# Amazon EC2 Security Groups

A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group. When we decide whether to allow traffic to reach an instance, we evaluate all the rules from all the security groups that are associated with the instance.

### Creating a Security Group

You can create a custom security group using the Amazon EC2 console. For EC2-VPC, you must specify the VPC for which you're creating the security group.

**To create a new security group**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Security Groups**.
3. Choose **Create Security Group**.
4. Specify a name and description for the security group.
5. (EC2-VPC) For **VPC**, choose a VPC ID to create a security group for that VPC.
6. You can start adding rules, or you can choose **Create** to create the security group now (you can always add rules later).

The Amazon EC2 console enables you to copy the rules from an existing security group to a new security group.

**To copy a security group**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Security Groups**.
3. Select the security group you want to copy, choose **Actions**, **Copy to new**.
4. The **Create Security Group** dialog opens, and is populated with the rules from the existing security group. Specify a name and description for your new security group. In the **VPC** list, choose a VPC ID to create a security group for that VPC. When you are done, choose **Create**.

You can assign a security group to an instance when you launch the instance. When you add or remove rules, those changes are automatically applied to all instances to which you've assigned the security group.

After you launch an instance in EC2-Classic, you can't change its security groups. After you launch an instance in a VPC, you can change its security groups.

### Describing Your Security Groups

**To describe your security groups for EC2-VPC**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Security Groups**.
3. Select **Network Platforms** from the filter list, then choose **EC2-VPC**.
4. Select a security group. We display general information in the **Description** tab, inbound rules on the **Inbound** tab, and outbound rules on the **Outbound** tab.

### Adding Rules to a Security Group

When you add a rule to a security group, the new rule is automatically applied to any instances associated with the security group.

**To add rules to a security group**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Security Groups** and select the security group.
3. On the **Inbound** tab, choose **Edit**.
4. In the dialog, choose **Add Rule** and do the following:
   * For **Type**, select the protocol.
   * If you select a custom TCP or UDP protocol, specify the port range in **Port Range**.
   * If you select a custom ICMP protocol, choose the ICMP type name from **Protocol**, and, if applicable, the code name from **Port Range**.
   * For **Source**, choose one of the following:
     + **Custom**: in the provided field, you must specify an IP address in CIDR notation, a CIDR block, or another security group.
     + **Anywhere**: automatically adds the 0.0.0.0/0 IPv4 CIDR block. This option enables all traffic of the specified type to reach your instance. This is acceptable for a short time in a test environment, but it's unsafe for production environments. In production, authorize only a specific IP address or range of addresses to access your instance.

**Note**

If your security group is in a VPC that's enabled for IPv6, the **Anywhere** option creates two rules—one for IPv4 traffic (0.0.0.0/0) and one for IPv6 traffic (::/0).

* + - **My IP**: automatically adds the public IPv4 address of your local computer.

1. Choose **Save**.
2. For a VPC security group, you can also specify outbound rules. On the **Outbound tab**, choose **Edit**, **Add Rule**, and do the following:
   * For **Type**, select the protocol.
   * If you select a custom TCP or UDP protocol, specify the port range in **Port Range**.
   * If you select a custom ICMP protocol, choose the ICMP type name from **Protocol**, and, if applicable, the code name from **Port Range**.
   * For **Destination**, choose one of the following:
     + **Custom**: in the provided field, you must specify an IP address in CIDR notation, a CIDR block, or another security group.
     + **Anywhere**: automatically adds the 0.0.0.0/0 IPv4 CIDR block. This option enables outbound traffic to all IP addresses.

**Note**

If your security group is in a VPC that's enabled for IPv6, the **Anywhere** option creates two rules—one for IPv4 traffic (0.0.0.0/0) and one for IPv6 traffic (::/0).

* + - **My IP**: automatically adds the IP address of your local computer.

1. Choose **Save**.

### Deleting Rules from a Security Group

When you delete a rule from a security group, the change is automatically applied to any instances associated with the security group.

**To delete a security group rule**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Security Groups**.
3. Select a security group.
4. On the **Inbound** tab (for inbound rules) or **Outbound** tab (for outbound rules), choose **Edit**. Choose **Delete**(a cross icon) next to each rule to delete.
5. Choose **Save**.

### Deleting a Security Group

You can't delete a security group that is associated with an instance. You can't delete the default security group. You can't delete a security group that is referenced by a rule in another security group in the same VPC. If your security group is referenced by one of its own rules, you must delete the rule before you can delete the security group.

**To delete a security group**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Security Groups**.
3. Select a security group and choose **Actions**, **Delete Security Group**.
4. Choose **Yes, Delete**.