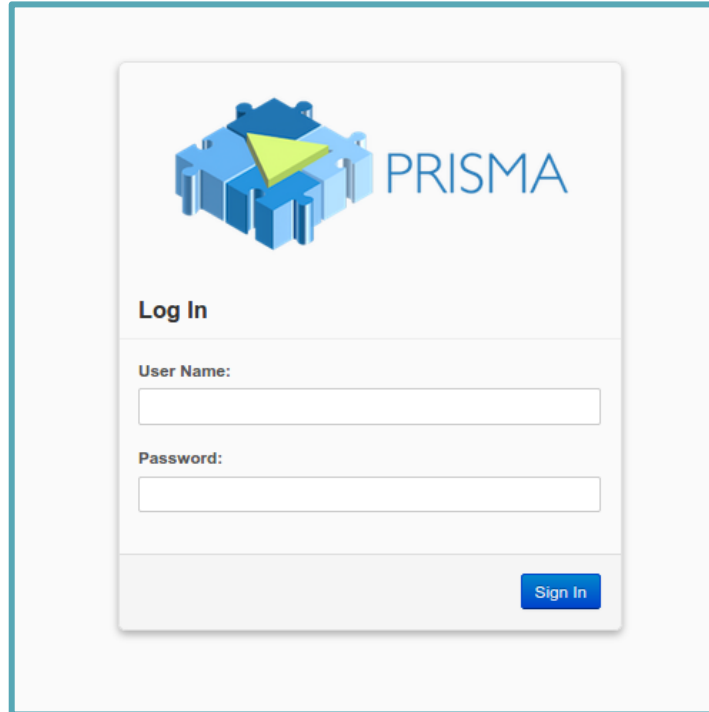


How to create a Security Group and to add rules

1. Log into the web dashboard (<https://prisma-cloud.ba.infn.it/>) with your username and password



The image shows a login form for Prisma Cloud. At the top, there is a logo consisting of a 3D arrangement of blue and yellow blocks forming a cube-like structure, followed by the word "PRISMA" in a blue, sans-serif font. Below the logo, the text "Log In" is displayed in a bold, black font. Underneath, there are two input fields: the first is labeled "User Name:" and the second is labeled "Password:". Both fields are empty and have a light gray border. At the bottom right of the form, there is a blue button with the text "Sign In" in white.

2. In the left panel, click on Project → Access & Security → Security Groups

The screenshot displays the PRISMA cloud management interface. The top header includes the PRISMA logo, a dropdown menu set to 'demo_outreach', a user profile for 'demo_user', and a 'Sign Out' button. The left sidebar contains a 'Project' dropdown menu with a sub-menu 'Compute'. Below 'Compute' are links for 'Overview', 'Instances', 'Volumes', and 'Images'. The 'Access & Security' section is highlighted with a blue bar. Below it are 'Network', 'Object Store', and 'Orchestration' sections. The main content area is titled 'Access & Security' and features tabs for 'Security Groups', 'Key Pairs', 'Floating IPs', and 'API Access'. The 'Security Groups' tab is active, showing a table with two security groups: 'default' and 'qwerqwer'. The table has columns for 'Name', 'Description', and 'Actions'. The 'Actions' column for 'default' has a 'Manage Rules' button, and for 'qwerqwer' it has 'Manage Rules' and a 'More' dropdown. Above the table are buttons for '+ Create Security Group' and 'Delete Security Groups'. A status bar at the bottom of the table indicates 'Displaying 2 items'. Three red arrows point from the text above to the 'Project' dropdown, the 'Access & Security' section, and the 'Security Groups' tab.

PRISMA demo_outreach demo_user Sign Out

Project

- Compute
 - Overview
 - Instances
 - Volumes
 - Images
 - Access & Security
 - Network
 - Object Store
 - Orchestration

Access & Security

Security Groups Key Pairs Floating IPs API Access

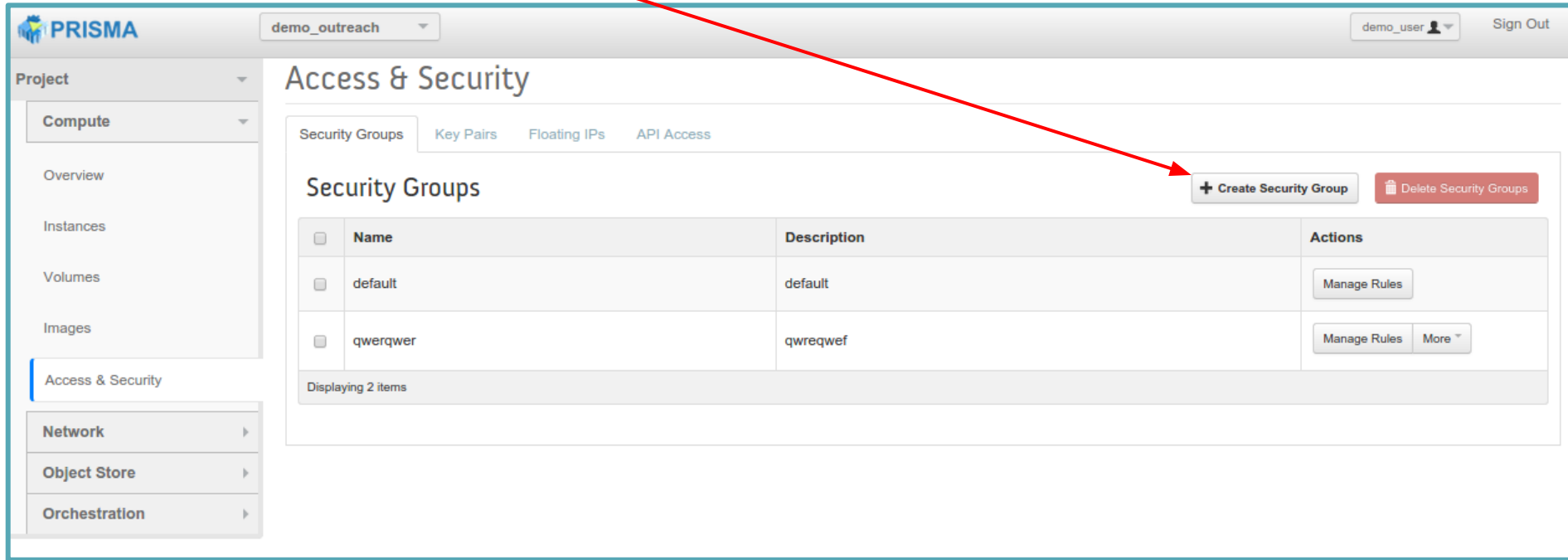
Security Groups

+ Create Security Group Delete Security Groups

<input type="checkbox"/>	Name	Description	Actions
<input type="checkbox"/>	default	default	Manage Rules
<input type="checkbox"/>	qwerqwer	qwerqwer	Manage Rules More

Displaying 2 items

3. Click on Create Security Group



The screenshot shows the PRISMA web interface. The top header includes the PRISMA logo, a dropdown menu set to 'demo_outreach', a user profile for 'demo_user', and a 'Sign Out' link. The left sidebar is titled 'Project' and contains a 'Compute' dropdown menu with options for 'Overview', 'Instances', 'Volumes', and 'Images'. Below these are 'Access & Security', 'Network', 'Object Store', and 'Orchestration'. The main content area is titled 'Access & Security' and has tabs for 'Security Groups', 'Key Pairs', 'Floating IPs', and 'API Access'. The 'Security Groups' tab is active, showing a table with two security groups: 'default' and 'qwerqwer'. Above the table are two buttons: '+ Create Security Group' and 'Delete Security Groups'. A red arrow points from the instruction text to the '+ Create Security Group' button.

PRISMA demo_outreach demo_user Sign Out

Project

- Compute
 - Overview
 - Instances
 - Volumes
 - Images
- Access & Security
- Network
- Object Store
- Orchestration

Access & Security

Security Groups Key Pairs Floating IPs API Access

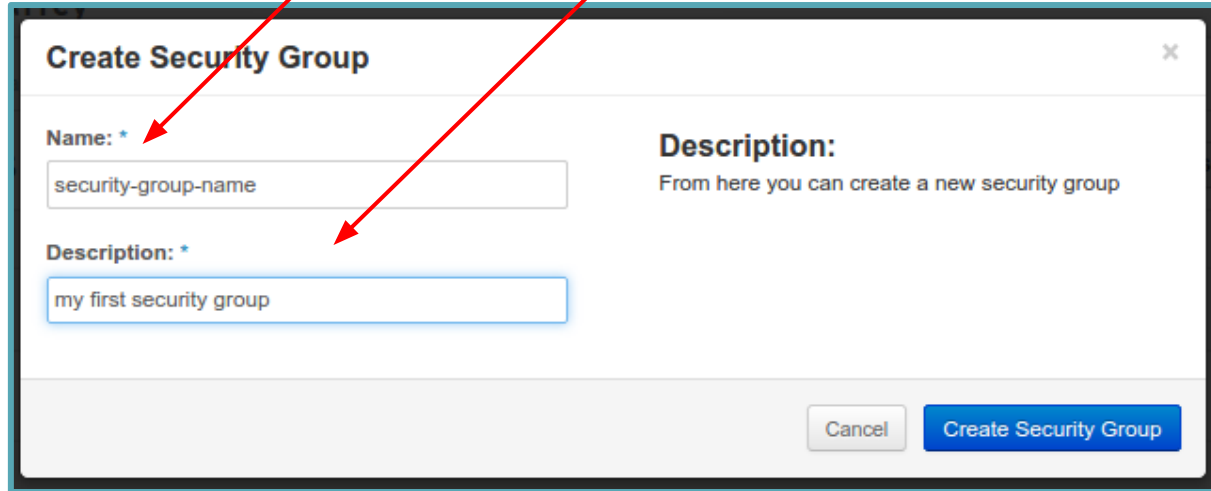
Security Groups

+ Create Security Group Delete Security Groups

<input type="checkbox"/>	Name	Description	Actions
<input type="checkbox"/>	default	default	Manage Rules
<input type="checkbox"/>	qwerqwer	qwreqwef	Manage Rules More

Displaying 2 items

4. In the new window, type a name and a description for the security group



The screenshot shows a 'Create Security Group' dialog box. It has a title bar with a close button (X) in the top right corner. The main content area is divided into two sections. The left section has a label 'Name: *' followed by a text input field containing 'security-group-name'. Below this is a label 'Description: *' followed by a text input field containing 'my first security group'. The right section has a label 'Description:' followed by a text area containing 'From here you can create a new security group'. At the bottom right, there are two buttons: 'Cancel' and 'Create Security Group'.

Create Security Group [X]

Name: *
security-group-name

Description: *
my first security group

Description:
From here you can create a new security group

Cancel Create Security Group

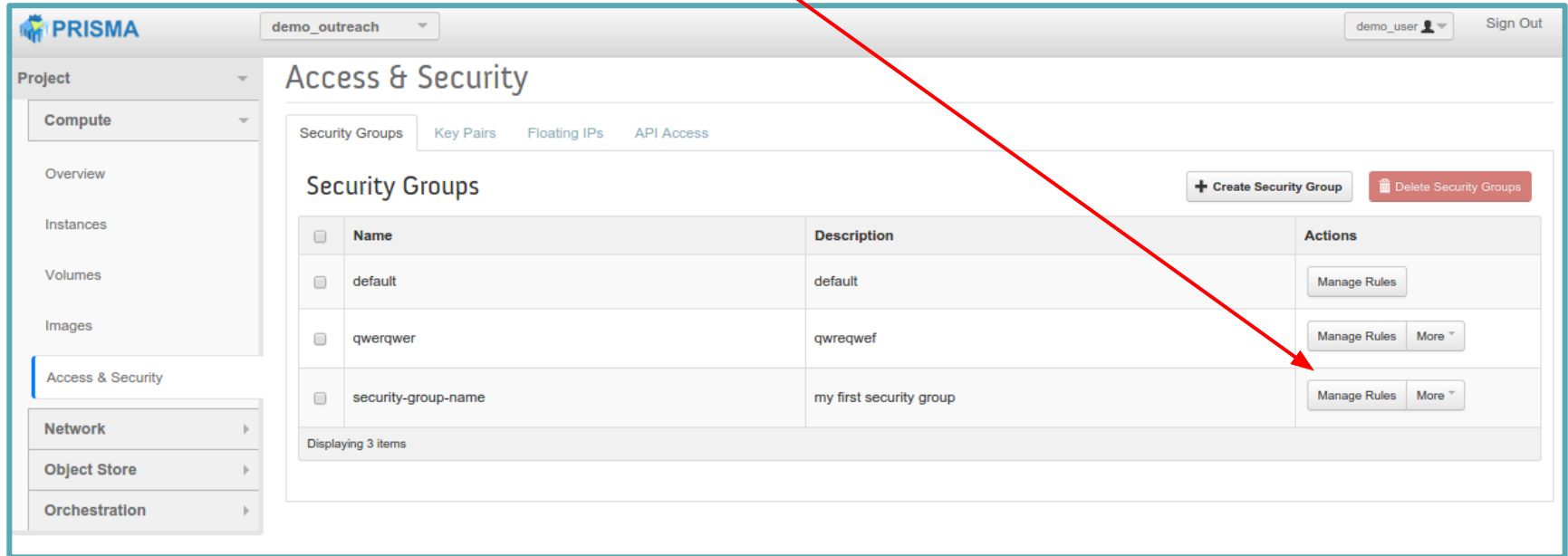
5. The security group is then created

The screenshot shows the PRISMA web interface. The top navigation bar includes the PRISMA logo, a project dropdown set to 'demo_outreach', a user profile for 'demo_user', and a 'Sign Out' link. The left sidebar contains a 'Project' menu with options: 'Compute' (selected), 'Overview', 'Instances', 'Volumes', 'Images', 'Access & Security' (highlighted), 'Network', 'Object Store', and 'Orchestration'. The main content area is titled 'Access & Security' and features tabs for 'Security Groups', 'Key Pairs', 'Floating IPs', and 'API Access'. The 'Security Groups' tab is active, displaying a table with three entries. The third entry, 'security-group-name', is circled in red. Above the table are buttons for '+ Create Security Group' and 'Delete Security Groups'. The table has columns for 'Name', 'Description', and 'Actions'.

	Name	Description	Actions
<input type="checkbox"/>	default	default	<button>Manage Rules</button>
<input type="checkbox"/>	qwerqwer	qwerqwer	<button>Manage Rules</button> <button>More ▾</button>
<input type="checkbox"/>	security-group-name	my first security group	<button>Manage Rules</button> <button>More ▾</button>

Displaying 3 items

6. To add new rules, click on **Manage Rules**



The screenshot shows the PRISMA web interface. The top navigation bar includes the PRISMA logo, a project dropdown set to 'demo_outreach', a user profile for 'demo_user', and a 'Sign Out' link. The left sidebar shows a navigation menu with 'Project' expanded, containing 'Compute' (selected), 'Overview', 'Instances', 'Volumes', 'Images', 'Access & Security' (highlighted), 'Network', 'Object Store', and 'Orchestration'. The main content area is titled 'Access & Security' and has tabs for 'Security Groups', 'Key Pairs', 'Floating IPs', and 'API Access'. The 'Security Groups' tab is active, displaying a table with three security groups. Above the table are buttons for '+ Create Security Group' and 'Delete Security Groups'. The table has columns for 'Name', 'Description', and 'Actions'. The 'security-group-name' row has a 'Manage Rules' button highlighted by a red arrow. The bottom of the table indicates 'Displaying 3 items'.

<input type="checkbox"/>	Name	Description	Actions
<input type="checkbox"/>	default	default	Manage Rules
<input type="checkbox"/>	qwerqwer	qwerqwer	Manage Rules More ▾
<input type="checkbox"/>	security-group-name	my first security group	Manage Rules More ▾

Displaying 3 items

7. The list of the rules for that security group will appear. Then, click on **Add Rules**

The screenshot shows the PRISMA console interface. The top navigation bar includes the PRISMA logo, a dropdown menu for 'demo_outreach', a user profile for 'demo_user', and a 'Sign Out' link. The left sidebar contains a 'Project' dropdown menu with 'Compute' selected, and a list of navigation items: Overview, Instances, Volumes, Images, Access & Security, Network, Object Store, and Orchestration. The main content area is titled 'Manage Security Group Rules: security-group-name' and 'Security Group Rules'. It features a table with two rules and two buttons: '+ Add Rule' and 'Delete Rules'.

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote	Actions
<input type="checkbox"/>	Egress	IPv4	Any	-	0.0.0.0/0 (CIDR)	<button>Delete Rule</button>
<input type="checkbox"/>	Egress	IPv6	Any	-	::/0 (CIDR)	<button>Delete Rule</button>

Displaying 2 items

8a. Example 1: Let us add the ssh rule

Add Rule

Rule: *

SSH

Remote: *

CIDR

CIDR

0.0.0.0/0

Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

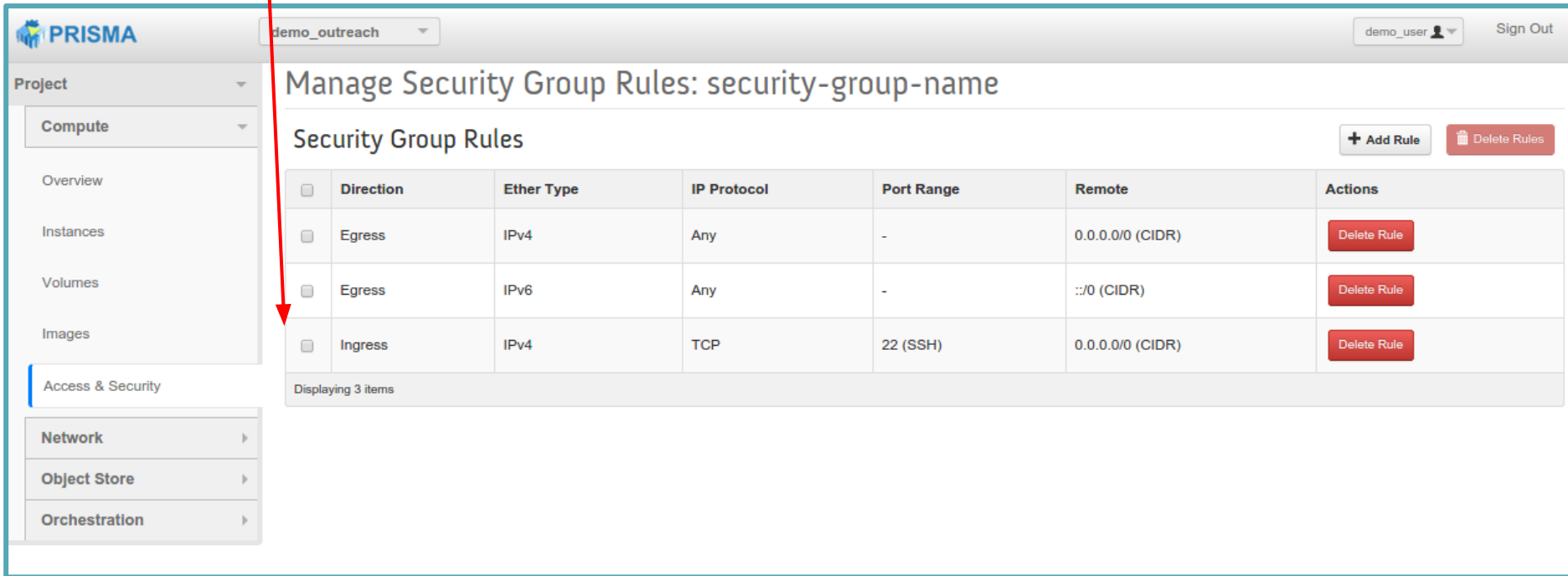
Cancel Add

you can choose
CIDR or
Security Group
as source of
traffic

indicate the network
which you want
to ssh the VM from
ex.: 90.147.66.0/24

leave 0.0.0.0/0 if
you want the port to
be open to traffic
coming from
everywhere

The new rule will appear in the list



The screenshot shows the PRISMA console interface. The top header includes the PRISMA logo, a dropdown menu for 'demo_outreach', a user profile for 'demo_user', and a 'Sign Out' button. The left sidebar contains a 'Project' dropdown menu with 'Compute' selected, and a list of navigation items: Overview, Instances, Volumes, Images, Access & Security, Network, Object Store, and Orchestration. The main content area is titled 'Manage Security Group Rules: security-group-name' and 'Security Group Rules'. It features a table with three rules and two buttons: '+ Add Rule' and 'Delete Rules'. A red arrow points to the 'Compute' menu item in the sidebar.

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote	Actions
<input type="checkbox"/>	Egress	IPv4	Any	-	0.0.0.0/0 (CIDR)	<button>Delete Rule</button>
<input type="checkbox"/>	Egress	IPv6	Any	-	:::/0 (CIDR)	<button>Delete Rule</button>
<input type="checkbox"/>	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0 (CIDR)	<button>Delete Rule</button>

Displaying 3 items

8b. Example 2: Let us add the http rule

Add Rule

Rule: *

HTTP

Remote: *

CIDR

CIDR

0.0.0.0/0

Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Cancel Add

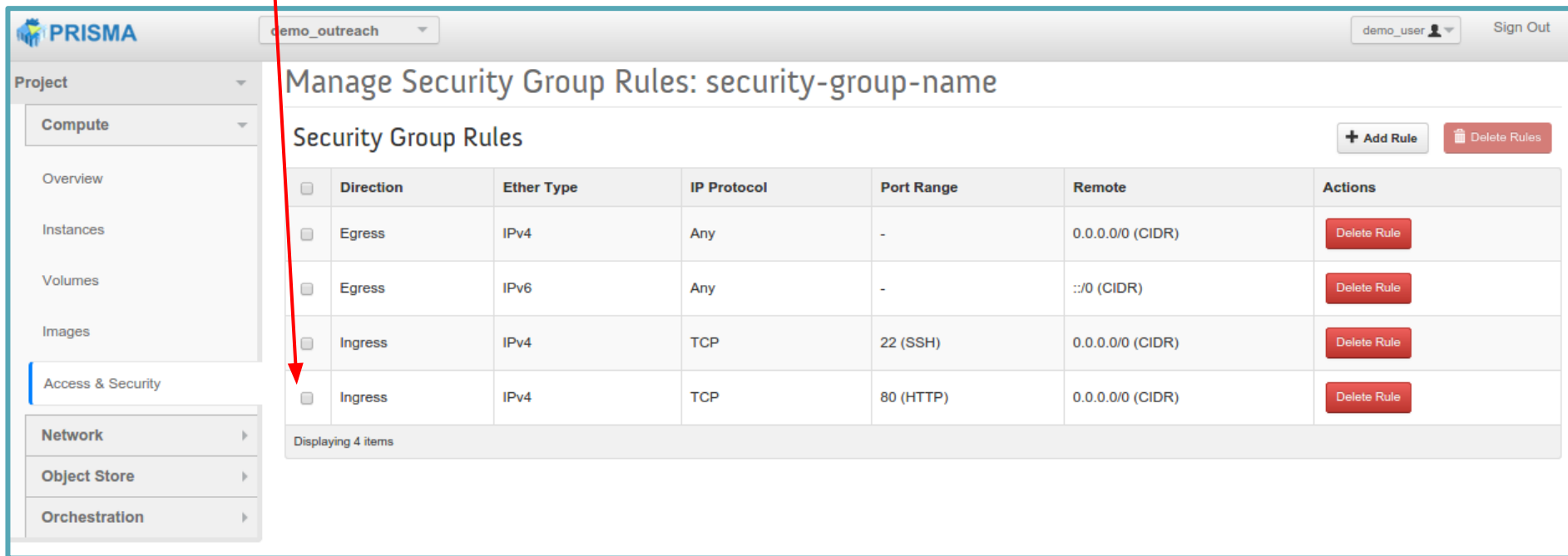
you can choose
CIDR or
Security Group

put here the
addresses you want
to accept http traffic
from

ex.: 90.147.66.0/24

leave 0.0.0.0/0 if
you want the port to
be open to traffic
coming from
everywhere

The new rule will appear in the list



The screenshot shows the PRISMA console interface. The top header includes the PRISMA logo, a project dropdown set to 'demo_outreach', a user profile for 'demo_user', and a 'Sign Out' button. The left sidebar contains a 'Project' dropdown and a list of navigation items: 'Compute', 'Overview', 'Instances', 'Volumes', 'Images', 'Access & Security' (highlighted with a blue bar), 'Network', 'Object Store', and 'Orchestration'. The main content area is titled 'Manage Security Group Rules: security-group-name' and 'Security Group Rules'. It features '+ Add Rule' and 'Delete Rules' buttons. Below these is a table with 7 columns: checkboxes, Direction, Ether Type, IP Protocol, Port Range, Remote, and Actions. The table contains 4 rows of rules. A red arrow points from the text 'The new rule will appear in the list' to the 'Access & Security' menu item in the sidebar.

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote	Actions
<input type="checkbox"/>	Egress	IPv4	Any	-	0.0.0.0/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Egress	IPv6	Any	-	:::/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0 (CIDR)	Delete Rule

Displaying 4 items

8c. Example 3: Let us add the All ICMP rule

Add Rule

Rule: *

ALL ICMP ▼

Direction

Ingress ▼

Remote: *

CIDR ▼

CIDR

0.0.0.0/0

Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

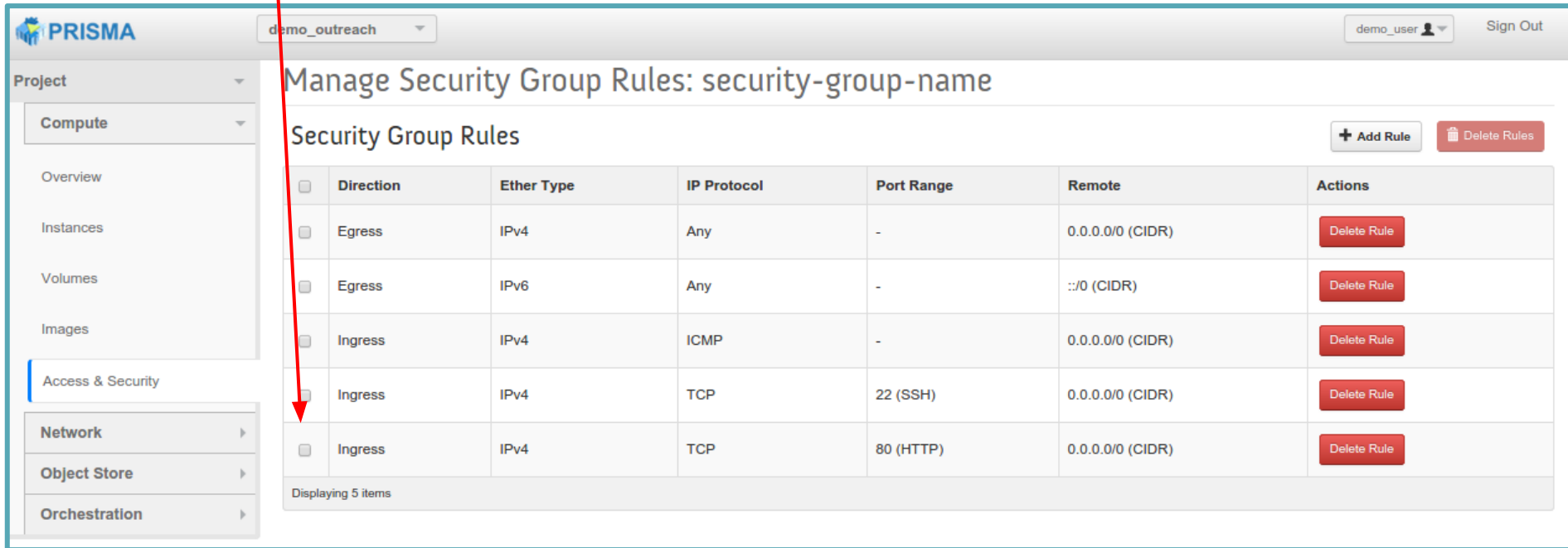
Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Cancel Add

you can choose
Ingress or
Egress

you can choose
CIDR or
Security Group

The new rule will appear in the list



The screenshot shows the PRISMA console interface. The left sidebar contains navigation links: Project, Compute, Overview, Instances, Volumes, Images, Access & Security, Network, Object Store, and Orchestration. The main content area is titled "Manage Security Group Rules: security-group-name" and "Security Group Rules". It features a table with 5 rules and buttons for "Add Rule" and "Delete Rules". A red arrow points to the checkbox of the newly added rule, which is the last row in the table.

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote	Actions
<input type="checkbox"/>	Egress	IPv4	Any	-	0.0.0.0/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Egress	IPv6	Any	-	::/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	ICMP	-	0.0.0.0/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0 (CIDR)	Delete Rule

Displaying 5 items

8d. Example 4: Let us add a Custom TCP rule

The screenshot shows the 'Add Rule' dialog box with the following fields and annotations:

- Rule:** A dropdown menu with 'Custom TCP Rule' selected. An arrow points to this field with the text: "choose an integer value between 1 and 65535".
- Direction:** A dropdown menu with 'Ingress' selected. An arrow points to this field with the text: "you can choose Ingress or Egress".
- Open Port:** A dropdown menu with 'Port' selected. An arrow points to this field with the text: "you can choose Port or Port Range".
- Port:** A text input field containing '60221'. An arrow points to this field with the text: "choose an integer value between 1 and 65535".
- Remote:** A dropdown menu with 'CIDR' selected. An arrow points to this field with the text: "you can choose CIDR or Security Group".
- CIDR:** A text input field containing '0.0.0.0/0'. An arrow points to this field with the text: "you can choose CIDR or Security Group".

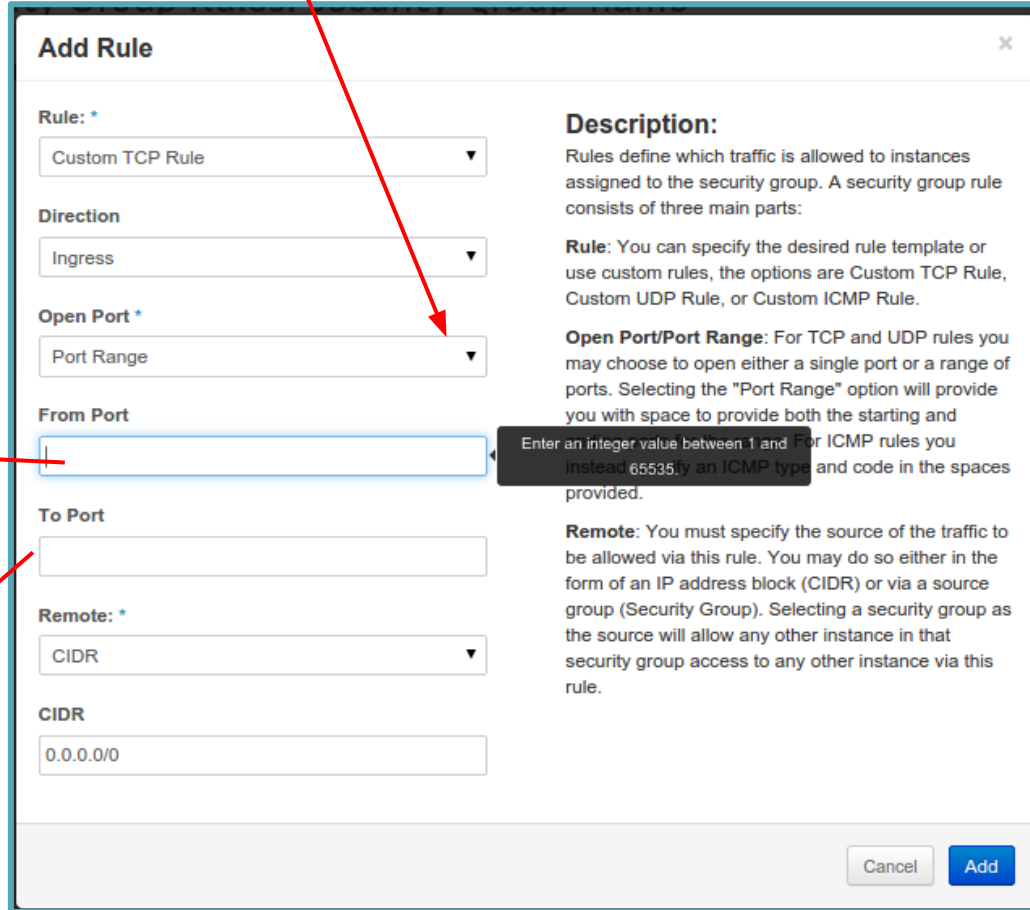
Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

- Rule:** You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.
- Open Port/Port Range:** For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.
- Remote:** You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Buttons: Cancel, Add

NB: you can specify a "Port Range" rather than a single port



The screenshot shows the 'Add Rule' dialog box with the following fields and annotations:

- Rule:** A dropdown menu with 'Custom TCP Rule' selected. A red arrow points from the text 'NB: you can specify a "Port Range" rather than a single port' to this dropdown.
- Direction:** A dropdown menu with 'Ingress' selected.
- Open Port:** A dropdown menu with 'Port Range' selected.
- From Port:** A text input field with a red arrow pointing to it from the text 'first port to be affected by the rule'.
- To Port:** A text input field with a red arrow pointing to it from the text 'last port to be affected by the rule'.
- Remote:** A dropdown menu with 'CIDR' selected.
- CIDR:** A text input field with '0.0.0.0/0' entered.

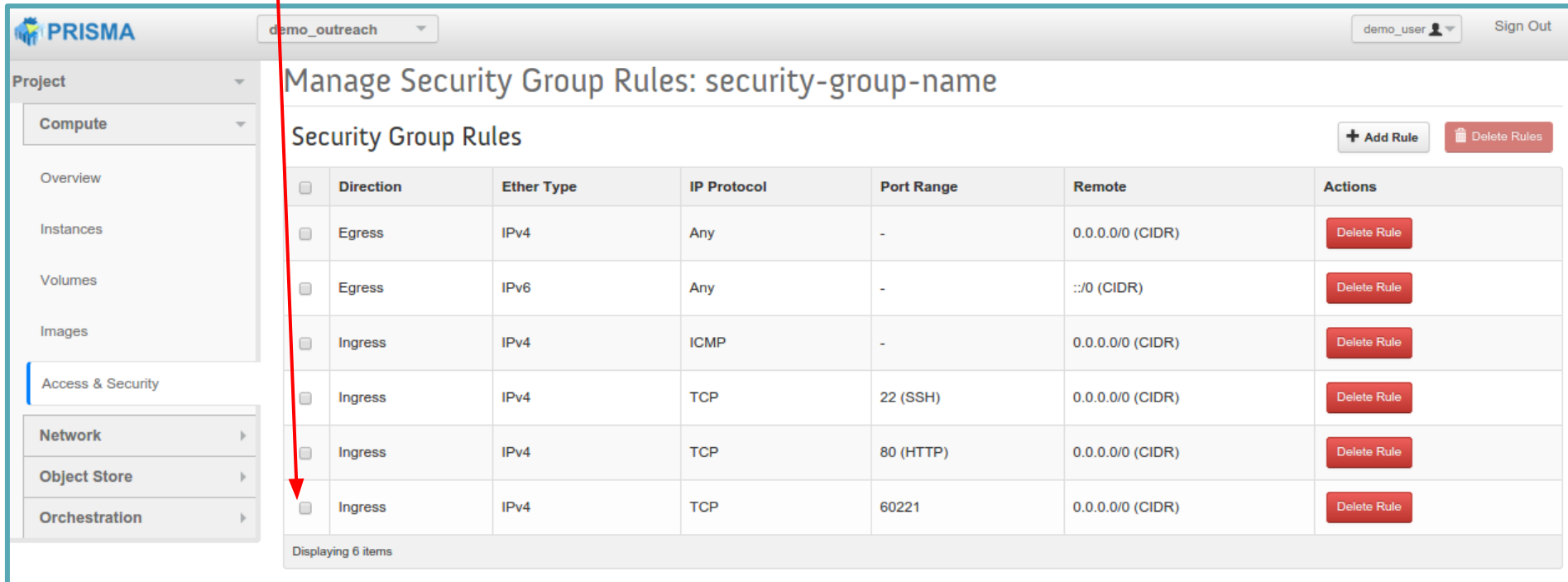
Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

- Rule:** You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.
- Open Port/Port Range:** For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending port. For ICMP rules you instead provide an ICMP type and code in the spaces provided.
- Remote:** You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Buttons: Cancel, Add

The new rule will appear in the list



The screenshot shows the Prisma Cloud console interface. The top header includes the Prisma logo, a dropdown menu set to 'demo_outreach', a user profile for 'demo_user', and a 'Sign Out' button. On the left, a sidebar menu lists various project components: Project, Compute, Overview, Instances, Volumes, Images, Access & Security (highlighted), Network, Object Store, and Orchestration. The main content area is titled 'Manage Security Group Rules: security-group-name' and 'Security Group Rules'. It features a table with columns for checkboxes, Direction, Ether Type, IP Protocol, Port Range, Remote, and Actions. The table contains six rows of rules. A red arrow points to the bottom of the table, indicating where a new rule will appear. The footer of the table states 'Displaying 6 items'.

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote	Actions
<input type="checkbox"/>	Egress	IPv4	Any	-	0.0.0.0/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Egress	IPv6	Any	-	::/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	ICMP	-	0.0.0.0/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0 (CIDR)	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	60221	0.0.0.0/0 (CIDR)	Delete Rule

Displaying 6 items