

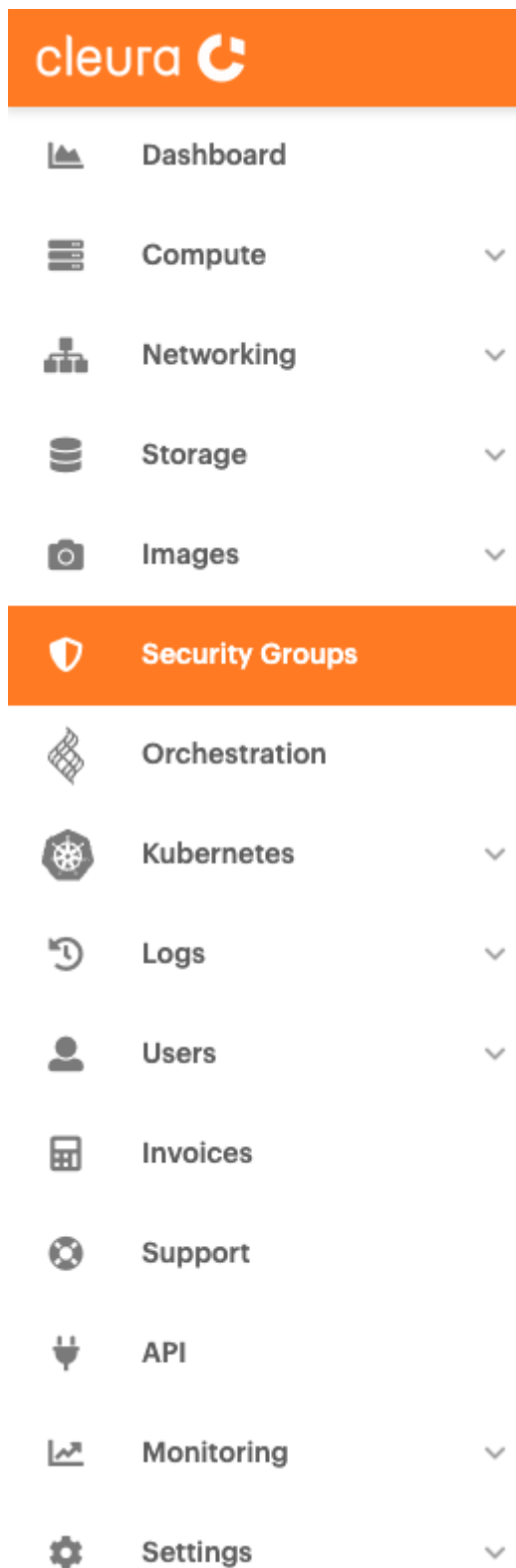
Creating security groups

By definition, security groups are *"[...] sets of IP filter rules that are applied to all project instances, which define networking access to the instance. Group rules are project specific; project members can edit the default rules for their group and add new rule sets."*


Creating a security group

Navigate to the **Cleura Cloud Management Panel** page, and log into your Cleura account. On the other hand, if you prefer to work with the OpenStack CLI, please do not forget to **source the RC file first**.

To create a security group click on *Security Groups* in the left-hand navigation menu:



and then click on *Create new Security Group* in the top-right corner:

Create new Security Group 

An alternative way to create a Security Group is by clicking on *Create ...* button in the top bar.

Now give the security group a name and description, and choose in which region to create it, then click *create*:

Create a Security Group

Name

Region

Choose Region



Description

Back



Create Another



Create

To create a security group use the following command:

```
openstack security group create <name>
```

When the command is executed successfully, you will get information regarding your new security group:

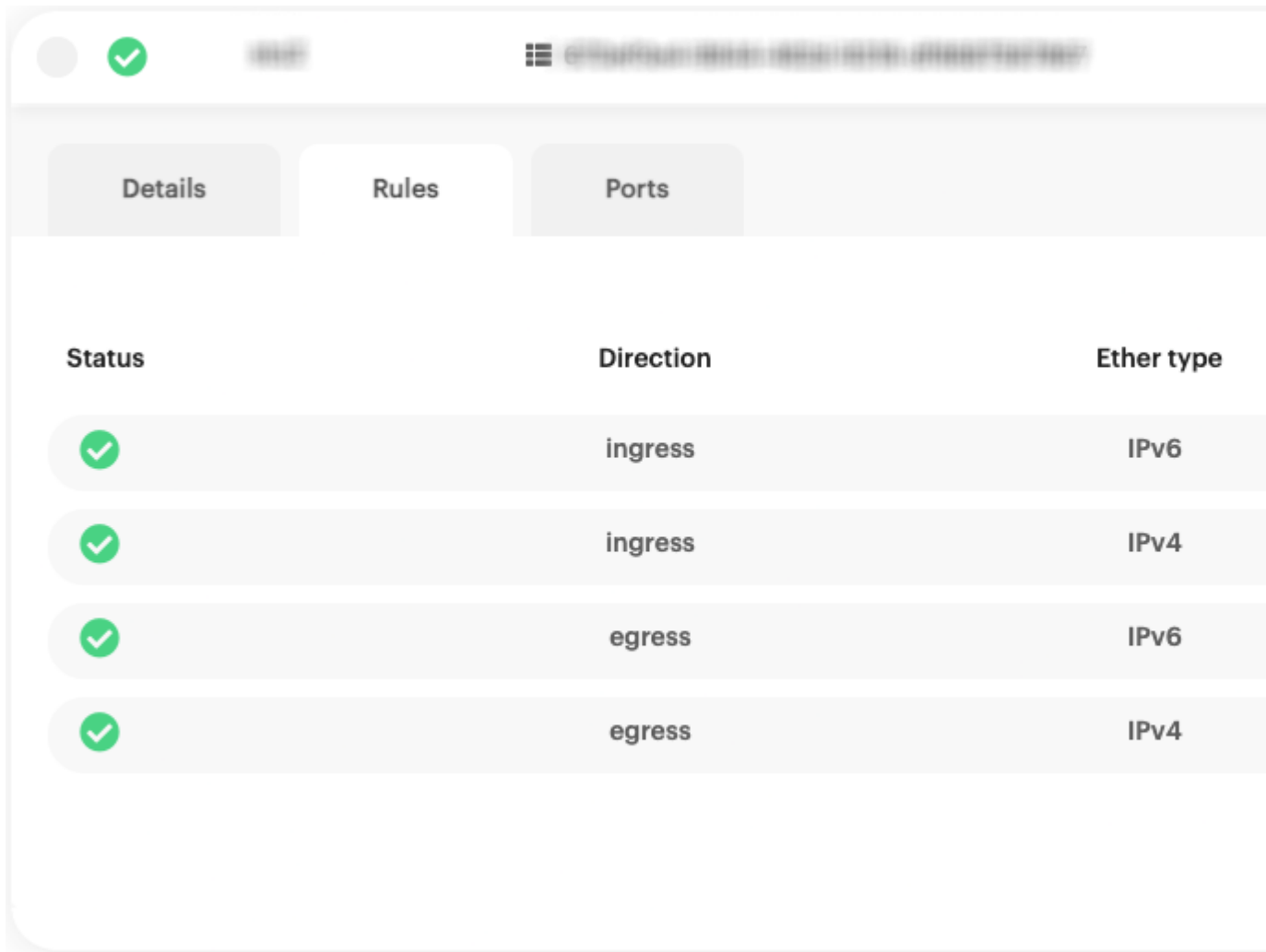
```
+-----+-----+
| Field      | Value                                     |
+-----+-----+
| created_at  | 2022-11-14T09:15:14Z                    |
| description  | <name>                                   |
| id          | 736da1d1-aa98-4da4-9ba4-2ab9aeea6a57     |
| name        | <name>                                   |
| project_id  | cb43f189f7904fb88f3bbcfa22653ab8       |
| revision_number | 1                                       |
| rules       | created_at='2022-11-14T09:15:14Z', direction='egress', ethertype='IPv4', |
|             | id='1f4c57cb-8e34-420c-a7e3-3b5625c79481', standard_attr_id='10579829', |
|             | updated_at='2022-11-14T09:15:14Z'      |
|             | created_at='2022-11-14T09:15:14Z', direction='egress', ethertype='IPv6', |
|             | id='7c2c287e-9596-42ef-a5a8-0b09e38b206a', standard_attr_id='10579832', |
|             | updated_at='2022-11-14T09:15:14Z'      |
| stateful    | True                                     |
| tags        | []                                       |
| updated_at  | 2022-11-14T09:15:14Z                    |
+-----+-----+
```

Removing default ingress rules

By default, a security group named `default` has been already created for you, allowing all traffic from any source (ingress), and to any destination (egress).

Cleura Cloud Management Panel OpenStack CLI

Click on it and select the *Rules* tab to view its rules:



Status	Direction	Ether type
✓	ingress	IPv6
✓	ingress	IPv4
✓	egress	IPv6
✓	egress	IPv4

View the details of the `default` security group using the following command:

```
openstack security group show default
```

you will get a printout similar to this:

```
+-----+-----+
| Field      | Value                                     |
+-----+-----+
| created_at  | 2022-09-12T15:00:57Z                    |
| description | Default security group                  |
| id          | 935b1317-a0c0-42e9-b68d-7cf16637df14    |
| name        | default                                 |
| project_id  | cb43f189f7904fb88f3bbcf22653ab8        |
| revision_number | 5                                       |
| rules       | created_at='2022-09-12T15:00:59Z', direction='ingress', ethertype='IPv4', |
|             | id='5e5e9f4d-1faa-492d-91f1-c105b464072b', normalized_cidr='0.0.0.0/0', |
|             | remote_ip_prefix='0.0.0.0/0', standard_attr_id='10422245',                |
|             | updated_at='2022-09-12T15:00:59Z'      |
```

```

|         | created_at='2022-09-12T15:00:59Z', direction='ingress', ethertype='IPv6', |
|         | id='86b9413a-ad23-46c4-a35e-9306945dc63c', normalized_cidr='::/0',         |
|         | remote_ip_prefix='::/0', standard_attr_id='10422248',                       |
|         | updated_at='2022-09-12T15:00:59Z'                                         |
|         | created_at='2022-09-12T15:00:57Z', direction='egress', ethertype='IPv6', |
|         | id='ad4a19ef-7fab-4eba-9982-e5b109be121c', standard_attr_id='10422242',    |
|         | updated_at='2022-09-12T15:00:57Z'                                         |
|         | created_at='2022-09-12T15:00:57Z', direction='egress', ethertype='IPv4', |
|         | id='f53b1a12-edbb-480b-910b-a71c4836346f', standard_attr_id='10422236',    |
|         | updated_at='2022-09-12T15:00:57Z'                                         |
| stateful | True                                                                       |
| tags     | []                                                                         |
| updated_at | 2022-09-12T15:00:59Z                                                    |
+-----+-----+

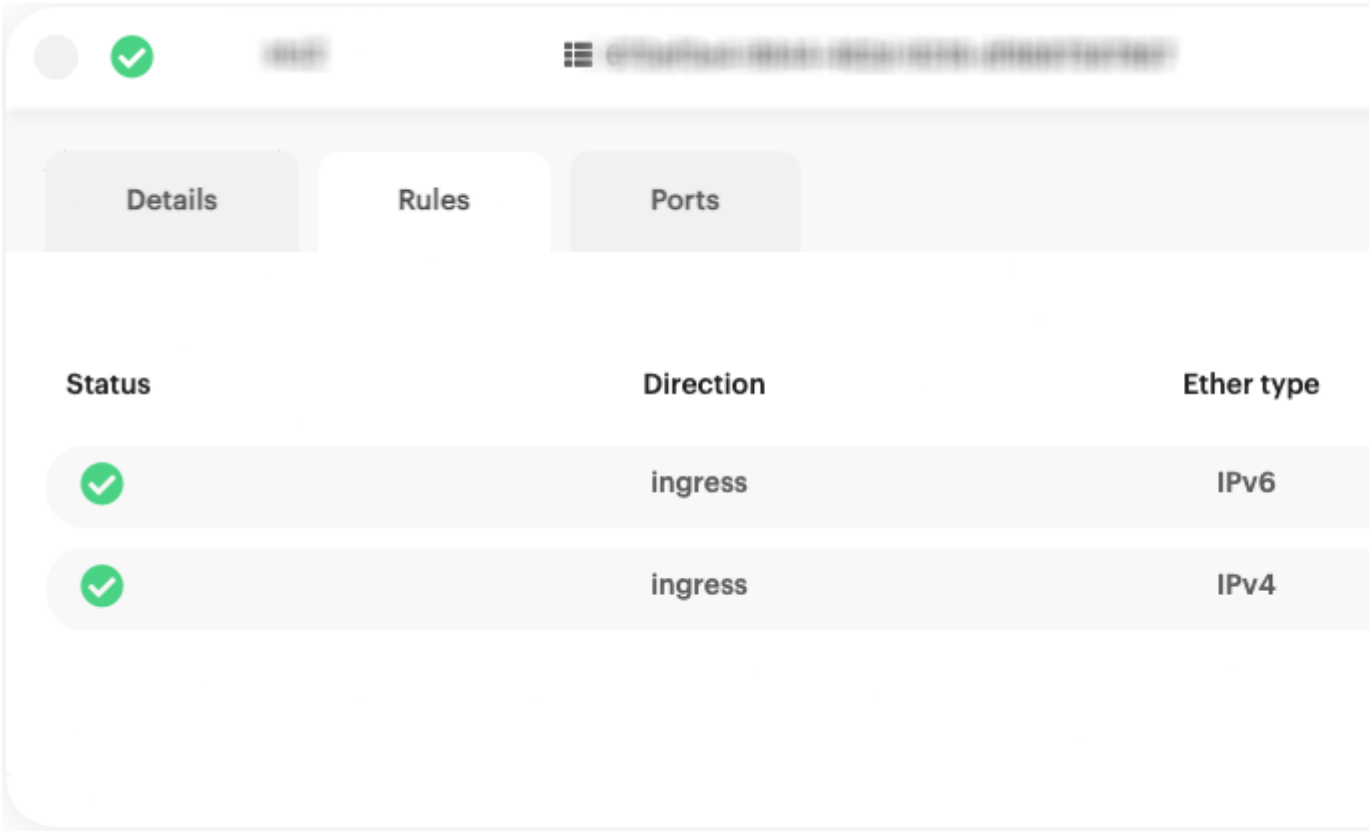
```

We recommend to either create and use a new security group other than the default one, **or** restrict ingress traffic to specific ports and sources.

If you want use the default group, **remove the two ingress rules** that allow all incoming traffic.

Cleura Cloud Management Panel **OpenStack CLI**
Click on the trashcan action button on the right-hand side for **both ingress** rules.

Your default or newly created security group rules will now looks like this:



To view the rules use the following command:

```
openstack security group rule list default
```

The printout will be similar to this:

ID	IP Protocol	Ethertype	IP Range	Port Range	Direction	Remote Security Group	Remote Address
5e5e9f4d-1faa-492d-91f1-c105b464072b	None	IPv4	0.0.0.0/0		ingress	None	None
86b9413a-ad23-46c4-a35e-9306945dc63c	None	IPv6	:::0		ingress	None	None
ad4a19ef-7fab-	None	IPv6	:::0		egress	None	None

Allowing SSH access

The next thing to do, is to allow SSH access on **port 22** to the server, only from specific networks.

To do this, click on the *Create new rule* button.

Create a Security Group Rule ?

Protocol

TCP

Direction

☒ Ingress ☐ Egress

Ether Type

☒ IPv4 ☐ IPv6

Port range !

22

22

From

☒ Network/IP ☐ Security Group

Network/IP

Choose option

Custom CIDR !

203.0.113.58/32

Back

☐ Create Another ☒ Create

To create this rule use the following command:

```
openstack security group rule create \  
--protocol tcp --dst-port 22 --remote-ip 203.0.113.58/32 default
```

If you don't know your IP, simply visit icanhazip.com. In this example your IP is 203.0.113.58 and you want to allow SSH access from this IP address only, enter 203.0.113.58/32 as CIDR. If you want to allow SSH access from any address in that **Class C subnet**, instead enter 203.0.113.0/24 as CIDR.

Allowing Web Traffic

Next create the rules that allow anyone access the server on **port 80** and **port 443**.

Using the same logic as before, click on *Create new rule*. Select TCP Protocol and port 80 as both

Create a Security Group Rule ?

Protocol

TCP

Direction

☒ Ingress ☐ Egress

Ether Type

☒ IPv4 ☐ IPv6

Port range !

80

80

From

☒ Network/IP ☐ Security Group

Network/IP

Choose option

Custom CIDR !

Example: 10.0.10.0/24

Back

☐ Create Another ☒ Create

The same applies to port 443.

Create a Security Group Rule



Protocol

TCP



Direction



Ingress



Egress

Ether Type



IPv4



IPv6

Port range

443

443

From



Network/IP



Security Group

Network/IP

Choose option



Custom CIDR

Example: 10.0.10.0/24

Back



Create Another

Create

<div> <div></div> <div>✓</div> <div>openstack security group rule list default</div> </div>		
Details	Rules	Ports
Status	Direction	Ether type
✓	egress	IPv6
✓	ingress	IPv4
✓	ingress	IPv4
✓	ingress	IPv4
✓	egress	IPv4

This time don't specify *-remote-ip* to allow traffic from all sources, using the following command:

```
openstack security group rule create --protocol tcp --dst-port 80 default
```

One more time for port 443:

```
openstack security group rule create --protocol tcp --dst-port 443 default
```

To view the updated rules, print the them again:

```
openstack security group rule list default
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID      | IP Protocol | Ethertype | IP Range | Port Range | Direction | Remote Security Group | Remote Address C
+-----+-----+-----+-----+-----+-----+-----+-----+
| 742bcc46- | tcp      | IPv4      | 0.0.0.0/0 | 80:80      | ingress   | None                  | None
| beb5-    |          |           |           |            |           |                       |
```

