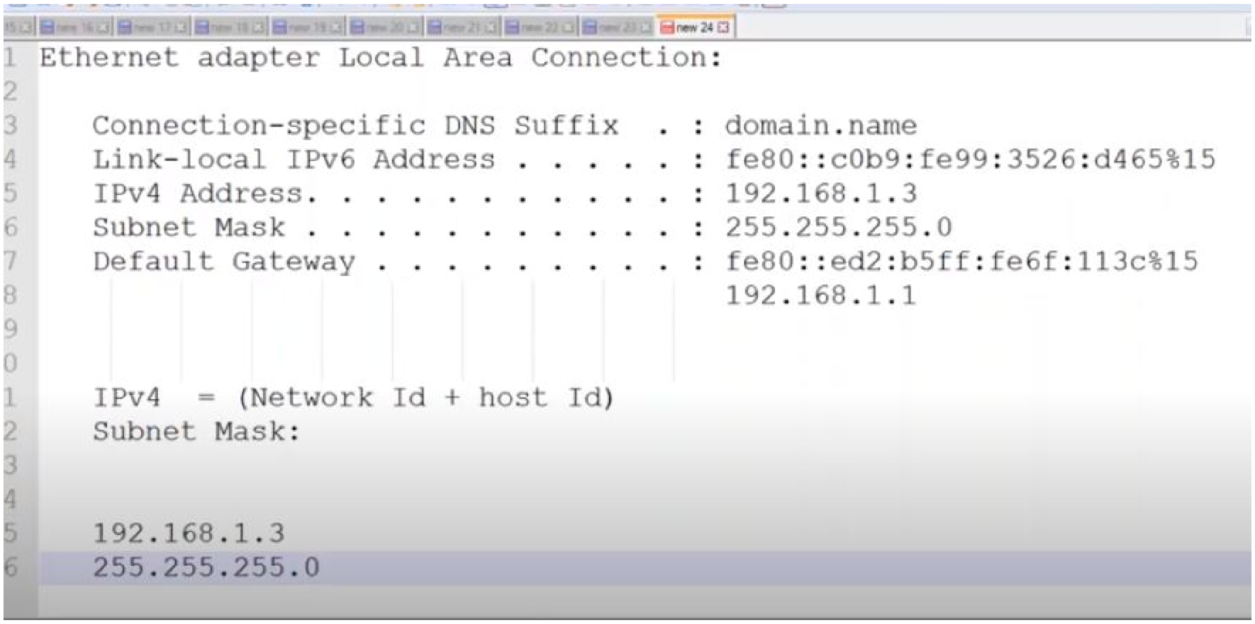
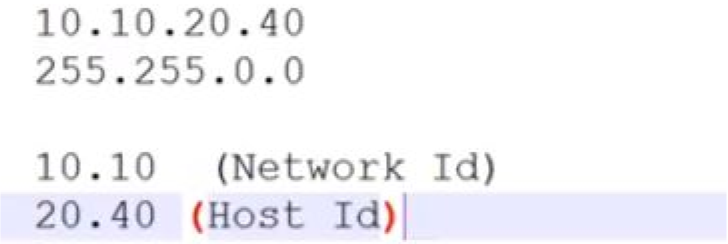


```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : domain.name
   Link-local IPv6 Address . . . . . : fe80::c0b9:fe99:3526:d465%15
   IPv4 Address. . . . . . . . . . . : 192.168.1.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::ed2:b5ff:fe6f:113c%15
                                       192.168.1.1



   IPv4  = (Network Id + host Id)
   Subnet Mask:


   192.168.1.3
   255.255.255.0
```



```
10.10.20.40
255.255.0.0

10.10  (Network Id)
20.40 (Host Id)
```

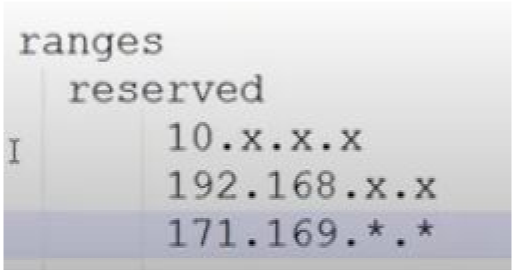
Network packet can be send from one machine to other machine if they have same network id(private network)
Router(route table) send the packet to outside network(default gateway)
Packet with in network we don't need anything

255.255.255.0 = 8 bites = 255 -2 = 253
1 is network id
2 is broadcast

For example
10.10.20.40
10.10 (network id =1)
20.40 (host id = 0) = 2^16 -2 (physical network calculation)
So ipv4(total bit 32 bit) = (network id + host id)
(software define network) Virtual network calculation 2^16 -5

Public IP- anyone with internet reach to your network(dynamic ip)

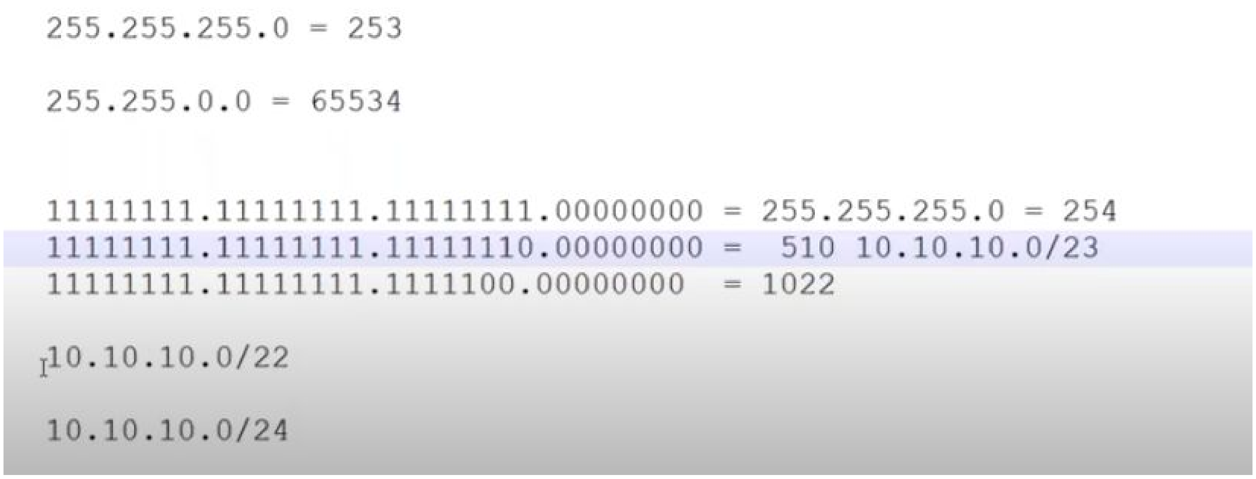
Private IP-



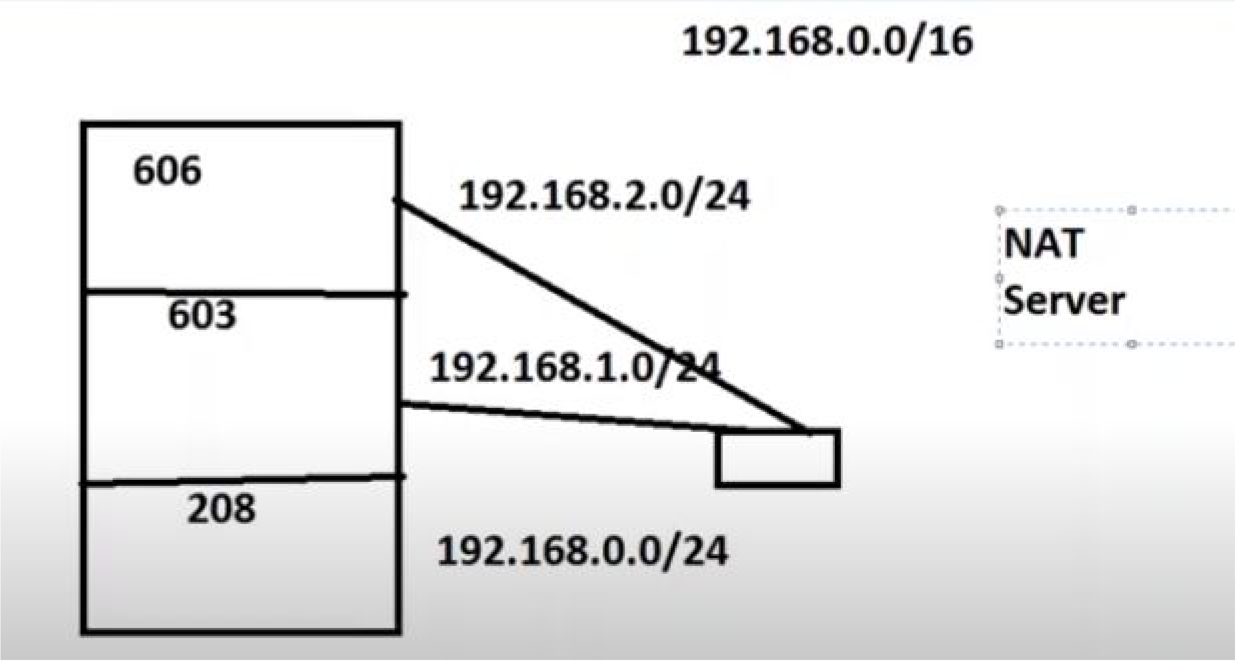
```
ranges
  reserved
      10.x.x.x
      192.168.x.x
      171.169.*.*
```

reserved ip so its costly(static ip)

CIDR-classless inter domain routing

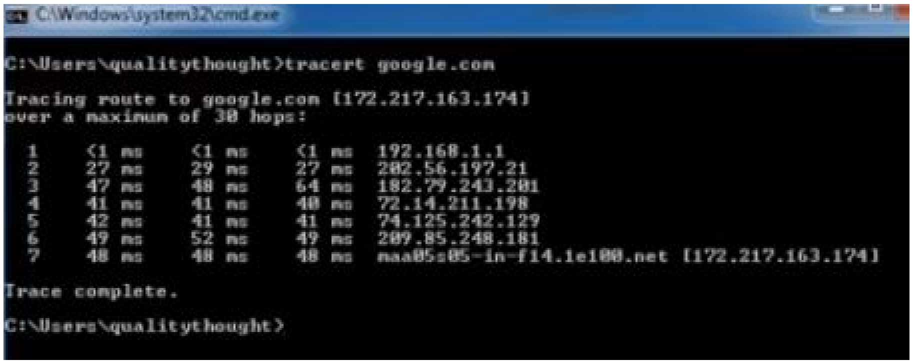


```
255.255.255.0 = 253

255.255.0.0 = 65534


11111111.11111111.11111111.00000000 = 255.255.255.0 = 254
11111111.11111111.11111110.00000000 =  510 10.10.10.0/23
11111111.11111111.1111100.00000000  = 1022

10.10.10.0/22

10.10.10.0/24
```



Router or routable use to send packet outside network

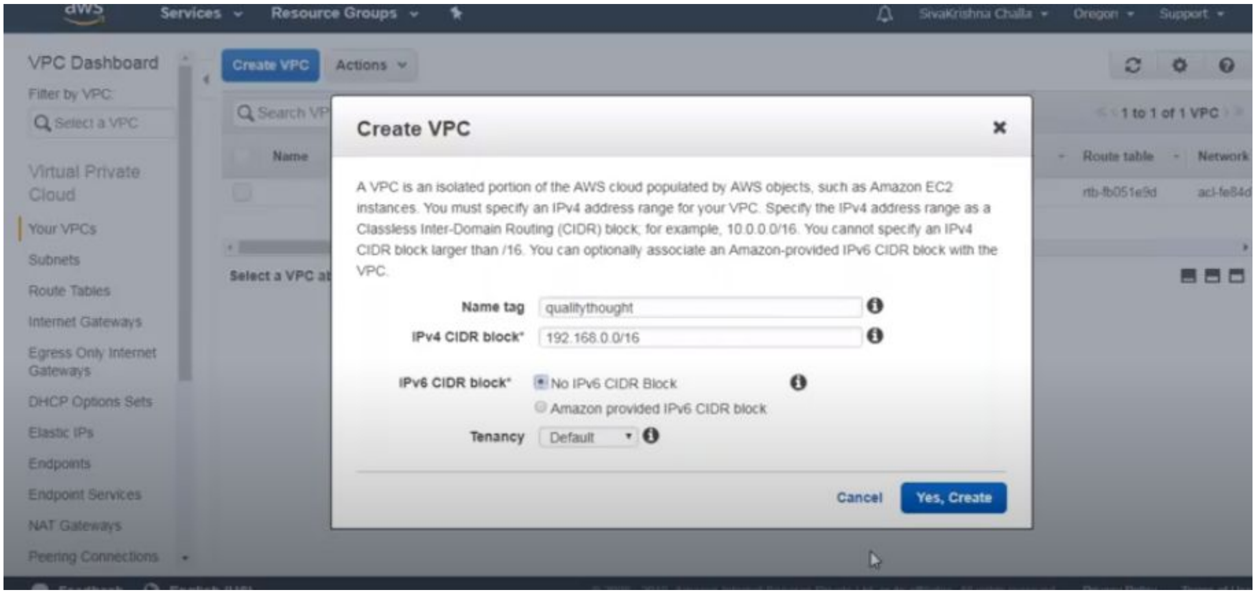
Nat server go in one direction only(nat server send packet to google.com and google.com will again response packet to nat server then nat convert it and send router we can get response



```
C:\Users\qualitythought>tracert google.com

Tracing route to google.com [172.217.163.174]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    27 ms    29 ms    27 ms  202.56.197.21
  3    47 ms    48 ms    64 ms  182.79.243.201
  4    41 ms    41 ms    40 ms  72.14.211.198
  5    42 ms    41 ms    41 ms  74.125.242.129
  6    49 ms    52 ms    49 ms  209.85.248.181
  7    48 ms    48 ms    48 ms  maa05s05-in-f14.1e100.net [172.217.163.174]

Trace complete.

C:\Users\qualitythought>
```

Packet travel trace windows and for linux we can use command traceroute

https://www.qualitythought.in/wp-content/uploads/2017/02/NetworkingBasics.pdf
https://www.qualitythought.in/wp-content/uploads/2017/02/VPC-Introduction.pdf
VPC



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.

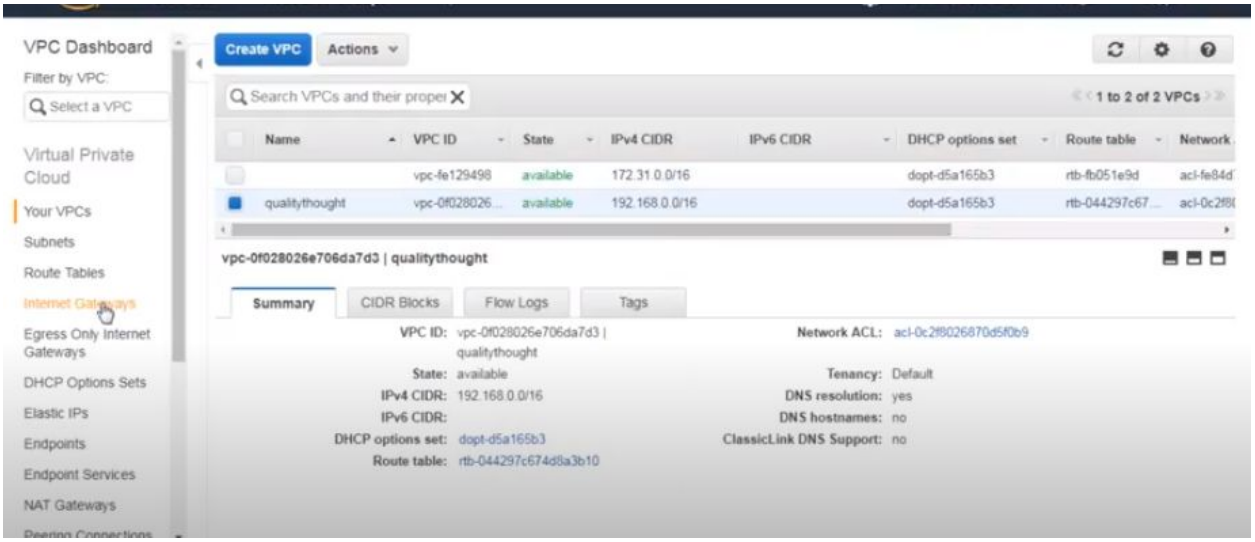
Name tag: qualitythought

IPv4 CIDR block*: 192.168.0.0/16

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

Tenancy: Default

Cancel | Yes, Create

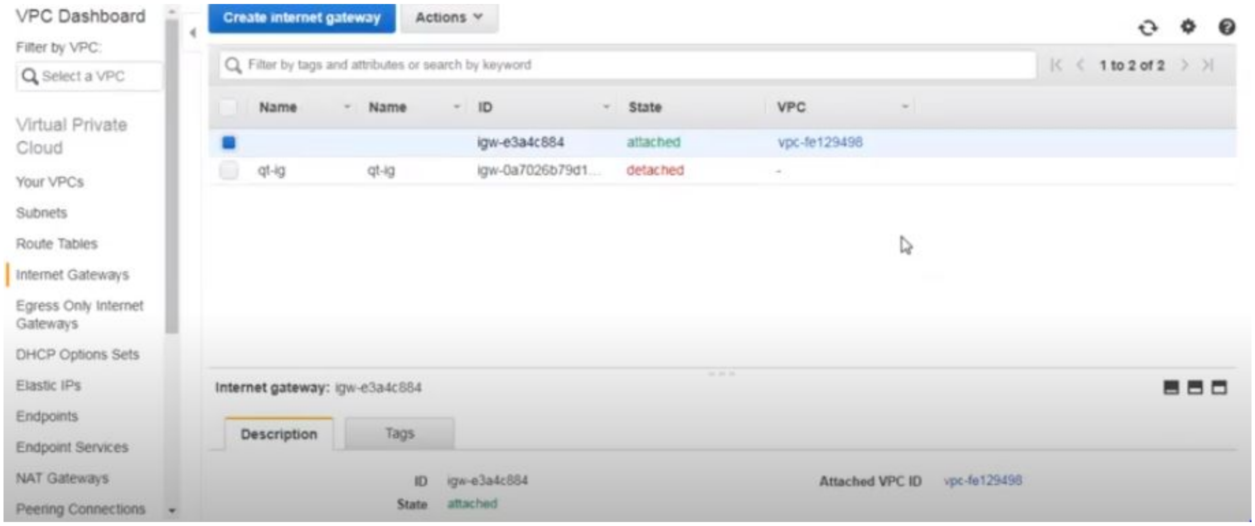


	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table	Network
□		vpc-fe129498	available	172.31.0.0/16		dopt-d5a165b3	rtb-fb051e9d	acl-fe84d
■	qualitythought	vpc-0f028026...	available	192.168.0.0/16		dopt-d5a165b3	rtb-044297c67...	acl-0c2f8

vpc-0f028026e706da7d3 | qualitythought

Summary | CIDR Blocks | Flow Logs | Tags

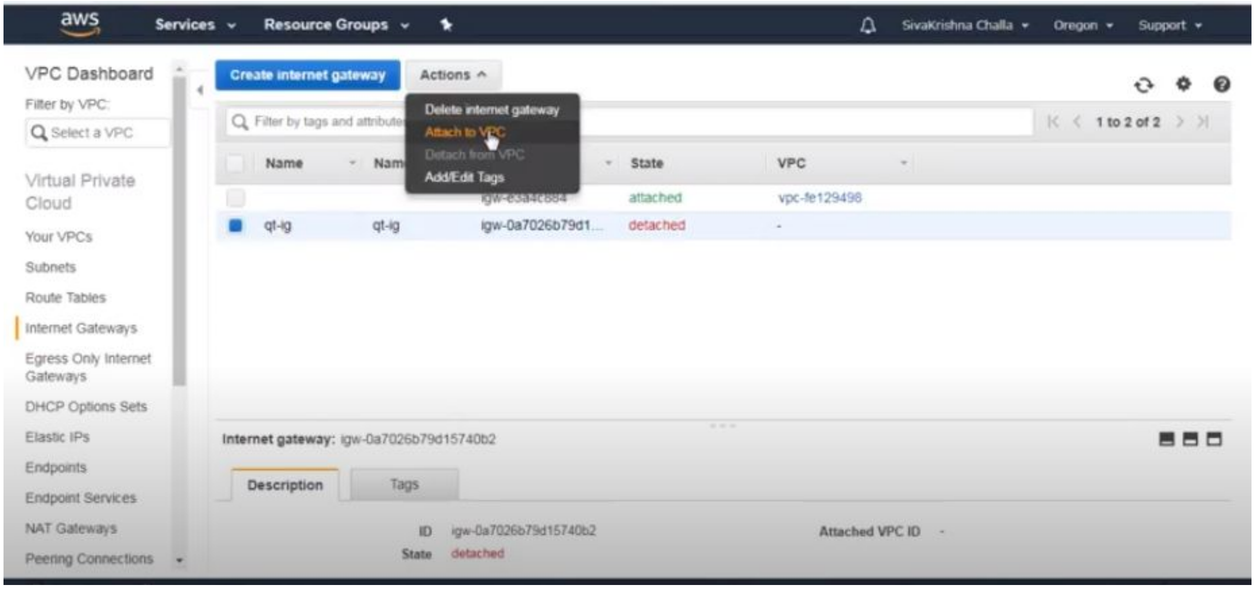
VPC ID:	vpc-0f028026e706da7d3 | qualitythought	Network ACL:	acl-0c2f8026870d5f0b9
State:	available	Tenancy:	Default
IPv4 CIDR:	192.168.0.0/16	DNS resolution:	yes
IPv6 CIDR:		DNS hostnames:	no
DHCP options set:	dopt-d5a165b3	ClassicLink DNS Support:	no
Route table:	rtb-044297c674d8a3b10		



Name	Name	ID	State	VPC
		igw-e3a4c884	attached	vpc-fe129498
qt-ig	qt-ig	igw-0a7026b79d1...	detached	-

Internet gateway: igw-e3a4c884

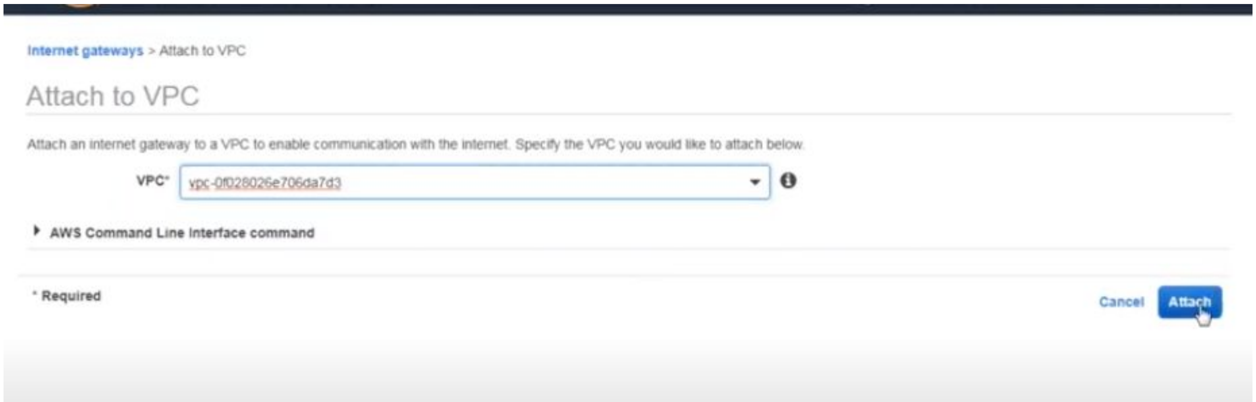
ID igw-e3a4c884
State attached
Attached VPC ID vpc-fe129498



Name	Name	ID	State	VPC
		igw-e3a4c884	attached	vpc-fe129498
qt-ig	qt-ig	igw-0a7026b79d1...	detached	-

Internet gateway: igw-0a7026b79d15740b2

ID igw-0a7026b79d15740b2
State detached
Attached VPC ID -

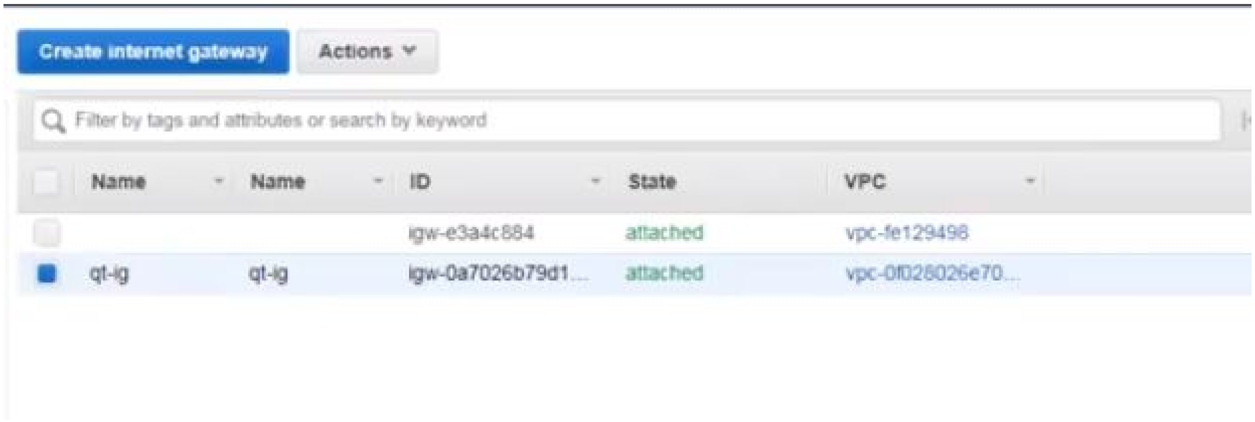

Internet gateways > Attach to VPC
AWS Command Line Interface command
Cancel
Attach

Attach to VPC

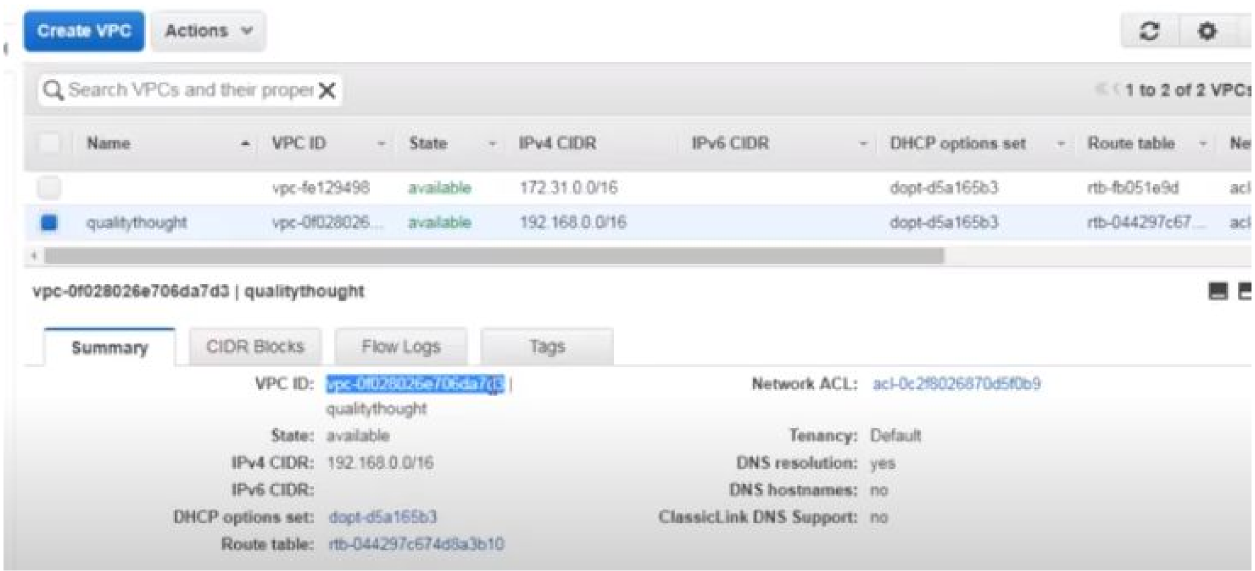
Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC* vpc-0f028026e706da7d3

* Required



Name	Name	ID	State	VPC
		igw-e3a4c884	attached	vpc-fe129498
qt-ig	qt-ig	igw-0a7026b79d1...	attached	vpc-0f028026e70...

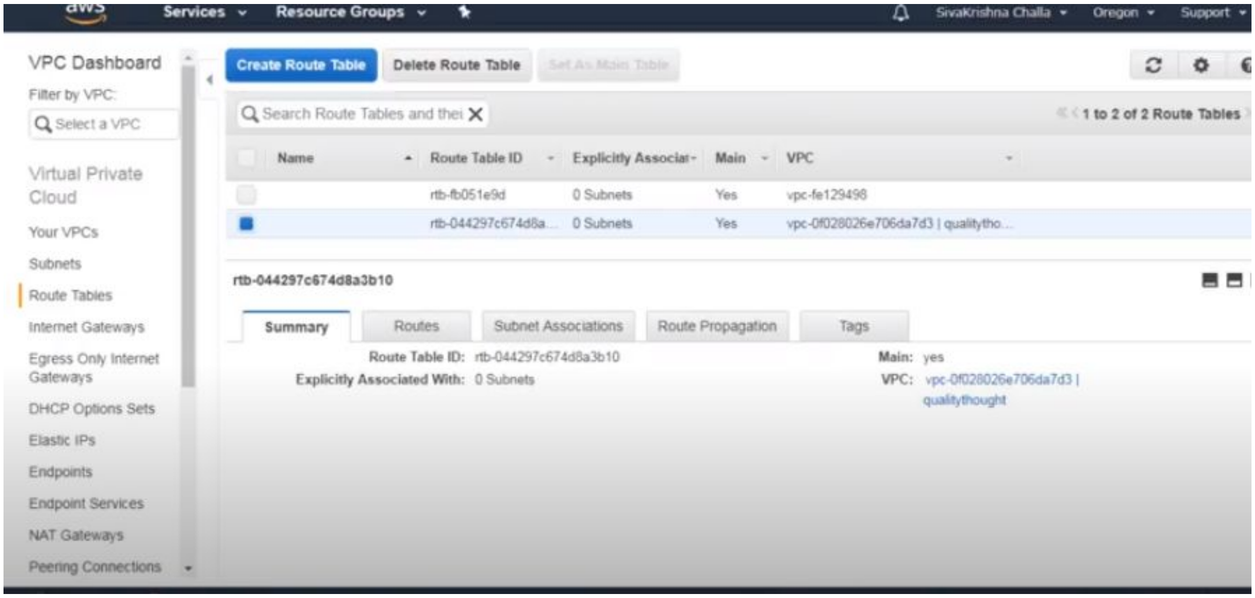


Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table	Ne
	vpc-fe129498	available	172.31.0.0/16		dopt-d5a165b3	rtb-fb051e9d	acl
qualitythought	vpc-0f028026...	available	192.168.0.0/16		dopt-d5a165b3	rtb-044297c67...	acl

vpc-0f028026e706da7d3 | qualitythought

VPC ID: vpc-0f028026e706da7d3 | qualitythought
State: available
IPv4 CIDR: 192.168.0.0/16
IPv6 CIDR:
DHCP options set: dopt-d5a165b3
Route table: rtb-044297c674d8a3b10

Network ACL: acl-0c2f8026870d5f0b9
Tenancy: Default
DNS resolution: yes
DNS hostnames: no
ClassicLink DNS Support: no



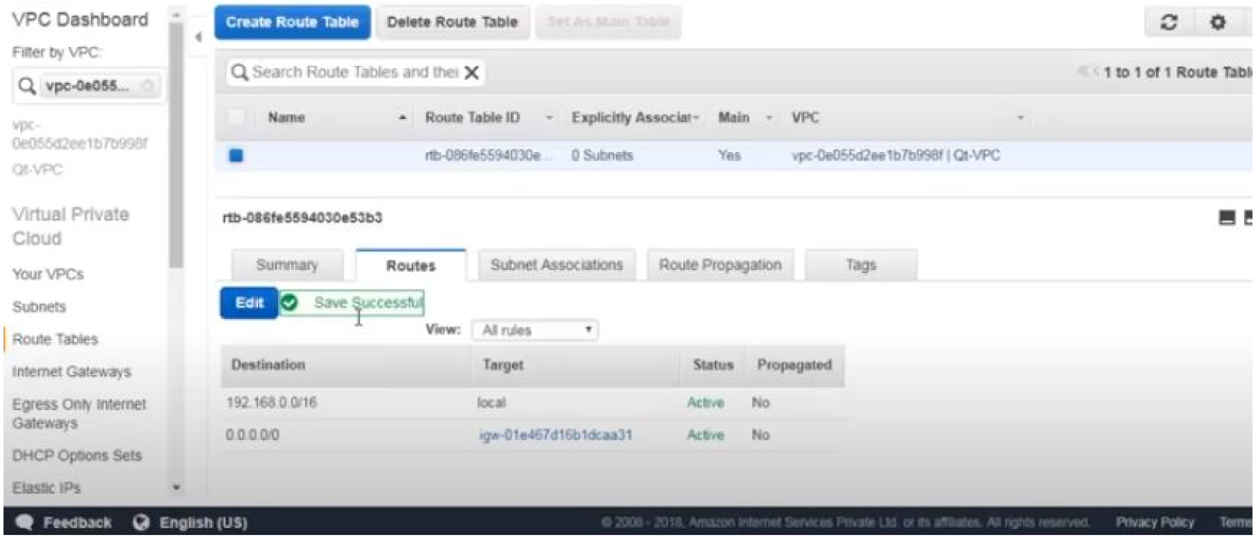
Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-fb051e9d	0 Subnets	Yes	vpc-fe129498
	rtb-044297c674d8a...	0 Subnets	Yes	vpc-0f028026e706da7d3 | qualitytho...

rtb-044297c674d8a3b10

Route Table ID: rtb-044297c674d8a3b10
Explicitly Associated With: 0 Subnets

Main: yes
VPC: vpc-0f028026e706da7d3 | qualitythought

By default when we create vpc amazon create route table



Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-086fe5594030e...	0 Subnets	Yes	vpc-0e055d2ee1b7b998f | Qt-VPC

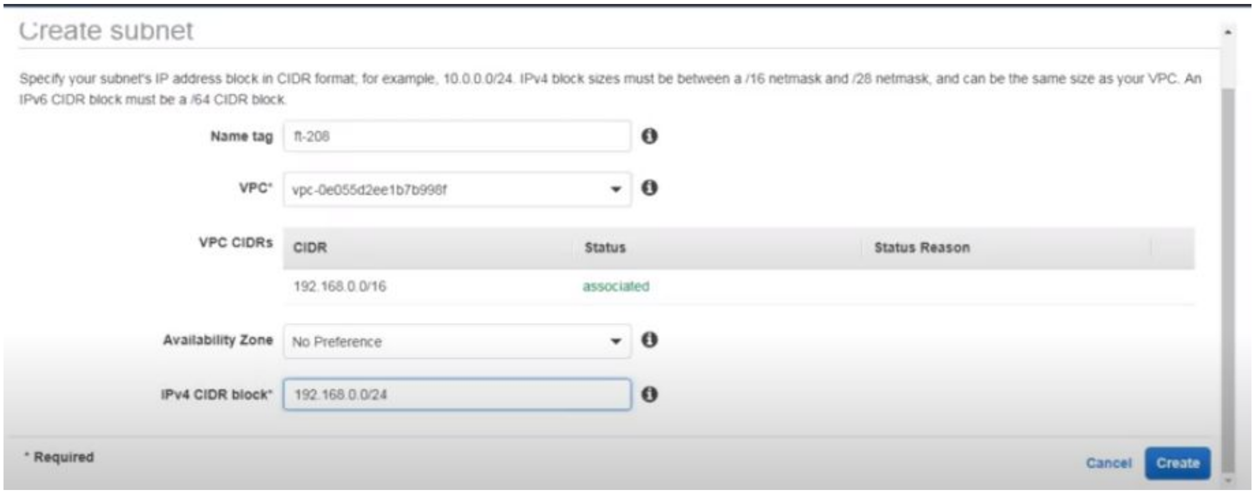
rtb-086fe5594030e53b3

View: All rules

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	igw-01e467d16b1dcaa31	Active	No

Add edit route table 0.0.0.0 to internet gateway

Create Subnet 1



Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: ft-208

VPC*: vpc-0e055d2ee1b7b998f

VPC CIDRs

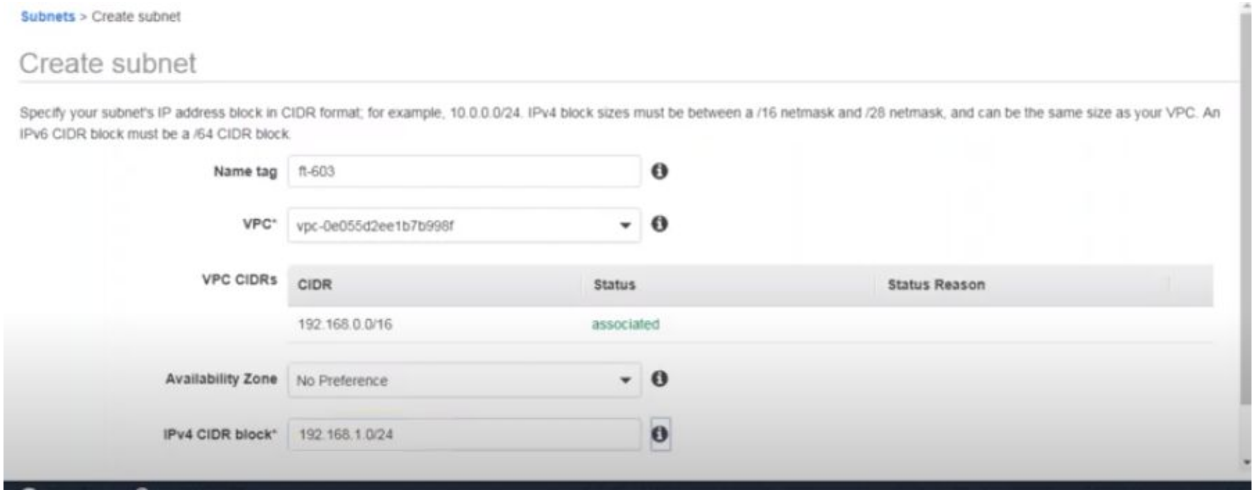
CIDR	Status	Status Reason
192.168.0.0/16	associated	

Availability Zone: No Preference

IPv4 CIDR block*: 192.168.0.0/24

* Required

Subnet 2



Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: ft-603

VPC*: vpc-0e055d2ee1b7b998f

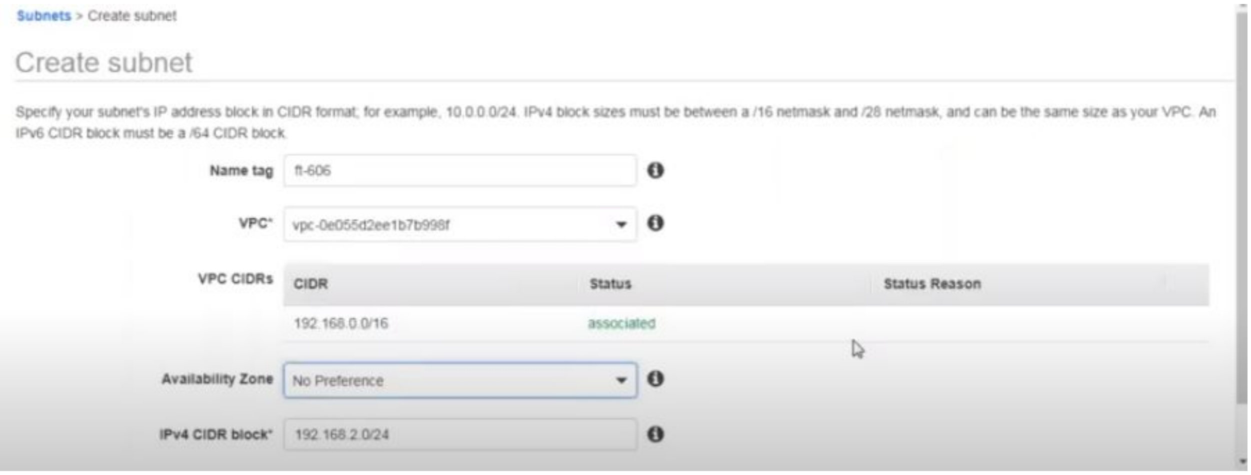
VPC CIDRs

CIDR	Status	Status Reason
192.168.0.0/16	associated	

Availability Zone: No Preference

IPv4 CIDR block*: 192.168.1.0/24

Subnet 3



Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: ft-606

VPC*: vpc-0e055d2ee1b7b998f

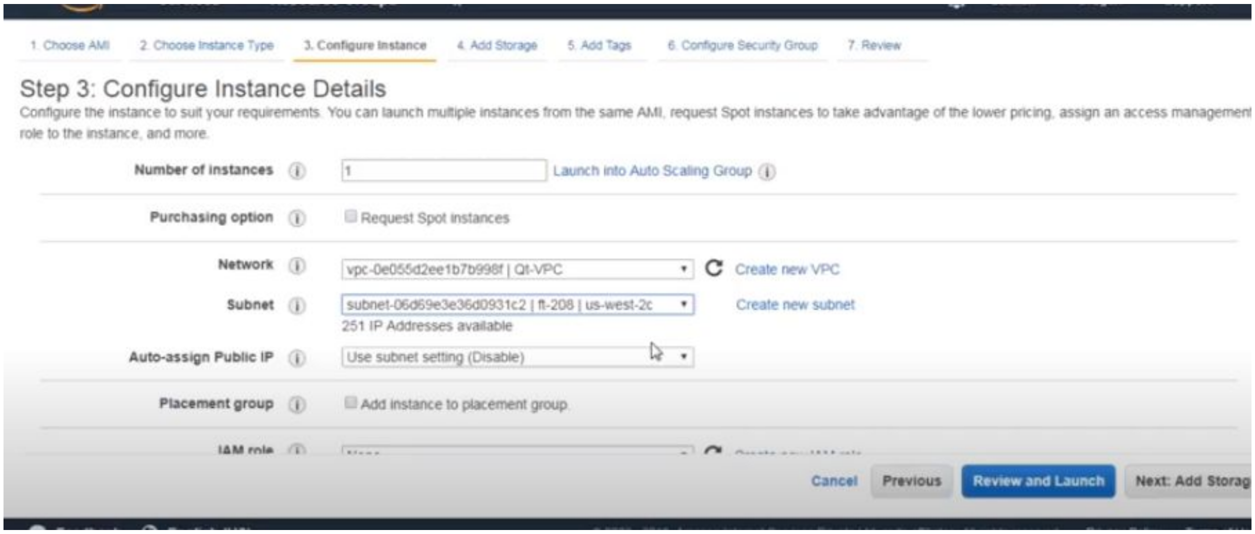
VPC CIDRs

CIDR	Status	Status Reason
192.168.0.0/16	associated	

Availability Zone: No Preference

IPv4 CIDR block*: 192.168.2.0/24

If main is yes in route table(no association) then all subnet connect to default route table
Now launch ec2 instance (select vpc and subnet 208 as per example and Enable auto assign public ip address)



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access managemen role to the instance, and more.

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-0e055d2ee1b7b998f | Qt-VPC — Create new VPC

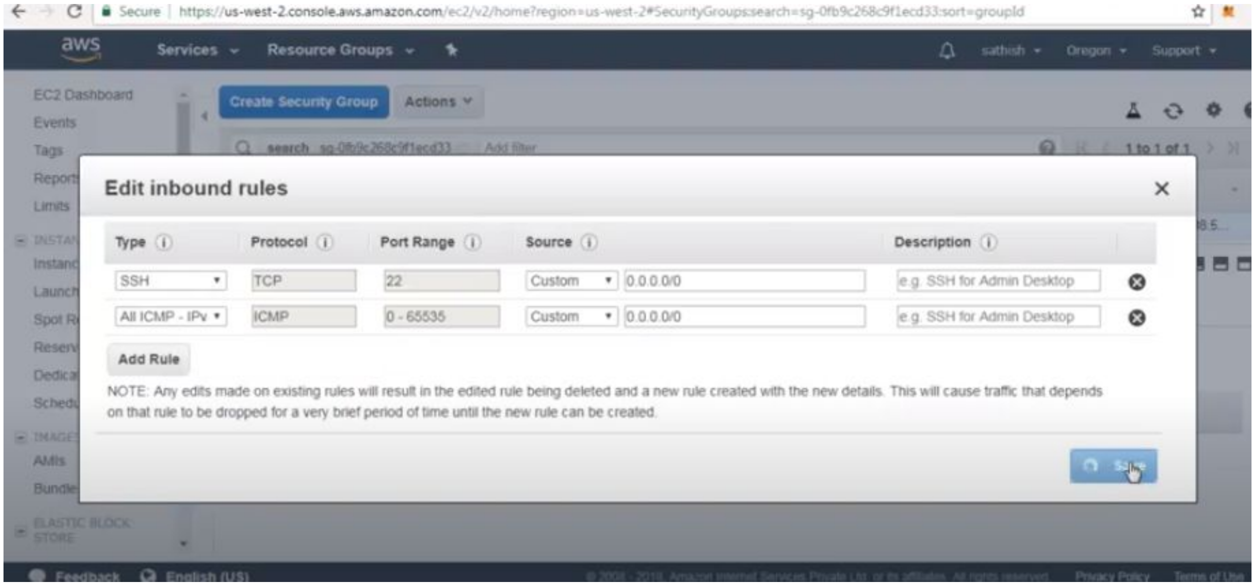
Subnet: subnet-06d69e3e36d0931c2 | ft-208 | us-west-2c — Create new subnet
251 IP Addresses available

Auto-assign Public IP: Use subnet setting (Disable)

Placement group: □ Add instance to placement group.

IAM role

Icmp security group use for allow ping from outside



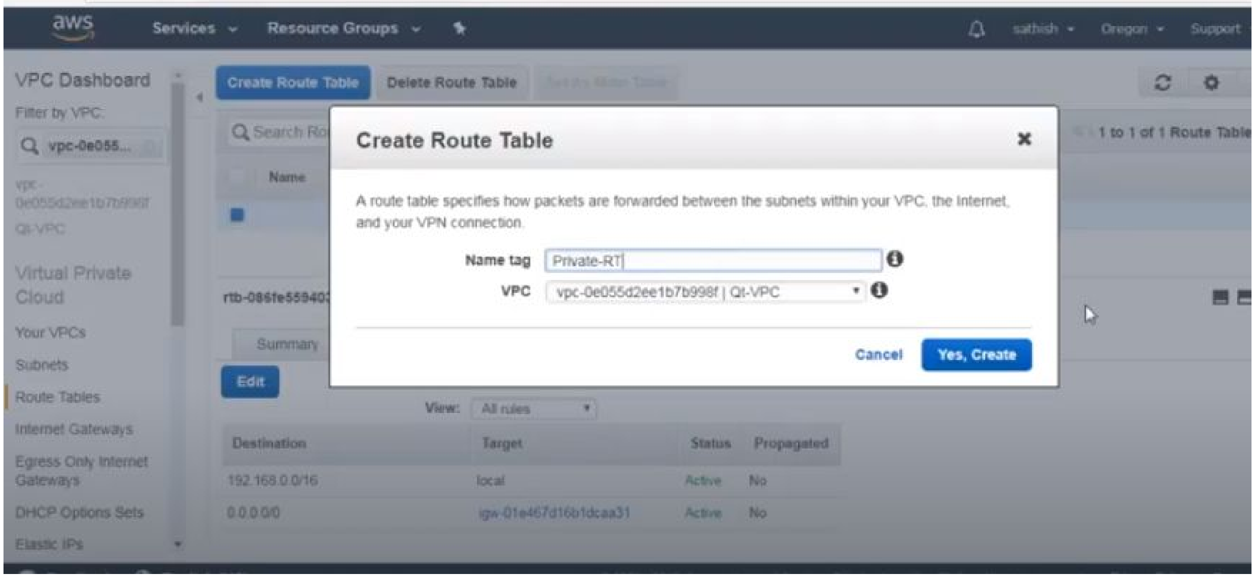
https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#SecurityGroups:search=sg-0fb9c268c9f1ecd33;sort=groupId

Edit inbound rules

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
All ICMP - IPv	ICMP	0 - 65535	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Private route Table (main is No)



Create Route Table

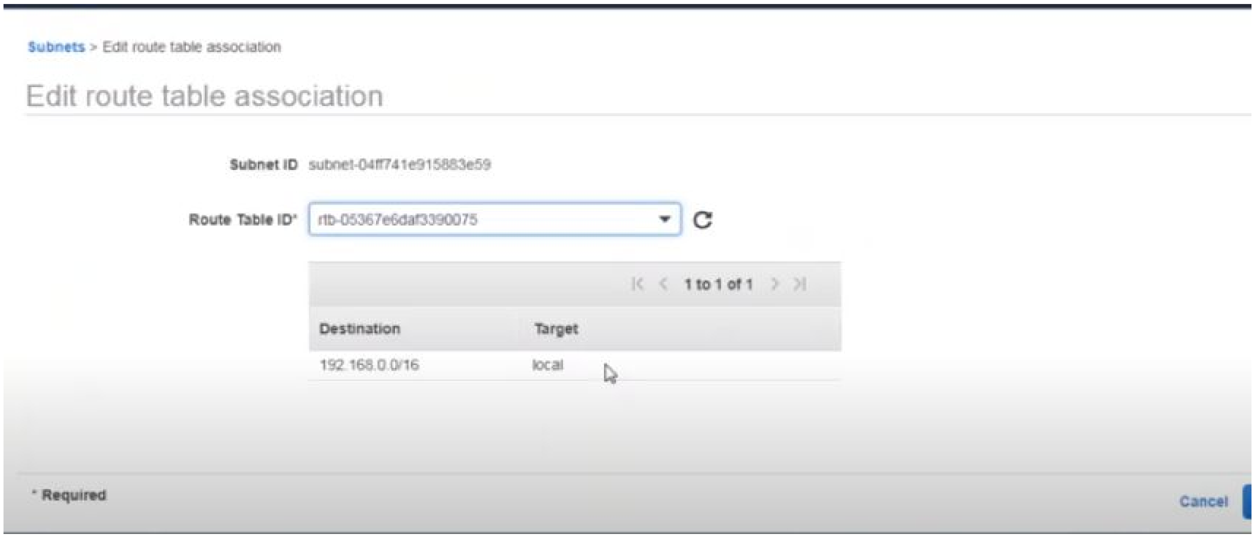
A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

Name tag: Private-RT

VPC: vpc-0e055d2ee1b7b998f | Qt-VPC

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	igw-01e467d16b1dcaa31	Active	No

Edit private subnet route table association



Subnets > Edit route table association

Edit route table association

Subnet ID subnet-04ff741e915883e59

Route Table ID* rtb-05367e6daf3390075

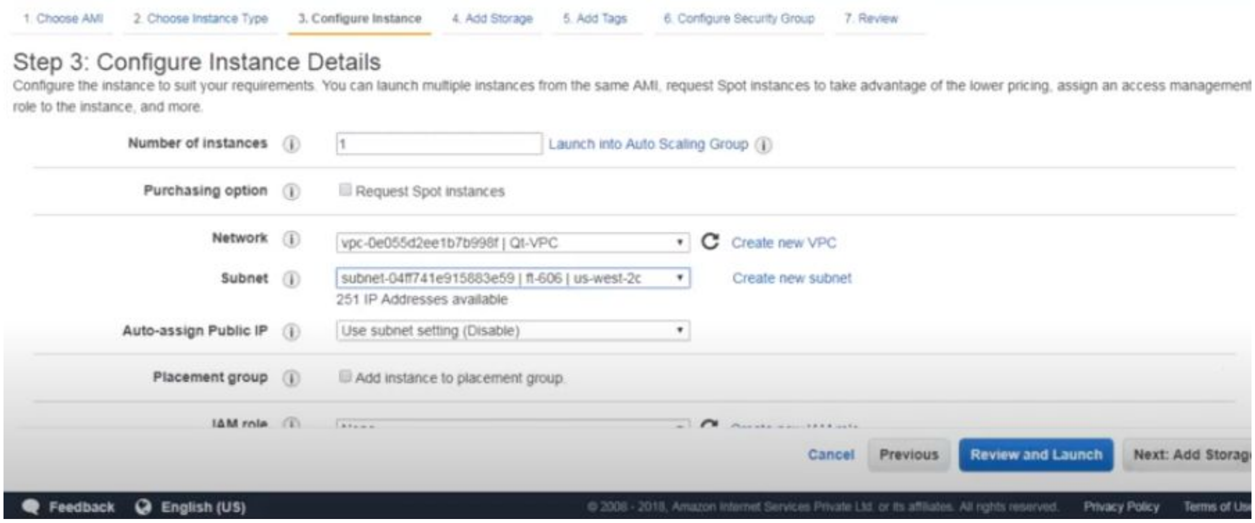
1 to 1 of 1

Destination	Target
192.168.0.0/16	local

* Required

Same as do for another private subnet

Now launch ec2 for both private subnet



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-0e055d2ee1b7b998f | Qt-VPC — Create new VPC

Subnet: subnet-04ff741e915883e59 | ft-606 | us-west-2c — Create new subnet
251 IP Addresses available

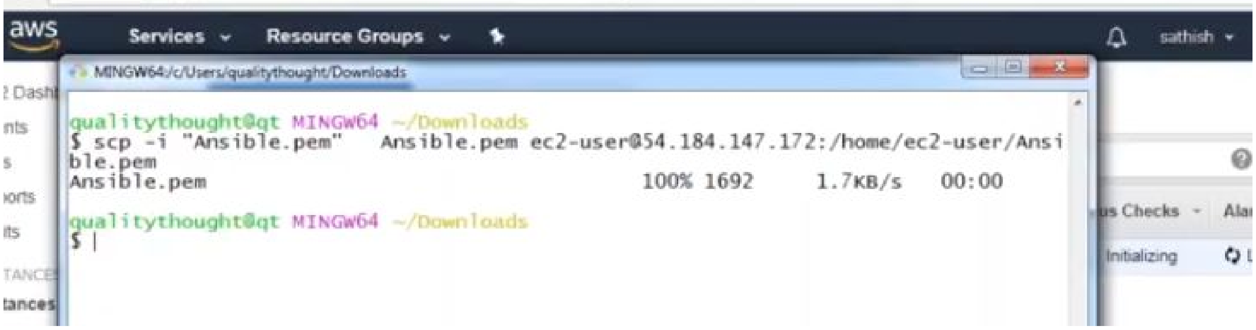
Auto-assign Public IP: Use subnet setting (Disable)

Placement group: □ Add instance to placement group

IAM role

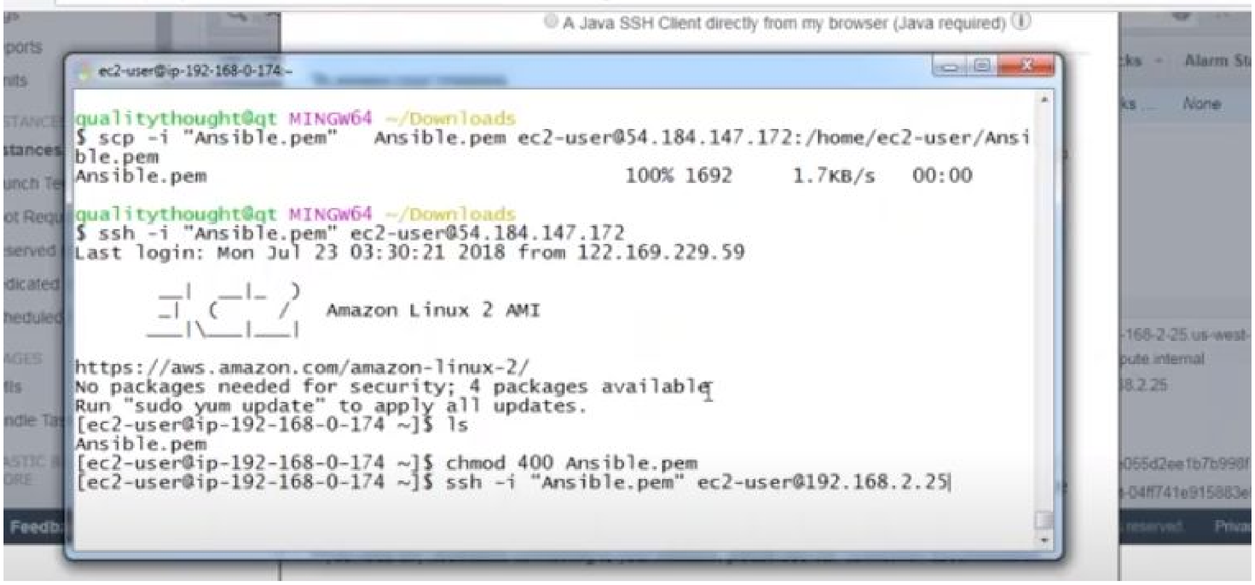
Cancel
Previous
Review and Launch
Next: Add Storag
Feedback
English (US)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Us

So to login private subnet ec2 machine we need to be inside public subnet ec2 machine and try to connect so now login public subnet ec2 machine
And test with ping ip of ec2 of private subnet machine
To transfer pem key file command



```
qualitythought@qt MINGW64 ~/Downloads
$ scp -i "Ansible.pem"   Ansible.pem ec2-user@54.184.147.172:/home/ec2-user/Ansi
ble.pem
Ansible.pem                                   100% 1692     1.7KB/s   00:00

qualitythought@qt MINGW64 ~/Downloads
$ |
```

Chmod 400 key


A Java SSH Client directly from my browser (Java required)
ec2-user@ip-192-168-0-174:~

```
qualitythought@qt MINGW64 ~/Downloads
$ scp -i "Ansible.pem"   Ansible.pem ec2-user@54.184.147.172:/home/ec2-user/Ansi
ble.pem
Ansible.pem                                   100% 1692     1.7KB/s   00:00

qualitythought@qt MINGW64 ~/Downloads
$ ssh -i "Ansible.pem" ec2-user@54.184.147.172
Last login: Mon Jul 23 03:30:21 2018 from 122.169.229.59

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
No packages needed for security; 4 packages available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-0-174 ~]$ ls
Ansible.pem
[ec2-user@ip-192-168-0-174 ~]$ chmod 400 Ansible.pem
[ec2-user@ip-192-168-0-174 ~]$ ssh -i "Ansible.pem" ec2-user@192.168.2.25
```

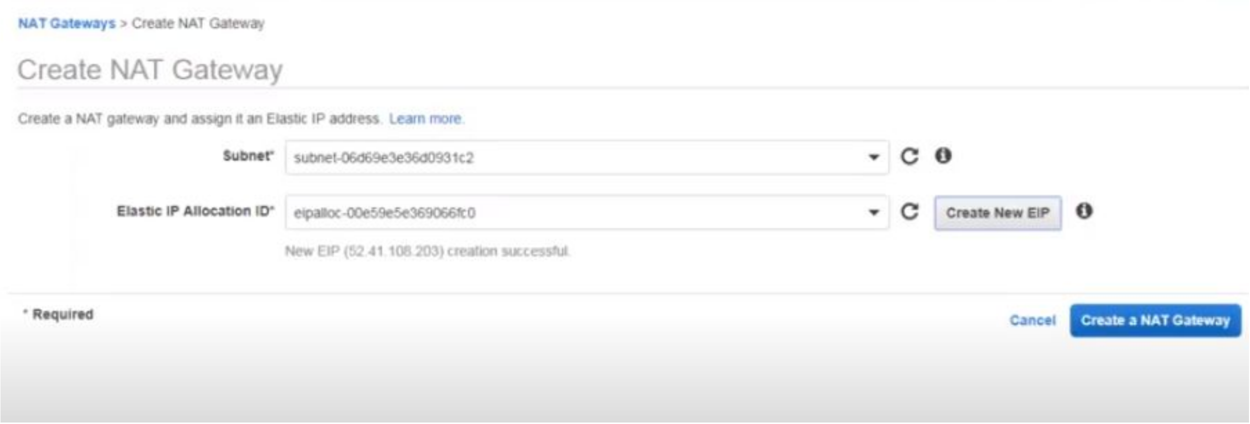
A machine which is present in public subnet and helps to connect private subnet is called
In azure jump box and in aws it's called a bastion server.

We can not access internet as of now in private subnet ec2 machine now we need to solve it
By using NAT Gateway so private subnet will get internet but can not access from outside world.
In aws two way to create nat server

1. Create ec2 instance and install nat software(older)
2. Nat gateway (latest approach)

Create nat gateway

Identify the above subnet id so it easy to find out public subnet
Also remember for nat gateway we need to have static ip(in amazon its called elastic ip)



NAT Gateways > Create NAT Gateway

Create NAT Gateway

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

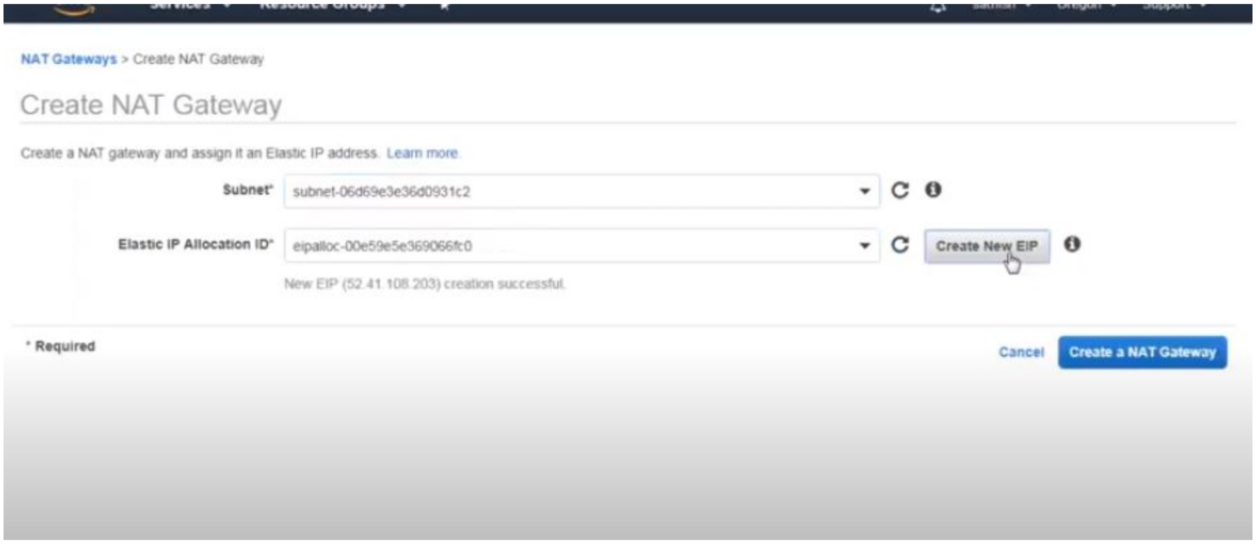
Subnet* subnet-06d69e3e36d0931c2

Elastic IP Allocation ID* eipalloc-00e59e5e369066fc0

New EIP (52.41.108.203) creation successful.

* Required

Now in route table private route edit and add 0.0.0.0/0 with nat gateway



NAT Gateways > Create NAT Gateway

Create NAT Gateway

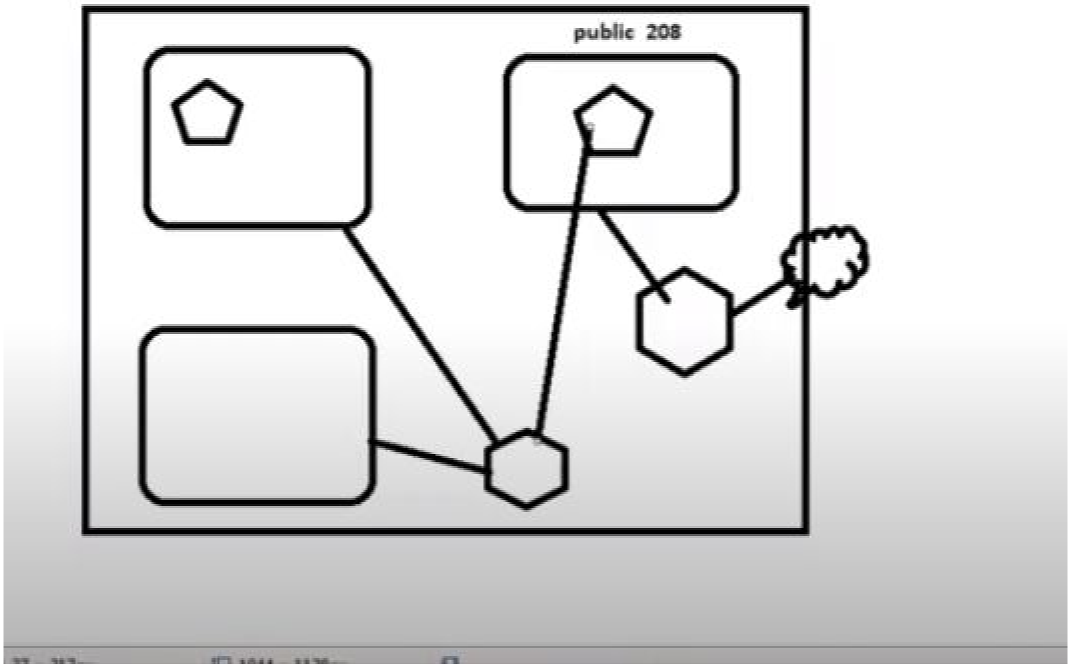
Create a NAT gateway and assign it an Elastic IP address. Learn more.

Subnet* subnet-06d69e3e36d0931c2

Elastic IP Allocation ID* eipalloc-00e59e5e369066fc0

New EIP (52.41.108.203) creation successful.

* Required

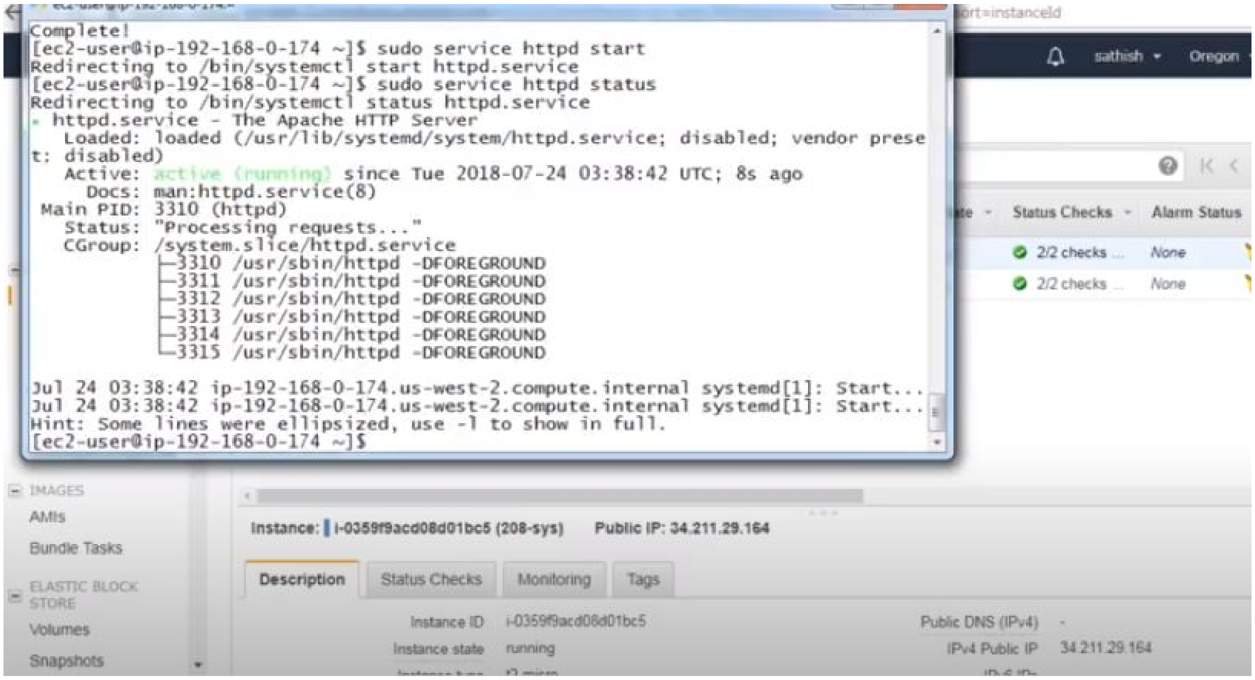


Vpc diagram

Nat is managed by amazon so there is no down time and Elastic ip is chargeable if you are not using.because we are block particular ip.

Proxy server: proxy server will use if packet need it will transfer or else it will block packet

Now let us install apache in public ec2



```
Complete!
[ec2-user@ip-192-168-0-174 ~]$ sudo service httpd start
Redirecting to /bin/systemctl start httpd.service
[ec2-user@ip-192-168-0-174 ~]$ sudo service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor prese
t: disabled)
   Active: active (running) since Tue 2018-07-24 03:38:42 UTC; 8s ago
     Docs: man:httpd.service(8)
 Main PID: 3310 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─3310 /usr/sbin/httpd -DFOREGROUND
           ├─3311 /usr/sbin/httpd -DFOREGROUND
           ├─3312 /usr/sbin/httpd -DFOREGROUND
           ├─3313 /usr/sbin/httpd -DFOREGROUND
           ├─3314 /usr/sbin/httpd -DFOREGROUND
           └─3315 /usr/sbin/httpd -DFOREGROUND

Jul 24 03:38:42 ip-192-168-0-174.us-west-2.compute.internal systemd[1]: Start...
Jul 24 03:38:42 ip-192-168-0-174.us-west-2.compute.internal systemd[1]: Start...
Hint: Some lines were ellipsized, use -l to show in full.
[ec2-user@ip-192-168-0-174 ~]$
```

Status Checks	Alarm Status
2/2 checks ...	None
2/2 checks ...	None

Instance: i-0359f9acd08d01bc5 (208-sys)   Public IP: 34.211.29.164

Instance ID: i-0359f9acd08d01bc5
Instance state: running
Public DNS (IPv4): -
IPv4 Public IP: 34.211.29.164

Security group:

Everything is closed in ec2 machine ,inbound incoming traffic and outbound is traffic out goingt

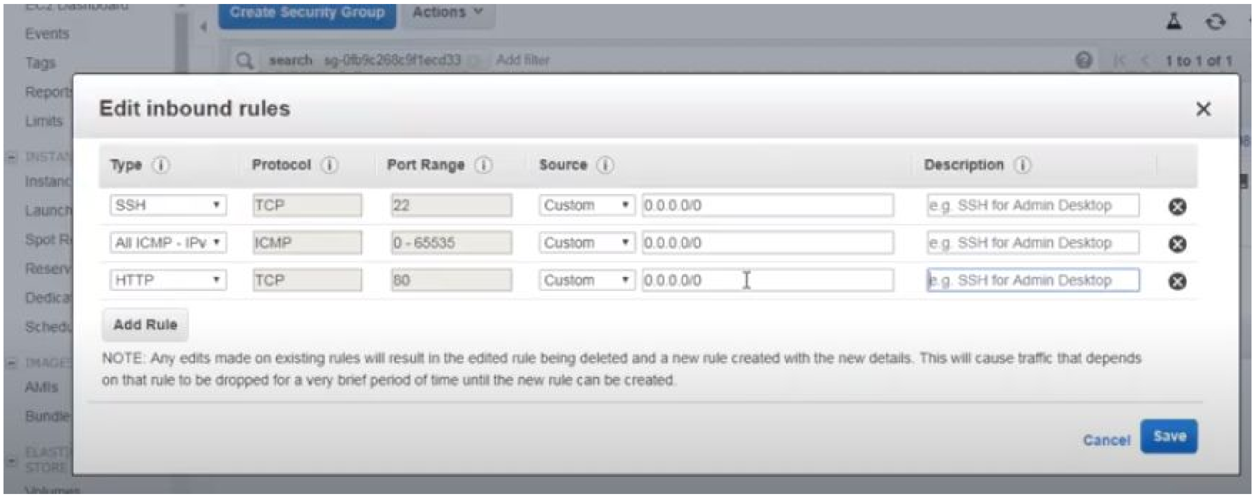
What ever you see it open remaining all port closed

Restriction are generally on network id not on host id

35.35.35.35/0 no network id or we can write like 0.0.0.0/0

35.35.35.35/32 means complete network id only one ip address

35.35.x.y/16 means allow any of the ip from the pool

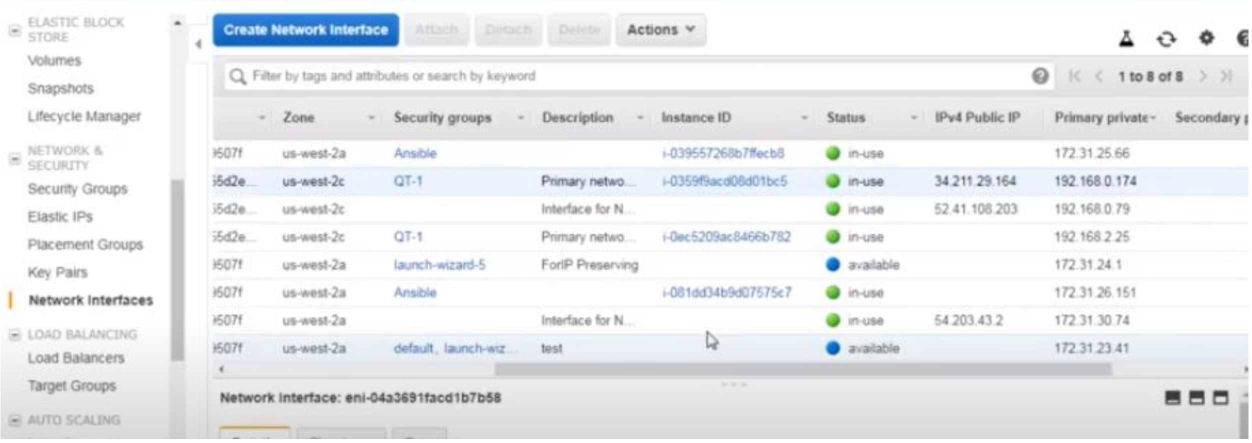


Edit inbound rules

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
All ICMP - IPv	ICMP	0 - 65535	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Network interface which is create when security group created s



	Zone	Security groups	Description	Instance ID	Status	IPv4 Public IP	Primary private	Secondary
507f	us-west-2a	Ansible		i-039557268b7ffecb8	● in-use		172.31.25.66	
5d2e...	us-west-2c	QT-1	Primary netwo...	i-0359f9acd08d01bc5	● in-use	34.211.29.164	192.168.0.174	
5d2e...	us-west-2c		Interface for N...		● in-use	52.41.108.203	192.168.0.79	
5d2e...	us-west-2c	QT-1	Primary netwo...	i-0ec5209ac8466b782	● in-use		192.168.2.25	
507f	us-west-2a	launch-wizard-5	ForIP Preserving		● available		172.31.24.1	
507f	us-west-2a	Ansible		i-081dd34b9d07575c7	● in-use		172.31.26.151	
507f	us-west-2a		Interface for N...		● in-use	54.203.43.2	172.31.30.74	
507f	us-west-2a	default, launch-wiz...	test		● available		172.31.23.41	

Network Interface: eni-04a3691facd1b7b58

You can create flow logs on your resources to capture IP traffic flow information for the network interfaces for your resources

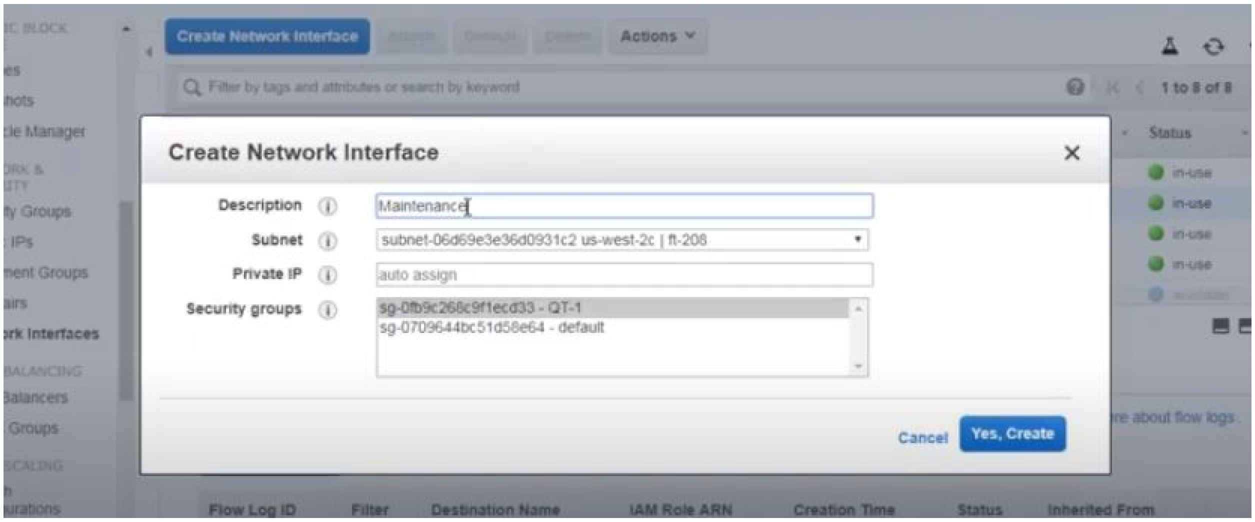
We can create flow logs in the network interface.

Your system can have multiple network interfaces and multiple ip.

We can not change the security group but we can change the rules and we can only kill the security group.

So for high availability of servers we can disassociate network interfaces and associate with other systems so there will be less down time.

We can create a network interface and you should know what is your vpc and availability zone.



Create Network Interface

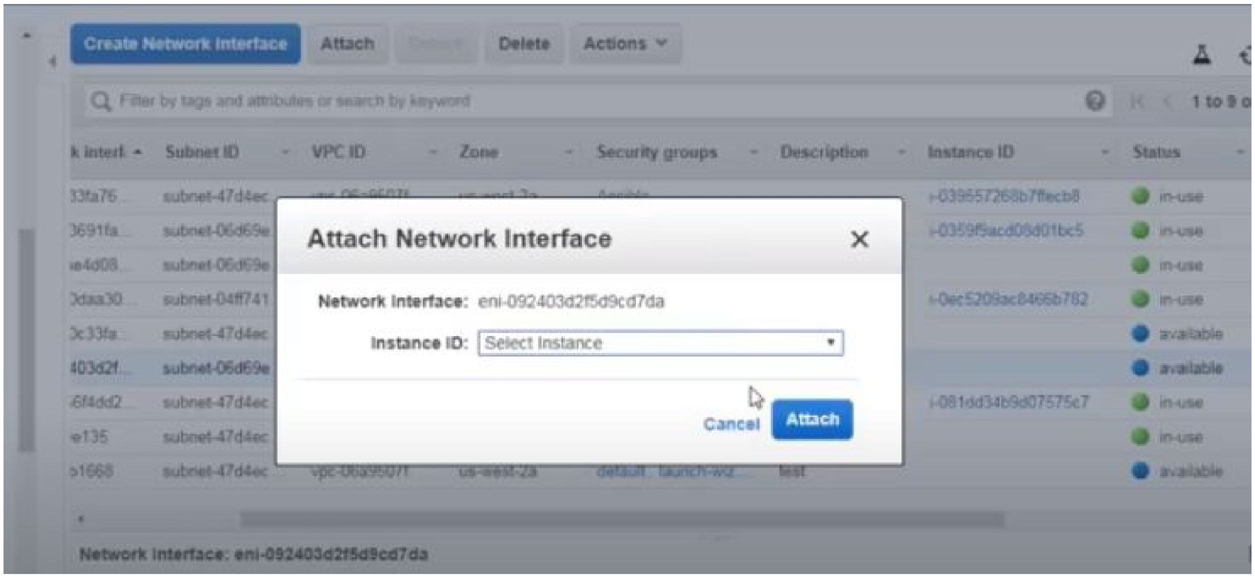
Description: Maintenance

Subnet: subnet-06d69e3e36d0931c2 us-west-2c | ft-208

Private IP: auto assign

Security groups: sg-0fb9c268c9f1ecd33 - QT-1
sg-0709644bc51d58e64 - default

Cancel Yes, Create



Attach Network Interface

Network Interface: eni-092403d2f5d9cd7da

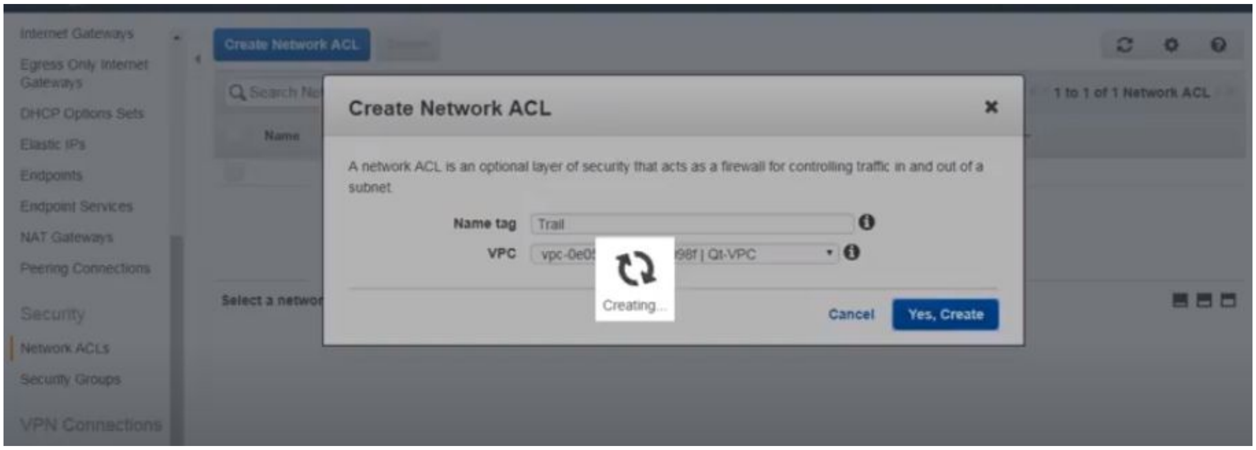
Instance ID: Select Instance

Cancel Attach

Network Interface: eni-092403d2f5d9cd7da

Security group(stateful) we are giving to the network interface so we can secure our ec2 instance so we can deny service attacks for unnecessary traffic .in sg we need only inbound setup.

NACL(stateless) network access control list which operate security in subnet level
So the 1st layer network interface for which we have a security group,here we write rules to only allow.
The 2nd layer is the subnet for which we use NACL,here we write rules for both allow and deny.,for nacl we need to setup both inbound and outbound



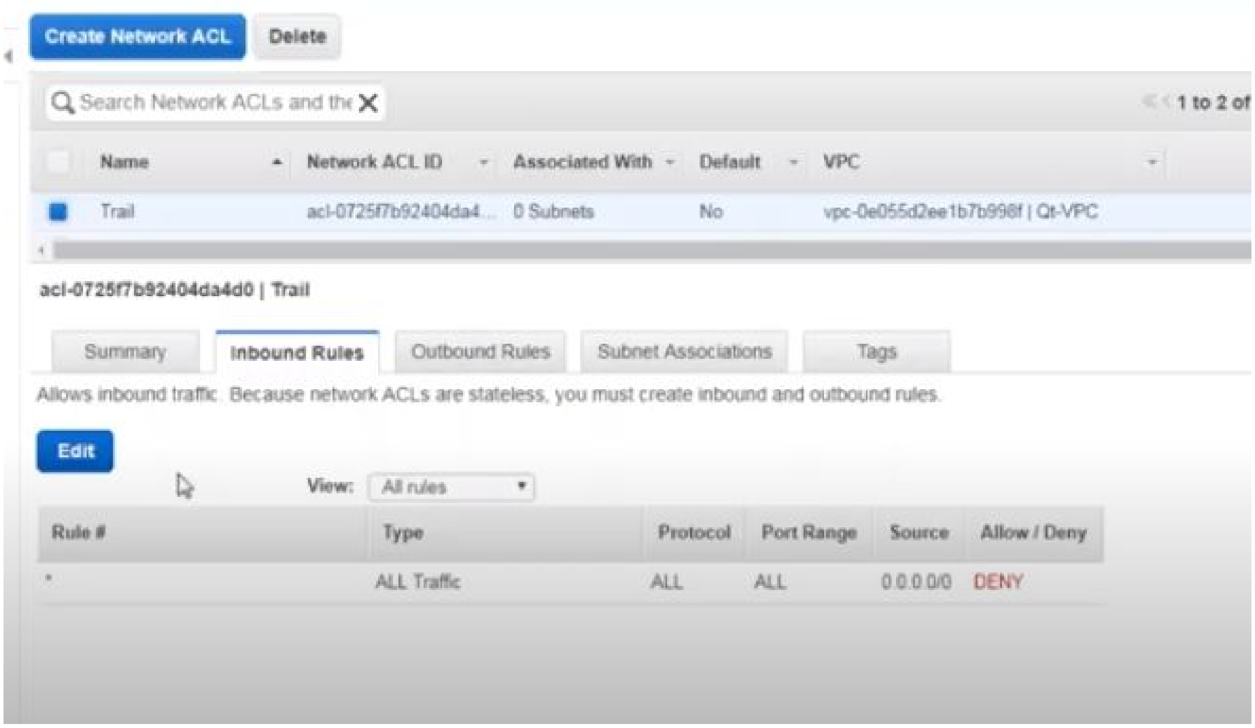
Create Network ACL

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: Trail

VPC: vpc-0e05 ... 98f | Qt-VPC

Rule will have priority based on number,lower the number higher the priority



Name	Network ACL ID	Associated With	Default	VPC
Trail	acl-0725f7b92404da4...	0 Subnets	No	vpc-0e055d2ee1b7b998f | Qt-VPC

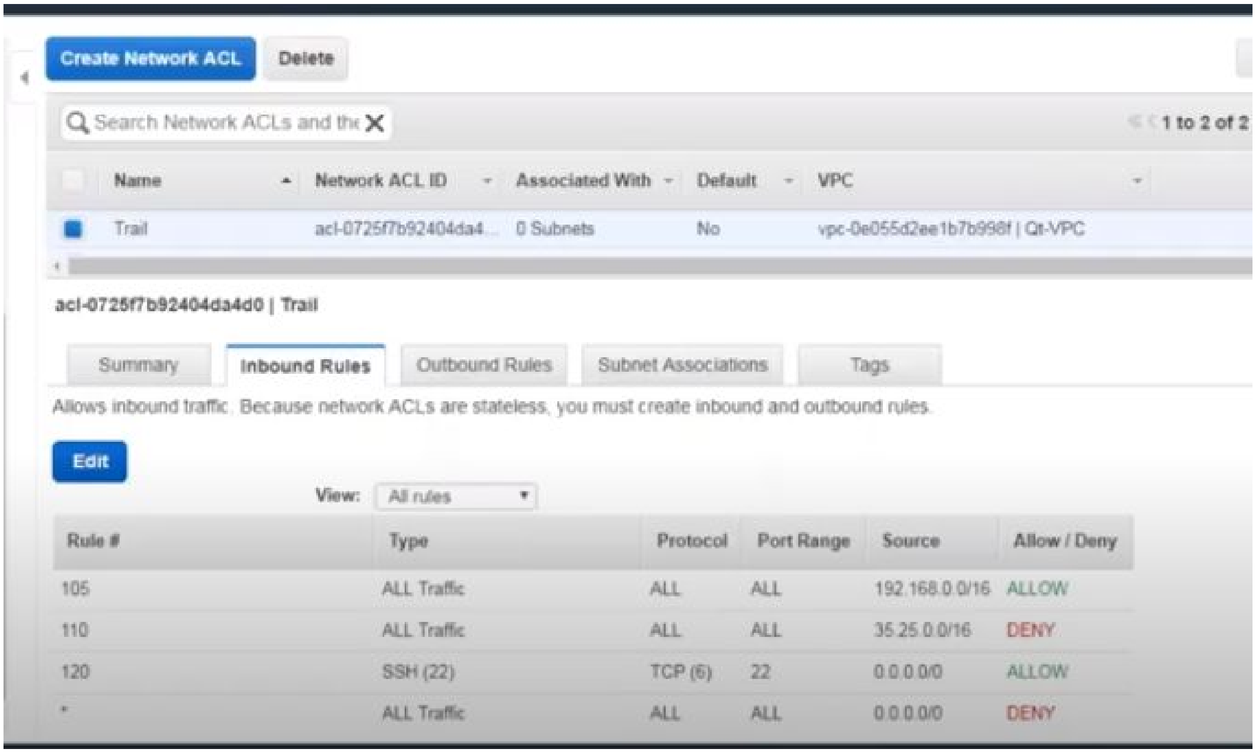
acl-0725f7b92404da4d0 | Trail

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
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

We can restrict traffic from particular ip which is unwanted for denial of service attack

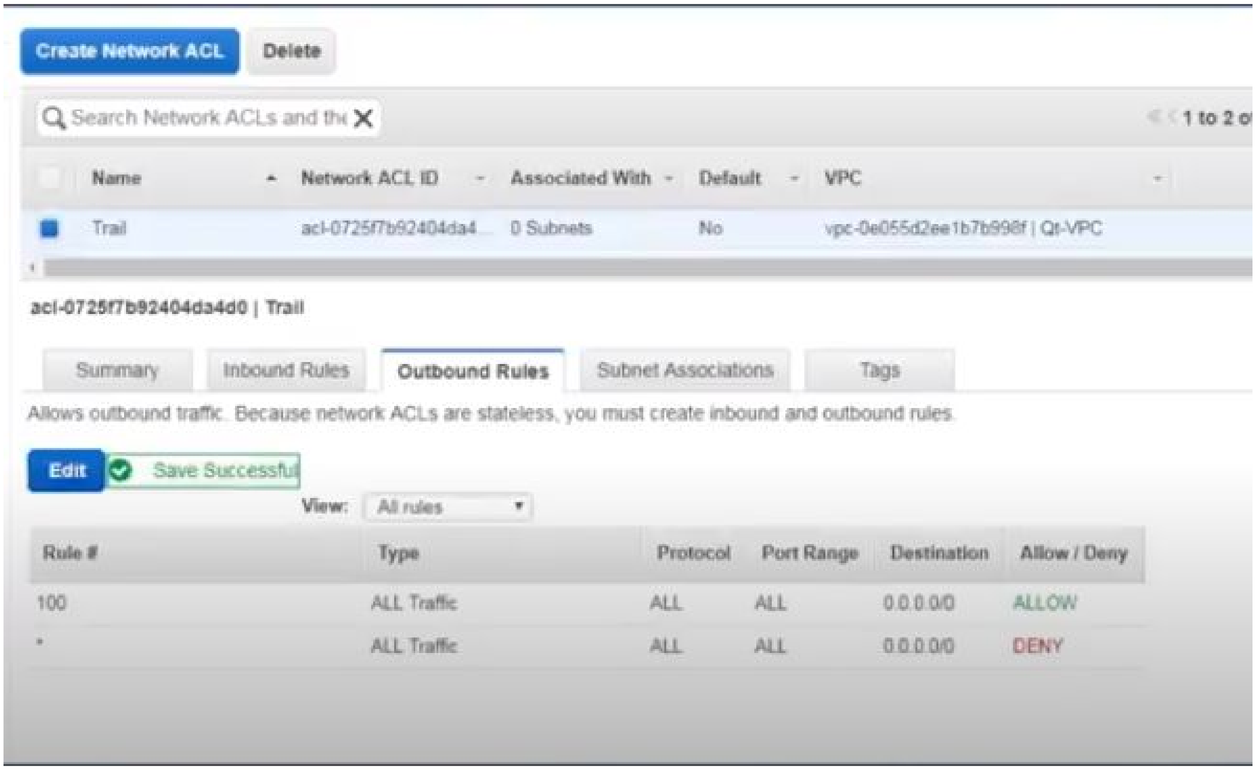


Name	Network ACL ID	Associated With	Default	VPC
Trail	acl-0725f7b92404da4...	0 Subnets	No	vpc-0e055d2ee1b7b998f | Qt-VPC

acl-0725f7b92404da4d0 | Trail

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

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
105	ALL Traffic	ALL	ALL	192.168.0.0/16	ALLOW
110	ALL Traffic	ALL	ALL	35.25.0.0/16	DENY
120	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY



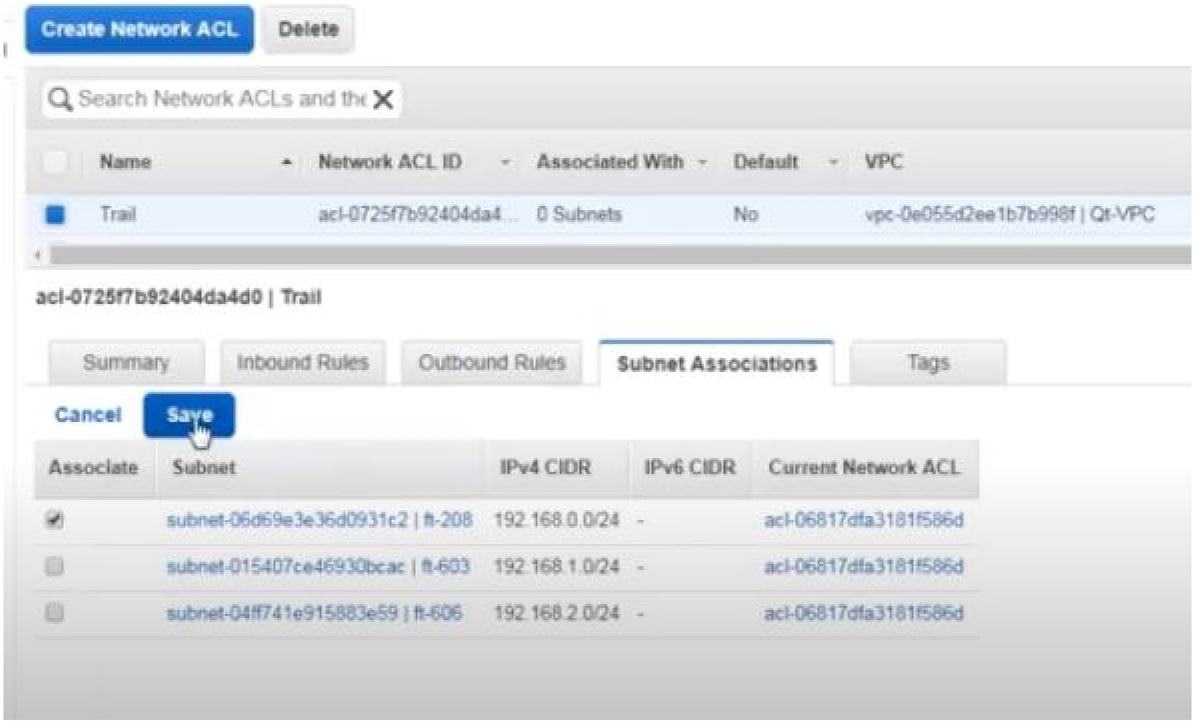
Name	Network ACL ID	Associated With	Default	VPC
Trail	acl-0725f7b92404da4...	0 Subnets	No	vpc-0e055d2ee1b7b998f | Qt-VPC

acl-0725f7b92404da4d0 | Trail

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

Save Successful

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

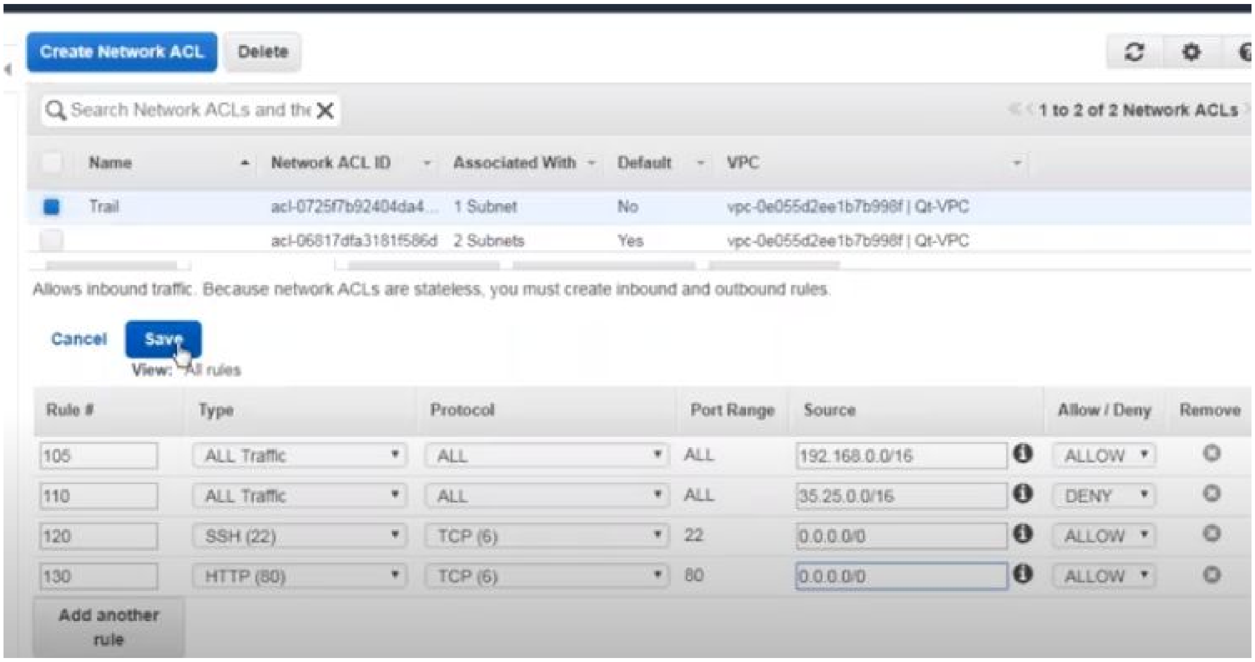


	Name	Network ACL ID	Associated With	Default	VPC
☑	Trail	acl-0725f7b92404da4...	0 Subnets	No	vpc-0e055d2ee1b7b998f | Qt-VPC

acl-0725f7b92404da4d0 | Trail

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Network ACL
☑	subnet-06d69e3e36d0931c2 | ft-208	192.168.0.0/24	-	acl-06817dfa3181f586d
□	subnet-015407ce46930bcac | ft-603	192.168.1.0/24	-	acl-06817dfa3181f586d
□	subnet-04ff741e915883e59 | ft-606	192.168.2.0/24	-	acl-06817dfa3181f586d

Subnet association



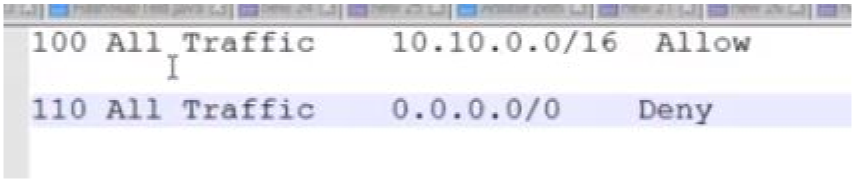
	Name	Network ACL ID	Associated With	Default	VPC
☑	Trail	acl-0725f7b92404da4...	1 Subnet	No	vpc-0e055d2ee1b7b998f | Qt-VPC
□		acl-06817dfa3181f586d	2 Subnets	Yes	vpc-0e055d2ee1b7b998f | Qt-VPC

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

Rule #	Type	Protocol	Port Range	Source	Allow / Deny	Remove
105	ALL Traffic	ALL	ALL	192.168.0.0/16	ALLOW	○
110	ALL Traffic	ALL	ALL	35.25.0.0/16	DENY	○
120	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW	○
130	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW	○

Default nacl is allow all both inbound and outbound(*)

Default security group is allow 22 port allow everything apart from that other block



```
100 All Traffic     10.10.0.0/16  Allow

110 All Traffic     0.0.0.0/0    Deny
```

here allow only 10. Network other all blocked