**Load balancer summary**

1. The user makes a request to the application, which is deployed on Compute Engine. The request first lands on Cloud Load Balancing.
2. Cloud Load Balancing distributes traffic to the Compute Engine managed instance group (MIG), which scales the number of instances based on traffic volume.

**Instance group**

1. An instance group is a collection of virtual machine (VM) instances that you can manage as a single entity.
2. A MIG is a collection of virtual machine (VM) **instances** that you can manage as a single entity

**Firewall rules**

1. Firewall rules allow or deny ingress traffic to, and egress traffic from your instances.
2. In a custom Virtual Private Cloud (VPC) network with multiple subnets, by default, egress traffic is allowed, but ingress traffic is denied.
3. To enable ingress traffic and allow VM instances in different subnets to communicate with each other, you can create a [global network firewall policy](https://cloud.google.com/firewall/docs/network-firewall-policies) in Cloud Next Generation Firewall on the VPC network, which allows ingress traffic from a specific IP address range of the subnet.

**RDP server**

1. Allow ingress RDP connections to VMs.
2. Create a firewall rule to allow Microsoft Remote Desktop Protocol (RDP) connections to your VM.

**Load balanced web app**

1. GDC provides load balancers that enable applications to expose services to one another.
2. Load balancers in GDC perform layer four (L4) load balancing, which means they map a set of configured frontend TCP or UDP ports to corresponding backend ports.