**Security Groups**

**Security group rules**  
1. When you launch an instance in a VPC, you must specify a security group that's created for that VPC. After you launch an instance, you can change its security groups.  
2. By default, security groups allow all outbound traffic.  
3. Security group rules are always permissive; you can't create rules that deny access.  
4. You can add and remove rules at any time. Your changes are automatically applied to the instances that are associated with the security group.

5. Name: The name for the security group (for example, my-security-group).  
A name can be up to 255 characters in length. Allowed characters are a-z, A-Z, 0-9, spaces, and .\_-/()#,@[]+=;{}!$\*. When the name contains trailing spaces, we trim the spaces when we save the name. For example, if you enter "Test Security Group " for the name, we store it as "Test Security Group".

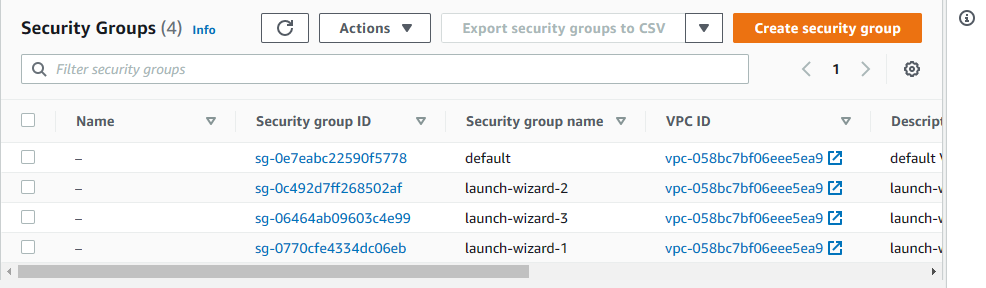
6. Protocol: The protocol to allow. The most common protocols are 6 (TCP), 17 (UDP), and 1 (ICMP).  
7. Port range: For TCP, UDP, or a custom protocol, the range of ports to allow. You can specify a single port number (for example, 22), or range of port numbers (for example, 7000-8000).  
8. ICMP type and code: For ICMP, the ICMP type and code. (if ping comes from this server we can enable this)  
9. Description: You can add a description for the rule, which can help you identify it later. A description can be up to 255 characters in length. Allowed characters are a-z, A-Z, 0-9, spaces, and .\_-:/()#,@[]+=;{}!$\*.

10. Source or destination: The source (inbound rules) or destination (outbound rules) for the traffic. Specify one of these options:  
An individual IPv4 address. You must use the /32 prefix length; for example, 203.0.113.1/32.  
An individual IPv6 address. You must use the /128 prefix length; for example, 2001:db8:1234:1a00::123/128.  
A range of IPv4 addresses, in CIDR block notation; for example, 203.0.113.0/24.  
A range of IPv6 addresses, in CIDR block notation; for example, 2001:db8:1234:1a00::/64.

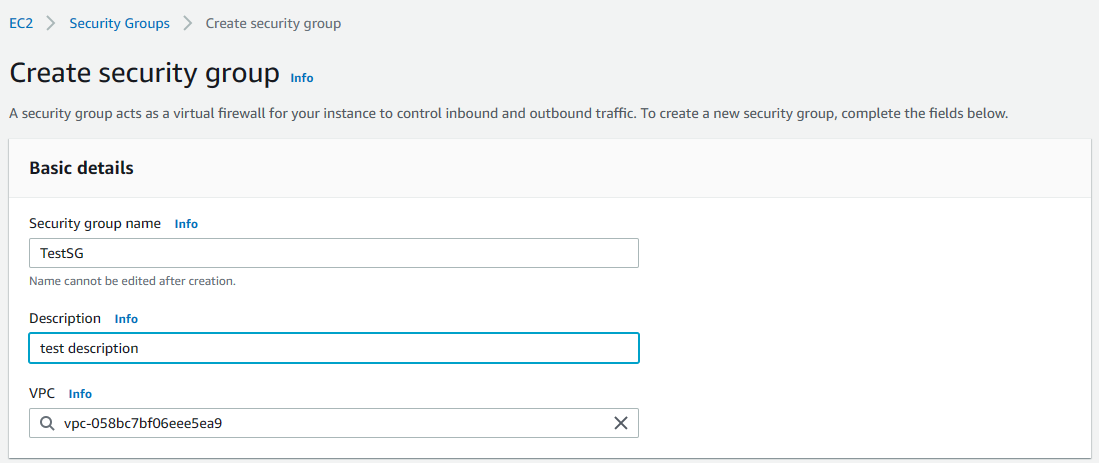
11. If there is more than one rule for a specific port, Amazon EC2 applies the most permissive rule. For example, if you have a rule that allows access to TCP port 22 (SSH) from IP address 203.0.113.1, and another rule that allows access to TCP port 22 from everyone, everyone has access to TCP port 22.  
12. Your AWS account automatically has a default security group for the default VPC in each Region. If you don't specify a security group when you launch an instance, the instance is automatically associated with the default security group for the VPC.

**Steps:**

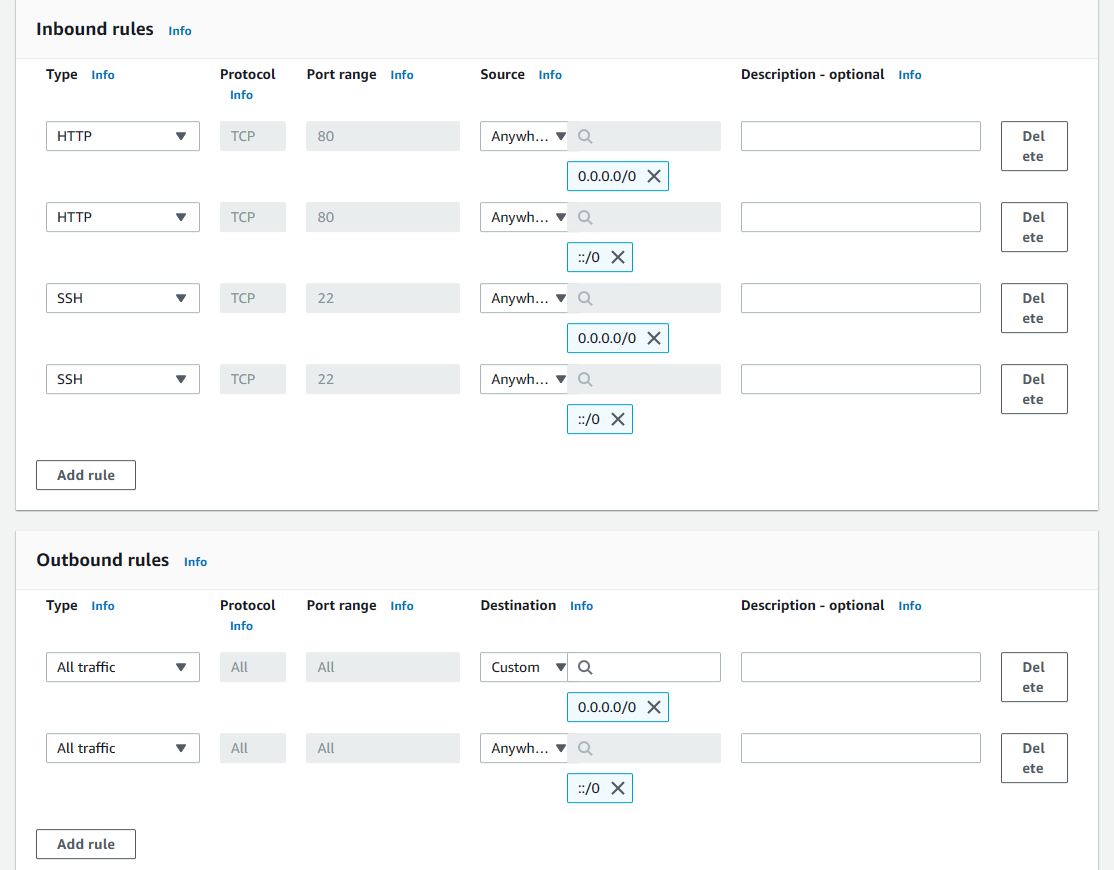
1. Navigate to Services->EC2->Network & Security->Security Groups
2. Click “Create security group”



1. Enter group name
2. Selected VPC is default VPC, we can select other VPC also.



1. Add inbound and outbound roles as we want



1. Add tags if want and click “Create security group”

