Google Cloud Platform Network Route and Firewall Rules

Routing (Traffic Engineering)

By default the routing table is populated with next hops for the default networks.

- Can not be shared between networks or projects.
- There is no router. Google uses Traffic Engineering.
- Applied to traffic as it exists the VM.
- Traffic not matching both a route and a firewall rule is dropped.
- Allowed traffic with a route is delivered to its target

Billing is for egress:

- To the internet.
- From one region to another in the same network.
- Between zones within a region.

Firewall Rules

Networks can have both ingress and egress firewall rules.

- Only supports allow rules.
- Rules can match a single IP address or a range.
- Rules can be applied to tags.
- Default rules are only created for auto-type networks.
- Can not be shared between networks or projects.
- Priority can be from 0 to 65535. 0 is the highest priority.

There are two implied firewall rules that are not shown in the Cloud Console:

- Implied allow egress rule:
  - Allows traffic to destination or 0.0.0.0
  - Has the lowest priority of 65535
- Implied deny ingress rule:
  - Denies traffic from source 0.0.0.0
  - Has the lowest priority of 65535

Default network firewall rules:

- default-allow-internal:
  - Allows ingress among instances in the network.
  - Has the second-to-lowest priority of 65534.
- default-allow-ssh:
  - Allows ingress connections on TCP port 22 from any source to any instance in the network.
  - This rule has a priority of 65534.
- default-allow-rdp:
  - Allows ingress connections on TCP port 3389 from any source to any instance in the network.
  - This rule has a priority of 65534.
- default-allow-icmp:
  - Allows ingress ICMP traffic from any source to any instance in the network.
  - This rule has a priority of 65534.