Knowledgebase > mCloud > What are Security Groups in mCloud Firewall

What are Security Groups in mCloud Firewall

Vincent (Vinnie) Curle - 2025-03-05 - 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)

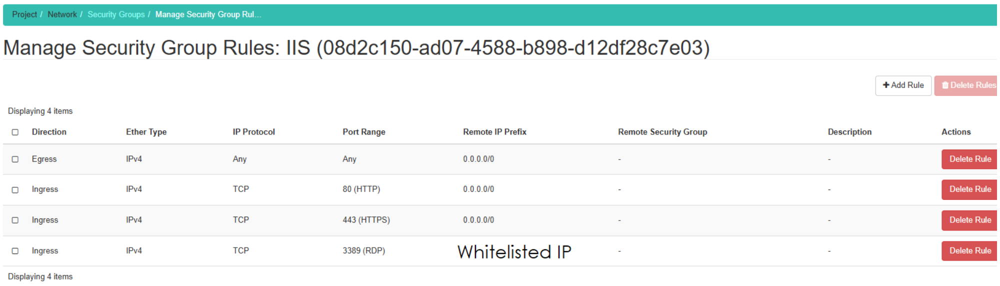
All instances that are a member of this default security group will have full access to other instances that it can route to, so long as the other instance is also a member of this group.

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.

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:

- 

  Project / Network / Security Groups / Manage Security Group Rul...

  Manage Security Group Rules: IIS (08d2c150-ad07-4588-b898-d12df28c7e03)

  + Add Rule
  Delete Rules

  Displaying 4 items

□	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
□	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
□	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0	-	-	Delete Rule
□	Ingress	IPv4	TCP	443 (HTTPS)	0.0.0.0/0	-	-	Delete Rule
□	Ingress	IPv4	TCP	3389 (RDP)	Whitelisted IP	-	-	Delete Rule

  Displaying 4 items

- A ruleset such as this can be locked down even further, by allowing outbound traffic to only required locations/services