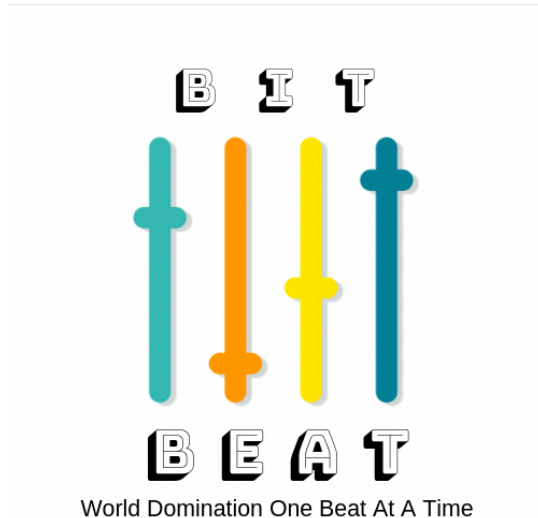


Lab 3: Creating NAT Gateway to provide internet in private subnet instance

Version: 1.0

READ ME



BitBeat is a new startup that is planning to take the record industry and the world by storm with its new product **BitBanger**, a web-based music mixer app.

As a new member of the **BitBeat** infrastructure team, you will need a variety of skills to assist in the growth of the startup. As the company is using many internal servers like DBServers with internet access. The company wants to use NAT Gateway to provide the internet access securely to these private subnet instances without exposing their public IPs. In this way, company will also save the cost for creating public IPs. NAT instance also provides facility similar to NAT gateway but, **BitBeat** does not want to use it because the NAT gateway provides high availability and a better bandwidth comparison to NAT instance.

BitBeat has hired you to setup their infrastructure, you've already gathered their requirements and are ready to get started.



BEFORE GETTING STARTED

Here's some important information to know before starting this hands-on activity.

Activity time: 240 min

Requirements: You must have an AWS Educate account. If you have not registered for an AWS Educate account, follow the instructions provided on [this page](#).

Getting help: If you experience any issues as you complete this activity, please ask your instructor

Lab 3: Creating NAT Gateway to provide internet in private subnet instance

Version: 1.0



DID YOU KNOW

You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances. Each gateway that you create can handle up to 10 GBps of bursty TCP, UDP and ICMP traffic and is managed by Amazon.

Task overview:

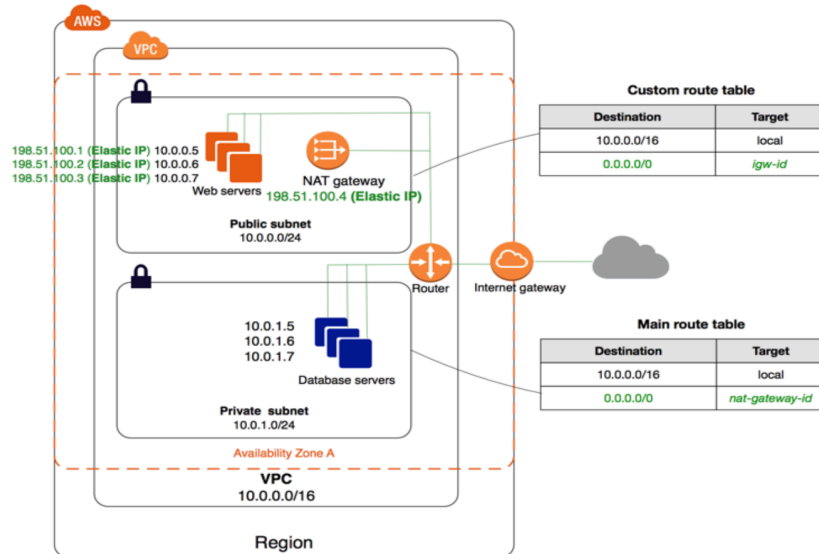
Configure a (Network address translation) NAT gateway to allow traffic to the internet or other AWS services from instances within our private VPC subnet.

Task objectives:

- Creating VPC
- Creating public subnet
- Creating private subnet
- Enabling Auto Assign IP for public subnet
- Creating and attaching internet gateway
- Creating and Configure route table
- Launching EC2 instance as a Webserver in public subnet
- Launching EC2 instance as a DBServer in private subnet
- Establishing connection between DBServer and Webserver
- Creating and Attaching NAT gateway in public subnet

Lab 3: Creating NAT Gateway to provide internet in private subnet instance

Version: 1.0



Learning outcomes

Once you've completed this activity you should be able to:

- Create VPC, Public and Private Subnet.
- Create Internet gateway
- Create NAT gateway.
- Create Route table for rules to provide internet access.
- Launch EC2 instances in public and private subnet
- Create and Attach NAT gateway in public subnet



Let's Get Started!

Lab 3: Creating NAT Gateway to provide internet in private subnet instance

Version: 1.0



DID YOU KNOW

VPC service mainly provides separate virtual cloud with desired IP range and gateways. When you create a subnet, it automatically gets associated with the main route table for the VPC. By default, the main route table doesn't contain a route to an internet gateway. It sends internet traffic from the instances in the private subnet to the NAT gateway. The NAT gateway sends the traffic to the internet gateway using the NAT gateway's Elastic IP address as the source IP address.

Follow the below steps to create NAT Gateway for private subnet instance.

1. Creating VPC

- Choose VPC from AWS services, click on **create VPC**.
- Enter the name of VPC as **BitVPC**, **10.0.0.0/16** in **IPv4 CIDR block**, select **amazon provided IPv6 CIDR block** from IPv6 CIDR block, **us-east-1** from availability zone and click on **create**.

2. Creating Public subnet

- Select subnet under navigation an of VPC, click on create subnet.
- Choose **BitVPC** VPC ID and provide subnet name as **10.0.1.0-public**, select US East(N. Virginia)/us-east-1a as a availability zone, type **10.0.1.0/24** in **IPv4 CIDR block**.

3. Creating Private subnet

- Select subnet under navigation an of VPC, click on create subnet.
- Choose **BitVPC** VPC ID and provide subnet name as **10.0.2.0-private**, select US East(N. Virginia)/us-east-1b as a availability zone, type **10.0.2.0/24** in **IPv4 CIDR block**.

4. Enabling Auto Assign IP for public subnet

- Select created public subnet 10.0.1.0-public.

Lab 3: Creating NAT Gateway to provide internet in private subnet instance

Version: 1.0

- b. Click on **action**, choose **modify auto assign IP settings** then check mark **Enable auto-assign public IPv4 address**.

5. Creating and Attaching Internet Gateway

- a. Open the **VPC dashboard**.
- b. In the navigation pane, choose **Internet Gateways**, type the name **bit-itgw** click on **Create internet gateway**.
- c. Select the internet gateway that you just created, and then choose **Actions, Attach** to the VPC.
- d. Select **BitVPC** VPC from the list, choose **Attach internet gateway**.

6. Creating and configuring Route Table

- a. Choose **Route Tables** from VPC dashboard, click on **Create Route Table**.
- b. In the Create Route Table dialog box, optionally name this route table **PublicRoute**, select the VPC **BitVPC**, and then choose **Yes, Create**.
- c. Select the custom route table that just created. On the **Routes** tab, choose **Edit routes, Add route**, and add the following routes as necessary. Choose **Save** when you're done.
 - Define two routes for **IPv4** and **IPv6** traffic, specify **0.0.0.0/0** and **::/0** in the Destination box, and select the **internet gateway ID** in the **Target** list shown in figure 1 .
- d. On the **Subnet Associations** tab, choose **Edit**, select the **Associate check box** for the public subnet, and then choose **Save**.

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local	active	No	
2600:1f18:113a:bc00::/56	local	active	No	
0.0.0.0/0	igw-058d8ad92d3ae6197		No	✕
::/0	igw-058d8ad92d3ae6197		No	✕

Add route

* Required

Cancel Save routes

Figure: 1

Lab 3: Creating NAT Gateway to provide internet in private subnet instance

Version: 1.0

7. Launching EC2 instance as a Webserver in public subnet

- Open **EC2** dashboard, click on **Launch instance**.
- Select **Amazon Linux 2 AMI**, choose type **t2.micro**, click on **Next:Configure instance Details**.
- Choose **BitVPC** under **Network** and **10.0.1.0-public** from **subnet**, Keep **Enable** in **Auto-assign public IP**.
- Write the below code in **user data** under **Advanced Details** then click on **Next:Storage**, **Next:Add Tags**.

This is #bash.

```
#!/bin/bash
yum -y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello, This is webserver running in
AWS! </h1></html>' > /var/www/html/index.html
```

- Enter **Name** in Key and **WebServer** in Value, Click on **Next:Configure Security Group**.
- Select **create a new security group** with name **WebDMZ**. Click **Add Rule**, enter type **SSH** in type and **0.0.0.0/0** in source.
- Again, **Add Rule**, enter type **HTTP** in type and **0.0.0.0/0** in source, click on **Review and Launch**, **Launch**.
- Choose **Create a new key**, enter the name of key **bitkey**, Click on **Download Key Pair** and store the key at safe place and provide the permission by running below command in terminal.

chmod 400 key

- After launching instance, click on **view instances**.

8. Launching EC2 instance as a DBServer in private subnet

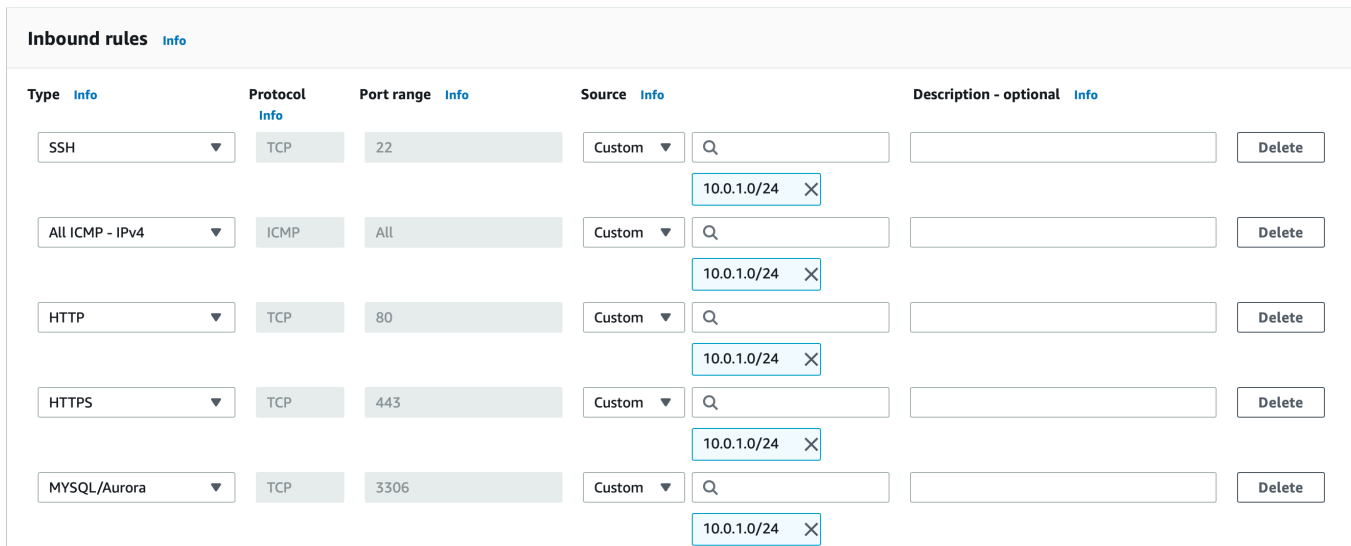
- Open **EC2** dashboard, click on **Launch instance**.
- Select **Amazon Linux 2 AMI**, choose type **t2.micro**, click on **Next:Configure instance Details**.
- Choose **BitVPC** under **Network** and **10.0.2.0-private** from **subnet**, Keep **Disable** in **Auto-assign public IP** then click on **Next:Storage**, **Next:Add Tags**.
- Enter **Name** in Key and **DBServer** in Value, Click on **Next:Configure Security Group**.
- Select default security group from **an existing security group**, click on **Review and Launch**, **Launch**.
- Choose **bitkey** from existing key pair, check mark on acknowledge, **view instances**.

Lab 3: Creating NAT Gateway to provide internet in private subnet instance

Version: 1.0

9. Establishing connection between DBServer and Webserver

- Choose **Security Group** under **Network & Security**, click on **Create Security Group**,
- Enter **DBSG** in **Security Group name** and **Description**, Select **BitVPC**, click on **Add rule** under **inbound rules** and add SSH, All ICMP- IP4, HTTP, HTTPS, MYSQL/Aurora and enter the Public subnet CIDR address 10.0.1.0/24 as shown in below figure 2 and click on create security group.
- Select the DBServer instance click on **Actions, Security, Change Security Group**.
- Add** above created security group **DBSG** and **remove default** security group and **save** these changes.



Type	Protocol	Port range	Source	Description - optional	Actions
SSH	TCP	22	Custom 10.0.1.0/24		Delete
All ICMP - IPv4	ICMP	All	Custom 10.0.1.0/24		Delete
HTTP	TCP	80	Custom 10.0.1.0/24		Delete
HTTPS	TCP	443	Custom 10.0.1.0/24		Delete
MYSQL/Aurora	TCP	3306	Custom 10.0.1.0/24		Delete

Figure: 2



Wait for both EC2 Instance State to display as **running**

Lab 3: Creating NAT Gateway to provide internet in private subnet instance

Version: 1.0

Test 1

1. Check the connection between WebServer and DBServer. Below steps are for linux or mac users and Windows users follow the SSH login steps provided in **Secure Shell (SSH) into Amazon EC2 (PC) Activity**.

- a. Open a terminal and login with SSH into Webserver with below command.

```
ssh ec2-user@publicIPofWebServer -I key.pem
```

- b. Open another terminal and copy this key into Webserver instance.

- c. And provide the permission for this key inside the Webserver.

```
chmod 400 key
```

- d. Now login to DBServer instance from WebServer instance with below command.

```
ssh ec2-user@privateIPofDBServer-i key.pem
```

2. Check the internet connection inside the DBServer with below commands.

```
ping google.com
```

```
sudo yum install mysql
```

You see that internet is not working in this private subnet instance DBServer. To provide internet access, please follow the below steps given in another task.

Important info

Please delete this created set up once you have completed this activity successfully. You are charged for creating and using a NAT gateway in your account. NAT gateway hourly usage and data processing rates apply

Lab 3: Creating NAT Gateway to provide internet in private subnet instance

Version: 1.0

Another task

- Creating NAT Gateway** to provide internet access inside private subnet instance Create Elastic IP
 - Search for Elastic IP in navigate pane of VPC, Click on Allocate Elastic IP Address and click on Allocate.
- Select **NAT gateway** from VPC and click on **create NAT gateway**. Provide the name **BitNATgw** for this, select **public subnet** and created **Elastic IP** and click on **create NAT gateway**.
- Now navigate main Route tables and add NAT gateway and choose created **BitNATgw** NAT gateway.

Test 2

Now check the again the internet access following the same steps mentioned in Test1.

You will get below output once internet is working.

```
[[ec2-user@ip-10-0-2-154 ~]$ ping google.com
PING google.com (172.217.7.142) 56(84) bytes of data:
64 bytes from iad30s08-in-f142.1e100.net (172.217.7.142): icmp_seq=1 ttl=112 time=2.38 ms
64 bytes from iad30s08-in-f142.1e100.net (172.217.7.142): icmp_seq=2 ttl=112 time=1.79 ms
64 bytes from iad30s08-in-f142.1e100.net (172.217.7.142): icmp_seq=3 ttl=112 time=1.80 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt: min/avg/max/mdev = 1.700/1.699/2.380/0.378 ms
```

Important info

You should be login to DBServer with its private IP from Webserver successfully. If there is any connection issue, please check the security groups.



DID YOU KNOW

To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside. You must also specify an Elastic IP address to associate with the NAT gateway when you create it. The Elastic IP address cannot be changed after you associate it with the NAT Gateway. After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point internet-bound traffic to the NAT gateway. This enables instances in your private subnets to communicate with the internet.

Great Job!

Lab 3: Creating NAT Gateway to provide internet in private subnet instance

Version: 1.0

Let's review

You have completed the activity and have successfully launched EC2 instances in public and private instances and provided internet access to private subnet instance with NAT Gateway and configuring Route table. In this activity you:

- Created VPC, Public and Private Subnet.
- Created Internet gateway
- Created NAT gateway.
- Created Route table for rules to provide internet access.
- Launched WebServer and DBServer EC2 instances in public and private subnet
- Create and Attach NAT gateway in public subnet

Test your knowledge

1. What is the purpose of NAT Gateway? _____
2. Why do you prefer NAT Gateway than NAT instance? _____
3. Why do you use Elastic IP for NAT gateway? _____
4. Maximum how much bursty TCP, UDP and ICMP traffic can be managed by Amazon? _____
5. Write the CIDR block for VPC and subnets which you used in above created activity? _____
6. Which security group did you use to set up a connection between WebServer and DBServer instance, explain in terms of rules? _____
7. Write True and False for below statements.
 - a. We launch NAT Gateway in private subnet.
 - b. NAT instance is highly available.
 - c. Main route table does not contain a route to an internet gateway.

Lab 3: Creating NAT Gateway to provide internet in private subnet instance

Version: 1.0

Bonus activity – Cleaning up this set up

1. Select **DBServer** and **WebServer EC2** in EC2 service, click on **terminate instance** under **instate state**.
2. Navigate **NAT Gateway**, select **BitNATgw**, click on **Delete NAT gateway**, type **delete** in dialogue box.
3. Navigate **internet Gateway**, select **bit-itgw**, click on **Delete Internet Gateway**.
4. Navigate **VPC**, select **BitVPC**, choose **Delete VPC** under **Action**, type **delete** in dialogue box to confirm.
5. Select **Elastic IP**, Click on **Disassociate Elastic IP address** under **Actions** and **confirm Disassociate, Release Elastic IP address**.