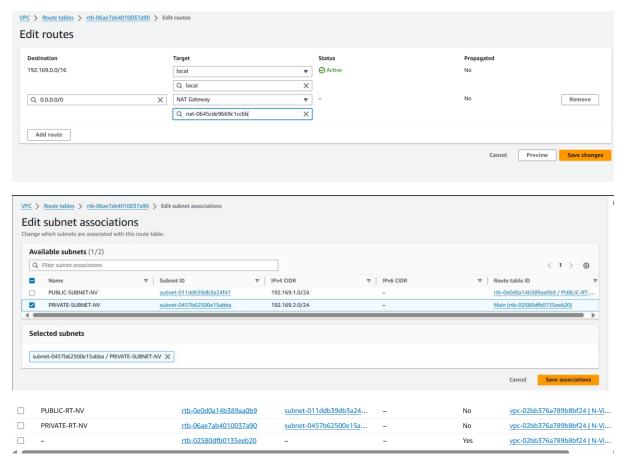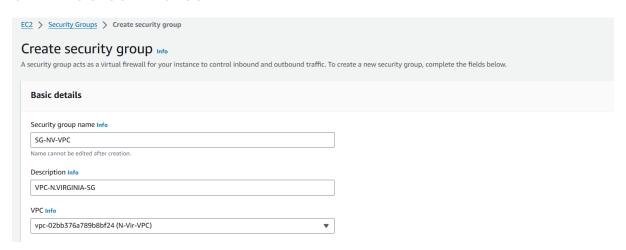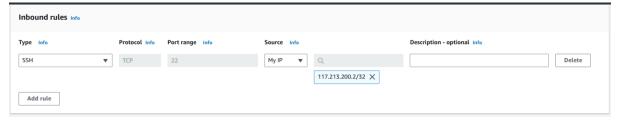Create a tag with a key of 'Name' and a value that you specify.

```
PRIVATE-RT-NV
```

VPC
The VPC to use for this route table.

```
vpc-02bb376a789b8bf24 (N-Vir-VPC)                          ▼
```

Edit routes

Destination	Target	Status	Propagated	
192.169.0.0/16	local ▼	⊘ Active	No	
	🔍 local ✕			
🔍 0.0.0.0/0 ✕	NAT Gateway ▼	–	No	Remove
	🔍 nat-0645cde9669c1cc6b ✕			

Add route

Cancel   Preview   **Save changes**

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

🔍 Filter subnet associations

‹ 1 › ⚙

	Name ▽	Subnet ID ▽	IPv4 CIDR ▽	IPv6 CIDR ▽	Route table ID ▽
☐	PUBLIC-SUBNET-NV	subnet-011ddb39db3a24f41	192.169.1.0/24	–	rtb-0e0d0a14b389aa0b9 / PUBLIC-RT-...
☑	PRIVATE-SUBNET-NV	subnet-0457b62500e15abba	192.169.2.0/24	–	Main (rtb-02580dfb0135eeb20)

Selected subnets

subnet-0457b62500e15abba / PRIVATE-SUBNET-NV ✕

Cancel   **Save associations**

	PUBLIC-RT-NV	rtb-0e0d0a14b389aa0b9	subnet-011ddb39db3a24...	–	No	vpc-02bb376a789b8bf24 | N-Vi...
☐	PRIVATE-RT-NV	rtb-06ae7ab4010037a90	subnet-0457b62500e15a...	–	No	vpc-02bb376a789b8bf24 | N-Vi...
☐	–	rtb-02580dfb0135eeb20	–	–	Yes	vpc-02bb376a789b8bf24 | N-Vi...

CREATING SECURITY GROUP

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

SG-NV-VPC

Name cannot be edited after creation.

Description Info

VPC-N.VIRGINIA-SG

VPC Info

vpc-02bb376a789b8bf24 (N-Vir-VPC) ▼

Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
SSH ▼	TCP	22	My IP ▼	🔍		Delete
				117.213.200.2/32 ✕		

Add rule

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0799b8716217f8bea	SSH ▼	TCP	22	Custom ▼	🔍		Delete
					117.213.200.2/32 ✕		
–	All traffic ▼	All	All	Custom ▼	🔍 sg-05f9feedfacae7979 ✕		Delete
					sg-05f9feedfacae7979 ✕		

Add rule

CREATING PRIVATE SUBNET IN N.VIRGINIA

EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

PRIVATE-NV

Add additional tags

Amazon Machine Image (AMI)

Red Hat Enterprise Linux 9 (HVM), SSD Volume Type   Free tier eligible
ami-0583d8c7a9c35822c (64-bit (x86)) / ami-07472131ec292b5da (64-bit (Arm))   ▼
Virtualization: hvm   ENA enabled: true   Root device type: ebs

Description

Red Hat Enterprise Linux version 9 (HVM), EBS General Purpose (SSD) Volume Type

Architecture

64-bit (x86) ▼

AMI ID

ami-0583d8c7a9c35822c   Verified provider

VPC - *required* Info

```
vpc-02bb376a789b8bf24 (N-Vir-VPC)                    ▼    ⟳
192.169.0.0/16
```

Subnet Info

```
subnet-0457b62500e15abba              PRIVATE-SUBNET-NV
VPC: vpc-02bb376a789b8bf24    Owner: 966481983228              ▼    ⟳   Create new subnet ⤢
Availability Zone: us-east-1b   Zone type: Availability Zone
IP addresses available: 251    CIDR: 192.169.2.0/24
```

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
```

Common security groups Info

```
Select security groups                               ▼
```

```
SG-NV-VPC   sg-05f9feedfacae7979  ✕          ⟳   Compare security
VPC: vpc-02bb376a789b8bf24                          group rules
```

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▶ **Advanced network configuration**

CONNECTING FROM BASTION[MUMBAI] TO PRIVATE SERVER[MUMBAI]

```
ec2-user@ip-192-168-2-146:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[ec2-user@ip-192-168-1-189 ~]$ sudo -s
[root@ip-192-168-1-189 ec2-user]# vi LearnAWS-1.pem
[root@ip-192-168-1-189 ec2-user]# ls
LearnAWS-1.pem
[root@ip-192-168-1-189 ec2-user]# ssh -i "LearnAWS-1.pem" ec2-user@192.168.2.146
The authenticity of host '192.168.2.146 (192.168.2.146)' can't be established.
ED25519 key fingerprint is SHA256:KczngcD73u2zXh9mR2nvNVKjVDTK/tSygPkeabnrwSU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.146' (ED25519) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@          WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'LearnAWS-1.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "LearnAWS-1.pem": bad permissions
ec2-user@192.168.2.146: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[root@ip-192-168-1-189 ec2-user]# chmod 400 LearnAWS-1.pem
[root@ip-192-168-1-189 ec2-user]# ssh -i "LearnAWS-1.pem" ec2-user@192.168.2.146
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[ec2-user@ip-192-168-2-146 ~]$
```
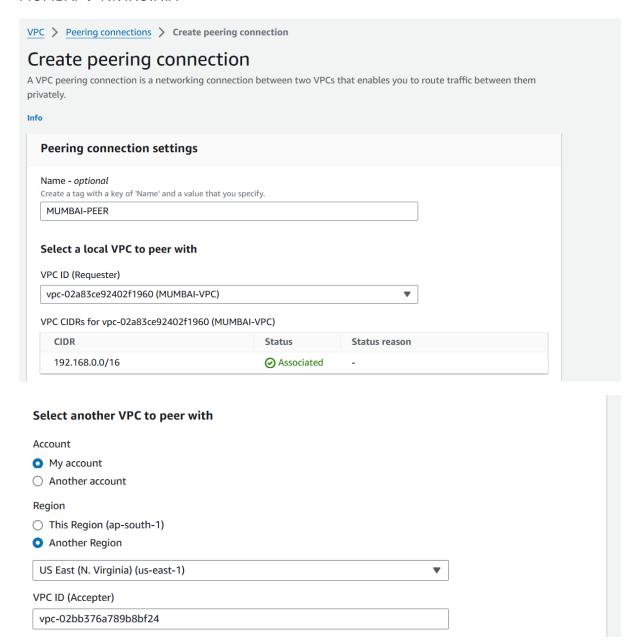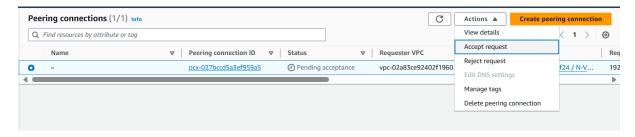
CONNECTING FROM PRIVATE SERVER[MUMBAI] TO PRIVATE SERVER [N.VIRGINIA]

FOR THIS WE NEED TO ESTABLISH THE PEERING CONNECTION IN VPC
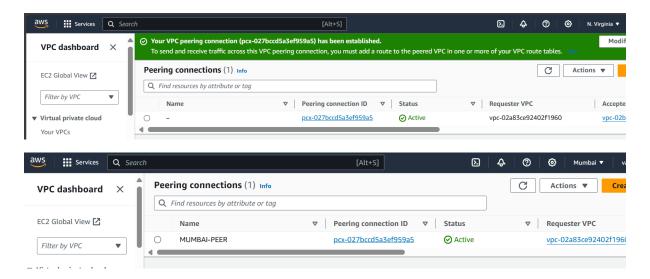
MUMBAI → N.VIRGINIA
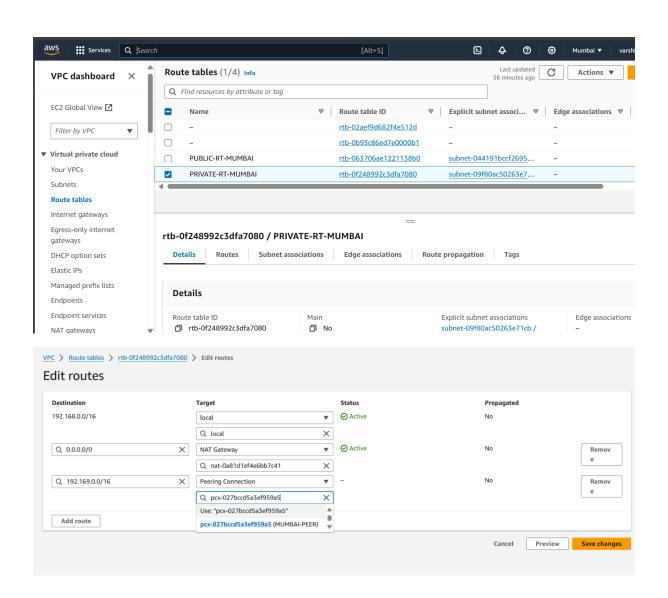
[IN ACCEPTOR PASTE THE N.VIRGINA VPC ID]
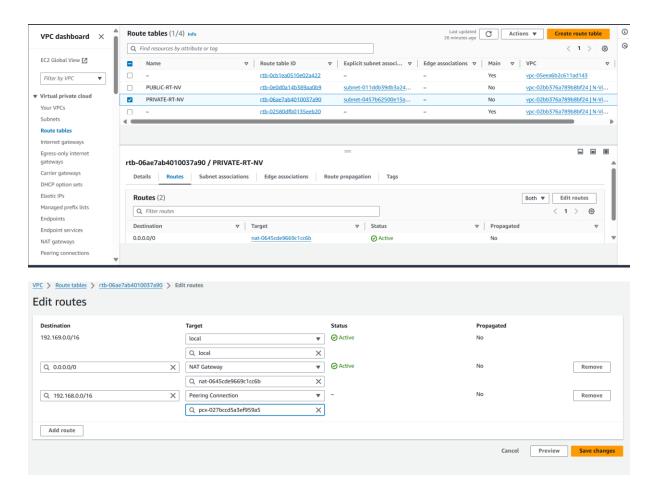
NOW GO TO N.VIRGINIA PEERING CONNECTION AND ACCEPT THE CONNECTION
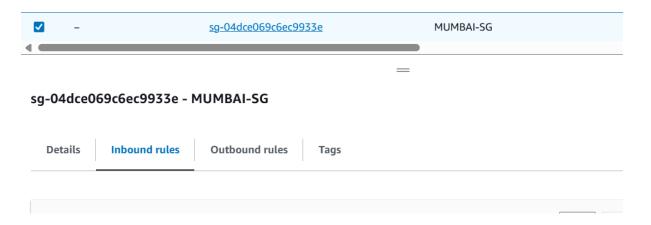
NOW I NEED TO ADD THE IP ADDRESS TO THE PRIVATE-SUBNET-MUMBAI ROUTE

WHICH WILL GIVE THE ACCESS FOR ACCESSING THE N.VIRGINIA PRIVATE & VICE-VERSA
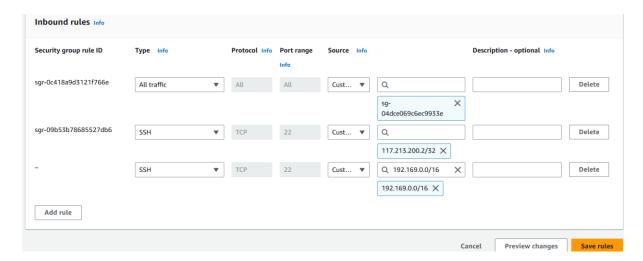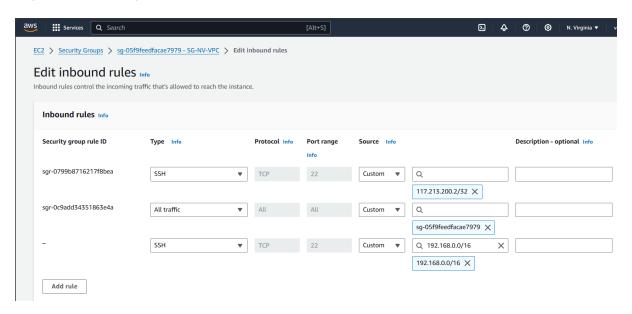
WE HAVE TO CHANGE THE SSH IP ALSO BECAUSE WE SELECTED MY-IP IN SECURITY GROUP
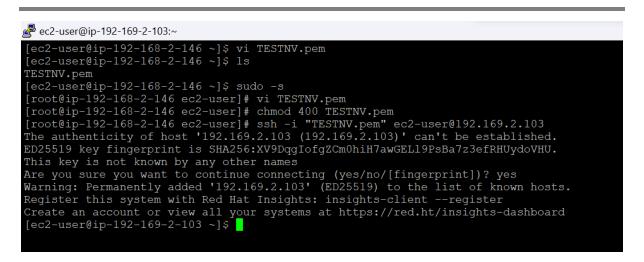
SO MODIFY THE SG IN MUMBAI AND ADD INBOUND RULES → SSH → 192.169.0.0/16

IN N,VIRGINIA MODIFY SG→ SSH→ 192.168.0.0/16

sg-04dce069c6ec9933e - MUMBAI-SG

| Details | **Inbound rules** | Outbound rules | Tags |

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0c418a9d3121f766e	All traffic ▼	All	All	Cust... ▼	🔍		Delete
					sg-04dce069c6ec9933e ✕		
sgr-09b53b78685527db6	SSH ▼	TCP	22	Cust... ▼	🔍		Delete
					117.213.200.2/32 ✕		
–	SSH ▼	TCP	22	Cust... ▼	🔍 192.169.0.0/16 ✕		Delete
					192.169.0.0/16 ✕		

Add rule

Cancel   Preview changes   Save rules

MODIFY IN N.VIRGINIA

aws   ⠿ Services   🔍 Search   [Alt+S]   ▣ ⌂ ⑦ ⚙   N. Virginia ▼

EC2 > Security Groups > sg-05f9feedfacae7979 - SG-NV-VPC > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info
sgr-0799b8716217f8bea	SSH ▼	TCP	22	Custom ▼	🔍	
					117.213.200.2/32 ✕	
sgr-0c9add34351863e4a	All traffic ▼	All	All	Custom ▼	🔍	
					sg-05f9feedfacae7979 ✕	
–	SSH ▼	TCP	22	Custom ▼	🔍 192.168.0.0/16 ✕	
					192.168.0.0/16 ✕	

Add rule

🖥 ec2-user@ip-192-169-2-103:~

```
[ec2-user@ip-192-168-2-146 ~]$ vi TESTNV.pem
[ec2-user@ip-192-168-2-146 ~]$ ls
TESTNV.pem
[ec2-user@ip-192-168-2-146 ~]$ sudo -s
[root@ip-192-168-2-146 ec2-user]# vi TESTNV.pem
[root@ip-192-168-2-146 ec2-user]# chmod 400 TESTNV.pem
[root@ip-192-168-2-146 ec2-user]# ssh -i "TESTNV.pem" ec2-user@192.169.2.103
The authenticity of host '192.169.2.103 (192.169.2.103)' can't be established.
ED25519 key fingerprint is SHA256:XV9DqgIofgZCm0hiH7awGEL19PsBa7z3efRHUydoVHU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.169.2.103' (ED25519) to the list of known hosts.
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[ec2-user@ip-192-169-2-103 ~]$ █
```

[SUCCESSFULLY PEERING COMPLETED]

DISMANTLE

Delete NAT gateway ✕

Will be deleted
The following NAT gateway will be deleted permanently and can't be recovered later.

Name	NAT gateway ID	State
NAT-GW-NV	nat-0645cde9669c1cc6b	⊘ Available

To confirm deletion, type *delete* in the field:

```
DELETE
```

Cancel **Delete**

Requester Region
Mumbai (ap-south-1)

Accepter Region
N. Virginia (us-east-1)

Requester owner ID
⧉ 966481983228
(This account)

Accepter owner ID
⧉ 966481983228
(This account)

Routes targeting this peering connection

Route table ID	Destination
rtb-0f248992c3dfa7080	192.169.0.0/16

Route table entries
Select whether or not to delete the entries that target this peering connection from the route tables.

🔘 Delete related route table entries
⚪ Do not delete route table entries

To confirm deletion, type *delete* in the field:

```
DELETE
```

Cancel **Delete**

[Alt+S]   ⌘ ⟁ ⑦ ⚙   N. Virginia ▼

Peering connections (1) Info

⟳   Actions ▼

🔍 Find resources by attribute or tag

	Name	▽	Peering connection ID	▽	Status	▽	Requester VPC		Accepte
⚪	–		pcx-027bccd5a3ef959a5		⊗ Deleted		vpc-02a83ce92402f1960		vpc-02b

Name	VPC ID	State
⊡ MUMBAI-VPC	⊡ vpc-02a83ce92402f1960	⊘ Available

⊘ Will also be deleted

The following 6 resources will also be deleted permanently and cannot be recovered later:

🔍 Find entries   ‹ **1** 2 ›

Name ▽	Resource ID ▽	State
MUMBAI-IGW	igw-0693580bbec8b626f	⊘ Availab
PUBLIC-RT-MUMBAI	rtb-063706ae1221138b0	-
PRIVATE-RT-MUMBAI	rtb-0f248992c3dfa7080	-
–	sg-04dce069c6ec9933e	-
PRIVATE-SUBNET	subnet-09f80ac50263e71cb	⊘ Availab

To confirm deletion, type *delete* in the field:

DELETE

Cancel   **Delete**

Delete VPC   ✕

⊘ Will be deleted

This VPC will be deleted permanently and cannot be recovered later:

Name	VPC ID	State
⊡ N-Vir-VPC	⊡ vpc-02bb376a789b8bf24	⊘ Available

⊘ Will also be deleted

The following 6 resources will also be deleted permanently and cannot be recovered later:

🔍 Find entries   ‹ **1** 2 ›

Name ▽	Resource ID ▽	State
N-Vir-IGW	igw-00511d292b571625c	⊘ Availab
PUBLIC-RT-NV	rtb-0e0d0a14b389aa0b9	-
PRIVATE-RT-NV	rtb-06ae7ab4010037a90	-
–	sg-05f9feedfacae7979	-
PUBLIC-SUBNET-NV	subnet-011ddb39db3a24f41	⊘ Availab

To confirm deletion, type *delete* in the field:

DELETE

Cancel   **Delete**

ses (1/1) Actions ▼ Allo

attribute or tag

Release Elastic IP addresses

Will be released

If you release the following Elastic IP addresses, they will no longer be allocated to your account and you can no longer associate them with your resources.

Name	IPv4 address	Allocation ID	Addre
–	3.109.67.72	eipalloc-00976f0e6d722028f	Public

Cancel Releas

Release Elastic IP addresses ✕

Will be released

If you release the following Elastic IP addresses, they will no longer be allocated to your account and you can no longer associate them with your resources.

Name	IPv4 address	Allocation ID	Address ty
–	98.80.84.222	eipalloc-0448ced6bf13054dd	Public

Cancel **Release**