Working with Networking and Security on GKE Clusters

Janani Ravi
CO-FOUNDER, LOONYCORN

www.loonycorn.com

Overview

Defining and applying security policies to clusters

Using private clusters to isolate workloads

Using an internal load balancer to direct traffic to clusters with internal IP addresses

Applying pod security policies to restrict pods on clusters

Demo

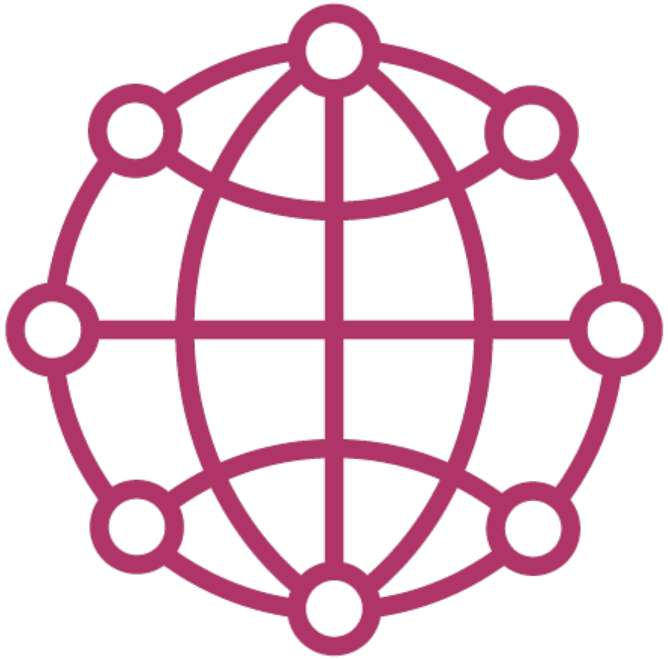
Create a cluster with network policies enabled

Apply ingress and egress network policies on this cluster

Network Policies

Restrict connections between pods. Improve security by reducing the exposure of apps running on the cluster.

By default all pods in a cluster can talk to other pods running on the same cluster



Network Policies

Ingress policies for incoming traffic

- Which pods can connect to me?

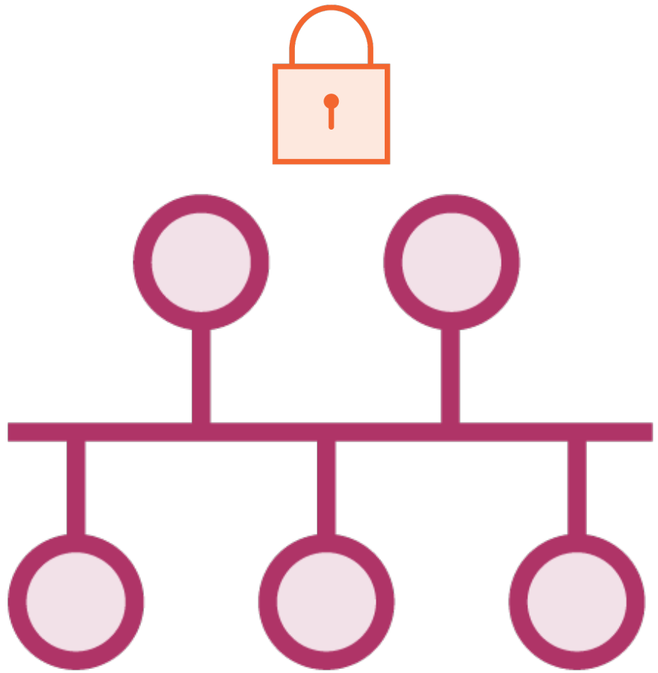
Egress policies for outgoing traffic

- Which pod can I send traffic to?

Private Clusters

Private Clusters

Nodes have only internal IP, not external IP addresses. Cluster workloads will be isolated from the public internet.



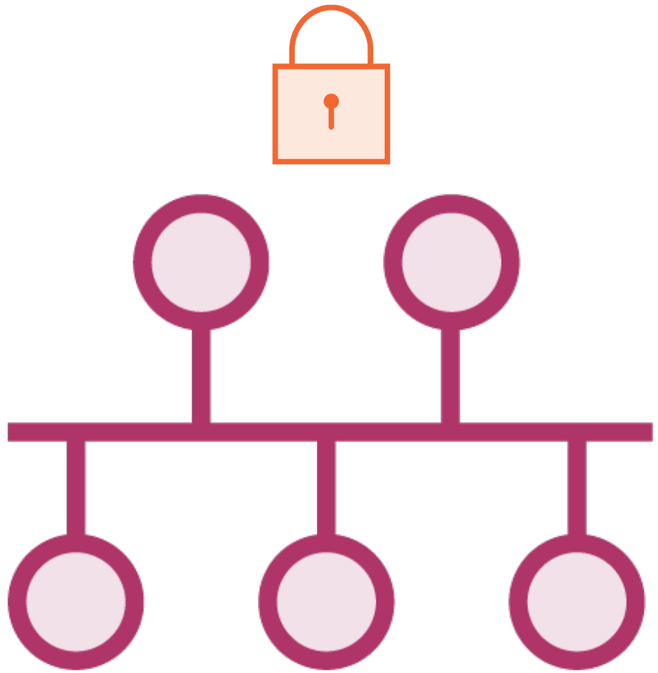
Private Clusters

All nodes have just internal IP addresses

Cannot be accessed by external clients

Cluster master endpoint is reachable

- Only from internal IP addresses
- Only from a set of authorized networks



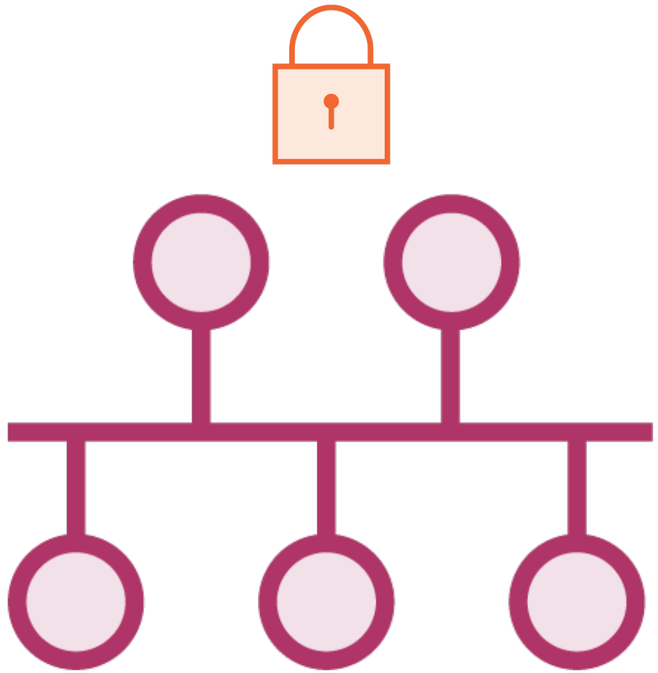
Private Clusters

Google has special access to the master for scheduling and cluster management

VPC network peering to connect with the Google-owned VPC network

Private Google access for specific use cases

- Pull container images from GCR
- Send logs to Stackdriver



Private Clusters

Not compatible with legacy networks on the GCP

Needs Kubernetes version >1.8.14-gke.0

Demo

Creating and working with a private GKE cluster

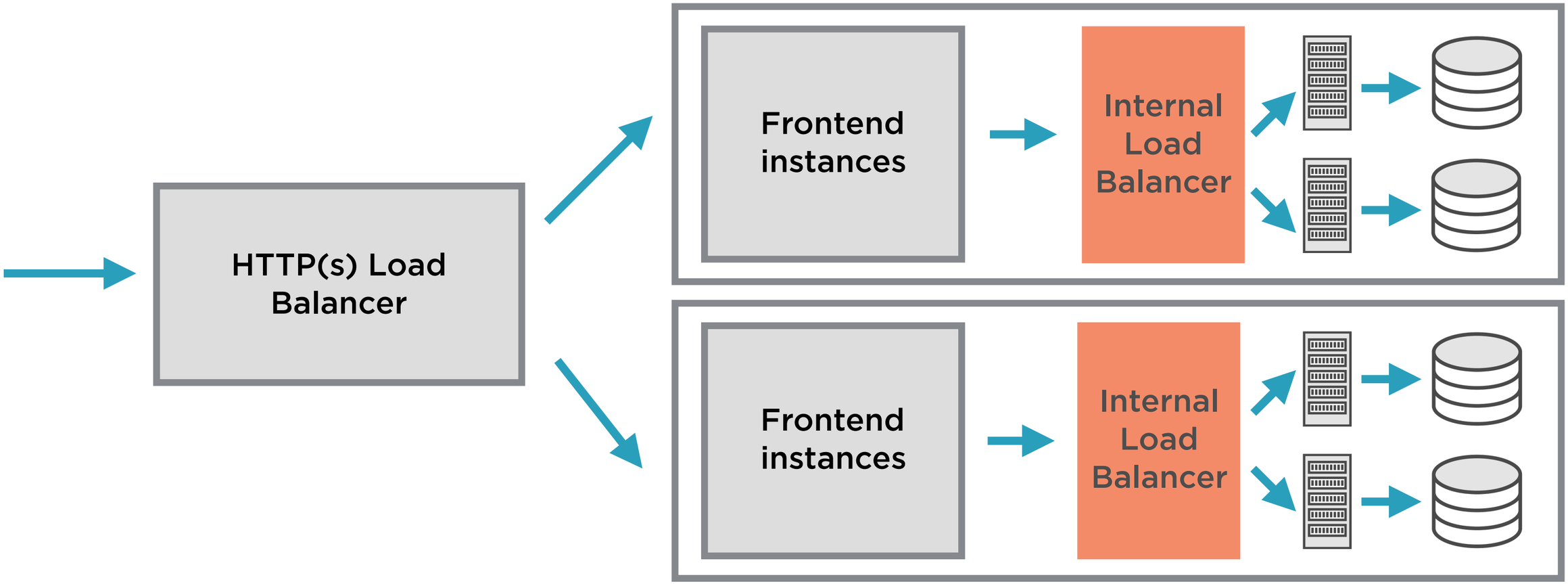
Authorizing VMs to access nodes in the private cluster

Internal Load Balancing

Internal Load Balancing

Run and scale your services behind a private load balancing IP address that is accessible only to instances in your VPC

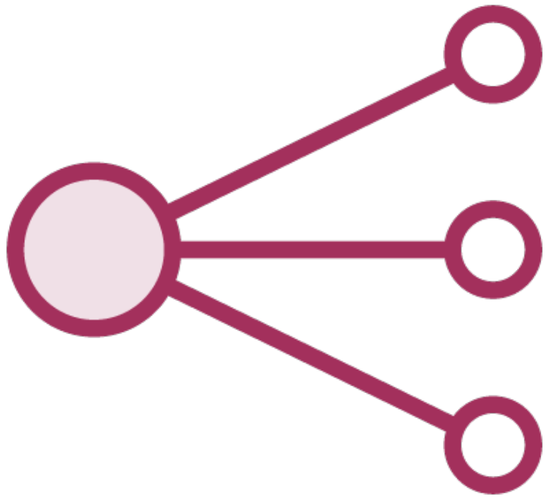
3-tiered Web Application



Internal Load Balancer

Acts as a frontend to your private backend instances

Internal load balancing makes your cluster's services accessible to applications on the **same network** **but outside** the cluster



Internal Load Balancer

External clients can access internal services on cluster

Clients should be on the same network and in the same region

Eliminates overhead of configuring an external load balancer

- No firewall rules to limit access
- No network routes to allow external access to applications

Demo

Create and configure an internal load balancer to access applications on the cluster

Accessible only to VMs on the same network and in the same region

Demo

Create a pod security policy

Apply and enable this policy on the cluster

Allow non-admin service accounts to use this policy

Allow pod service accounts to use this policy

PodSecurityPolicy

An admission control resource that validates requests to create and update pods on the cluster. Defines a set of conditions that pods must meet to be accepted by the cluster.

Using the PodSecurityPolicy

Define policy

Create and define rules that pods deployed on the cluster should adhere to

Enable controller

Admissions controller validates requests to create and update pods against defined policies

When multiple policies are available, the controller uses the first policy that successfully validates

Summary

Defining and applying security policies to clusters

Using private clusters to isolate workloads

Using an internal load balancer to direct traffic to clusters with internal IP addresses

Applying pod security policies to restrict pods on clusters