Google Cloud Platform VPC Firewall Rules



|  |  |  |  |
| --- | --- | --- | --- |
| Date | Name | Description | Version |
| 05/12/2022 | Caitlin Parker | Created first Draft | 1.0 |
|  |  |  |  |
|  |  |  |  |

## Version Control

Table of Contents

[Version Control 1](#_Toc121240495)

[GCP VPC Firewall Location 3](#_Toc121240496)

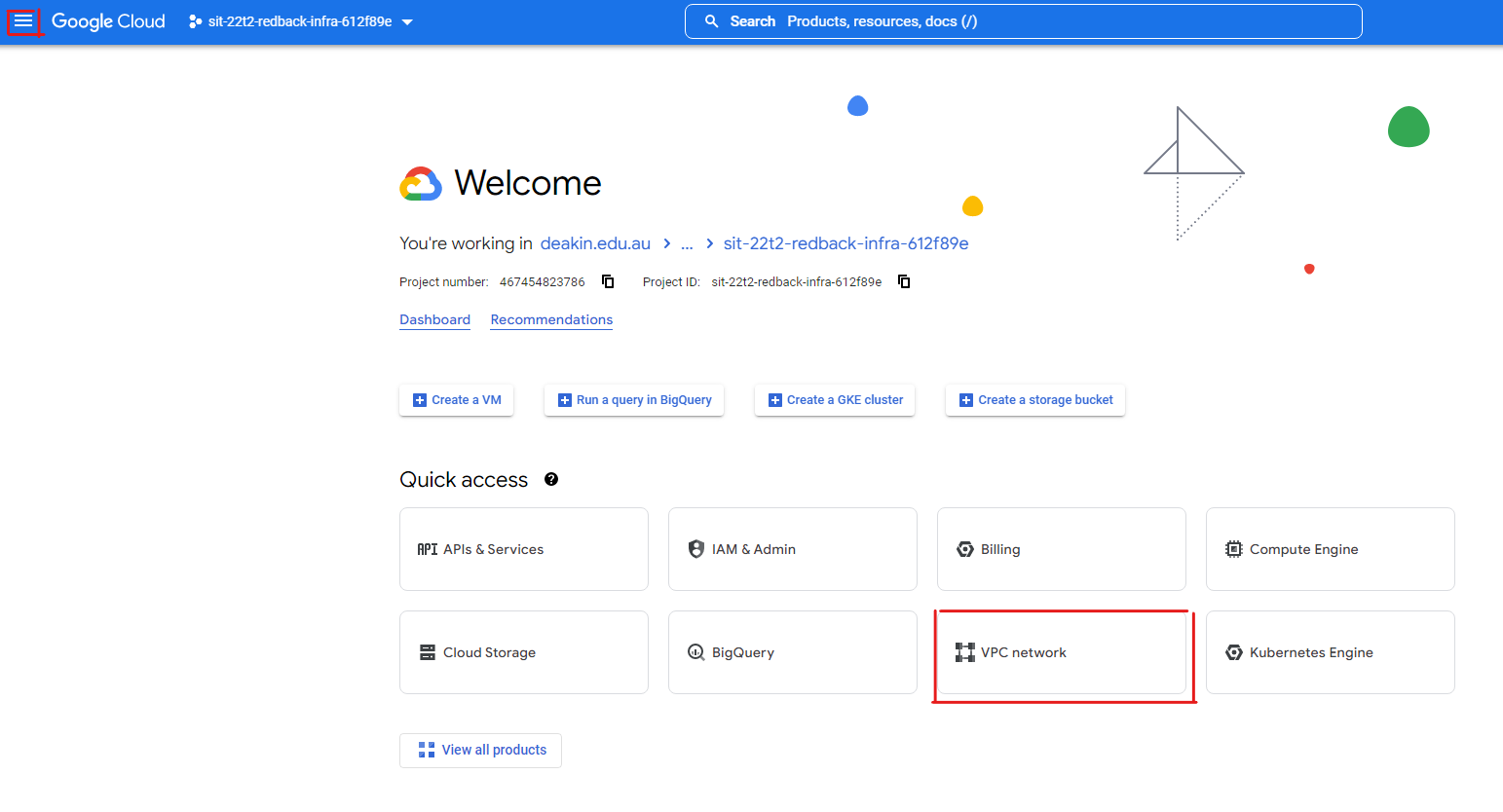
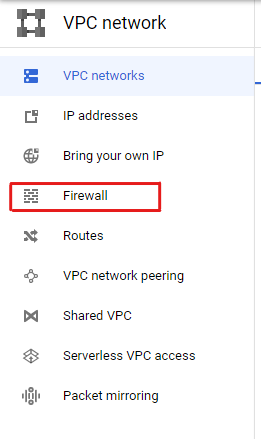
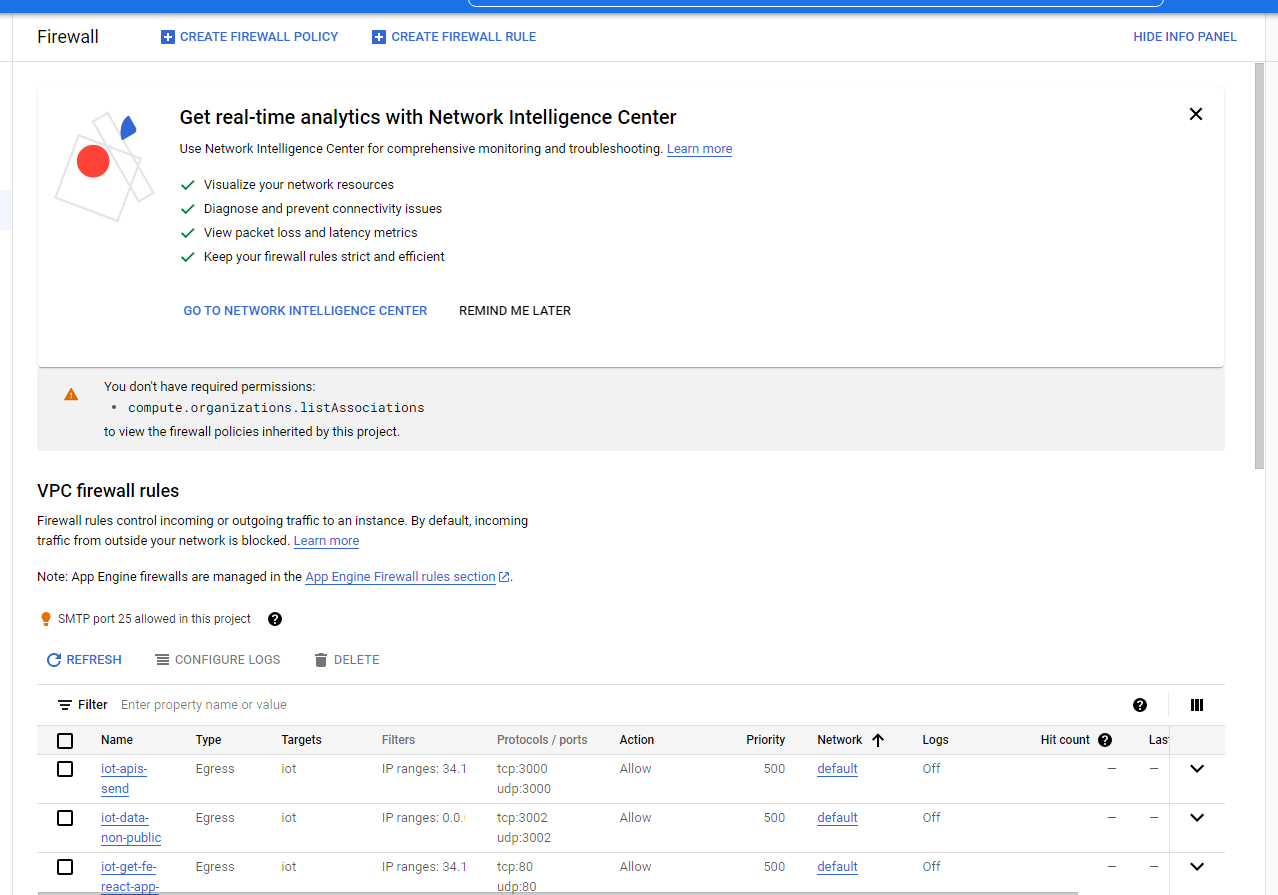
[Edit Existing Firewall Rule 4](#_Toc121240497)

[Create Firewall Rule 4](#_Toc121240498)

[Google Default Firewall Rules 5](#_Toc121240499)

[IoT VMs Specific firewall rules 6](#_Toc121240500)

# GCP VPC Firewall Location

1. Log into the [Google Cloud Platform](https://console.cloud.google.com/) with your Deakin account. Access is granted after a form is filled out for the team.
2. Click on “VPC network” in the quick access section or go to the hamburger menu.
3. Navigate to “Firewall” in the side menu.  
   
4. The firewall page is where all the existing firewall rules for the project can be found, edited and where new ones can be created.  
   

### Edit Existing Firewall Rule

* To edit a firewall rule, click on the name of the rule that needs to be changed and then click the edit button.
* There are some sections of the firewall rule that cannot be edited. This includes the name, the direction, and action on match. A rule can also be disabled and enabled in the edit option.

### Create Firewall Rule

* To create a firewall rule, click on the “CREATE FIREWALL RULE” button.
* Fill out the information on the form. To better understand the form section, read over the [Firewall rule components](https://cloud.google.com/vpc/docs/firewalls#firewall_rule_components).[1]

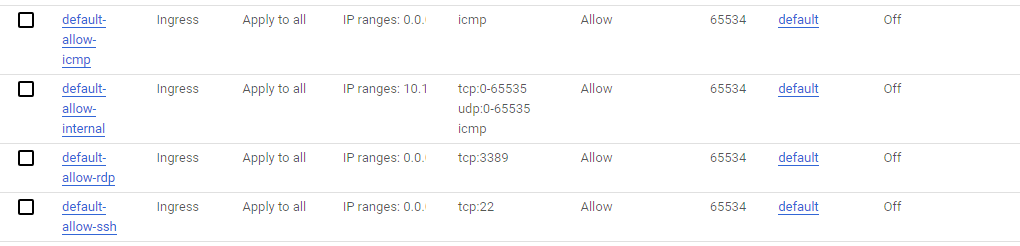
# Google Default Firewall Rules

The Google VPC network have two implied rules for IPv4 and another two for IPv6 [2] that are not listed in the firewall rule sections.

* Implied IPv4 allow egress rule
* Implied IPv4 deny ingress rule
* Implied IPv6 allow egress rule
* Implied IPV6 deny Ingress rule.

All rules are set to the lowest possible priority on GCP which is priority 65535 and have the destination of the internet which is 0.0.0.0/0 for IPv4 and ::/0 for IPv6. [2]

On top of the implied rules from Google Cloud there are a set of default firewall rules that google implements to the VPC network. These rules are listed towards the bottom of the firewall list as they have a priority level of 65534. [2]



# IoT VMs Specific firewall rules

The IoT VM has the following stipulations for firewall rules.

* HTTP GET requests from <http://34.129.10.237:80> (for a FE React app)
* HTTP GET/PUT/POST/DELETE requests from <http://34.129.10.237:3000> (for the BE IoT APIs)
* 0.0.0.0:3002 is processing non-public IoT data.
* MQTT websocket connection in the FE React app is running through the URL f5b2a345ee944354b5bf1263284d879e.s1.eu.hivemq.cloud on port 8884
* MongoDB connection in running through URL //username:password@cluster-redback.pa0yu.mongodb.net
* MQTT connection in the BE IoT service is running through URL f5b2a345ee944354b5bf1263284d879e.s1.eu.hivemq.cloud on port 8883.

The following firewall rules were created from the stipulations written above. URLs are unable to be selected in the firewall so those instances will be using the internet IPv4 of 0.0.0.0.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Type | Range | Ports | Action | Priority |
| [iot-apis-send](https://console.cloud.google.com/networking/firewalls/details/iot-apis-send?project=sit-22t2-redback-infra-612f89e) | Engress | 34.192.10.237 | TCP: 3000 UDP: 3000 | Allow | 500 |
| [iot-data-non-public](https://console.cloud.google.com/networking/firewalls/details/iot-data-non-public?project=sit-22t2-redback-infra-612f89e) | Engress | 0.0.0.0 | TCP: 3002 UDP: 3002 | Allow | 500 |
| [iot-get-fe-react-app-send](https://console.cloud.google.com/networking/firewalls/details/iot-get-fe-react-app-send?project=sit-22t2-redback-infra-612f89e) | Engress | 34.129.10.237 | TCP: 80 UDP: 80 | Allow | 500 |
| [iot-mqtts-be-connection](https://console.cloud.google.com/networking/firewalls/details/iot-mqtts-be-connection?project=sit-22t2-redback-infra-612f89e) | Engress | 0.0.0.0 | TCP: 8883 UDP: 8883 | Allow | 500 |
| [iot-wss-mqtt-websocket](https://console.cloud.google.com/networking/firewalls/details/iot-wss-mqtt-websocket?project=sit-22t2-redback-infra-612f89e) | Engress | 0.0.0.0 | TCP: 8884 UDP:8884 | Allow | 500 |
| [iot-data-non-public-send](https://console.cloud.google.com/networking/firewalls/details/iot-data-non-public-send?project=sit-22t2-redback-infra-612f89e) | Ingress | 0.0.0.0 | TCP: 3002 UDP:3002 | Deny | 500 |
| [iot-apis-reiceve](https://console.cloud.google.com/networking/firewalls/details/iot-apis-reiceve?project=sit-22t2-redback-infra-612f89e) | Ingress | 34.129.10.237 | TCP: 3000 UDP:3000 | Allow | 500 |
| [iot-get-fe-rect-app](https://console.cloud.google.com/networking/firewalls/details/iot-get-fe-rect-app?project=sit-22t2-redback-infra-612f89e) | Ingress | 34..129.10.237 | TCP: 80 UDP:80 | Allow | 500 |

References

[1] Google Cloud (2022, Nov. 30). *VPC firewall rules: Firewall rule components* [Website]. Available: <https://cloud.google.com/vpc/docs/firewalls#firewall_rule_components>

[2] Google Cloud (2022, Nov. 30). *VPC firewall rules: Implied rules* [Website]. Available: <https://cloud.google.com/vpc/docs/firewalls#default_firewall_rules>