**Task: Launch EC2 with Custom Security Group (Allowing Only Your IP)**

**Name:** Abhishek Hengade

**Batch:** B-56

This guide explains how to launch an Amazon EC2 instance and configure its security group to only allow access from your specific IP address. This is a critical security practice, especially for management ports like SSH or RDP, as it prevents unauthorized access from the public internet.

**1. Understanding the Process**

An EC2 **Security Group** acts as a virtual firewall that controls inbound and outbound traffic for your instance. By default, all inbound traffic is denied. To allow traffic, you must add "inbound rules." The principle of least privilege dictates that you should only open ports to trusted sources. In this guide, we will create a rule that opens the SSH port (22) exclusively to the public IP address of your own computer.

**2. Step-by-Step Guide**

**Step 1: Begin the Instance Launch Process** Navigate to the **EC2 Dashboard** in the AWS Management Console and click the **Launch instances** button. Proceed with the initial steps of configuring your instance, such as giving it a name, selecting an Amazon Machine Image (AMI), and choosing an instance type.

**Step 2: Configure a Key Pair** In the **Key pair (login)** section, select an existing key pair or create a new one. A key pair is mandatory for securely connecting to your instance after it has launched.

**Step 3: Create a New Security Group** In the **Network settings** section, locate the **Firewall (security groups)** area. Select the **Create security group** option.

* **Security group name:** Provide a descriptive name (e.g., My-IP-Only-Access).
* **Description:** Add a clear description (e.g., Allows SSH access only from my home IP).

**Step 4: Configure the Inbound Rule for Your IP** This is the most critical step. In the **Inbound security groups rules** section, you will configure the firewall rule.

* **Type:** From the dropdown, select **SSH**. The protocol and port range (TCP, 22) will be filled automatically.
* **Source type:** By default, this might be "Anywhere" (0.0.0.0/0). Click the dropdown and select **My IP**.
* AWS will automatically detect your computer's public IP address and populate the **Source** field with it, followed by a /32 CIDR notation (e.g., 203.0.113.25/32). This /32 means the rule applies *only* to that single IP address.

**Step 5: Launch and Verify the Instance** Review the rest of your instance configuration in the summary panel. When you are ready, click the **Launch instance** button. Once the instance is in the "running" state, try to connect to it using SSH and your key pair. The connection should be successful because your IP is whitelisted. Any attempt to connect from a different network (and therefore a different IP address) will be blocked and will time out.

