What are Security Groups in mCloud Firewall

Vincent (Vinnie) Curle - 2026-05-05 - mCloud

Security groups are sets of IP filter firewall rules that are applied to all project instances. They are used to define networking access to the instance. These are applied to all traffic to an instance EXCEPT for traffic on the same subnet, which is allowed by default.

Default Security Group

Each mCloud project has its own Default Security Group. As it is created, it has the following rules:

- IPv4 ALLOW all OUT
- IPv6 ALLOW all OUT
- IPv4 ALLOW all IN FROM members of the default security group
- IPv6 ALLOW all IN FROM members of the default security group
- DENY all (implicit)

All instances that are a member of this default security group will have full access to other instances that it can route to, so long as the other instance is also a member of this group.

You can add and delete rules from this group, but keep in mind any changes will apply to all members of the default group that already exist and will be created in the future.

Managing Security Groups

Creating a New Security Group

Security groups and their associated rules can be managed from the “Security Groups” section of the mCloud dashboard.

1. Go to **Project > Network > Security Groups**.
2. Click “**Create Security Group**”, enter a name and (optionally) description, then press the confirmation button.
3. You will be brought to a page where you can add/remove/edit rules for your newly created Security Group.

Applying a Security Group

A new security group will not do anything until it is applied to a network port. You can apply security either to an mCloud network port directly or through an instance.

Apply Directly to a Port.

1. Navigate to **Project > Network > Networks**.
2. Select the **name** of the network the port is on.
3. Go to the **Ports** tab.
4. Click **Edit Port** on the port you want to apply the security group to.
5. Under the **Security Groups** tab, click the plus (+) and minus (-) buttons to add/remove a security group.

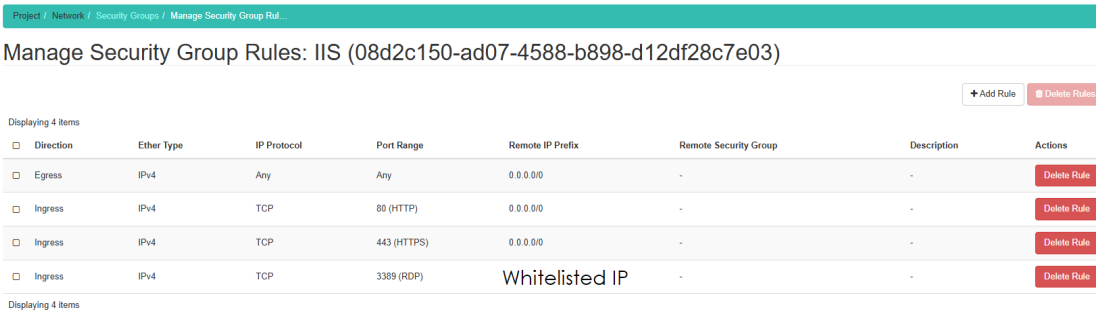
Apply Through an Instance.

1. Navigate to **Project > Compute > Instances**.
2. Click the dropdown next to the Create Snapshot button on the instance you want to add the security group to.
3. Select **Edit Port Security Groups**. This will bring you to the instance Interfaces tab.
    1. The **Edit Security Groups** option can be used instead. Applying a security group this way applies that group to every interface/port attached to the instance
4. Click **Edit Security Groups** next to the interface you want to add a security group to.
5. Click the **plus (+)** or **minus (-)** buttons to add/remove a security group.

Security Group Considerations for Internet-facing Servers

When creating security groups and rules for Internet-facing servers, the industry-standard approach is that only necessary services should be exposed to the Internet. Any sensitive services should be secured behind whitelisting.

An example ruleset for a Webserver would look something like this:



A ruleset such as this can be locked down even further, by allowing outbound traffic

to only required locations/services