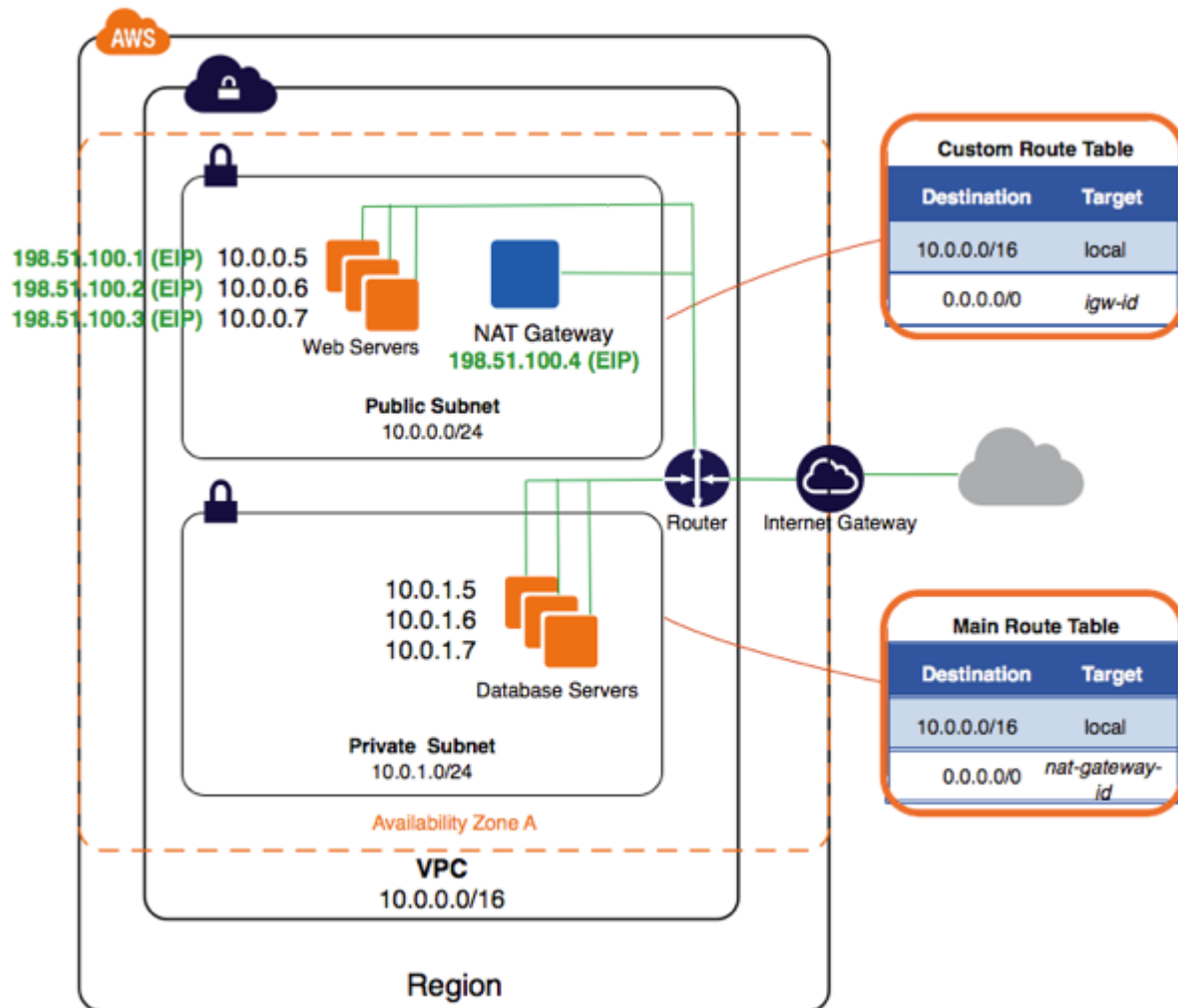


## VPC with Public and Private Subnets (NAT)



You can use the VPC wizard to create the VPC, subnets, and NAT gateway for scenario 2. If you want to use an existing Elastic IP address for your NAT gateway, ensure that it's not currently associated with another instance or network interface. The NAT gateway is automatically created in the public subnet of your VPC.

### To implement scenario 2 with a NAT gateway

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **VPC Dashboard, Start VPC Wizard**.

3. Choose the second option, **VPC with Public and Private Subnets**, and **Select**.
4. On the **Step 2** page of the wizard, you can specify names for your VPC and subnets, and leave the default values for the VPC CIDR block, the subnet CIDR blocks, Availability Zone, endpoints, DNS hostnames, hardware tenancy, and ClassicLink settings.
5. In the **Specify the details of your NAT gateway** section, specify an Elastic IP address. When you are done, choose **Create VPC**.

Because the WebServerSG and DBServerSG security groups reference each other, create all the security groups required for this scenario before you add rules to them.

### To create the WebServerSG and DBServerSG security groups









1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **Security Groups, Create Security Group**.
3. Specify `WebServerSG` as the name of the security group, and provide a description. For **VPC**, select the ID of the VPC you created and choose **Yes, Create**.
4. Choose **Create Security Group** again.
5. Specify `DBServerSG` as the name of the security group, and provide a description. For **VPC**, select the ID of your VPC and choose **Yes, Create**.

### To add rules to the WebServerSG security group

1. Select the WebServerSG security group that you created. The details pane displays the details for the security group, plus tabs for working with its inbound and outbound rules.
2. On the **Inbound Rules** tab, choose **Edit** and add rules for inbound traffic as follows:
  - a. Choose **Type, HTTP**. For **Source**, enter `0.0.0.0/0`.
  - b. Choose **Add another rule, Type, HTTPS**. For **Source**, enter `0.0.0.0/0`.
  - c. Choose **Add another rule, Type, SSH**. For **Source**, enter your network's public IP address range.
  - d. Choose **Add another rule, Type, RDP**. For **Source**, enter your network's public IP address range.
  - e. Choose **Save**.

Summary **Inbound Rules** Outbound Rules Tags

Cancel Save

Type	Protocol	Port Range	Source	Remove
HTTP (80)	TCP (6)	80	0.0.0.0/0	 
HTTPS (443)	TCP (6)	443	0.0.0.0/0	 
SSH (22)	TCP (6)	22	192.0.2.0/24	 
RDP (3389)	TCP (6)	3389	192.0.2.0/24	 

Add another rule

3. On the **Outbound Rules** tab, choose **Edit** and add rules for outbound traffic as follows:
  - a. Locate the default rule that enables all outbound traffic and choose **Remove**.
  - b. Choose **Type, MS SQL**. For **Destination**, specify the ID of the DBServerSG security group.
  - c. Choose **Add another rule, Type, MySQL**. For **Destination**, specify the ID of the DBServerSG security group.
  - d. Choose **Add another rule, Type, HTTPS**. For **Destination**, enter 0.0.0.0/0.
  - e. Choose **Add another rule, Type, HTTP**. For **Destination**, enter 0.0.0.0/0.
  - f. Choose **Save**.

### To add the recommended rules to the DBServerSG security group

1. Select the DBServerSG security group that you created. The details pane displays the details for the security group, plus tabs for working with its inbound and outbound rules.
2. On the **Inbound Rules** tab, choose **Edit** and add rules for inbound traffic as follows:
  - a. Choose **Type, MS SQL**. For **Source**, specify the ID of your WebServerSG security group.
  - b. Choose **Add another rule, Type, MYSQL**. For **Source**, specify the ID of your WebServerSG security group.
  - c. Choose **Save**.
3. On the **Outbound Rules** tab, choose **Edit** and add rules for outbound traffic as follows:
  - a. Locate the default rule that enables all outbound traffic and choose **Remove**.
  - b. Choose **Type, HTTP**. For **Destination**, enter 0.0.0.0/0.
  - c. Choose **Add another rule, Type, HTTPS**. For **Destination**, enter 0.0.0.0/0.
  - d. Choose **Save**.

You can now launch instances into your VPC.

### To launch an instance (web server or database server)

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. From the dashboard, choose **Launch Instance**.
3. Select an AMI and an instance type and choose **Next: Configure Instance Details**.
4. On the **Configure Instance Details** page, for **Network**, select the VPC that you created earlier and then select a subnet. For example, launch a web server into the public subnet and the database server into the private subnet.
5. (Optional) By default, instances launched into a nondefault VPC are not assigned a public IP address. To be able to connect to your instance in the public subnet, you can assign a public IP address now, or allocate an Elastic IP address and assign it to your instance after it's launched. To assign a public IP address now, ensure that you choose **Enable** from the **Auto-assign Public IP** list. You do not need to assign a public IP address to an instance in the private subnet.

#### Note

You can only assign a public IP address to a single, new network interface with the device index of eth0. For more information, see [Assigning a Public IP Address During Launch](#).

6. On the next two pages of the wizard, you can configure storage for your instance, and add tags. On the **Configure Security Group** page, choose the **Select an existing security group** option, and select one of the security groups you created earlier (**WebServerSG** for a web server or **DBServerSG** for a database server). Choose **Review and Launch**.
7. Review the settings that you've chosen. Make any changes that you need and choose **Launch** to choose a key pair and launch your instance.

If you did not assign a public IP address to your instance in the public subnet in step 5, you will not be able to connect to it. Before you can access an instance in your public subnet, you must assign it an Elastic IP address.

### To allocate an Elastic IP address and assign it to an instance

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.

2. In the navigation pane, choose **Elastic IPs**.
3. Choose **Allocate New Address**.
4. Choose **Yes, Allocate**.

#### **Note**

If your account supports EC2-Classic, first choose **EC2-VPC** from the **Network platform** list.

5. Select the Elastic IP address from the list and choose **Actions, Associate Address**.
6. In the **Associate Address** dialog box, select the network interface or instance. For **Private IP address**, select the corresponding address to associate the Elastic IP address with and choose **Yes, Associate**.