Guide to firewall rules

So far, you've learned about some key cloud boundary concepts, like perimeter protection, which is the security armor that protects cloud environments from unauthorized access and threats. You also explored the significance of firewalls, which act as checkpoints within networks, controlling traffic between the internal network and the public network that is accessible to anyone. In this reading, you'll learn more about creating and configuring Virtual Private Cloud (VPC) firewalls to protect an organization's cloud resources.

VPC firewall rules

As a cloud security professional, you can apply VPC firewall rules in Google Cloud to a project, network, or multiple VPC networks in your organization using firewall policies. VPC firewall rules control connections to or from virtual machine (VM) instances in your VPC network. By default, incoming traffic from outside your network is blocked.

Create a firewall rule in Google Cloud console

Create a firewall rule using the Google Cloud console:

1. In the Google Cloud console, click the **Navigation** menu.
2. Click **VPC network** > **Firewall**, and then click **+ Create firewall rule.**

When you create a VPC firewall rule, you must specify the required settings and set any optional settings. These settings include the following:

- **Name and description**: Enter a name for the firewall rule. You can also provide an optional description of the firewall rule.
- **Logs**: Select **On** to enable firewall rules logging. Logs record the network connections that the firewall rule allows or denies. You can enable firewall rules logging for each firewall rule.
- **Network**: Select the network from the drop-down that the firewall rule applies to.
- **Priority**: Enter the order that a rule will be applied within a network. The default priority level is **1000.** Rules with lower numbers indicate a higher priority and rules with a higher value indicate a lower priority. For example, a rule with a priority of **1000** takes precedence over a rule with a priority of **1100.**
- **Direction of traffic**: Select the direction of the traffic. **Ingress** applies to inbound traffic, while **Egress** applies to outbound traffic.
- **Action on match**: Select to have the firewall rule **Allow** or **Deny** traffic.
- **Targets and target tags**: Select from the **Targets** drop-down to specify which targets to apply the firewall rule to.

    - **All instances in the network**: Apply the firewall rule to all Virtual Machine (VM) instances in the network.
    - **Specified target tags**: Apply the firewall rule to a specific group of instances using target tags.
        - **Target tags:** Enter identifier value strings that apply to the firewall rule, like **web.**
    - **Specified service account:** Apply the firewall rule to a specific service account.
- **Source filter and ranges**: This setting allows you to enter the source of traffic that the firewall rule applies to. You can select either **IPv4 ranges** or **IPv6 ranges from the** drop-down. You then must enter the range of IP addresses in Classless Inter-Domain Routing (CIDR) notation, like 10.128.0.0/9.
- **Second source filter**: Select additional filters to apply your rule to specific sources of traffic from the drop-down.
- **Destination filter and ranges:** This setting allows you to select **None, IPv4 ranges,** or **IPv6 ranges** from the drop-down as the destination of traffic that the firewall rule applies to. You must also specify the range of IP addresses in CIDR notation.
- **Protocols and ports**: Select the protocols this traffic rule applies to, like **TCP** and / or **UDP,** and the protocol's port to open, like **80**.
- **Disable rule**: Select **Enabled** to enforce this firewall rule is enforced. Or, select **Disabled** to not enforce the rule. The default enforcement is enabled.

Pro tip: In Google Cloud, you can create VPC firewall rules using the Google Cloud console, the Google Cloud CLI, or the REST API.

Firewall Rules logs and VPC Flow Logs

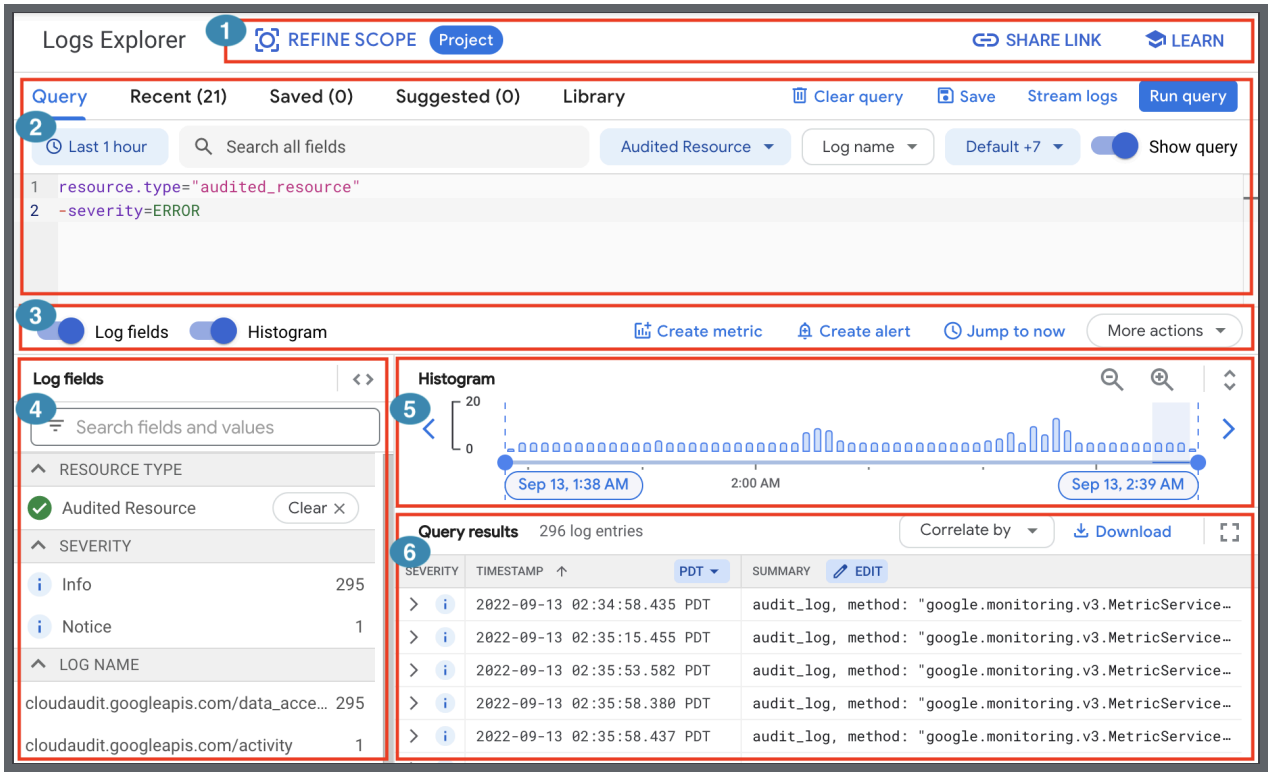
Cloud Logging collects logs from your Google Cloud resources which you can then retrieve, access, and analyze with Logs Explorer**.** There are two types of logs that you should be familiar with: Firewall Rule logs and VPC Flow Logs.

Firewall Rules logs record the connections relating to actions of firewall rules. For example, use a Firewall Rules log to determine if a firewall rule is working as intended to deny traffic from a specific IP address range. When you enable Firewall Rules logging, Google Cloud creates a *connection record* which records each time the rule allows or denies traffic. You can access connection records in Cloud Logging. Each connection record contains the source and destination IP addresses, the protocol, ports, data and time, and more.

VPC Flow Logs record information about connections entering and exiting VMs in a VPC. VPC Flow Logs include information, like source and destination IP addresses, ports, protocols, and timestamps. You can use VPC Flow Logs to monitor network traffic patterns, identify potential security threats, and troubleshoot network connectivity issues.

Logs Explorer

With the **Logs Explorer,** you can build queries in the **query editor** to filter logs. The **Logs Explorer** contains the following sections:



1. **Action**: Use the **Action** toolbar to refine the scope of a log search with options, like scope by current **Project** or scope by **Storage**
2. **Query**: Use the **query editor** to build and refine queries.
3. **Results**: Use the **Results** toolbar to configure the settings for the logs explorer results. Select toggle options to hide **Log fields** or the **Histogram,** configure log-based metrics or alerts, and refresh query results to include the current time.
4. **Log fields**: Use the **Log fields** pane to search from a high-level summary of logs data and refine a query. The pane shows log entries broken down by different dimensions, like resource type and severity.
5. **Histogram**: Use the **Histogram** pane to visualize the distribution of logs over time.
6. **Query results**: Use the **Query results** pane to access your query results.

Key takeaways

Firewall rules are integral to protecting cloud resources. Understanding how to create and configure firewall rules is an important part of cloud security. In addition, understanding how to retrieve and filter log entries is a crucial ability in monitoring and analyzing network threats.

Resources for more information

- If you would like to learn more about configuring settings for VPC firewalls, review VPC firewall rules.
- To learn more about effective log querying, investigate Logs Explorer.