

Firewall Conf:

Activities Firefox Web Browser Wed 17:55

VPC network - Training - Google Cloud Platform - Mozilla Firefox

https://console.cloud.google.com/networking/firewalls/add?network=vpc-akash&project=pe-train

Google Cloud Platform Training

VPC network

Firewall rules

Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name

Description (Optional)

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)

☐ On

☒ Off

Network

Priority

Priority can be 0 - 65535 Check priority of other firewall rules

Direction of traffic ☒ Ingress

☐ Egress

Action on match ☒ Allow

☐ Deny

Specify the IP range of Quantiphi

Activities Firefox Web Browser Wed 17:56

VPC network - Training - Google Cloud Platform - Mozilla Firefox

https://console.cloud.google.com/networking/firewalls/add?network=vpc-akash&project=pe-train

Google Cloud Platform Training

VPC network

Firewall rules

Create a firewall rule

Direction of traffic ☒ Ingress

☐ Egress

Action on match ☒ Allow

☐ Deny

Targets

Source filter

Source IP ranges

Second source filter

Protocols and ports ☒ Allow all

☒ Specified protocols and ports

☒ tcp:

☐ udp:

☐ Other protocols

☒ Disable rule

Attach the created firewall rule to the vpc

The screenshot shows the Google Cloud Platform console interface. The left sidebar contains navigation icons for VPC networks, External IP addresses, Firewall rules, Routes, VPC network peering, Shared VPC, and Serverless VPC access. The main content area is titled 'VPC network details' for the network 'vpc-akash'. It shows configuration details such as Subnet creation mode (Custom subnets), Dynamic routing mode (Regional), and DNS server policy (None). Below these details, there are tabs for Subnets, Static internal IP addresses, Firewall rules (which is currently selected), Routes, VPC Network Peering, and Private service connection. Under the 'Firewall rules' tab, there are 'Add firewall rule' and 'Delete' buttons. A table lists the existing firewall rules:

Name	Type	Targets	Filters	Protocols / ports	Action	Priority
fw-akash	Ingress	Apply to all	IP ranges: 59.152.53.168/30	tcp:22	Allow	1000

Below the table, there is a link for 'Equivalent REST'.