**Security Group in AWS**

Cybersecurity has grown to be a crucial component of any business in the modern digital age. Access management is a fundamental element of cybersecurity. Controlling access includes deciding who has access to what resources and for what goals. The management of resource access in the cloud is done using security groups.

We shall define security groups in this article and explain how they operate and may be created in Amazon Web Services (AWS). We’ll also define a few crucial terms related to security groups, offer pertinent examples, and give step-by-step directions with screenshots.

An example of one of these features is the security group, which functions as a virtual firewall to regulate the inbound and outgoing traffic for Amazon EC2 instances or other AWS resources in a VPC. We shall go over a security group’s definition and formation in this article.

1. **Security Group**: It performs the function of a virtual firewall, managing the inbound and outbound traffic for one or more Amazon EC2 instances or other AWS services within a VPC.
2. **Inbound Rules:** These outline the types of traffic that are permitted to use the resources. It serves as a virtual firewall, controlling the traffic going in and coming out of a VPC for one or more Amazon EC2 instances or other AWS services.
3. **Outbound Rules:** These regulate the traffic that is permitted to depart from the resources. The destination for incoming traffic is dealt with by outbound rules. They may be forwarded to an alternative Security Group, a CIDR block, a single IPv4 or IPv6 address, or all three.
4. **Amazon EC2:** A web service called Amazon Elastic Compute Cloud offers scalable computation capability in the cloud. For developers, it is intended to make web-scale cloud computing simpler.
5. **VPC:**A virtual network called a virtual private cloud enables you to launch Amazon resources into a defined virtual network.
6. **CIDR:**A technique for allocating IP addresses and rerouting Internet Protocol packets is called classless inter-domain routing (CIDR).
7. **Protocol:**A protocol is a collection of guidelines that controls how two devices communicate with one another.
8. **Port:**A port on a computer serves as the communication endpoint for a particular process or service.

**Steps to Create a Security Group**

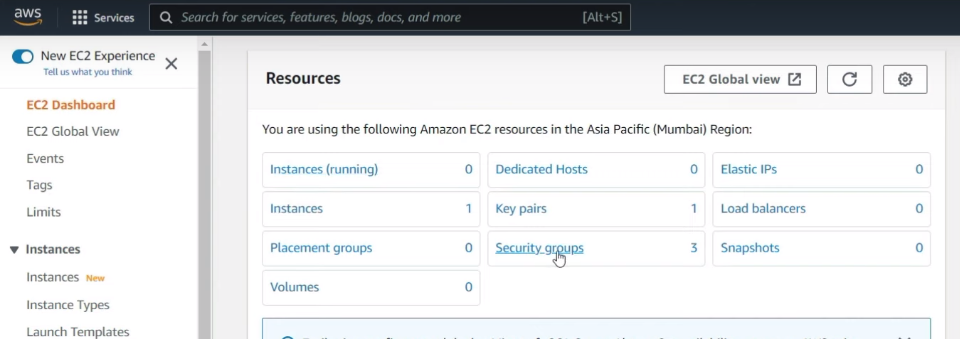
Let’s talk about how to form a security group in AWS now that we have identified certain critical terms.

**Step 1:** Visit the EC2 Dashboard after logging into the Amazon Management Console.

Go to the AWS console and sign into your account first.

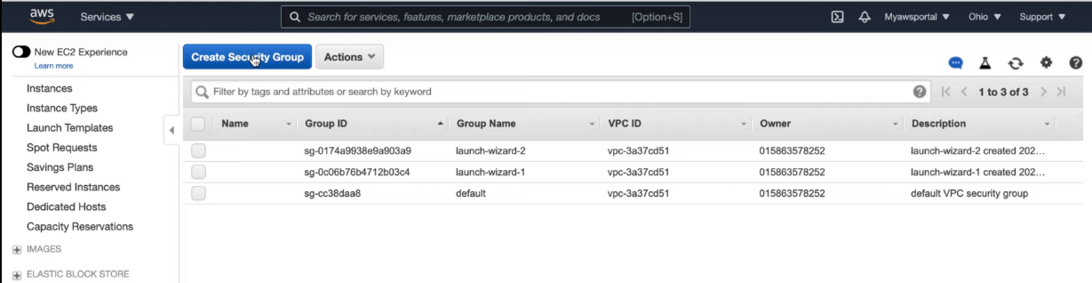
**Step 2:**Choose “Security Groups” from the panel.

Go to the EC2 dashboard from the AWS console.

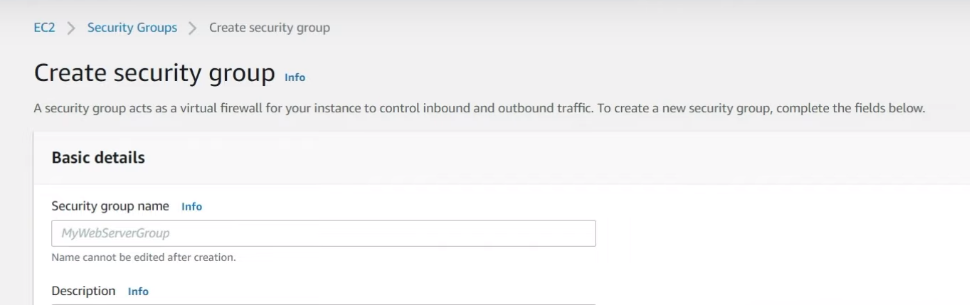


**Step 3:** Choose “Create Security Group” from the menu.

Click the “Create Security Group” button after selecting the “Security Groups” option from the left-hand menu.



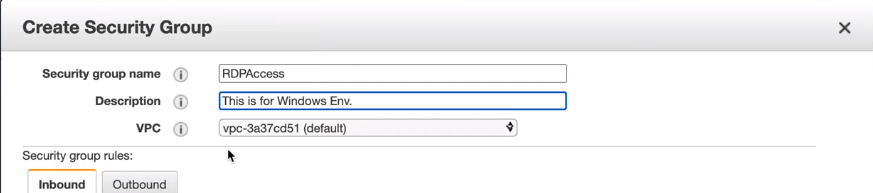
**Step 4:** Your security group’s name and description should be entered.



Insert your security group’s information, including its name, description, and VPC. For your security group, you must also provide inbound and outgoing rules.

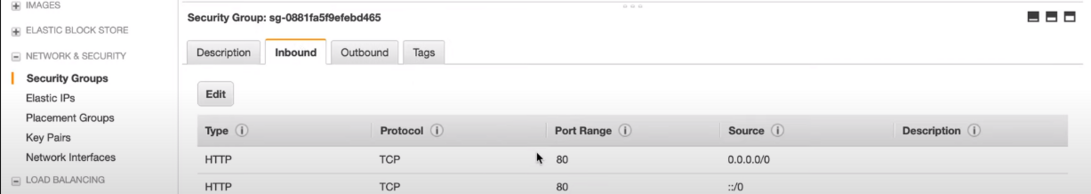
**Step 5:** Choose your choice for the VPC where the security group will be created.

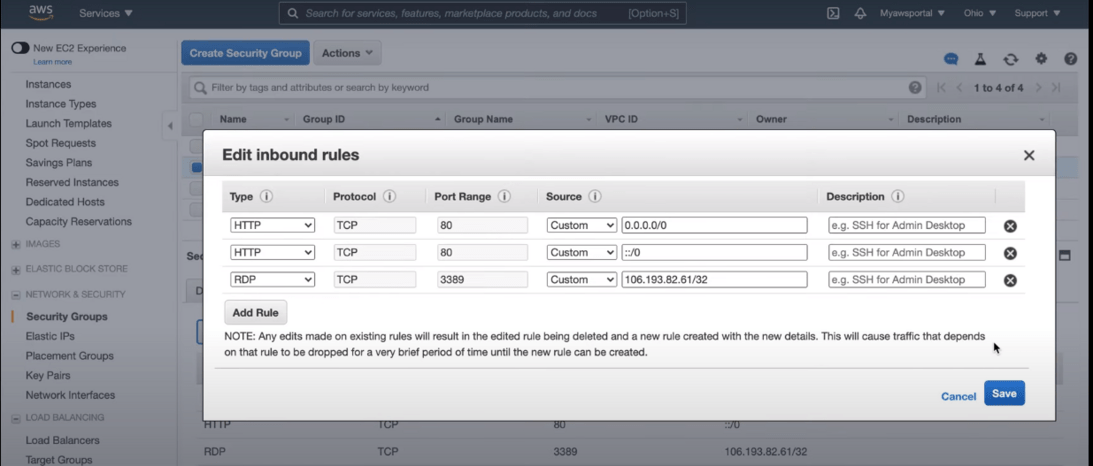
Choose the “Inbound Rules” tab, then select the “New Rule” option to establish inbound rules. The protocol, port range, source IP, and description can all be used to define rules in this area.



**Step 6:** Create inbound rules to enable access to your resources. To allow traffic from particular IP addresses or ranges, protocols, and ports, you can establish rules. Also, you can include outbound rules to manage the traffic that is permitted to leave your resources.

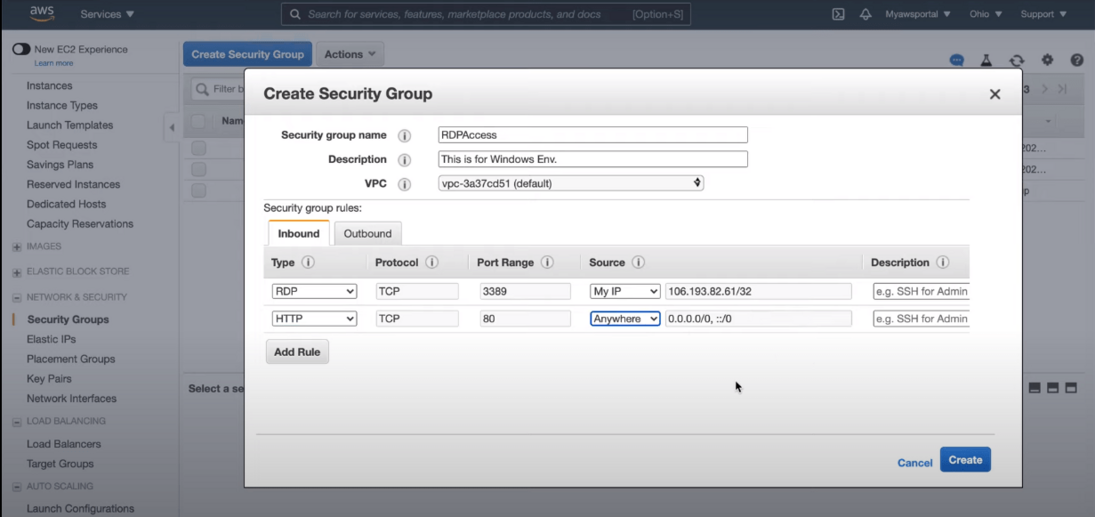
Choose the “Outbound Rules” tab, then select the “New Rule” button to set outbound rules. The protocol, port range, destination IP address, and description can all be used to build rules in this area.





**Step 7:** After reading the guidelines, use the “Create” button.

Review the options and select “Create Security Group” once you have specified the inbound and outgoing rules for your security group.



* **Note:** Inbound and outbound security Group Rules comprise four different fields: **Source**, **Protocol**, **Port Range** & **Description**.
* **Source:** Typically, this is a private IP address, a subnet mask, or another security group. If you use the “anywhere (0.0.0.0/0)” option, you can also allow access to the entire internet. The everywhere (0.0.0.0/0) value must only be used when necessary, and you should be well aware of the risks involved.
* **Protocol:**TCP is usually the default protocol and is often greyed out. But you can adjust the protocols if you’re using specially-made rules that you wrote.
* **Port Range:** Usually, port ranges are pre-filled. Still, you have the option to choose a custom port range of your choice.
* **Description:**You can add a description to the rule you’ve generated in this area. The more specific you are, the better.