Using Firewall Rules Logging

Firewall Rules Logging allows you audit, verify, and analyze the effects of your firewall rules. For example, you can determine if a firewall rule designed to deny traffic is functioning as intended. Logging is also useful if you need to determine how many connections are affected by a given firewall rule.

This page shows you how to enable and disable logging and how to view generated logs. For more information what is logged, examples of logging, and log formats, see the Firewall Rules Logging Overview (https://cloud.google.com/vpc/docs/firewall-rules-logging).

Permissions

To modify firewall rules or access Stackdriver Logs, IAM members need one of the following roles.

Task	Required Role
Create, delete, or update firewall rules	Project owner or editor (https://cloud.google.com/iam/docs/understanding-roles#primitive_roles) *or* Security Admin (https://cloud.google.com/compute/docs/access/iam#compute.securityAdmin)
View Stackdriver Logs	Project owner, editor or viewer (https://cloud.google.com/iam/docs/understanding-roles#primitive_roles) *or* Logs Viewer (https://cloud.google.com/iam/docs/understanding-roles#logging-roles) See the Stackdriver Access Control Guide (https://cloud.google.com/logging/docs/access-control#permissions_and_roles) for details about Stackdriver IAM roles and permissions.

Enabling and disabling firewall rules logging

When you create a firewall rule, you can choose to turn on firewall rules logging. See creating firewall rules (https://cloud.google.com/vpc/docs/using-firewalls#creating_firewall_rules) for more information.

To enable or disable firewall rules logging for an existing firewall rule, follow these directions.

Enabling firewall rules logging

CONSOLE GCLOUD API

1. Go to the Firewall rules page in the Google Cloud Console.
   GO TO THE FIREWALL RULES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/NETWORKING/FIRE
2. Select the firewall rule that you want to update.
3. Click **Edit**.
4. For the **Logs** setting, select **On**.
5. Click **Save**.

Disabling firewall rules logging

CONSOLE GCLOUD API

1. Go to the Firewall rules page in the Google Cloud Console.
   GO TO THE FIREWALL RULES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/NETWORKING/FIRE
2. Select the firewall rule that you want to update.
3. Click **Edit**.
4. For the **Logs** setting, select **Off**.
5. Click **Save**.

Viewing logs

Firewall rule logs are created in the project that hosts the network containing the VM instances and firewall rules. With Shared VPC (https://cloud.google.com/vpc/docs/shared-vpc), VM instances are created in service projects, but they use a *Shared VPC Network* located in the host project. Firewall rules logs are stored in that host project.

Use the Logs section (https://cloud.google.com/logging/docs/view/logs_viewer_v2) of the Cloud Console to view firewall rule logs.

The following advanced Stackdriver filters demonstrate how you can search for specific firewall events. In each filter, replace ***PROJECT_ID*** with your project ID (https://cloud.google.com/resource-manager/docs/creating-managing-projects#identifying_projects).

All firewall logs

```
resource.type="gce_subnetwork"
logName="projects/PROJECT_ID/logs/compute.googleapis.com%2Ffirewall"
```

Specific subnets

```
resource.type="gce_subnetwork"
logName="projects/PROJECT_ID/logs/compute.googleapis.com%2Ffirewall"
resource.labels.subnetwork_name="SUBNET_NAME"
```

Replace ***SUBNET_NAME*** with the name of the specific subnet.

Specific VMs

```
resource.type="gce_subnetwork"
logName="projects/PROJECT_ID/logs/compute.googleapis.com%2Ffirewall"
jsonPayload.instance.vm_name="INSTANCE_NAME"
```

Replace ***INSTANCE_NAME*** with the name of the specific VM instance.

Connections from a specific country

```
resource.type="gce_subnetwork"
logName="projects/PROJECT_ID/logs/compute.googleapis.com%2Ffirewall"
```

```
jsonPayload.remote_location.country=COUNTRY
```

where ***COUNTRY*** is the ISO 3166-1 alpha-3 (https://wikipedia.org/wiki/ISO_3166-1_alpha-3#Current_codes) code.

Exporting logs

To export firewall rules logs, follow these Stackdriver directions: Exporting with the Logs Viewer (https://cloud.google.com/logging/docs/export/configure_export_v2).

You can use the example advanced filters (#viewing_logs) to narrow the logs that you export.

Table of interactions

- In the case of VM-to-VM communication, log records might be generated by both VMs, depending on their respective firewall rules.
- The logged connection includes packets flowing both ways if the initial packet was allowed by the firewall.
- For a given VM, incoming connections are matched against firewall rules configured on that VMs and outgoing connections are matched against egress firewall rule configured on that VM.
- An allowed connection that matches a firewall rule with "allow and logging" is logged only once. The log entry is not repeated every 5 sec even if the connection endures.
- A denied connection matching a firewall rule with "denied and logging" does repeat the log entry every 5 seconds for as long as there are packets observed in that denied connection.

This table shows the firewall logging behavior from the perspective of a single VM.

In a scenario in which a VM1 has an ingress rule R1 that matches packets and egress rule R2 that also matches packets, the behavior of firewall logging is as follows:

VM1 has Ingress Rule R1 (matching packets)	VM1 has Egress Rule R2 (matching packets)	Connection Direction	ActionLog

VM1 has Ingress Rule R1 (matching packets)	VM1 has Egress Rule R2 (matching packets)	Connection Direction	Action	Log
Allow + Log	Allow	Ingress	Allow	One log entry: disposition=allow, rule=R1
	Deny			
	Allow + Log			
	Deny + Log			
Allow	Allow	Ingress	Allow	No logging
	Deny			
	Allow + Log			
	Deny + Log			
Deny + Log	N/A	Ingress	Deny	One log entry every 5 seconds: disposition=deny, rule=R1
Deny	N/A	Ingress	Deny	No logging
Allow	Allow + Log	Egress	Allow	One log entry: disposition=allow, rule=R2
Deny				
Allow + Log				
Deny + Log				
Allow	Allow	Egress	Allow	No Logging
Deny				
Allow + Log				
Deny + Log				
N/A	Deny + Log	Egress	Deny	One log entry every 5 seconds: disposition=deny, rule=R2
N/A	Deny	Egress	Deny	No logging

Note that ingress and egress are symmetric.

This is the detailed description of the firewall logs semantics:

- Allow + Log (logging is supported for TCP and UDP only)
  - Connection initiated in the direction to which the rule applies causes a single log record to be created.
  - Reply traffic is allowed due to connection tracking. Reply traffic does not cause any logging to occur, regardless of firewall rules in that direction.
  - If the connection expires from the firewall (inactive for 10 minutes or TCP RST received), then another packet in either direction may trigger logging.
  - Logging is based on 5-tuples. TCP flags do not affect logging behavior.
- Deny + Log (logging is supported for TCP and UDP only)
  - Packets are dropped (no connection is initiated).
  - Each packet that corresponds to a unique 5-tuple is logged as a failed connection attempt.
  - The same 5-tuple is logged again every 5 seconds if it continues to receive packets.

Troubleshooting

Cannot view logs

If you cannot view firewall rules logs in the Logs section of the Cloud Console, check the following:

Possible cause: Insufficient permissions

Ask the project owner to make sure your IAM member at least has the Logs Viewer (https://cloud.google.com/iam/docs/understanding-roles#logging-roles) role for the project. Refer to permissions (#permissions) for more information.

Possible cause: Subnetwork logs might be excluded from Stackdriver

In the Cloud Console, navigate to **Logging > Logs ingestion**, and verify that either *GCE Subnetwork* is **not** excluded or, if it is partially excluded, that the exclusion filter does **not**

apply to firewall logs.

Possible cause: Legacy networks not supported

You cannot use firewall rules logging in a legacy network (https://cloud.google.com/vpc/docs/legacy). Only VPC networks (https://cloud.google.com/vpc/docs/vpc) are supported.

Possible cause: Make sure you're looking in the correct project

Because firewall rule logs are stored with the project that contains the **network**, it's important to make sure you're looking for logs in the correct project. With Shared VPC, VM instances are created in service projects, but they use a *Shared VPC Network* located in the host project. For Shared VPC scenarios, firewall rules logs are stored in that host project.

If Shared VPC is involved, you'll need appropriate permissions (#permissions) to the host project in order to view firewall rules logs. Even though the VM instances themselves are located in service projects, firewall rules logs for them are located in the host project.

Log entries missing

Possible cause: Connections might not match the firewall rule you expect

Verify that the firewall rule you expect is in the list of applicable firewall rules for an instance. Use the Cloud Console to view details for the relevant instance, then click the **View details** button in the *Network interfaces* section on its *VM instance details* page. Inspect applicable firewall rules in the *Firewall rules and routes details* section of its *Network interface details* page.

Review the firewall rules overview (https://cloud.google.com/vpc/docs/firewalls) to make sure you have created your firewall rules correctly.

You can use tcpdump (http://www.tcpdump.org/) on the VM to determine if connections it sends or receives have addresses, ports, and protocols that would match the firewall you expect.

Possible cause: A higher priority rule with firewall rules logging disabled might apply

Firewall rules are evaluated according to their priorities (https://cloud.google.com/vpc/docs/firewalls#priority_order_for_firewall_rules). From the perspective of a VM instance, only one firewall rule applies to the traffic.

A rule that you think would be the highest priority applicable rule might not actually be the highest priority applicable rule. A higher priority rule that does not have logging enabled might apply instead.

To troubleshoot, you can temporarily enable logging for *all* possible firewall rules applicable to a VM. Use the Cloud Console to view details for the relevant VM, then click the **View details** button in the *Network interfaces* section on its *VM instance details* page. Inspect applicable firewall rules in the *Firewall rules and routes details* section of its *Network interface details* page, and identify your custom rules in that list. Temporarily enable logging for all of those custom firewall rules.

With logging enabled, you can identify the applicable rule. Once identified, be sure to disable logging for all rules that do not actually need it.

Missing metadata for some log entries

Possible cause: Configuration propagation delay

If you update a firewall rule that has firewall logging enabled, it might take a few minutes before Google Cloud finishes propagating the changes necessary to log traffic that matches the rule's updated components.

What's next

- View Stackdriver Logging (https://cloud.google.com/logging/docs) documentation
- View Stackdriver Logging export (https://cloud.google.com/logging/docs/export/configure_export_v2) documentation

Last updated December 4, 2019.