

# **AWS-VPC**

**Ques 1. When to use Elastic IP over Public IP**

**Ans 1.**

- Use case:

Elastic IP is used when you are working on a long time project and configuration of IP sometimes consumes more time.

Public IP is used when you are working on small projects and running 2-3 servers. Here in this situation you make use of IP for a short time.

- Do remember one thing if you have elastic IP in your account and it's not in use, then you will be charged for it.
- Elastic IP addresses are used by AWS to manage its dynamic cloud computing services. Within the AWS infrastructure, customers have virtual Private cloud. Within the VPCs, users have instances. The Elastic IP address is what is used to advertise the data within the instance to the public internet.

**Ques 2. Valid IP Ranges for LAN, Implication of using Public IP ranges for Private Network.**

**Ans 2.**

192.168.0.0 - 192.168.255.255 (65,536 IP addresses)

172.16.0.0 - 172.31.255.255 (1,048,576 IP addresses)

10.0.0.0 - 10.255.255.255 (16,777,216 IP addresses)

**Ques 3.** List down the things to keep in mind while VPC peering.

**Ans 3.**

1. Choosing the proper VPC configuration for your organization's needs
2. Choosing a CIDR block for your VPC implementation
3. Isolating your VPC environments
4. Best practices for securing your AWS VPC implementation
5. Creating your disaster recovery plan
6. Traffic control and security
7. Keep your data close
8. Determining the NAT instance type
9. ELB on Amazon VPC

**Ques 5.** Differentiate between NACL and Security Groups.

**Ans 5.**

Security Group	NACL (Network Access Control List)
It supports only <b>allow</b> rules, and by default, all the rules are denied. You cannot deny the rule for establishing a connection.	It supports both <b>allow and deny</b> rules, and by default, all the rules are denied. You need to add the rule which you can either allow or deny it.
It is a <b>stateful</b> means that any changes made in the inbound rule will be automatically reflected in the outbound rule. For example, If you are allowing an incoming port 80, then you also have to add the outbound rule explicitly.	It is a <b>stateless</b> means that any changes made in the inbound rule will not reflect the outbound rule, i.e., you need to add the outbound rule separately. For example, if you add an inbound rule port number 80, then you also have to explicitly add the outbound rule.
It is associated with an EC2 instance.	It is associated with a subnet.
All the rules are evaluated before deciding whether to allow the traffic.	Rules are evaluated in order, starting from the lowest number.
Security Group is applied to an instance only when you specify a security group while launching an instance.	NACL has applied automatically to all the instances which are associated with an instance.
It is the first layer of defense.	It is the second layer of defense.

Ques 6. Implement a 2-tier vpc with following requirements:

1. Create a private subnet, attach NAT, and host an application server(Tomcat)
2. Create a public subnet, and host a web server(Nginx), also proxypass to Tomcat from Nginx

After Implementing this on AWS, create an architecture diagram for this use case.

Note: For hosting Nginx in public subnet, use Elastic IP.

Ans 6. First we have to make a VPC then create two subnets one is for private and other is for public  
When ever we are creating the NAT we need the Elastic IP

Create subnet Actions

search: t34ak Add filter

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID
vaibhav1c	subnet-0c169b103f20655c	available	vpc-01d9bca1ea53f9ce9	10.0.102.0/24	251	-	us-east-1c	use1-az2
t34ak-private	subnet-0dba4ee75a08a389d	available	vpc-01d9bca1ea53f9ce9	10.0.48.0/20	4090	-	us-east-1f	use1-az5

Subnet: subnet-0dba4ee75a08a389d

Description Flow Logs Route Table Network ACL Tags Sharing

Edit route table association

Route Table: rtb-0373d7dd075f2ff88 | t34ak-Private-Route

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-0d7338eb7ed8f54f7

## Creating NAT with Elastic IP

Elastic IP address allocated.  
Elastic IP address 52.45.130.234

Associate this Elastic IP address

EC2 > Elastic IP addresses

Elastic IP addresses (1/1)

Filter Elastic IP addresses

Public IPv4 address: 52.45.130.234 Clear filters

✓	Name	Public IPv4 address	Allocation ID	Associated Instance ID	Private IP address	Associat
✓		52.45.130.234	eipalloc-01b7aefed0713b0c	-	-	-

-----

NAT Gateways > Create NAT Gateway

### Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. [Learn more.](#)

Subnet\* subnet-062a1eaac2376ac86

Elastic IP Allocation ID\* eipalloc-01b7aefed0713b0c

Allocate Elastic IP address

\* Required

Cancel Create a NAT Gateway


## Now we have to launch the instance

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details [Edit AMI](#)

 **Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-07ebfd5b3428b6f4d**  
Ubuntu Server 18.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).  
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	--	Low to Moderate

Security Groups [Edit security groups](#)

**Security group name** launch-wizard-163  
**Description** launch-wizard-163 created 2020-02-24T17:26:39.032+05:30

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
This security group has no rules				

Instance Details [Edit instance details](#)

To access the instance with the private IP we have to access it with the Instance launch details with which it is attach with public subnet

```
ubuntu@ip-10-0-0-253:~$ ssh -i "T34aK.pem" ubuntu@10.0.63.53
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

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

System information as of Tue Feb 25 04:58:15 UTC 2020

System load:  0.02               Processes:    93
Usage of /:   20.4% of 7.69GB    Users logged in:  0
Memory usage: 28%               IP address for eth0: 10.0.63.53
Swap usage:   0%

 * Multipass 1.0 is out! Get Ubuntu VMs on demand on your Linux, Windows or
   Mac. Supports cloud-init for fast, local, cloud devops simulation.

   https://multipass.run/

7 packages can be updated.
7 updates are security updates.

Last login: Tue Feb 25 04:56:07 2020 from 10.0.0.253
ubuntu@ip-10-0-63-53:~$ service tomcat9 status
● tomcat9.service - Apache Tomcat 9 Web Application Server
   Loaded: loaded (/lib/systemd/system/tomcat9.service; enabled; vendor preset:
   Active: active (running) since Mon 2020-02-24 12:17:39 UTC; 16h ago
     Docs: https://tomcat.apache.org/tomcat-9.0-doc/index.html
   Main PID: 22281 (java)
     Tasks: 34 (limit: 1152)
    CGroup: /system.slice/tomcat9.service
            └─22281 /usr/lib/jvm/default-java/bin/java -Djava.util.logging.config
```

## 2. Create a public subnet, and host a web server(Nginx), also proxypass to Tomcat from Nginx

-Now we have to create a public subnet and also have to attach the IGW(internet Gateway) to that public subnet.

Create route table Actions

search: t34ak Add filter 1 to 3 of 3

Name	Route Table ID	Explicit subnet associatio	Edge associations	Main	VPC ID	Owner
t34ak-Privat...	rtb-0373d7dd075f2ff88	-	-	No	vpc-01d9bca1ea53fdce9 [...]	187632318301
t34ak-Publi...	rtb-0b022abe431ead1fa	-	-	Yes	vpc-01d9bca1ea53fdce9 [...]	187632318301
t34ak-Publi...	rtb-0c580c7690f56ec5e	-	-	No	vpc-01d9bca1ea53fdce9 [...]	187632318301

Route Table: rtb-0c580c7690f56ec5e

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-03a02a50d44d4bf60	active	No

## Now we have to launch Instance with the public subnet

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details [Edit AMI](#)

Free tier eligible **Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-07ebfd5b3428b6f4d**  
Ubuntu Server 18.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).  
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security group name: launch-wizard-163  
Description: launch-wizard-163 created 2020-02-24T17:26:39.032+05:30

Type	Protocol	Port Range	Source	Description
This security group has no rules				

Instance Details [Edit instance details](#)



Now we have to ssh in to that public INSTANCE then we have to install the the nginx

```
fahad@fahad ~/Downloads <master*>
➤ ssh -i "T34aK.pem" ubuntu@100.26.148.157
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

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

System information as of Tue Feb 25 04:53:33 UTC 2020

System load:  0.08               Processes:           92
Usage of /:   17.6% of 7.69GB    Users logged in:    0
Memory usage: 18%               IP address for eth0: 10.0.0.253
Swap usage:   0%

* Multipass 1.0 is out! Get Ubuntu VMs on demand on your Linux, Windows or
  Mac. Supports cloud-init for fast, local, cloud devops simulation.

  https://multipass.run/

7 packages can be updated.
7 updates are security updates.

Last login: Mon Feb 24 12:19:53 2020 from 182.71.160.186
ubuntu@ip-10-0-0-253:~$ service nginx status
● nginx.service - A high performance web server and a reverse proxy se
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor
   Active: active (running) since Mon 2020-02-24 12:22:46 UTC; 16h ago
     Docs: man:nginx(8)
  Main PID: 10978 (nginx)
    Tasks: 2 (limit: 1152)
   CGroup: /system.slice/nginx.service
           └─10978 nginx: master process /usr/sbin/nginx -g daemon on;
              └─10979 nginx: worker process
```

For proxy passing we have to change the conf file

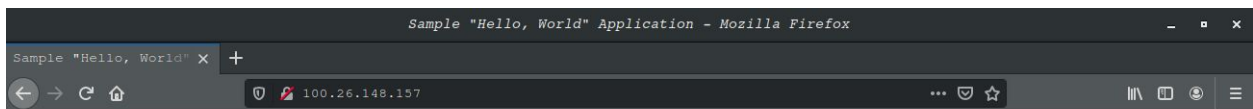
```
root /var/www/html;

# Add index.php to the list if you are using PHP
index index.html index.htm index.nginx-debian.html;

server_name _;

location / {
    # First attempt to serve request as file, then
    # as directory, then fall back to displaying a 404.
    proxy_pass http://10.0.63.53:8080/sample/;
    try_files $uri $uri/ =404;
}
```

After proxypassing it is redirecting to the tomcat page



Architecture diagram for this use case