What is a Network?

A computer network is a collection of computing devices that are logically connected to communicate and share resources. For example, a network is like a national highway system in India that connects various cities, towns and states. It forms a transportation network that makes the movement of travellers easier and more efficient.

Networking in the Cloud:

Networking in the cloud involves the use of virtualized infrastructure and services to create secure, scalable, and flexible communication pathways between cloud resources and between cloud-based and on-premises systems. Here we will compare the traditional on-premises infrastructure to AWS Cloud Services.

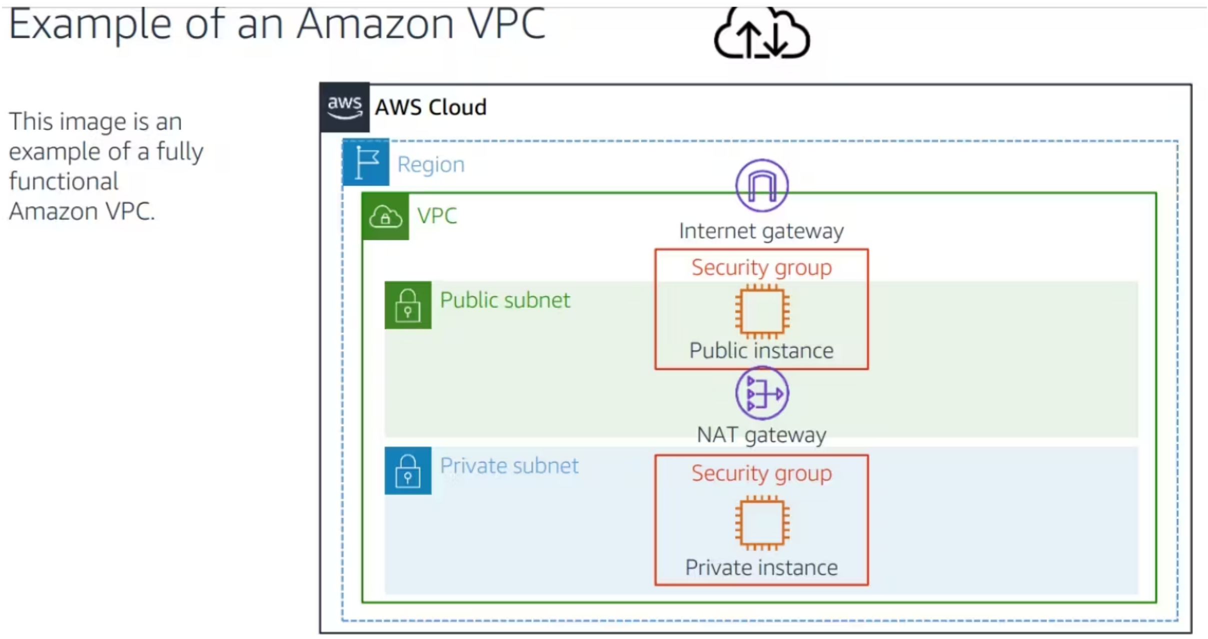
Traditional Topology	AWS Services

Data Centers	**Amazon VPC**
Routers	Route Tables
Switches(Subnets)	Subnets
Firewall	Security Groups and Network Access Control List(Nacl)
Servers	EC2

What is Amazon VPC:

Amazon VPC allows you to create a virtual private network in the cloud that uses the same concepts as on-premises network, with the benefits of using the scalable infrastructure of AWS. It is more cost-effective than maintaining equipment in a company data centre; you pay for only the resources that you use. It is designed so that companies can migrate and use AWS Cloud services easily. It’s secure, scalable, and reliable.

With an Amazon VPC, you can launch your AWS resources in a virtual network that you define. VPC belongs to a single Region and spans several Availability Zones(AZ).



Example of an Amazon VPC

This image is an example of a fully functional Amazon VPC.

Important concepts within the VPC:

• CIDR block: A private range should be given from /16–/28. To determine the private IP address range allocation, you can use RFC 1918: https://datatracker.ietf.org/doc/html/rfc1918.

• Subnets: Allocate a range of IP addresses within your VPC. These Subnets are either public or private subnets. Public Subnet has a route table with the internet gateway associated with it. For example, assume Subnet as a floor in a building , divide the building into floors, each representing a subnet. Each floor (subnet) contains a specific group of offices (devices) that need to communicate with each other frequently.

• Route table: Rules (also known as routes) that the VPC uses to route traffic. Targets are Internet Gateway, NAT Gateway, VPC Endpoints. The routes are specific routes that goes to Targets. for eg. the route for Internet Gateway is 0.0.0.0/0 because it is routing to internet and target will be IGW-xxxxxxxx.

• Internet gateway: Attaches to your VPC and permits communication from your VPC to the internet. This service must be created and attached to the VPC and should be added to the route table of Public Subnet in order to reach the internet

• VPC endpoint: A private connection between AWS services without the need of internet.

Hands-On Part 1:

1. Creating VPC
2. Creating Subnets
3. Creating Network Access Control List(NACL)

Let's create a VPC :
1. Navigate Your VPC tab in the VPC section of the console and click the Create VPC button.

1. Enter `VPC A` as the Name tag

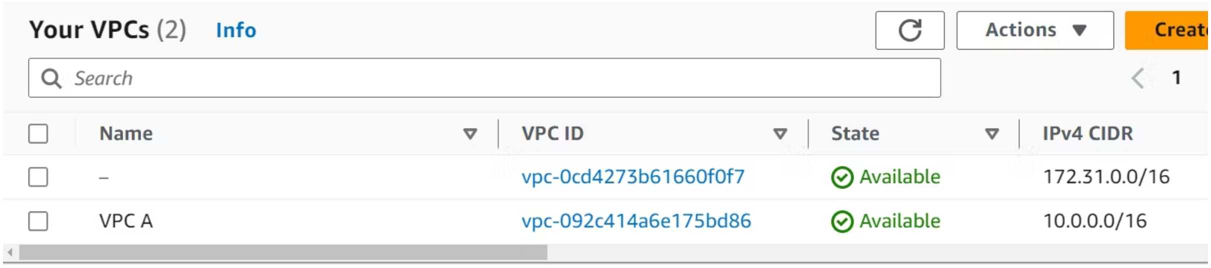
2.1 Specify `10.0.0.0/16` as IPv4 CIDR block.

2.2 Do not enable IPv6.

2.3 Leave `Default` selected as Tenancy.

2.4 Accept proposed Tags

2.4 Click Create VPC

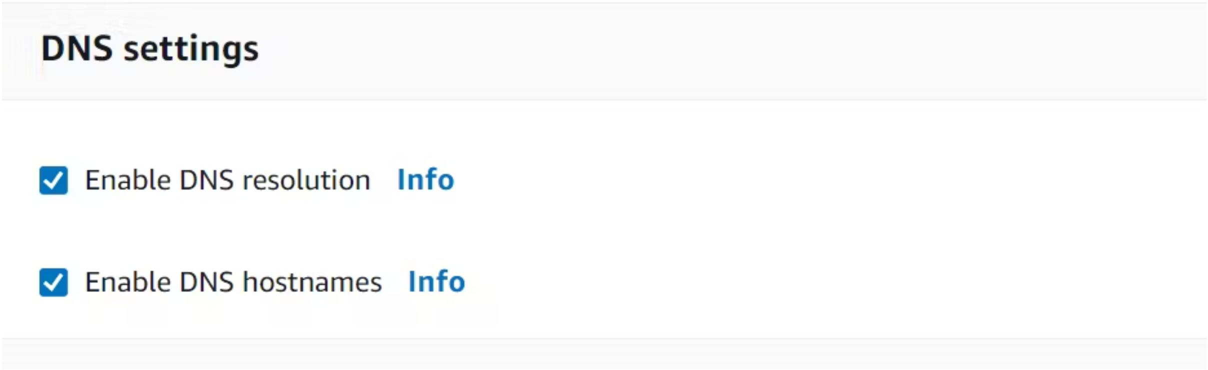


Your VPCs (2) Info

□	Name	VPC ID	State	IPv4 CIDR
□	–	vpc-0cd4273b61660f0f7	✓ Available	172.31.0.0/16
□	VPC A	vpc-092c414a6e175bd86	✓ Available	10.0.0.0/16

Select the VPC A and then click on Actions and select Edit VPC settings from the dropdown

3.1 Check the box to enable DNS hostnames and select Save.



DNS settings

☑ Enable DNS resolution Info

☑ Enable DNS hostnames Info

Congratulations, your first VPC is now built

** When you create a VPC, you must specify the IPv4 address range by choosing a CIDR block, such as 10.0.0.0/16. • An Amazon VPC address range could be as large as /16 (65,536 addresses) or as small as /28 (16 addresses). • Private IP ranges should be used according to RFC 1918.

Hands-On of Subnets:

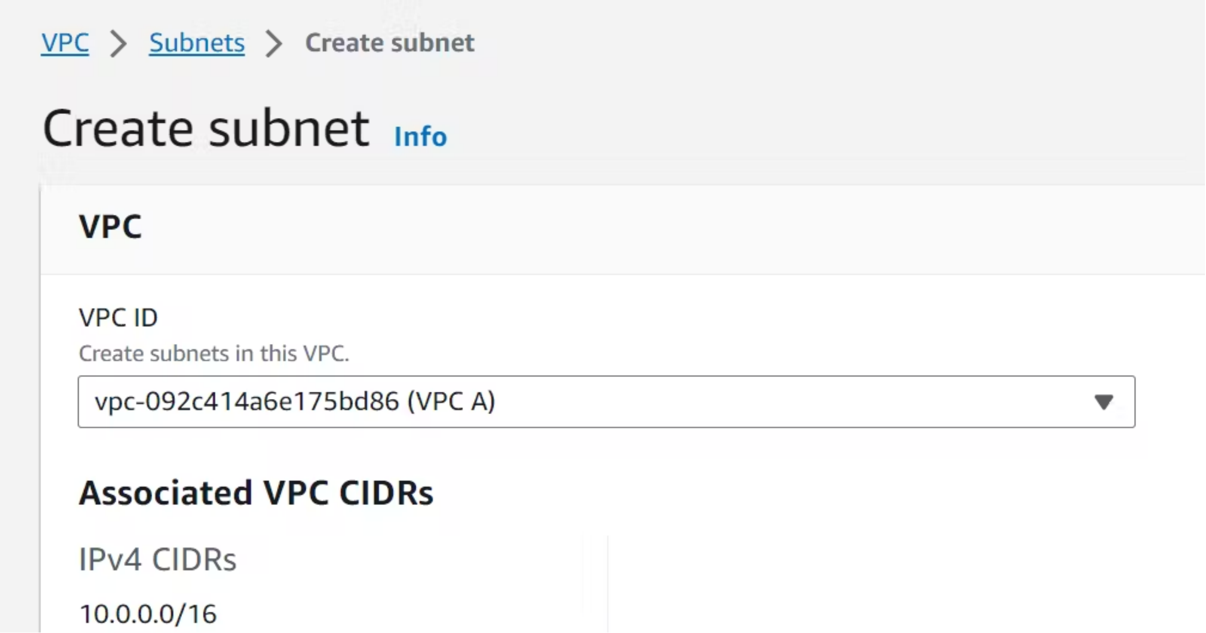
A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet. Public subnets are for resources that must be connected to the Internet, and private subnets for resources that won't be exposed to the internet.

In this section, we will create two public and two private subnets in each of the two availability zones within your VPC.

In the VPC panel on the left click on Subnets

1.1 Click on Create subnet button in the top right corner.

1.2 Choose `VPC A` from the VPC ID dropdown.



Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

vpc-092c414a6e175bd86 (VPC A)

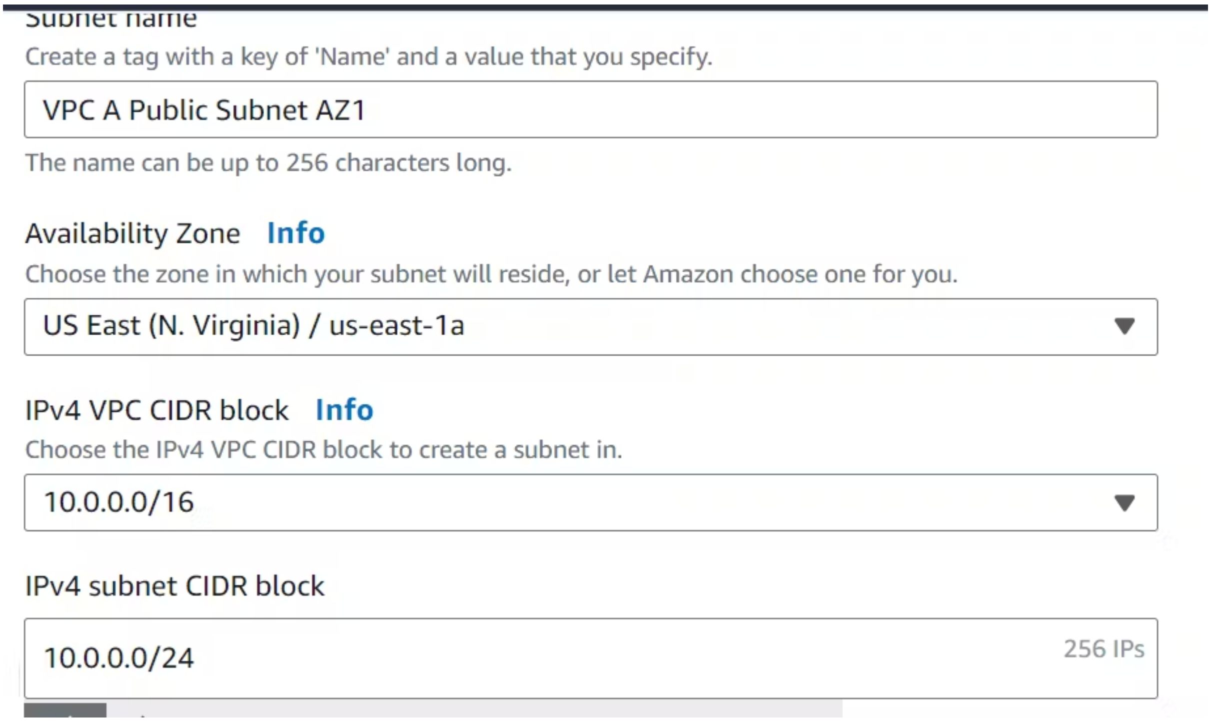
Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

1.3 In the Subnet settings section

- Enter the name as `VPC A Public Subnet AZ1`
- Select the Availablity Zone of `us-east-1a`
- Enter a CIDR block of `10.0.0.0/24`:
- Click Create subnet



Subnet name

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

VPC A Public Subnet AZ1

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 IPv4 VPC CIDR block to create a subnet in.

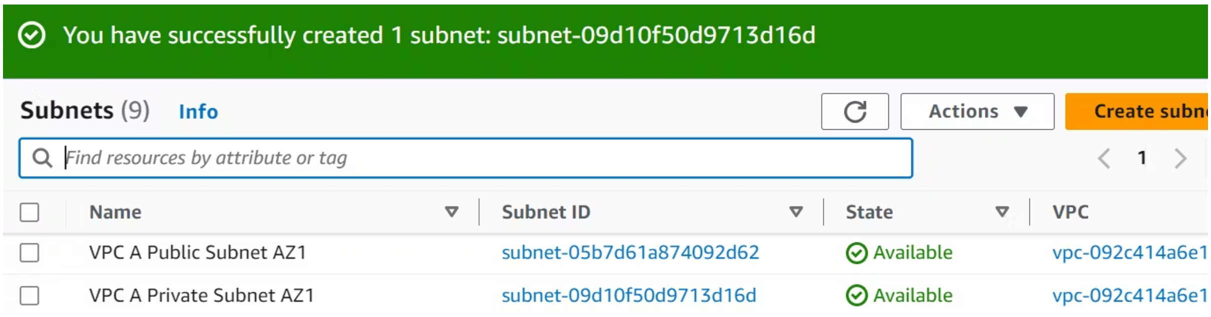
10.0.0.0/16 ▼

IPv4 subnet CIDR block

10.0.0.0/24 256 IPs

Now we will create Private Subnet

- Click on Create subnet again
- Under Subnet settings
  - Select `VPC A`
  - Enter name of `VPC A Private Subnet AZ1`
  - Select the Availablity Zone of `us-east-1a`
  - Enter a CIDR block of `10.0.1.0/24`
  - Click Create subnet
-

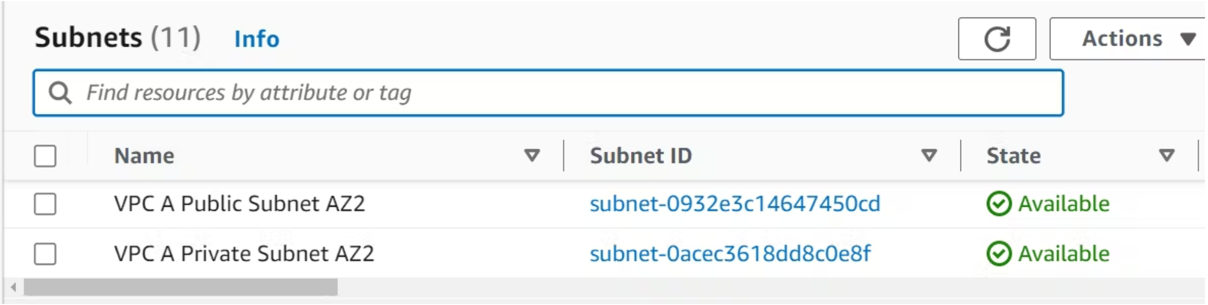


You have successfully created 1 subnet: subnet-09d10f50d9713d16d

Subnets (9) Info

□	Name	Subnet ID	State	VPC
□	VPC A Public Subnet AZ1	subnet-05b7d61a874092d62	✓ Available	vpc-092c414a6e1
□	VPC A Private Subnet AZ1	subnet-09d10f50d9713d16d	✓ Available	vpc-092c414a6e1

Similarly create Public Subnet and Private Subnet in us-west-1b with CIDR of Public Subnet as 10.0.2.0/24 and Private Subnet as 10.0.3.0/24



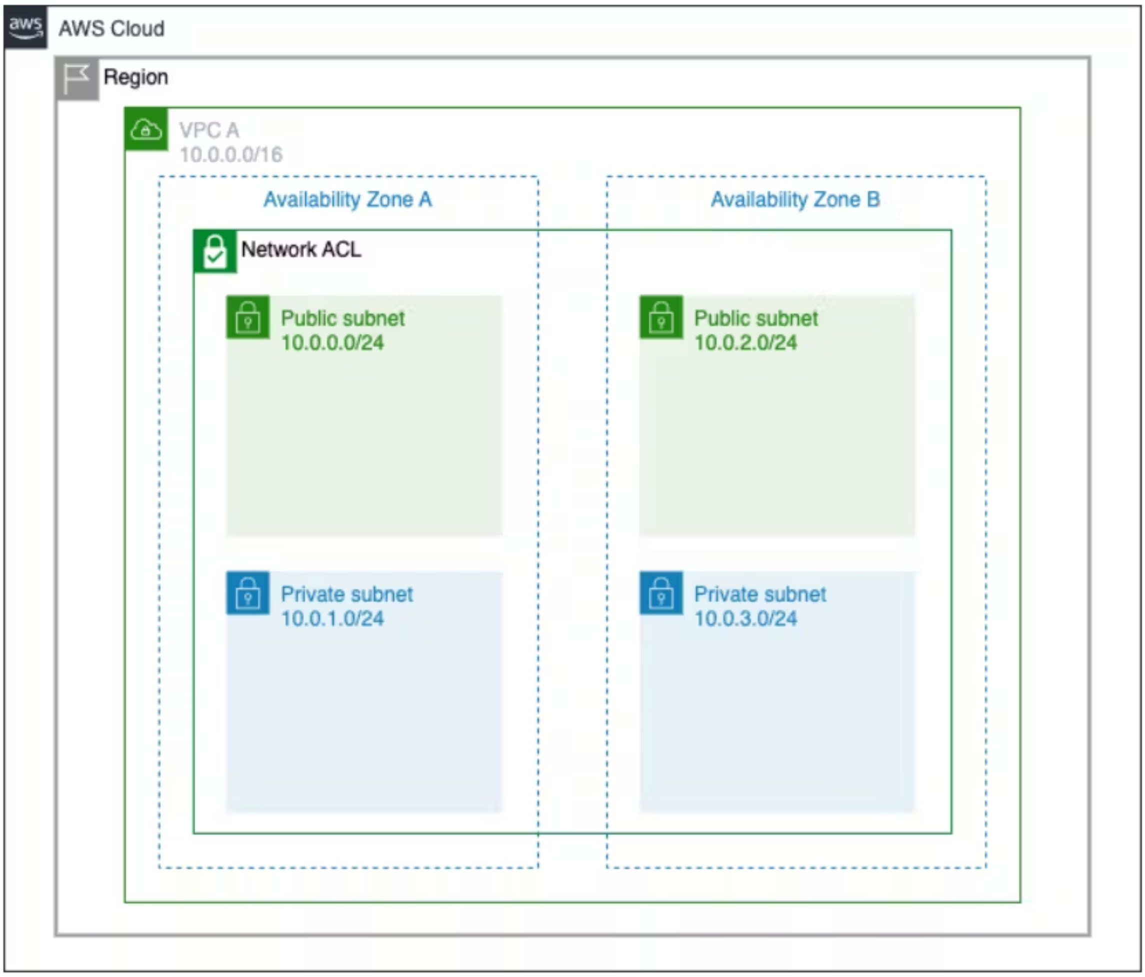
Subnets (11)

□	Name	Subnet ID	State
□	VPC A Public Subnet AZ2	subnet-0932e3c14647450cd	✓ Available
□	VPC A Private Subnet AZ2	subnet-0acec3618dd8c0e8f	✓ Available

Network ACL:

A network access control list (ACL) is an optional layer of security for your VPC for controlling traffic in and out of one or more subnets. It acts as a firewall at the subnet level. It is Stateless, Traffic that is let out must be let back in. It allows all traffic by default, you can create rules to allow or deny traffic. Custom ACL blocks or denies all traffic (inbound and outbound) until rules are added.

Rules are evaluated in order from lowest to highest. If the traffic doesn’t match any rules, the * rule is applied, and the traffic is denied. Default NACLs allow all inbound and outbound traffic, as shown below, unless customised. Network ACLs have separate inbound and outbound rules. Each rule can either allow or deny traffic by increments of 10 or 100.



Create a new Network ACL for workload subnets in VPC A

1. On the VPC Dashboard click on Network ACLs
2. Click Create network ACL

In the Network ACL settings screen

- Enter a name of `VPC A Workload Subnets NACL`
- Select `VPC A` from the dropdown
- Click Create network ACL

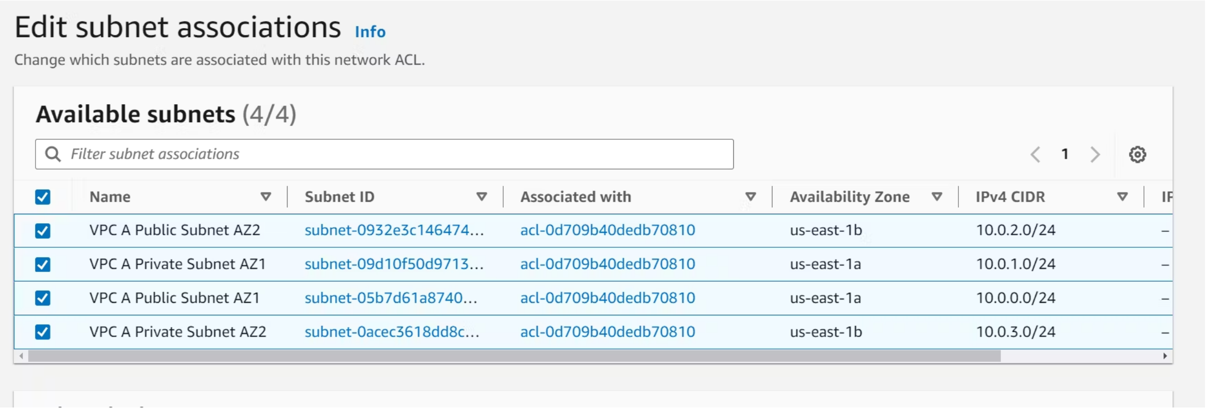
  The result will be a new NACL for VPC A alongside the default NACL created when the VPC was created.

  In the resulting Network ACLs screen

  Select the checkbox for `VPC A Workload Subnets NACL`

  Scroll down to the Subnet associations tab

  Click Edit subnet associations



Edit subnet associations Info

Change which subnets are associated with this network ACL.

Available subnets (4/4)

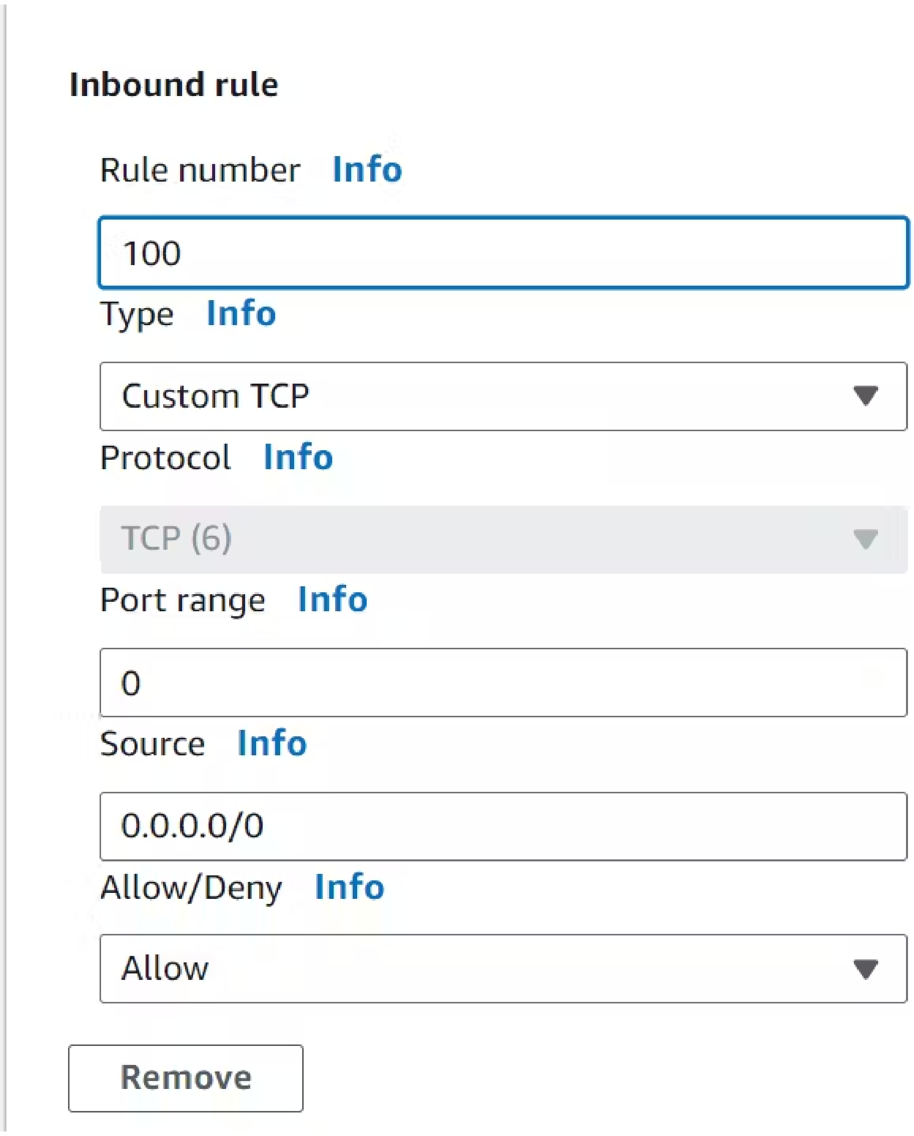
Filter subnet associations

☑	Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IP
☑	VPC A Public Subnet AZ2	subnet-0932e3c146474…	acl-0d709b40dedb70810	us-east-1b	10.0.2.0/24	–
☑	VPC A Private Subnet AZ1	subnet-09d10f50d9713…	acl-0d709b40dedb70810	us-east-1a	10.0.1.0/24	–
☑	VPC A Public Subnet AZ1	subnet-05b7d61a8740…	acl-0d709b40dedb70810	us-east-1a	10.0.0.0/24	–
☑	VPC A Private Subnet AZ2	subnet-0acec3618dd8c…	acl-0d709b40dedb70810	us-east-1b	10.0.3.0/24	–

The NACL should now be associated with four subnets on the following screen but because NACLs are created with only a DENY rule for inbound and outbound we will now change the default NACL rules to allow all traffic in both directions.

In the Network ACLs screen

- Select the check box for `VPC A Workload Subnets NACL` for VPC A
- Scroll down and select the Inbound Rules tab below
- Notice that we have only `DENY` all rule
- Click Edit inbound rules
- In Edit inbound rules screen
    - Click Add new rule
    - Input `100` in Rule number
    - Choose `All traffic` in Type
    - Leave Source as `0.0.0.0/0`
    - Click Save changes



Inbound rule

Rule number Info

100

Type Info

Custom TCP

Protocol Info

TCP (6)

Port range Info

0

Source Info

0.0.0.0/0

Allow/Deny Info

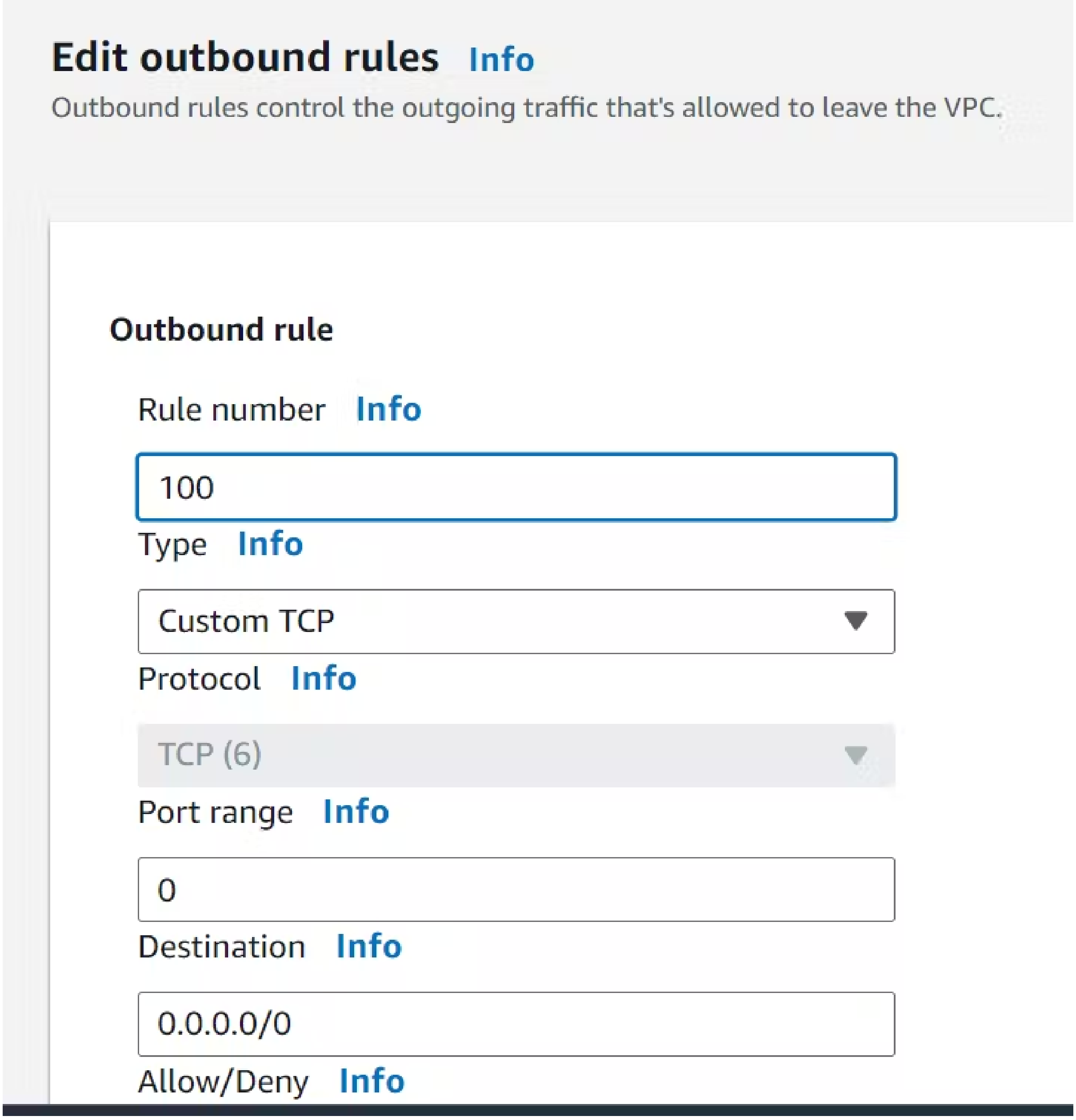
Allow

In the resulting screen you should have a success banner and a new `Allow` rule under the Inbound rules tab:

Now follow the same steps described above for Inbound, but work on Outbound Rules tab of NACLs

1. /On the Outbound Rules tab
    - Note that we have only `DENY` all rule
    - Click Edit outbound rules

2. In the Edit outbound rules screen
    - Click Add new rule
    - Input `100` in Rule number
    - Choose `All traffic` in Type
    - Leave Source as `0.0.0.0/0`
    - Click Save changes
    -



Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the VPC.

Outbound rule

Rule number Info

100

Type Info

Custom TCP

Protocol Info

TCP (6)

Port range Info

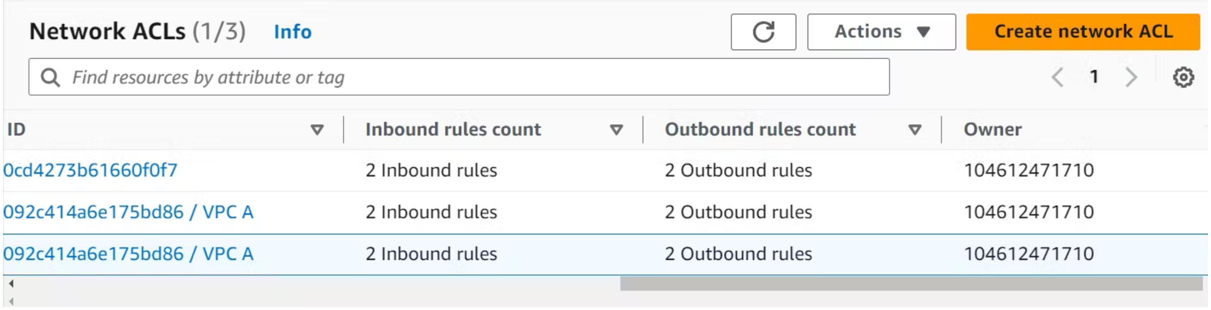
0

Destination Info

0.0.0.0/0

Allow/Deny Info

Allowing all traffic in and out of your subnets is not a good security posture. You can use NACLs to set broad rules and/or DENY rules, and then use *Security Groups* to create fine grained rules. For example, you can deny traffic from specific IPs with NACLs but not with Security Groups.



ID	Inbound rules count	Outbound rules count	Owner
0cd4273b61660f0f7	2 Inbound rules	2 Outbound rules	104612471710
092c414a6e175bd86 / VPC A	2 Inbound rules	2 Outbound rules	104612471710
092c414a6e175bd86 / VPC A	2 Inbound rules	2 Outbound rules	104612471710

Thats how it shows two inbound rules and two outbound rule.

Dear Friends, In Next Part of Blog you will learn about Route Tables, Internet Connectivity, VPC Endpoints and many more things. Stay tuned!!!

Thank you for reading all the way through.