This page describes the commands for working with firewall rules and offers some examples in using them.

Refer to the Firewall rules overview (/compute/docs/vpc/firewalls), to learn more about firewall rules, such as implied rules and system generated rules for default networks.

Before configuring firewall rules, review the firewall rule components (/vpc/docs/firewalls#firewall_rule_components) to become familiar with firewall components as used in Google Cloud.

Firewall rules are defined at the network level, and only apply to the network where they are created; however, the name you choose for each of them must be unique to the project.

If you want to specify multiple service accounts for the target or source service account field, use the **`gcloud`** comma

You can modify some components of a firewall rule, such as the specified protocols and ports for the match condition. You cannot modify a firewall rule's name, network, the action on match

(/vpc/docs/firewalls#action_of_the_rule), and the direction of traffic (/vpc/docs/firewalls#direction_of_the_rule).

If you need to change the name, network, or the action or direction component, you must delete the rule (#deleting_firewall_rules) and create a new one (#creating_firewall_rules) instead.

If you want to add or remove multiple service accounts, use the `gcloud` command or API. You cannot use the conso
/ multiple target service accounts or source service accounts.

For each network interface, the Cloud Console lists all of the firewall rules that apply to the interface and the rules that are actually being used by the interface. Firewall rules can mask other rules, so all of the rules that apply to an interface might not actually be used by the interface.

Firewall rules are associated and applied to a VM instances through a rule's target parameter. By viewing all of the applied rules, you can check whether a particular rule is being applied to an interface.

To view all of the firewall rules that apply to a specific network interface of a VM instance:

1. Go to the VM instances page in the Google Cloud Console and find the instance to view.

   Go to the VM instances page (https://console.cloud.google.com/compute/instances)

2. In the instance's **more actions** menu (⋮), select **View network details**.

3. If an instance has multiple network interfaces, select the network interface to view in the **Network interface details** section.

4. Click the **Firewall rules** tab to see all the rules that apply to the network interface, sorted by rule name.

Of the rules that apply to a network interface, the interface might not use all of them. Some rules might be overridden by a rule with a more specific range or a higher priority. By viewing the rules that are in use, you can quickly verify which IP ranges, protocols, and ports are open or closed to the instance.

To view the rules that are being used by a specific network interface of a VM instance:

1. Go to the VM instances page in the Google Cloud Console and find the instance to view.

   Go to the VM instances page (https://console.cloud.google.com/compute/instances)

2. In the instance's **more actions** menu (⋮), select **View network details**.

3. If an instance has multiple network interfaces, select the network interface to view in the **Network interface details** section.

4. In the **Network Analysis** section, select the **Ingress analysis** or **Egress analysis** tab.

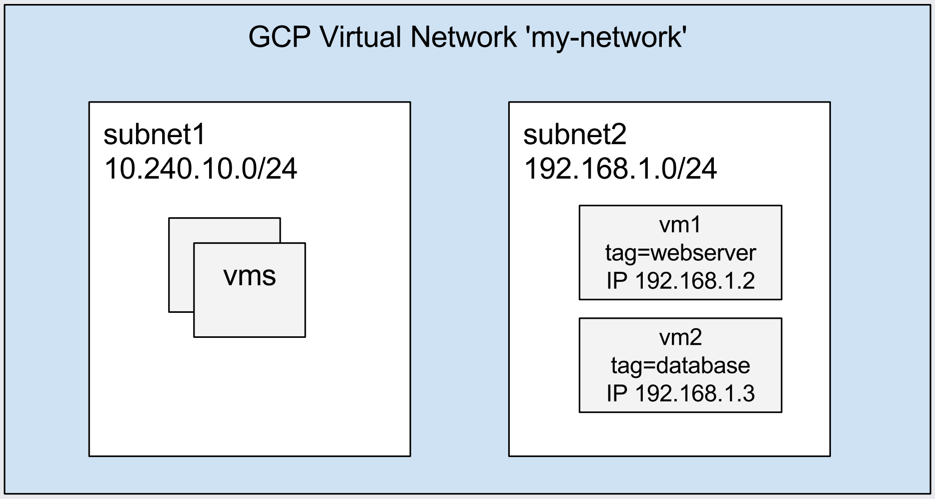
5. View the table, which is sorted from the most specific to least specific IP address range, to determine if traffic to or from a specific IP address is permitted.

You can inspect a firewall rule to see its name, applicable network, and components (/vpc/docs/firewalls#firewall_rule_components), including whether the rule is enabled or disabled.

You can enable logging for firewall rules to see which rule allowed or blocked which traffic. See Using Firewall Rules Logging (/vpc/docs/using-firewall-rules-logging) for instructions.

The diagram below demonstrates an example firewall configuration. The scenario involves a `my-network` that contains the following:.

- a subnet `subnet1` with IP range `10.240.10.0/24`
- a subnet `subnet2` with IP range `192.168.1.0/24`
- instance `vm1` in `subnet2` having tag `webserver` and internal IP `192.168.1.2`
- instance `vm2` in `subnet2` having tag `database` and internal IP `192.168.1.3`



(/vpc/images/firewalls/firewall-network-example.svg)
Sample network configuration (click to enlarge)

This example creates a set of firewall rules that deny all ingress TCP connections except connections destined to port `80` from `subnet1`.

1. Create a firewall rule to deny all ingress TCP traffic to instances tagged with `webserver`.

2. Create a firewall rule to allow all IPs in `subnet1` (`10.240.10.0/24`) to access TCP port `80` on instances tagged with `webserver`.

1. Create a firewall rule to deny all egress TCP traffic.

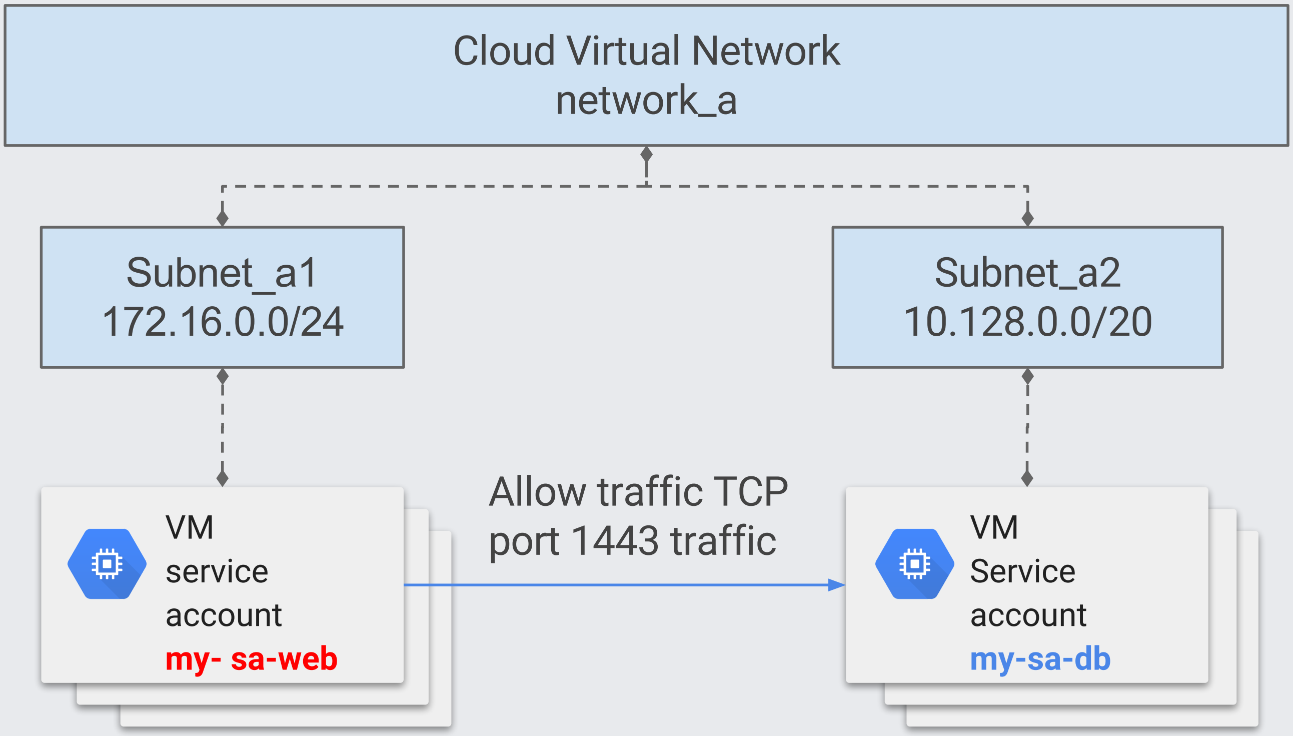
2. Create firewall rule to allow TCP traffic destined to `vm1` port `80`.

Create a firewall rule that allows instances tagged with `webserver` to send egress TCP traffic to port `443` of a sample external IP address, `192.0.2.5`.

Create firewall rule that allows SSH traffic from instances with tag `database` (`vm2`) to reach instances with tag `webserver` (`vm1`).

For additional information on service accounts and roles, see Granting roles to service accounts (/iam/docs/granting-roles-to-service-accounts).

Consider the scenario in the diagram below, in which there are two applications that are autoscaled through templates, a webserver application `my-sa-web`, and a database application 'my-sa-db". A Security admin wants to allow TCP flows on port `1443` from `my-sa-web` to `my-sa-db`.



(/vpc/images/firewalls/firewall-service-accounts-example.svg)
Using firewall rules with service accounts (click to enlarge)

The configuration steps, including the creation of the service accounts, is as follows:

1. A project EDITOR or project OWNER creates the service accounts (/iam/docs/managing-service-accounts#creating_a_service_account) `my-sa-web` and `my-sa-db`.

2. A project OWNER assigns the webserver developer `web-dev@example.com` a serviceAccountUser (/iam/docs/understanding-roles#service-accounts-roles) role for service account `my-sa-web` by setting an IAM policy.

3. A project OWNER assigns the database developer "db-dev@example.com" a serviceAccountUser (/iam/docs/understanding-roles#service-accounts-roles) role for service account `my-sa-db` by setting an IAM policy.

4. Developer `web-dev@example.com`, which has the Instance admin role, creates webserver instance template and authorize instances to run as service account `my-sa-web`.

5. Developer `db-dev@example.com`, which has the Instance Admin role, creates the database instance template and authorize instances to run as service account `my-sa-db`.

6. Security admin creates the firewall rules using service accounts to allow traffic `TCP:1443` from service account `my-sa-web` to service account `my-sa-db`.

You may see one of the following error messages:

- `Should not specify destination range for ingress direction.`

  Destination ranges are not valid parameters for ingress firewall rules. Firewall rules are assumed to be ingress rules unless a direction of `egress` is specifically specified. If you create a rule that does not specify a direction, it will be created as an ingress rule, which does not allow a destination range. Also, source ranges are not valid parameters for egress rules.

- `Firewall direction cannot be changed once created.`

  You cannot change the direction of an existing firewall rule. You have to create a new rule with the correct parameters, then delete the old one.

- `Firewall traffic control action cannot be changed once created.`

  You cannot change the action of an existing firewall rule. You have to create a new rule with the correct parameters, then delete the old one.

- `Service accounts must be valid RFC 822 email addresses.` The service account specified in firewall rule must be an email address formatted per RFC 822 (https://www.ietf.org/rfc/rfc0822.txt).

- `ServiceAccounts and Tags are mutually exclusive and can't be combined in the same firewall rule.` You cannot specify both both service accounts and tags in the same rule.

If you cannot connect to a VM instance, check your firewall rules.

1. If you are initiating the connection from another VM instance, list the egress firewall rules for that instance.

2. Check if the destination IP is denied by any egress rules. The rule with the highest priority (lowest priority number) overrides lower priority rules. For two rules with same priority, the deny rule take precedence.

3. Check ingress firewall rule for the network that contains the destination VM instance.

Sample output. Your output will depend on your list of firewall rules

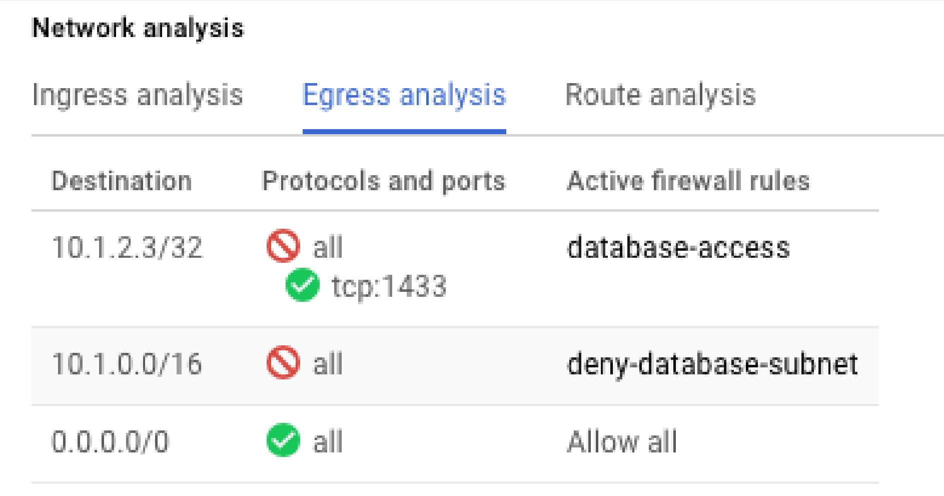
To see if a firewall rule is enabled or disabled, view the firewall rules details (#describe).

In the Google Cloud Console (https://console.cloud.google.com/), look for `Enabled` or `Disabled` under **Enforcement**.

In the `gcloud` command line tool output, look for the `disabled` field. If it says `disabled:false`, the rule is enabled and being enforced. If it says `disabled: true`, the rule is disabled.

Imagine that you add a new firewall rule to a VPC network, which allows traffic to a database server at `10.1.2.3` over `tcp:1433`. After you create the rule, you can check to see if it's being applied correctly on a particular instance. For more information, see Listing firewall rules for a network interface of a VM instance (#listing-rules-vm).

In the following example, the console lists the `database-access` rule in the **Egress analysis** tab for this VM instance, meaning `10.1.2.3` egress traffic on port `1433` is permitted. Other egress traffic in the `10.1.0.0/16` range is blocked due to the `deny-database-subnet` firewall rule.



Destination	Protocols and ports	Active firewall rules
10.1.2.3/32	⊘ all ✓ tcp:1433	database-access
10.1.0.0/16	⊘ all	deny-database-subnet
0.0.0.0/0	✓ all	Allow all

(/vpc/images/firewalls/firewall-analysis.png)

Permitted egress traffic for a VM instance (click to enlarge)

Ingress firewall rules that use source tags can take time to propagate. For details, see the considerations (/vpc/docs/add-remove-network-tags#considerations) that are related to source tags for ingress firewall rules.

- See the Firewall Rules Overview (/vpc/docs/firewalls) for an introduction to firewall rules