Configuring Load Balancers in the Google Cloud Platform

Vitthal Srinivasan
CO-FOUNDER, LOONYCORN

www.loonycorn.com

Overview

Configuring and using different kinds of load balancers

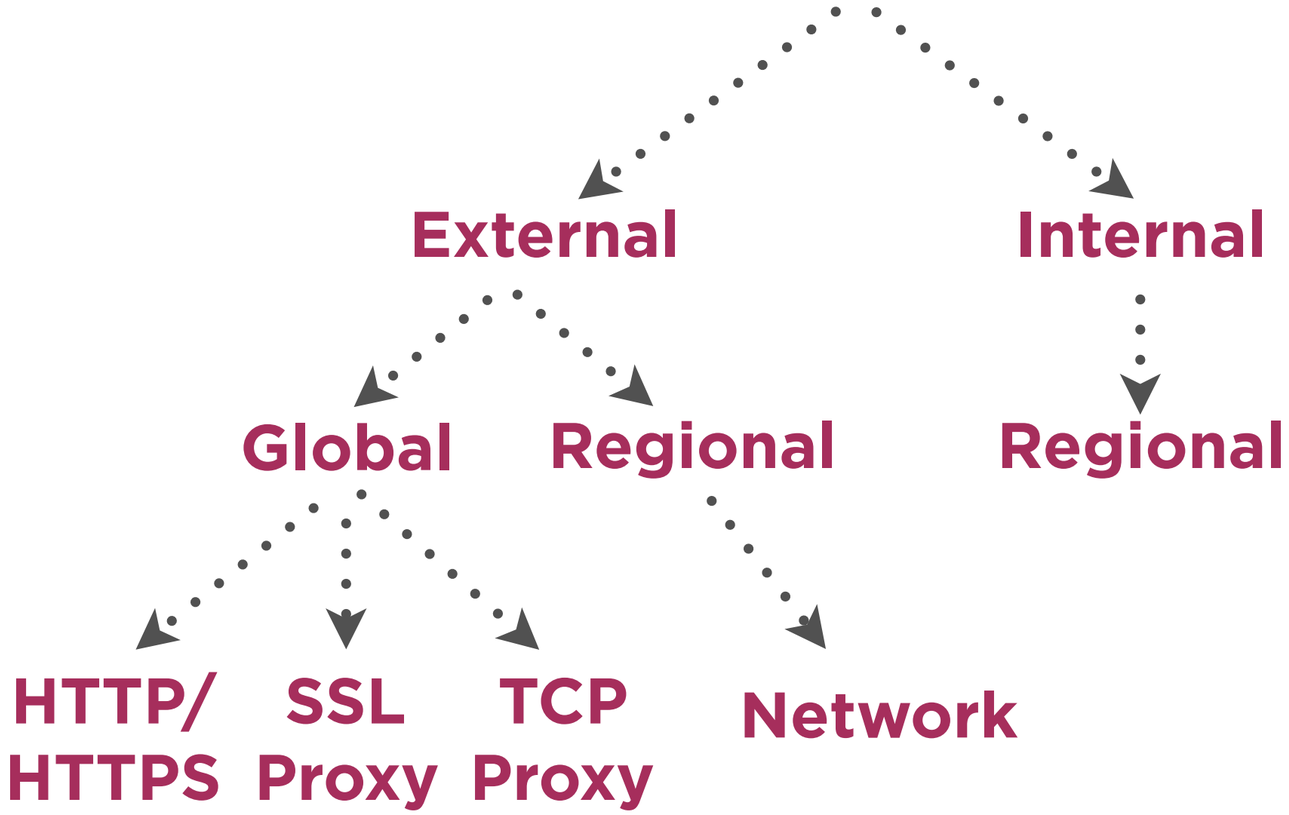
SSL proxy for secure connections, TCP proxy for TCP connections

Network load balancing for UDP traffic

Internal load balancing for traffic from instances on the GCP

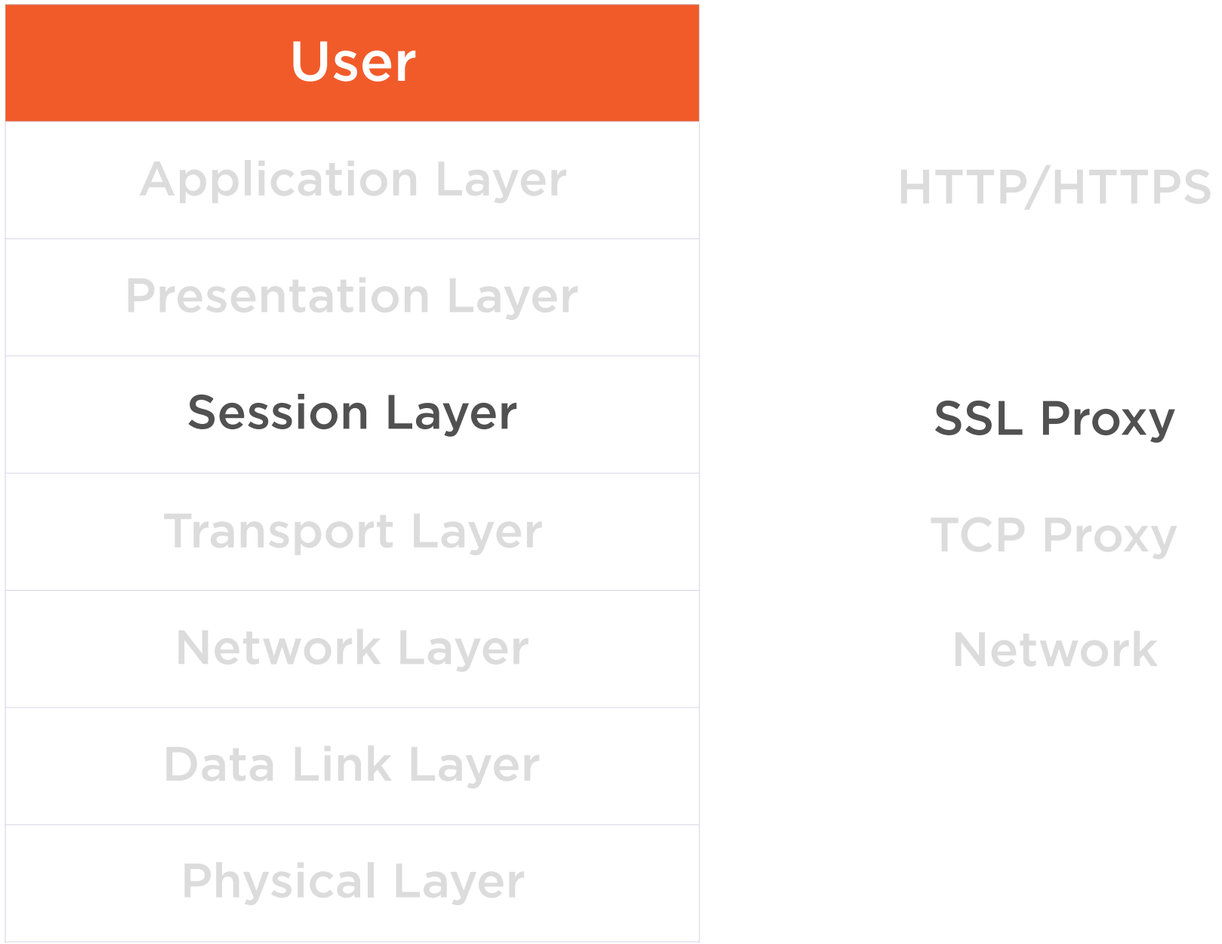
SSL Proxy Load Balancer

Load Balancing



Load Balancing

SSL Proxy Load Balancing



SSL operates in the session layer

SSL Proxy Load Balancing

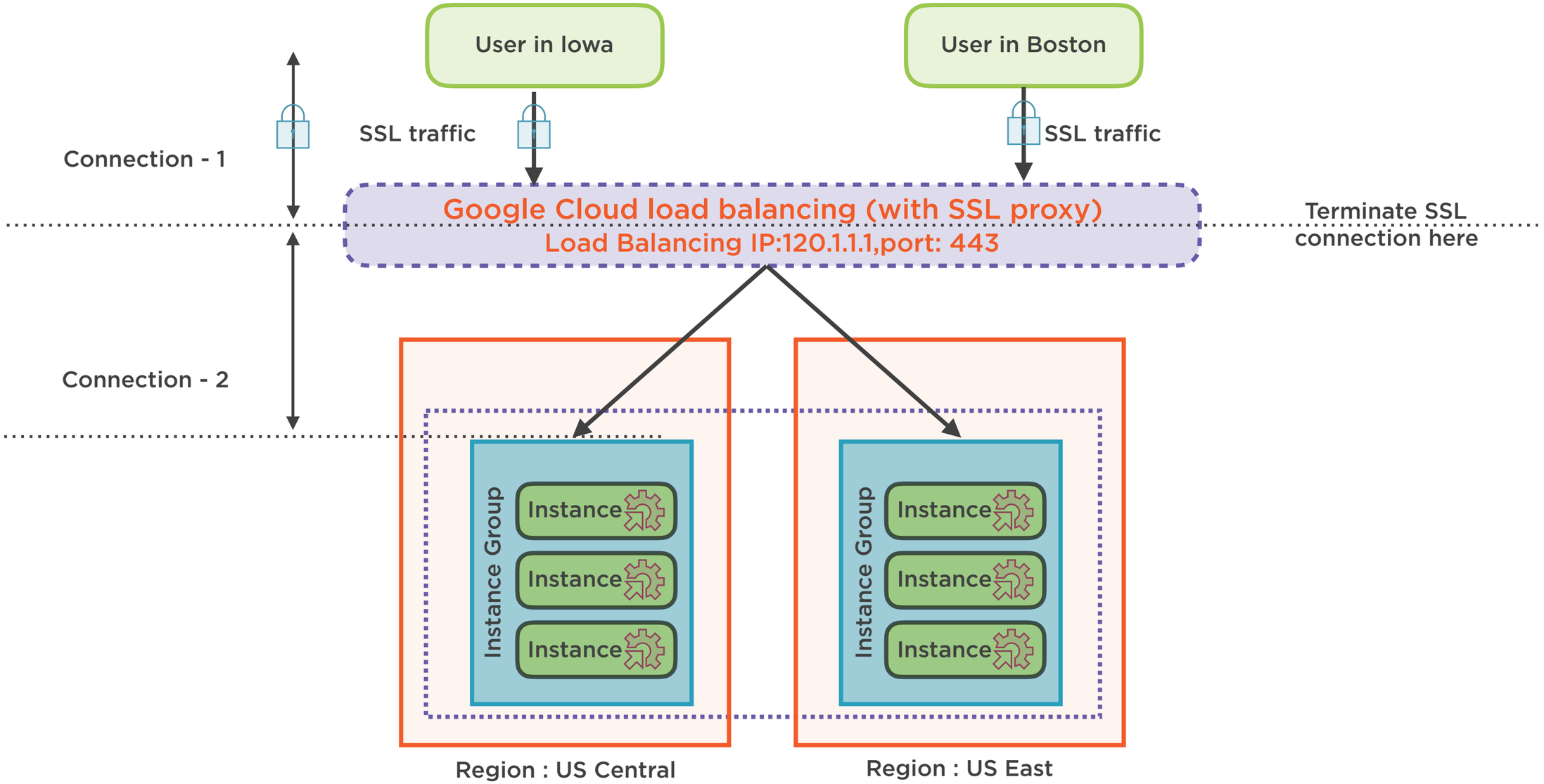
Use only for non-HTTP(S) SSL traffic

For HTTP(S), just use HTTP(S) load balancing

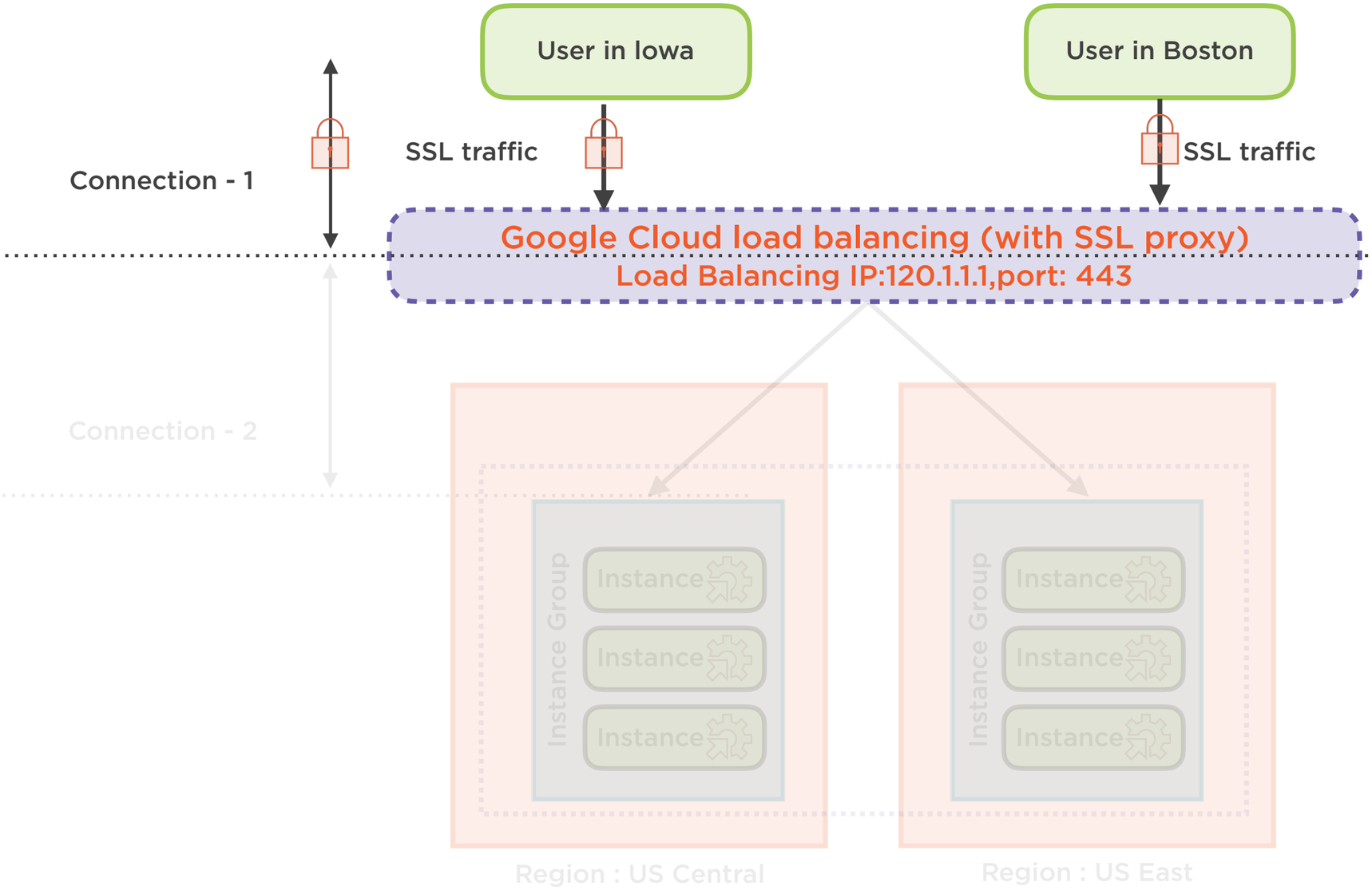
SSL connections are terminated at the global layer

Then proxied to the closest available instance group

SSL Proxy Load Balancing



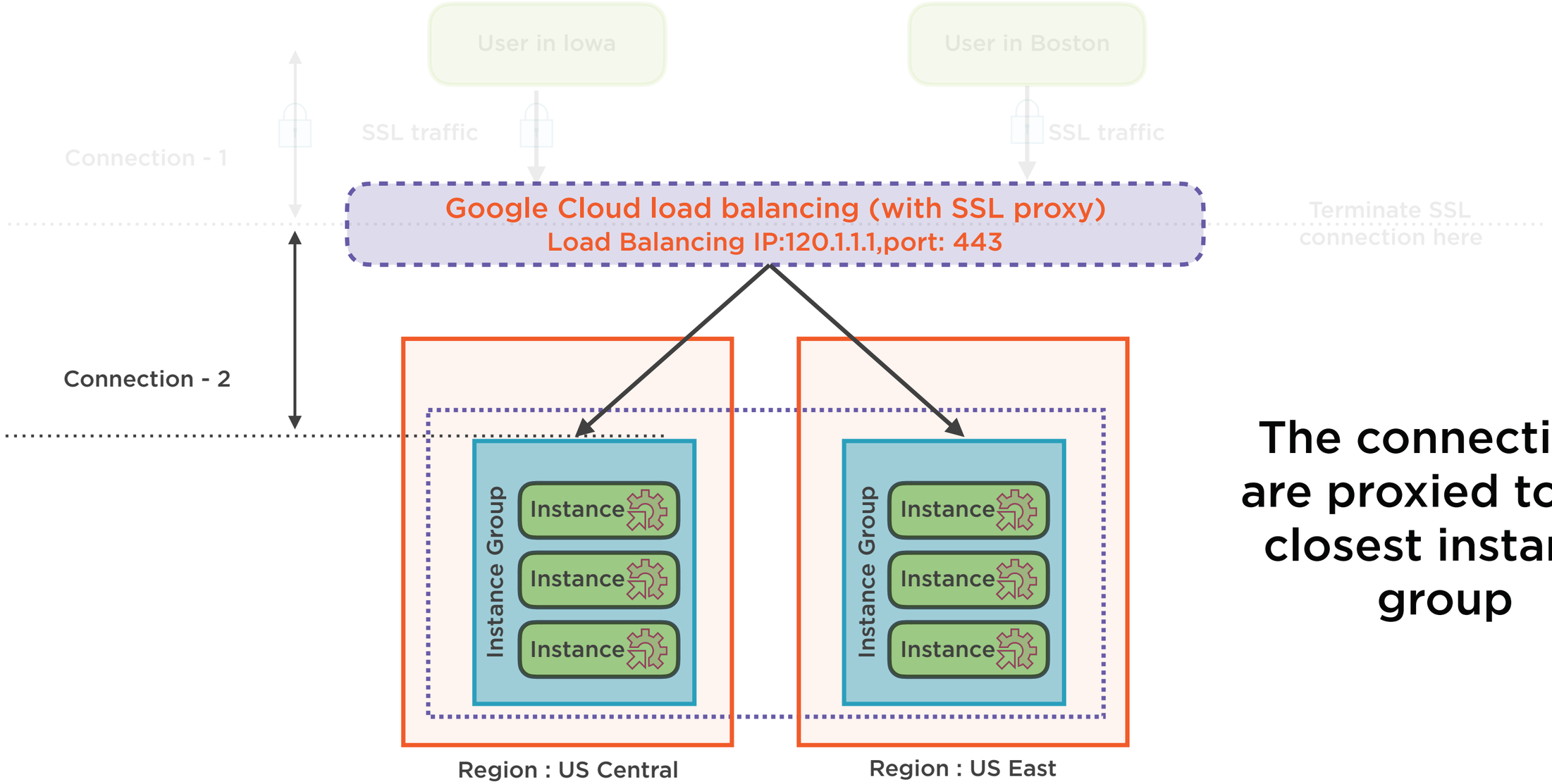
User Connects Using SSL



Users have a secure connection to the SSL proxy

The SSL connection is terminated at the load balancer

New Connections to Backends



The connections are proxied to the closest instance group

SSL Certificate Management

Customer facing SSL certificates can be self-managed or Google managed certificates

Vulnerabilities in the TCP and SSL stack patched at the load balancer

Can use SSL policies with the load balancer

SSL Certificate Management

Self-signed certificates:

- Generated with OpenSSL
- Fine for development
- Browser errors if used in production

HTTPS traffic:

- Apache SSL module
- Do not code up a non-HTTPS SSL application

Demo

Configuring and using an SSL Proxy load balancer

TCP Proxy Load Balancer

Load Balancing

TCP Proxy Load Balancing

User	
Application Layer	HTTP/HTTPS
Presentation Layer	
Session Layer	SSL Proxy
Transport Layer	**TCP Proxy**
Network Layer	Network
Data Link Layer	
Physical Layer	

TCP Proxy Load Balancing

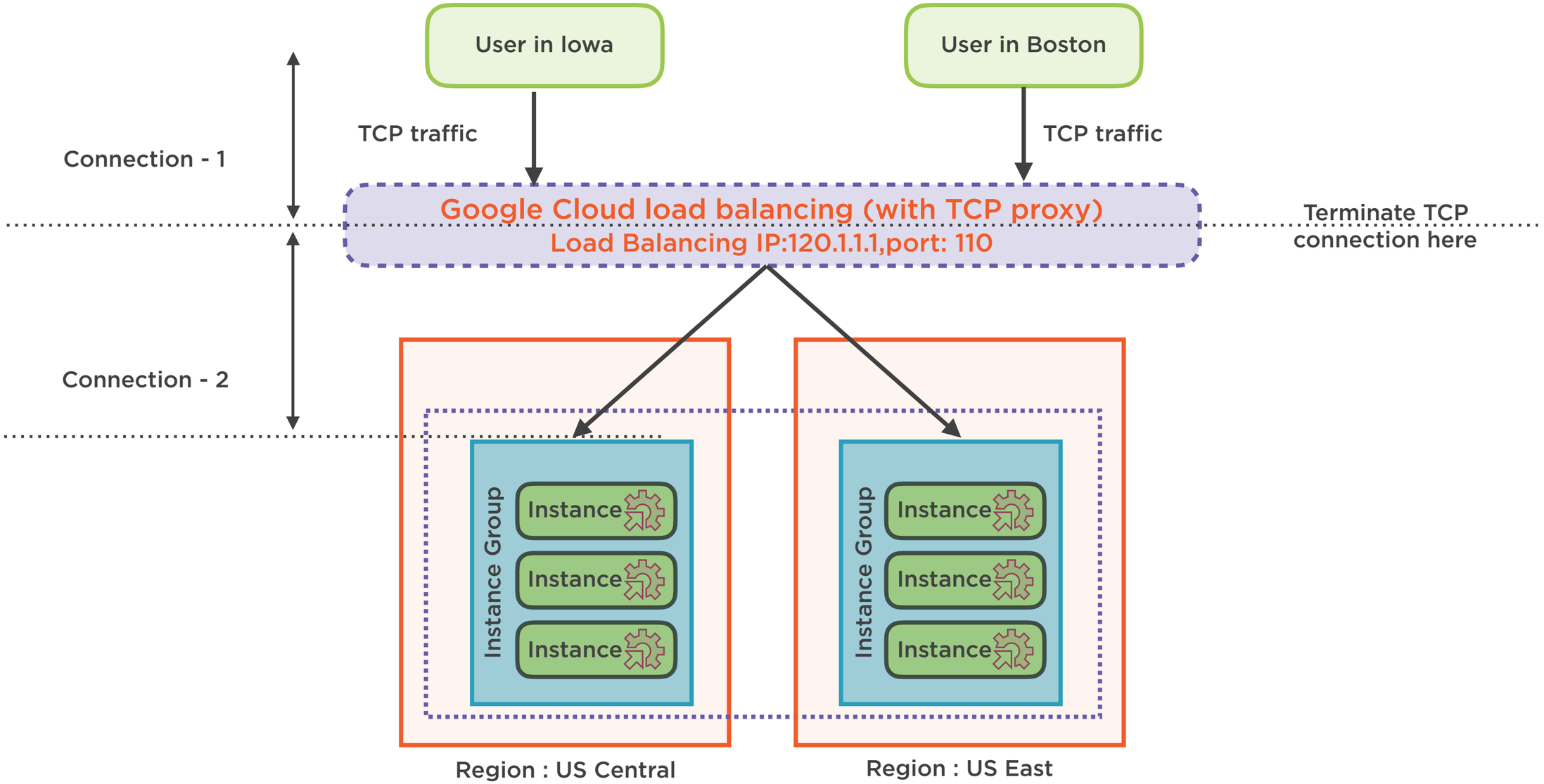
Allows you to use a single IP address for all users around the world

Automatically routes traffic to the instances that are closest to the user

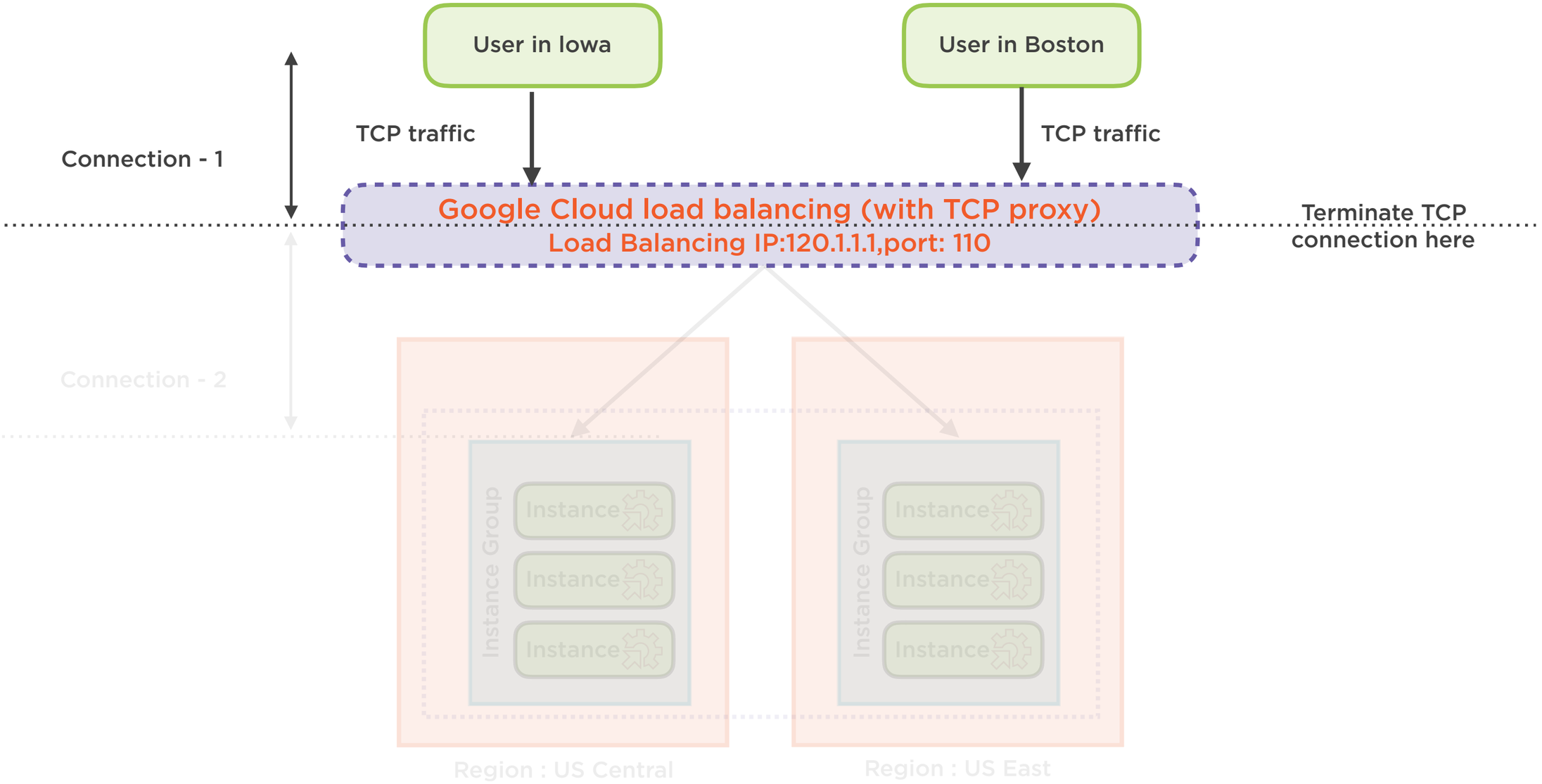
More intelligent routing than network load balancing

Better security, TCP vulnerabilities patched at the load balancer

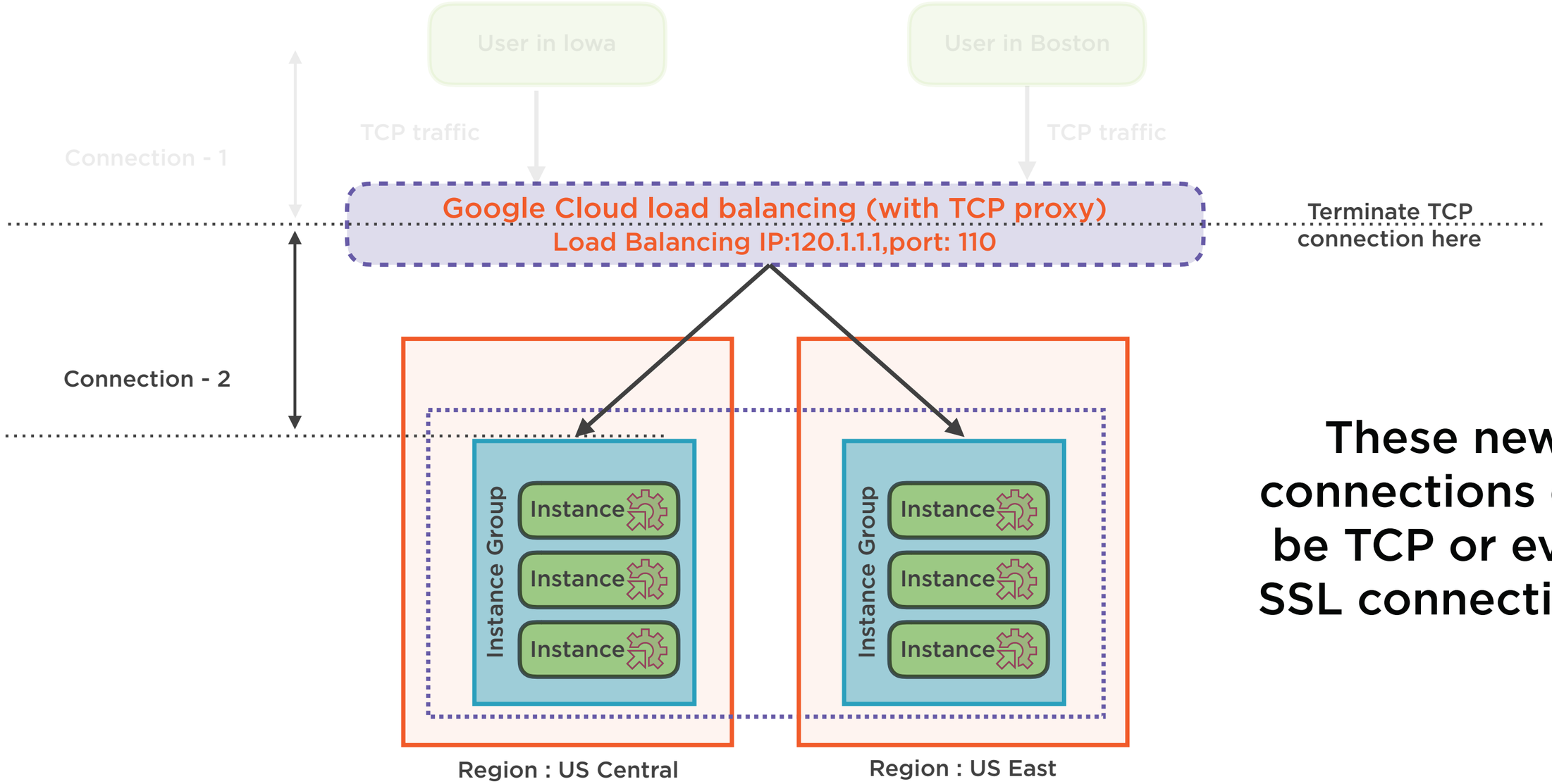
TCP Proxy Load Balancing



Users Connect Using TCP



New Connections are Made to Backends



These new connections can be TCP or even SSL connections

Demo

Configuring and using a TCP Proxy load balancer

Network Load Balancing

Load Balancing

Network Load Balancing

User	
Application Layer	HTTP/HTTPS
Presentation Layer	
Session Layer	SSL Proxy
Transport Layer	TCP Proxy
Network Layer	**Network**
Data Link Layer	
Physical Layer	

Network Load Balancing

Based on incoming IP protocol data, such as address, port, and protocol type

Pass-through, regional load balancer - does not proxy connections from clients

Use it to load balance UDP traffic, and TCP and SSL traffic

Load balances traffic on ports that are not supported by the SSL proxy and TCP proxy load balancers

Network Load Balancing

Picks an instance based on a hash of:

- Source IP and port
- Destination IP and port
- Protocol

This means that incoming TCP connections are spread across instances

Each new connection may go to a different instance

Forwarding Rules and Target Pools

Network load balancing forwards traffic to target pools

A group of instances which receive incoming traffic from forwarding rules

Can only be used with forwarding rules for TCP and UDP traffic

Target Pools and Failover Ratio

Can have backup pools which will receive requests if the first pool is unhealthy

failoverRatio is the ratio of healthy instances to failed instances in a pool

If primary target pool's ratio is below the failoverRatio traffic is sent to the backup pool

Demo

Configuring and using a network load balancer

Internal Load Balancing

Load Balancing

Internal Load Balancing

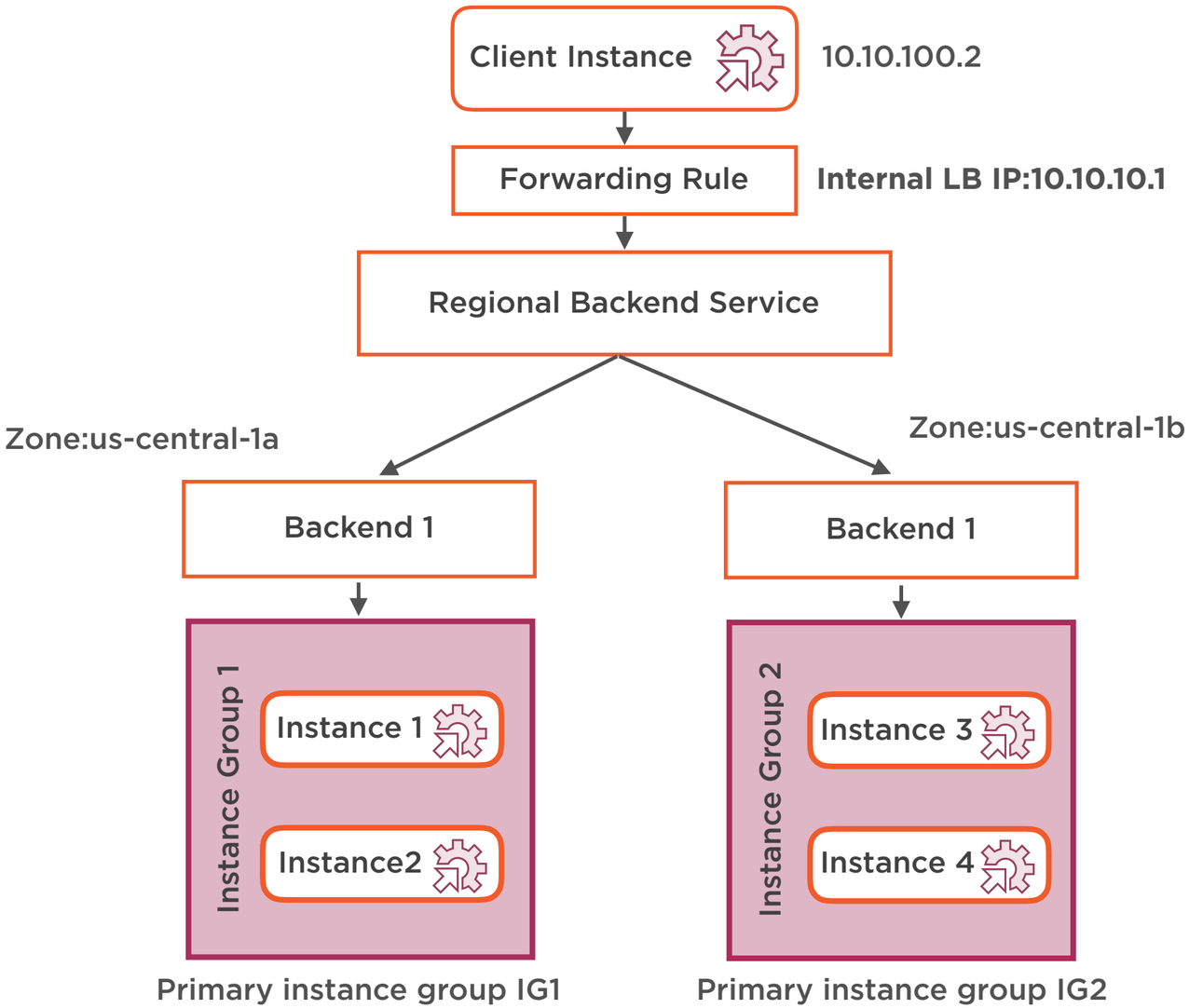
Private load balancing IP address that only your VPC instances can access

VPC traffic stays internal - less latency, more security

No public IP address needed

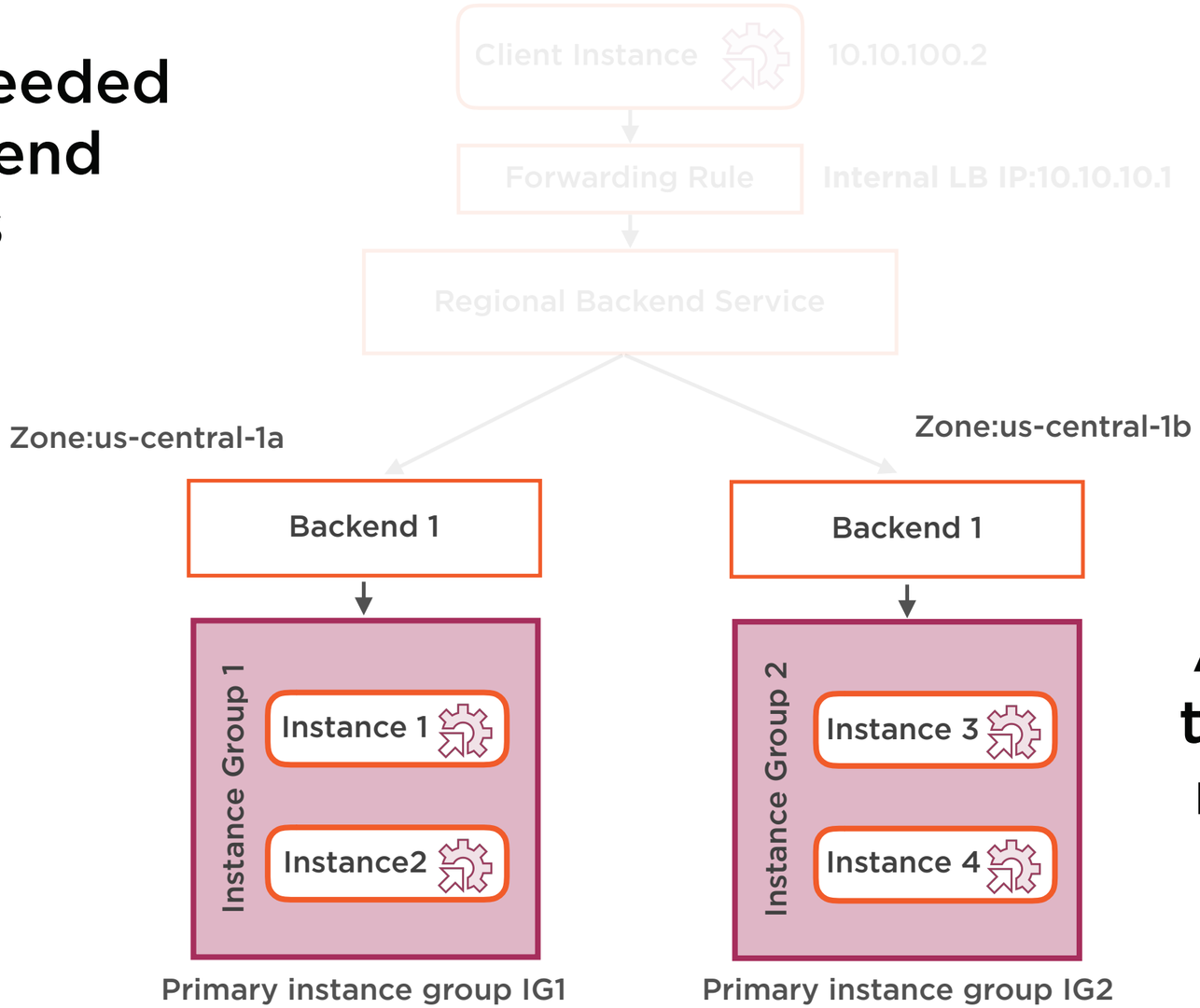
Useful to balance requests from your frontend to your backend instances

Internal Load Balancing



Internal Load Balancing

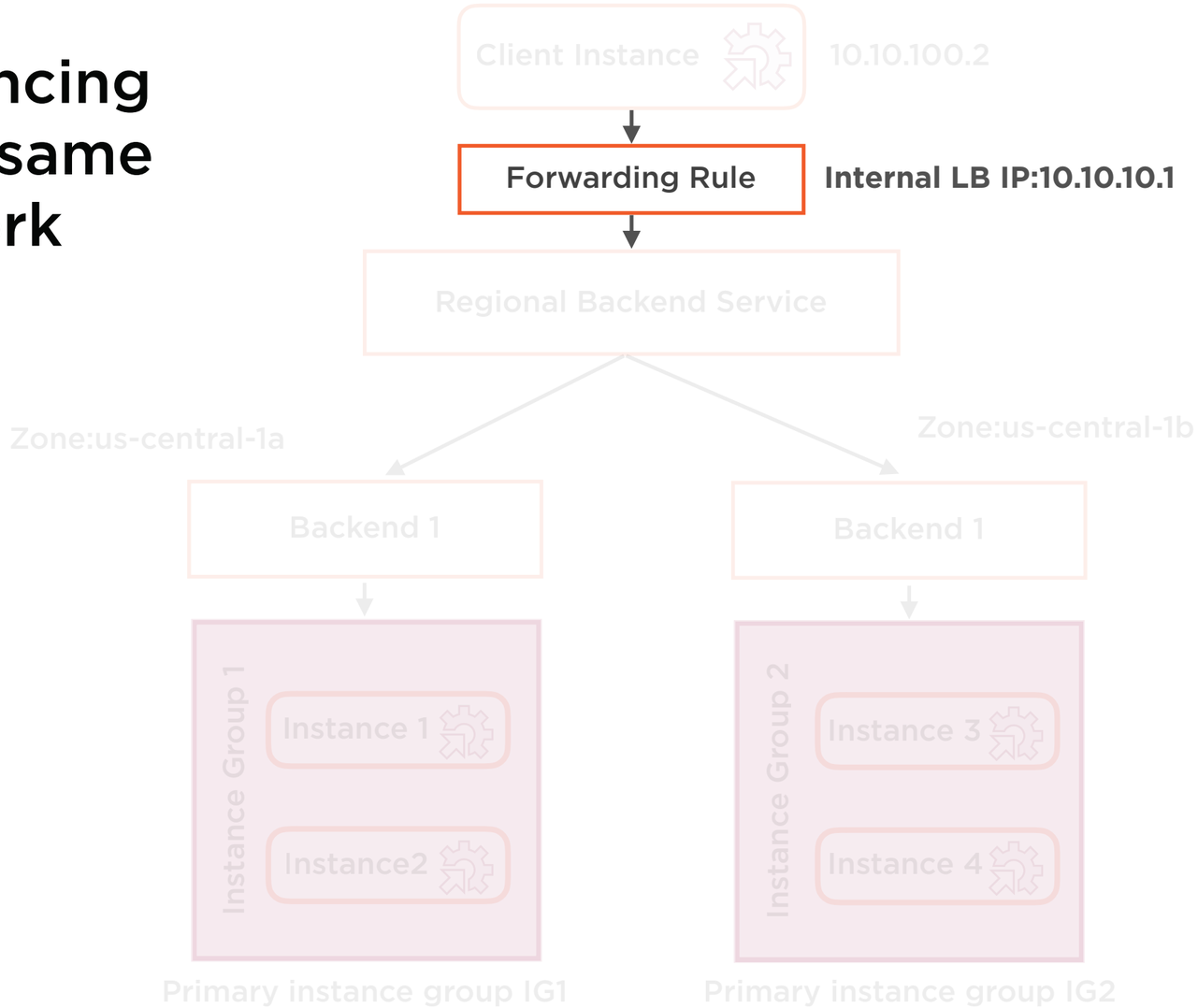
No public IP needed for the backend instances



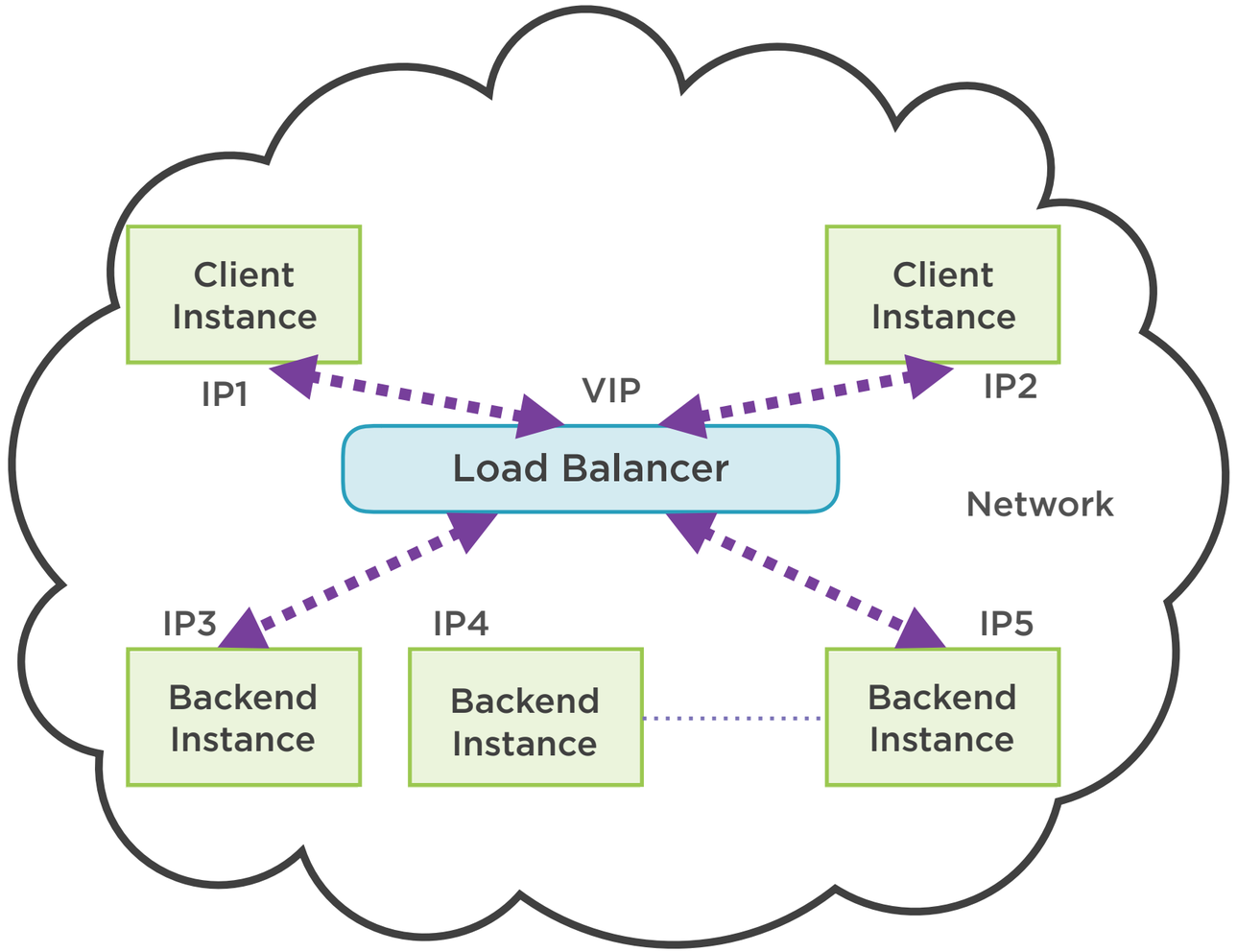
All instances belong to the same VPC and region but can be in different subnets

Internal Load Balancing

The load balancing IP is from the same VPC network

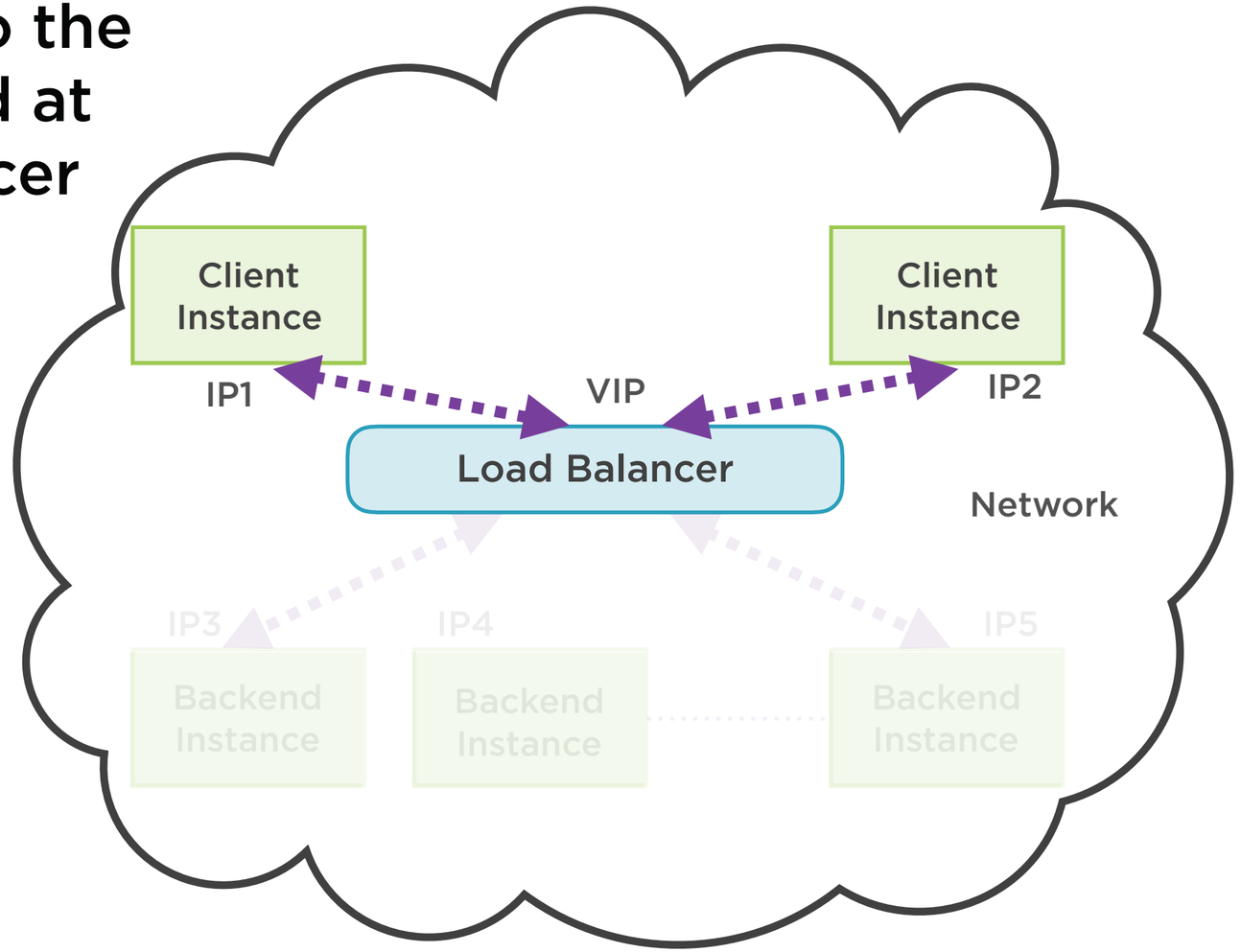


Traditional Proxy Internal Load Balancing

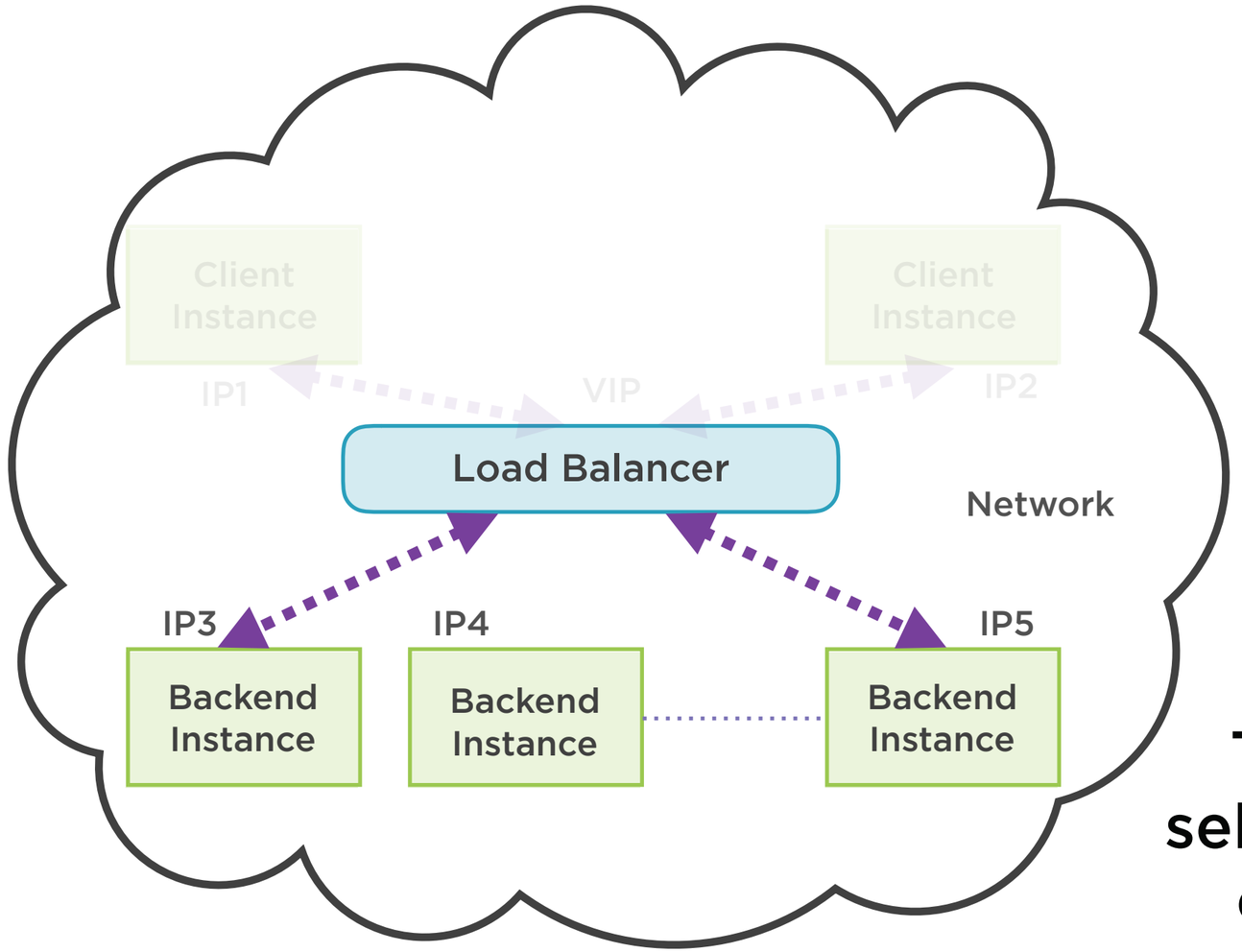


Traditional Proxy Internal Load Balancing

Traffic coming to the IP is terminated at the load balancer

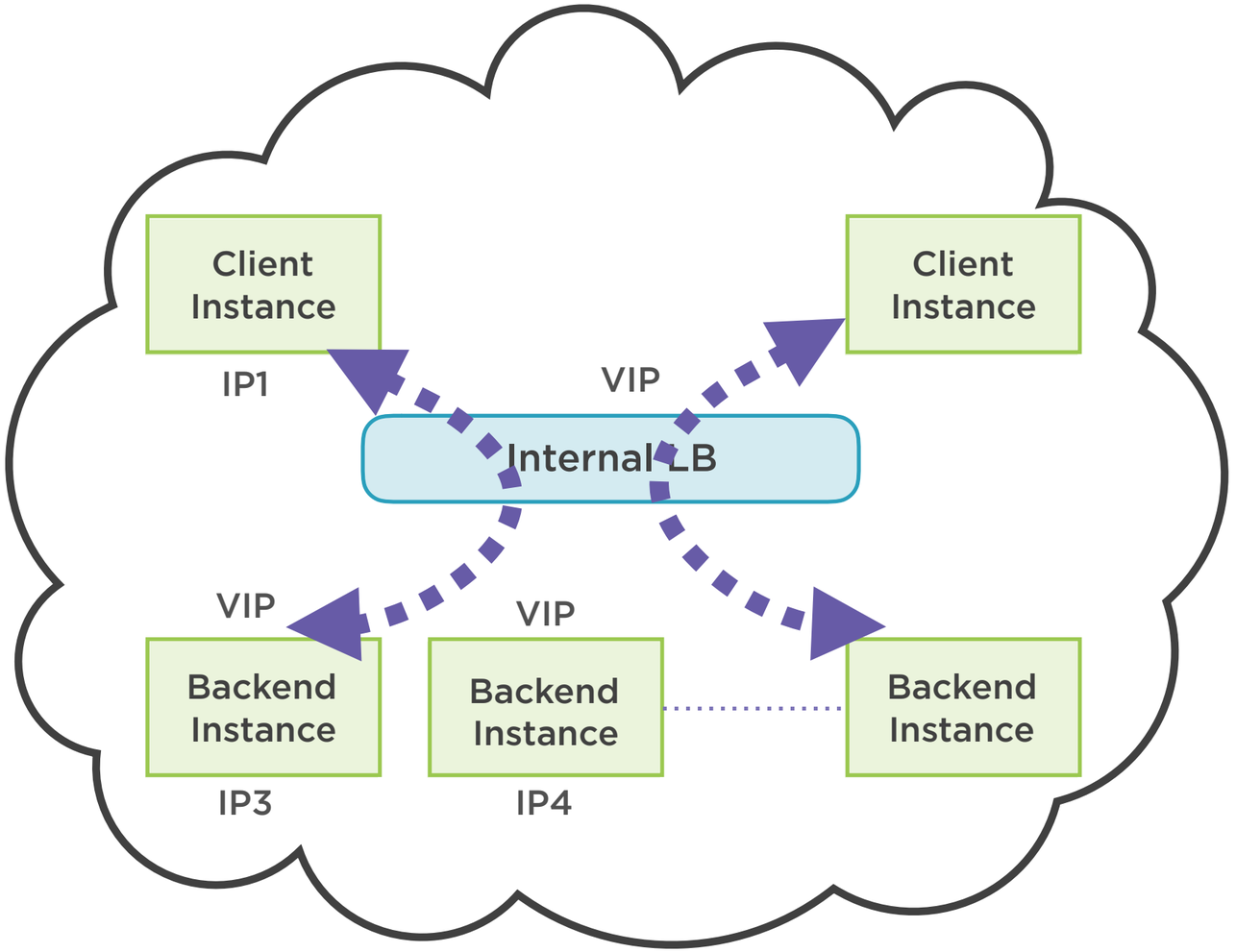


Traditional Proxy Internal Load Balancing

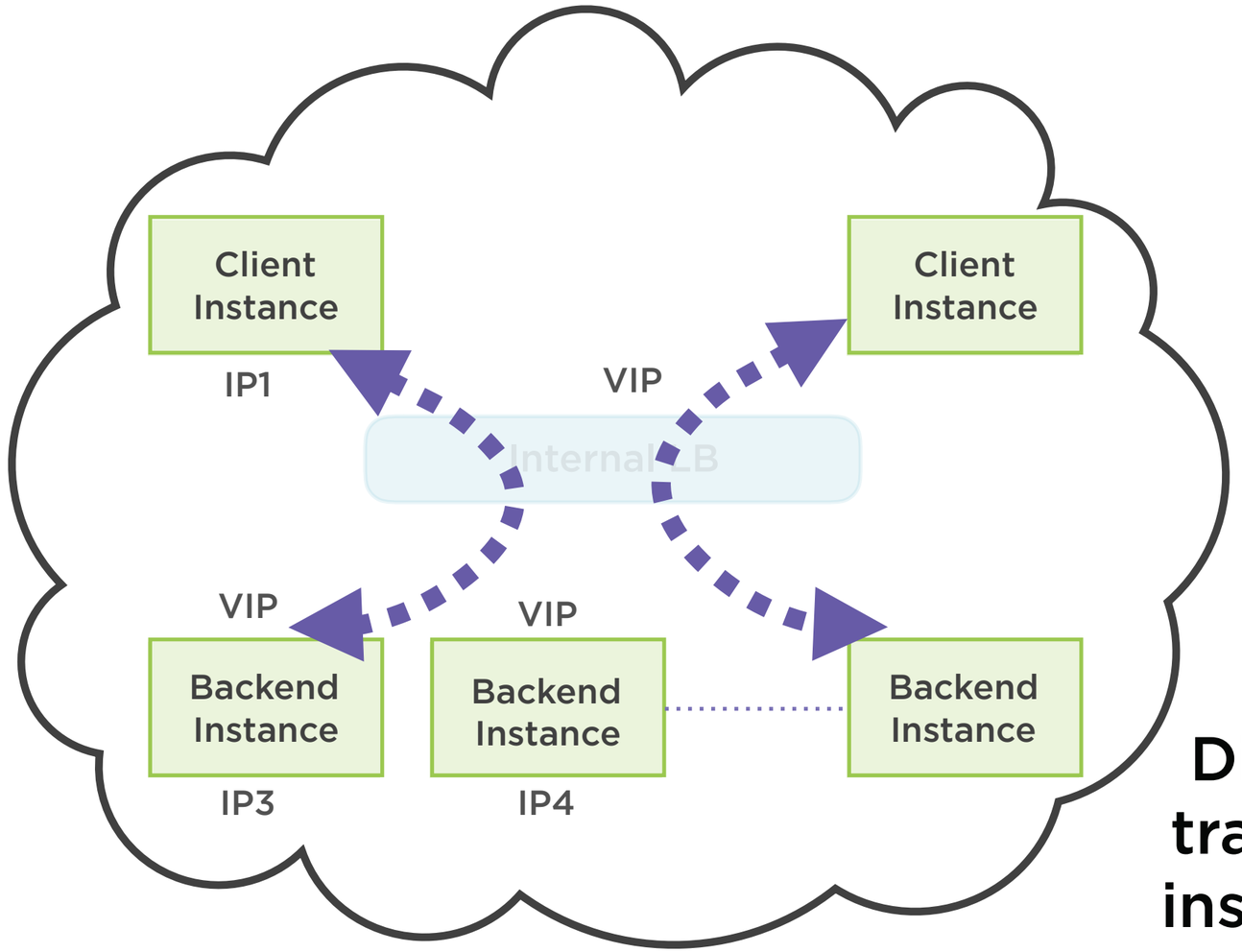


The load balancer selects a backend and establishes a new connection to it

GCP Internal Load Balancing

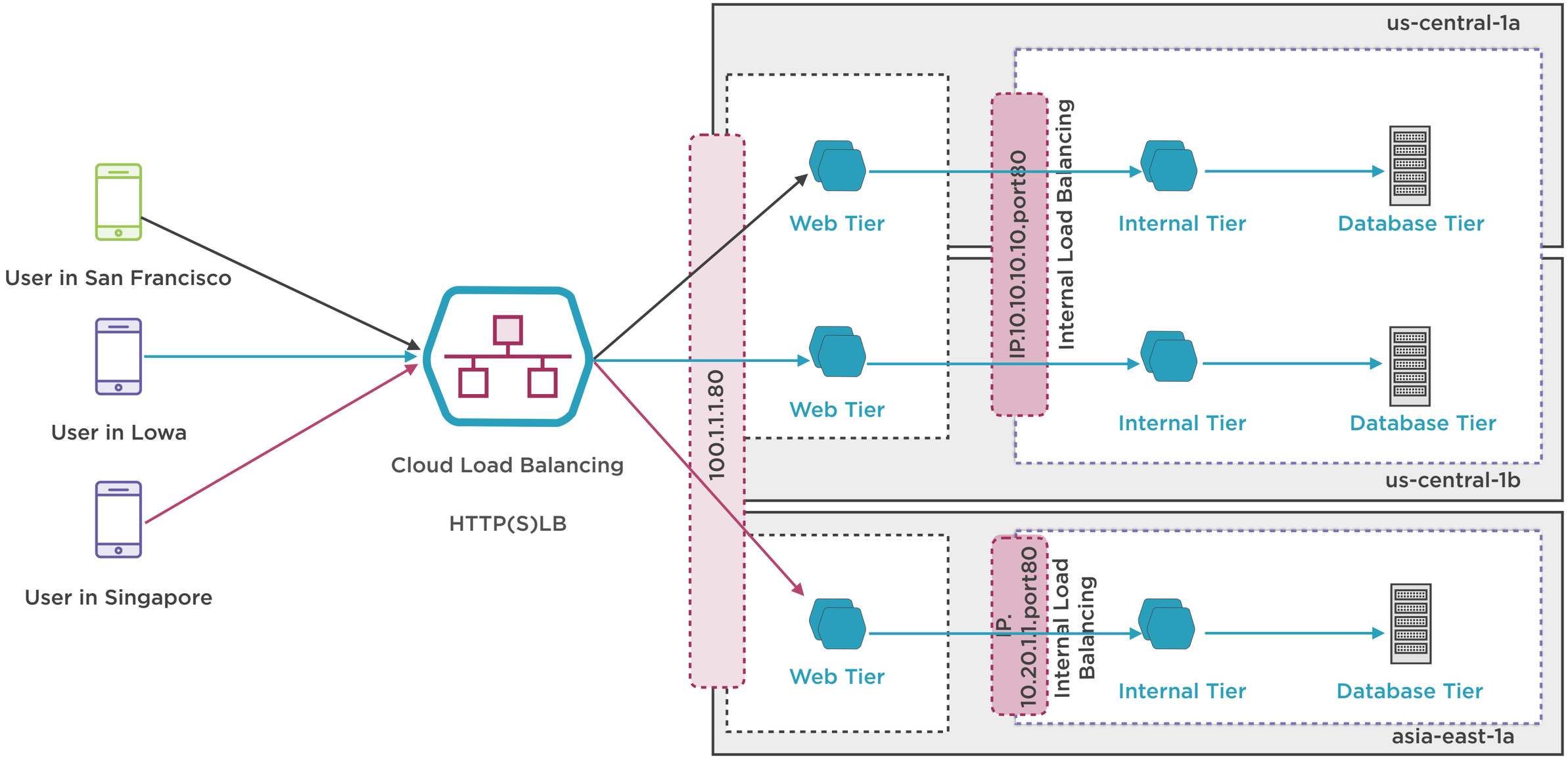


GCP Internal Load Balancing

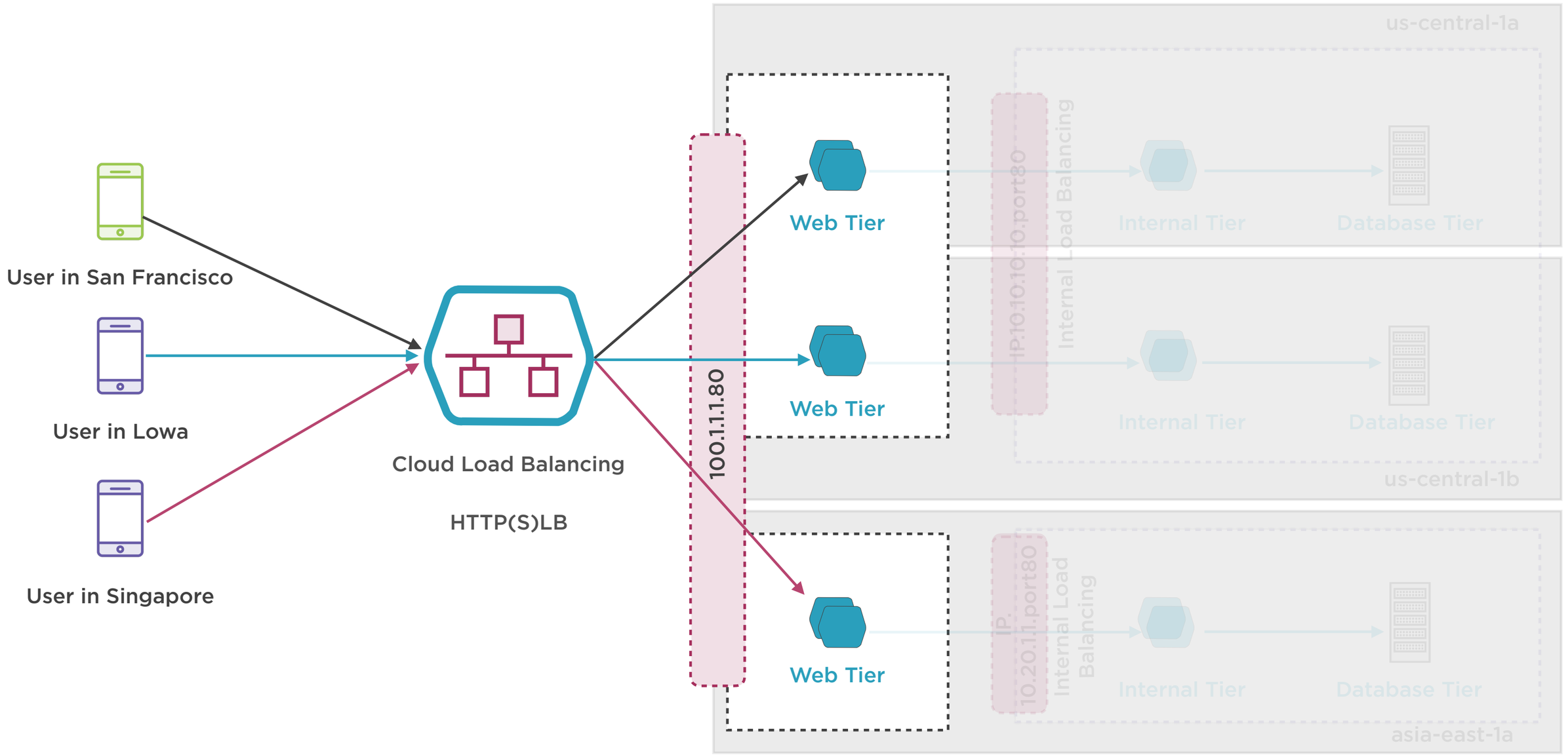


Directly delivers the traffic from the client instance to a backend instance

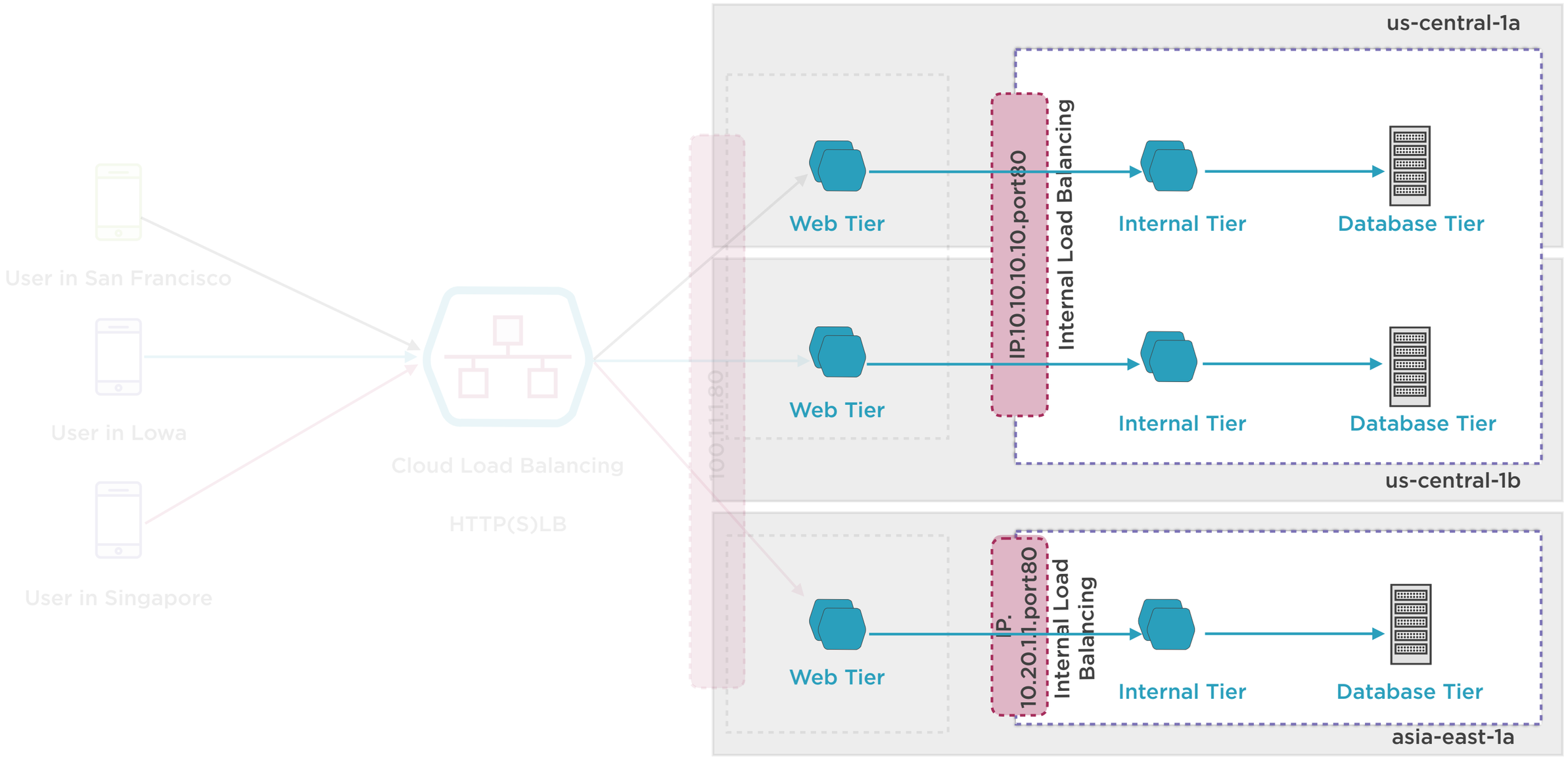
ILB Use Case: 3-tier Web App



External HTTP(S) Load Balancer



Internal Load Balancer



Demo

Configuring and using an internal load balancer

Summary

Configuring and using different kinds of load balancers

SSL proxy for secure connections, TCP proxy for TCP connections

Network load balancing for UDP traffic

Internal load balancing for traffic from instances on the GCP

Delete Resources

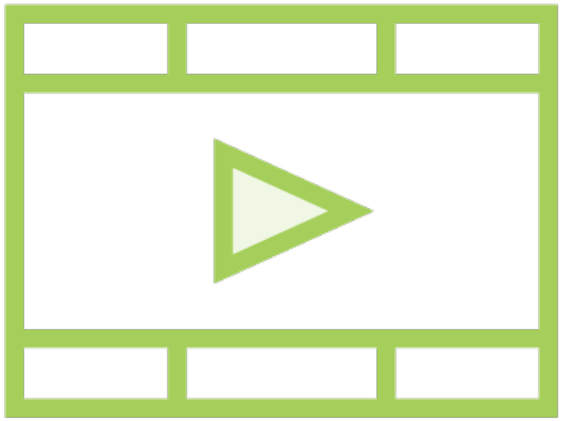
Load balancers

All managed and unmanaged instance groups

All VM instances for traffic and load testing

Any Cloud Storage buckets

Related Courses



Leveraging Advanced Networking and Load Balancing Services on the GCP

AWS Networking Deep Dive: Elastic Load Balancing (ELB)