AWS Cloud Quest  
**Task 4. Networking Concepts**Review and change VPC network configurations to fix a connection issue.

|  |  |
| --- | --- |
| Person | Welcome to our banking headquarters. I'm so glad you came to help. |
| Me | I'm always happy to help. What can I do for you? |
| Person | We recently migrated our services to the cloud, but we've noticed some connectivity issues with our Amazon EC2 instances and Databases. The EC2 instances cannot connect to the internet, and our databases are unable to communicate with our instances. |
| Me | Have you checked you VPC settings? In your route tables, you can check that an internet gateway is attached and that the VPC is set to allow outside traffic. |
| Person | Is that complicated? I'm little concerned. We need these changes to happen immediately. We can't afford to wait too long for network updates. |
| Me | I understand your concern. Security group and route table modifications are applied immediately. Also, setting up an internet gateway for internet access can be done in minutes. |
| Person | That's great. But how did my engineer create a VPC without internet access? Isn't that included? |
| Me | On AWS, by default, VPCs are not configured with internet connectivity. When you create a new VPC, you have the option to enable internet access for all or part of the VPC. This allows you to customize your network security configuration according to your requirements. |
| Person | Interesting. I will check with our engineers later. This sounds like a great solution to these urgent issues.  Will you help solve our VPC connectivity issues? |
| Me | Accepted |
| Person | Perfect! Thanks for assisting with our networking issues. |

**1. Learn:**

**Networking Concepts:** Review and change VPC network configurations to fix a connection issue.

**1. AWS Global Infrastructure Overview:** This solution uses a common network architectural configuration that allows only internet traffic to reach publicly exposed AWS resources.

**2. Amazon VPC Overview:** A webserver and DB server are deployed within a Virtual Private Cloud (VPC), which is logically isolated virtual network within the AWS cloud.

**3. Amazon VPC Concepts:** The webserver is deployed inside a publicly exposed subnet and is assigned a public IP address to make it accessible from the internet.

**4. Amazon VPC Security:** The Security Group for the webserver is configured to allow access through port 80, the default port for HTTP connections.

**5. Amazon VPC - Internet Connectivity:** A route table is configured within the VPC that allows internet traffic, through an internet gateway, to the public subnet only.

**6. Amazon VPC - Internet Connectivity:** The DB server resides in a private subnet, which does not have a route table that allows access from the internet.

**7. Amazon VPC Security:** For the webserver to connect to the DB server, the DB server's security group must be configured to allows a connection on port 3306.

**2. Plan:**

**Practice Lab Goals**

Step-by-step guided learning:

* Explore the components that comprise a virtual private cloud (VPC).
* Configure a route table attached to a subnet within a VPC.
* Configure an internet gateway inside a VPC.
* Configure inbound rules within a security group to control access.

**DIY**

Build on what you have learned.

* Change the security group rules to allow traffic, over port 3306, into the DB server.

**3. Practice**

**Step 2:**

1. On the top navigation bar, review the Region selector to confirm that the Region is set to N. Virginia (us-east-1).
2. In the Services search box, type: ec2
3. In the search results, under Services, click EC2.
4. Go to the next step

**Step 3:**

1. In the left navigation pane, click Instances.
2. In the Instances section, choose the check box to select the Web Server instance.
3. On the Details tab, under Public IPv4 address, click the copy icon to copy the provided address.

The public IP addresses in your practice lab will not match what is displayed in the screenshot examples.

1. Go to the next step.

The Public IP address is an IPv4 address that is reachable from the internet. You can use the public addresses for communication between instances and the internet.

**Step 4:**

1. In a new browser tab (or window) address bar, paste the IP address that you just copied and press Enter.

- After about a minute, a site timeout message should appear.

1. To solve this issue, return to the Amazon EC2 console browser tab (not shown).
2. Go to the next step.

**Step 5:**

1. Review to confirm that the Web Server instance is still selected.
2. Click the Networking tab.
3. Review the Public and Private IPv4 addresses.
4. Go to the next step.

Using Amazon Virtual Private Cloud (Amazon VPC), you can launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own datacenter, with the benefits of using the scalable infrastructure of AWS.

**Step 6:**

1. Under Subnet ID, click the provided ID.

The subnet ID opens the Amazon VPC console in a new browser tab (or window).

1. Go to the next step.

A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet. Each subnet must reside entirely within one Availability zone and cannot span zones.

**Step 7:**

1. In the Subnets section, choose the check box to select the subnet name that starts with network-concepts.
2. Click the Route table tab.
3. Next to Route table, click the link name that contains web-server-netSubnet1.
4. Go to the next step.

A **route table** contains a **set of rules**, named routes, that are used to determine where network traffic from your subnet or gateway is directed. Use a **public subnet** for **internet connected resources** and a **private subnet** for **resources not connected to the internet**.

**Step 8:**

1. In the Route tables section, choose the check box to select the route table name that starts with network-concepts.
2. Click the Routes tab.
3. Review the two route table entries.

One route sends local traffic to the local network only. The other route sends all other traffic to the internet through a NAT gateway.

1. Click Edit routes.
2. Go to the next step.

A **NAT gateway** is a **Network Address Translation** service. With NAT gateway, instances in a private subnet can connect to services outside your VPC. External services, however, cannot initiate a connection with those instances.

**Step 9:**

1. To delete the NAT gateway from the route table, click Remove.

By removing this route, the instances in this subnet can no longer connect to external services.

1. Go to the next step.

The CIDR naming convention 0.0.0.0/0 represents all possible IPv4 addresses (::/0 for IPv6)

**Step 10:**

1. Click Add route.
2. For Destination, on the dropdown list, choose 0.0.0.0/0.
3. For Target, choose Internet Gateway.
4. Below that, choose igw-xxxxxxx.
5. Click Save changes.
6. Go to the next step.

**An Internet Gateway serves two purposes:**

* Provide a target in your VPC route tables for internet routable traffic.
* Perform Network Address Translation (NAT) for instances that have been assigned a Public IPv4 addresses.

**Step 11:**

1. On the Routes tab, under Target, review the new internet gateway association.
   1. The subnet is now reachable from the internet.
2. Return to the Amazon EC2 console in the other browser tab.
3. Go to the next step.

An Internet Gateway is horizontally scaled, redundant, and highly available, imposing no availability risks or bandwidth constraints on network traffic. There’s no additional charge for having an Internet Gateway in your account.

It serves two main purposes:

* Provide a target in your VPC route tables for internet routable traffic.
* Perform Network Address Translation (NAT) for instances that have been assigned a Public IPv4 addresses.

**Step 12:**

1. In the Instances section, choose the check box to select the Web Server instance.
2. Click the Security tab.
3. Under Security groups, click WebServerSecurityGroup.
4. Go to the next step.

A **Security Group** is a **virtual firewall** that controls traffic to and from AWS resources.

**Step 13:**

1. In the Details section, review the security group details.
2. On the Inbound rules tab, click Edit inbound rules.
3. Go to the next step.

For each Security Group, you can add rules that control the traffic based on protocols and port numbers. Separate sets of rules exist in inbound traffic and outbound traffic.

**Step 14:**

* Click Add rule.
* Go to the next step.

When you create a VPC, it comes with a default security group. You can create additional security groups for each VPC.

**Step 15:**

1. For Type, on the dropdown list, scroll down to see the various available predefined protocols.
   1. Note the MYSQL/Aurora protocol, which you must use in the upcoming DIY section of this solution.
2. Choose HTTP.
   1. Make sure you did not choose HTTPS.
3. Go to the next step.

You can create a security group and add rules that reflect the role of the instance that is associated with the security group. For example, an instance that is configured as a web server needs security group rules that allow inbound HTTP and HTTPS access. Likewise, a database instance needs rules that allow access for the type of database, such as access over port 3306 for MySQL.

**Step 16:**

1. For Source, choose Anywhere-IPv4.
   1. In the upcoming DIY section, you must use the Source search box to find the needed security group.
2. In the warning alert (not shown), review the recommended setting.
3. Click Save rules.
4. Go to the next step.

Security groups are stateful, meaning they retain information about their interactions over time. For example, if you send a request from an instance, the response traffic for that request is allowed to reach the instance regardless of the inbound security group rules. Responses to allowed inbound traffic are allowed to leave the instance, regardless of the outbound rules.

**Step 17:**

* In the success alert, review the message.
* In the tab ribbon, click Outbound rules.
* Go to the next step.

It is a security best practice to limit inbound rules to specific IP addresses and not open to the whole wide world.

**Step 18:**

1. Review that an existing outbound rule exist allowing traffic on port 3306
   1. 3306 is the default port used by MySQL database server.
2. Click Edit outbound rules.
3. Go to the next step.

**Step 19:**

1. Click Add rule.
2. For Type, use the dropdown to choose All traffic.
3. For Destination, use the dropdown to choose the CIDR range 0.0.0.0/0.
4. Click Save rules.
5. Go to the next step.

**Step 20:**

1. Review that the Outbound security group rules were updated successfully.
2. In the left navigation pane, click Instances.
3. Go to the next step.

**Step 21:**

1. In the Instances section, choose the check box to select the Web Server instance.
2. Click the Networking tab.
3. Under Public IPv4 address, click the copy icon to copy the provided address.
   1. Do not click open address or the page will not load.
4. Go to the next step.

**Step 22:**

1. In a new browser tab (or window) address bar, paste the instance IP address that you just copied and press Enter.
   * Make sure you use HTTP, not HTTPS.
   * The address should look similar to this: http://xxx.xxx.xxx.xxx
2. Review the diagram that loads from the public IP address.
3. Review the connection from the internet to the web server.
   * A connection should be established.
4. Review the connection from the web server to the database (DB server).
   * The connection should display as failed.
5. Go to the next step.

To deploy a working Internet Gateway, the following must be completed:

* The Internet Gateway must be attached to a VPC.
* Route tables associated with your public subnet must have a route to your internet gateway.
* Security Groups associated with your VPC must allow traffic to / from the internet.
* Any instances in the VPC must have a public IP or elastic IP address assigned.