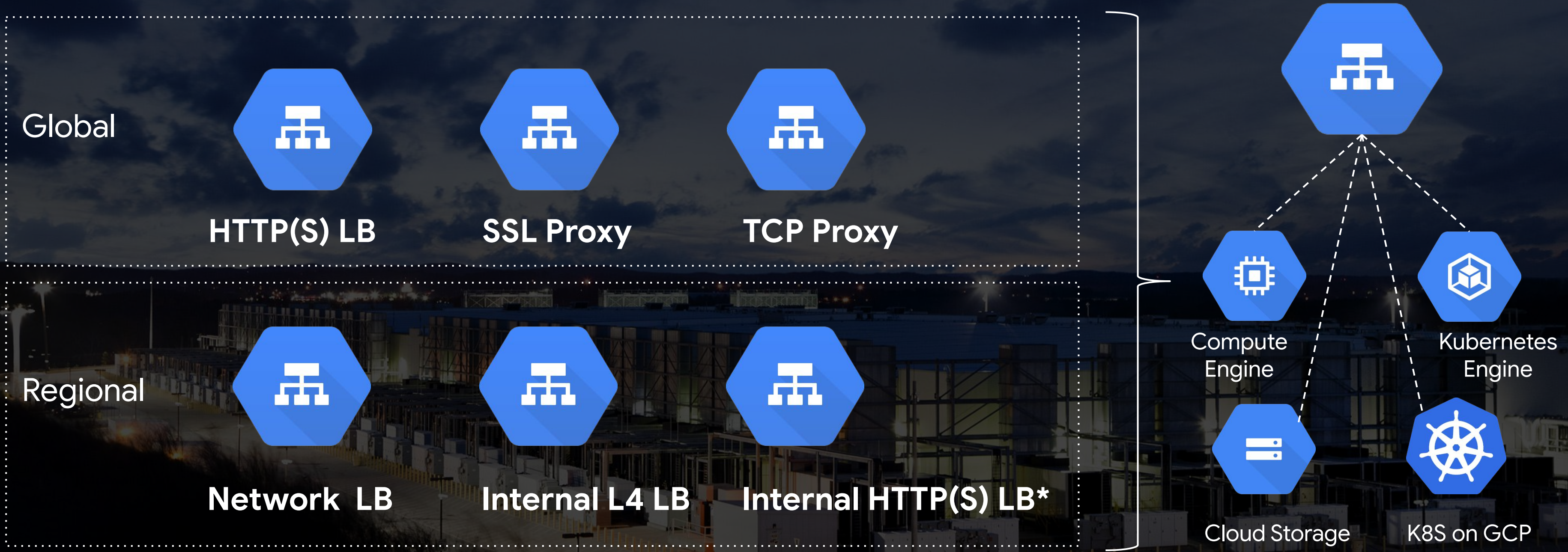
Google Cloud Global Load Balancing and DDoS Defense

Harry Lin 林書平
Customer Engineering Lead
Google Cloud

Meet the Cloud Load Balancing family



Global

HTTP(S) LB

SSL Proxy

TCP Proxy

Regional

Network LB

Internal L4 LB

Internal HTTP(S) LB*

Compute Engine

Kubernetes Engine

Cloud Storage

K8S on GCP

* In alpha

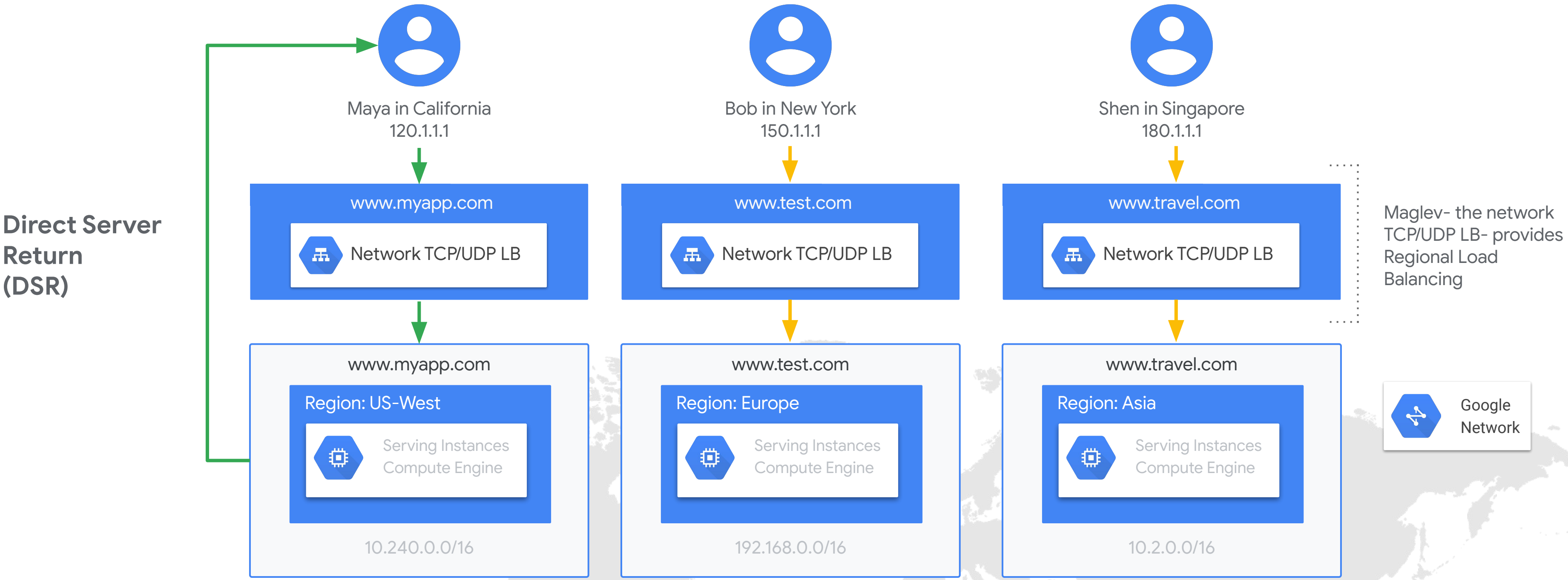
Network Load Balancer

Our First Cloud Load Balancer

01

Google Cloud

Network LB



Direct Server Return (DSR)

Maya in California
120.1.1.1

Bob in New York
150.1.1.1

Shen in Singapore
180.1.1.1

www.myapp.com
Network TCP/UDP LB

www.test.com
Network TCP/UDP LB

www.travel.com
Network TCP/UDP LB

Maglev- the network TCP/UDP LB- provides Regional Load Balancing

www.myapp.com
Region: US-West
Serving Instances
Compute Engine
10.240.0.0/16

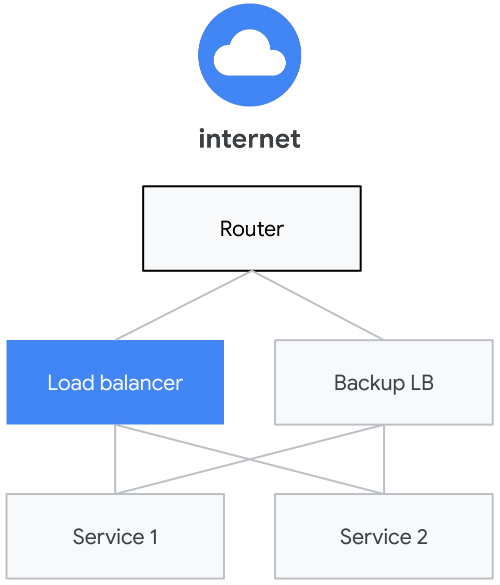
www.test.com
Region: Europe
Serving Instances
Compute Engine
192.168.0.0/16

www.travel.com
Region: Asia
Serving Instances
Compute Engine
10.2.0.0/16

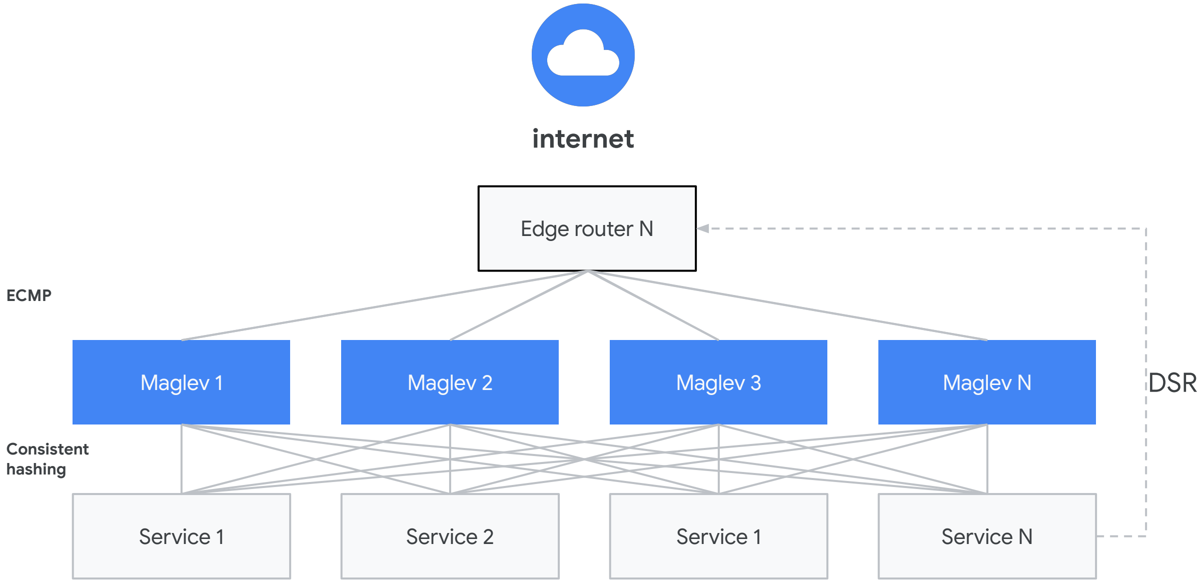
Google Network

Google Cloud

Network LB: what's under the hood? Maglev



Traditional Proxy



Google Network Load Balancer

Google Cloud

Network TCP/UDP LB features

1 Regional
= HA with multiple zones

2 Load Balance TCP/UDP
Does not look at L7

3 Client IP preserved
= don’t need x-forwarded-for, proxy protocol

4 Client access can be controlled with the VPC Firewall

5 Balances traffic using 2, 3, or 5-tuple hashing

6 IP-based session affinity

7 HTTP health checks

8 High performance
= 1 million+ requests per second

Google Cloud

What does the Network LB not provide?

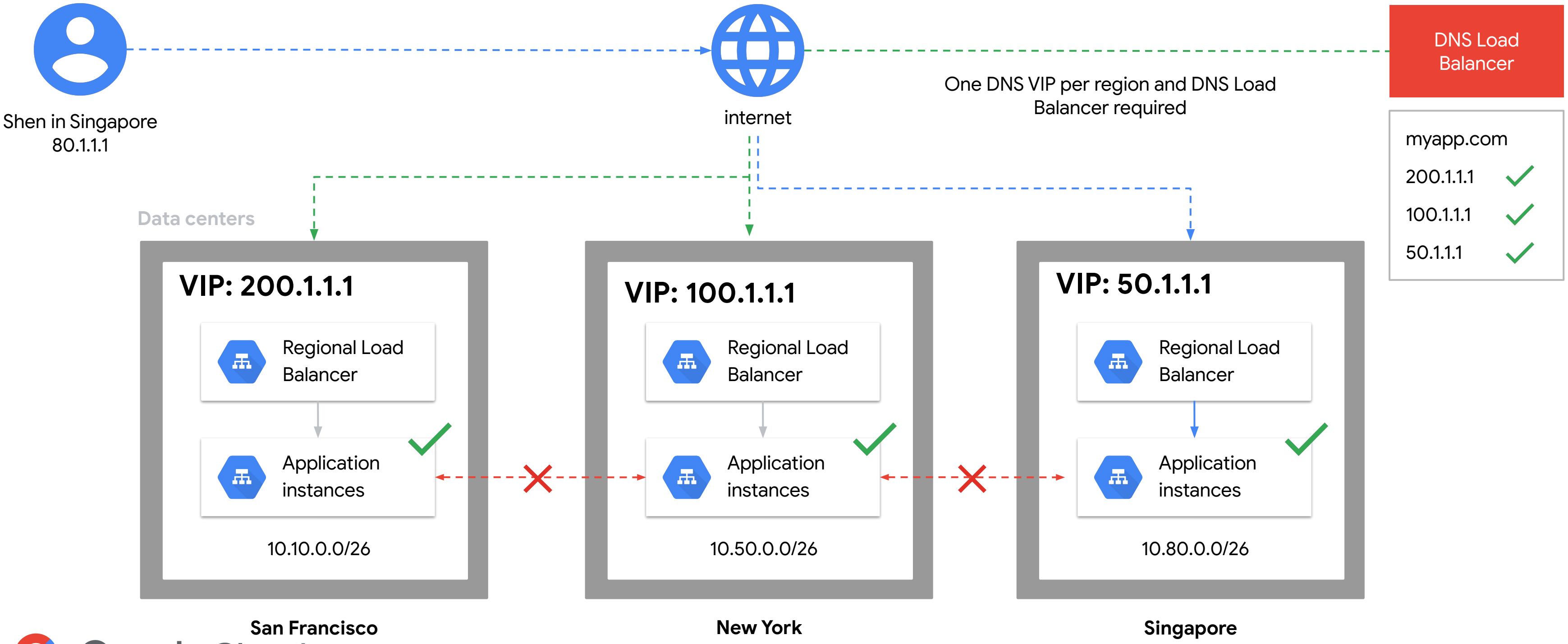
- No Global load balancing for IPv4/IPv6 clients
- No traffic routing based on L7
- No TLS termination/offload

Google Cloud

Global Load Balancer

02

Traditional public cloud: Regional LB only



Shen in Singapore
80.1.1.1

internet

DNS Load Balancer

One DNS VIP per region and DNS Load Balancer required

myapp.com

200.1.1.1	✓
100.1.1.1	✓
50.1.1.1	✓

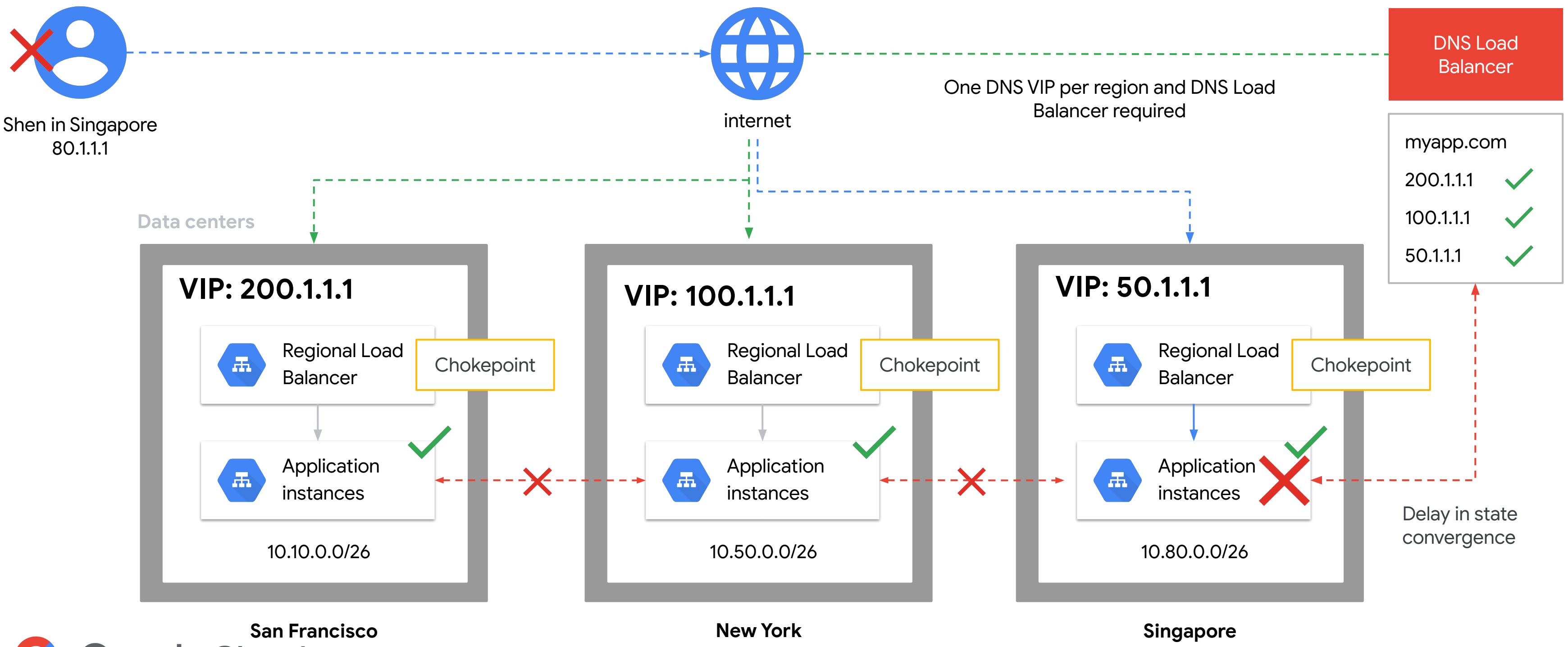
Data centers

VIP: 200.1.1.1
Regional Load Balancer
Application instances ✓
10.10.0.0/26
San Francisco

VIP: 100.1.1.1
Regional Load Balancer
Application instances ✓
10.50.0.0/26
New York

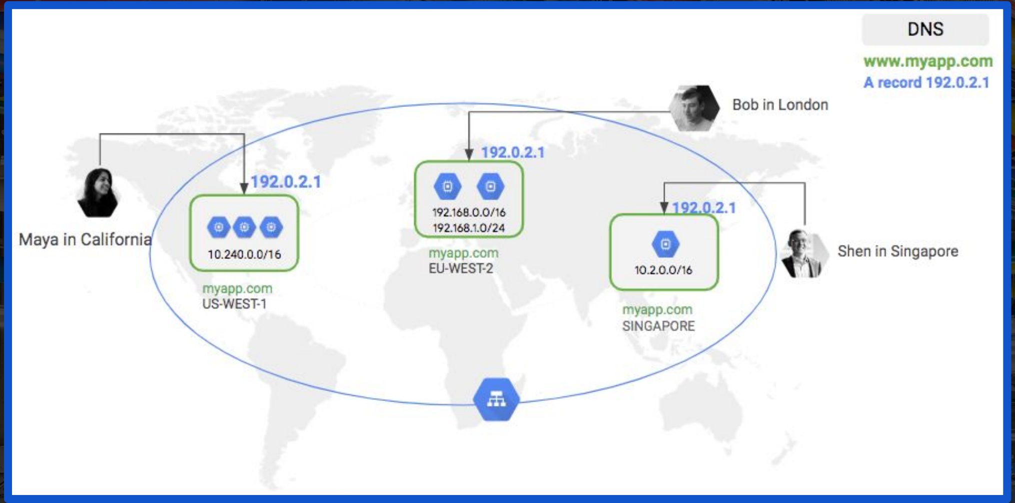
VIP: 50.1.1.1
Regional Load Balancer
Application instances ✓
10.80.0.0/26
Singapore

Traditional public cloud: DNS-based global LB



Google Cloud

Global IPv4/IPv6 LB



Single Global Anycast VIP (IPv4/IPv6) across region

Worldwide Capacity

Cross-region failover and fallback

Fast autoscaling

Single point to apply global policies

1 Million+ QPS

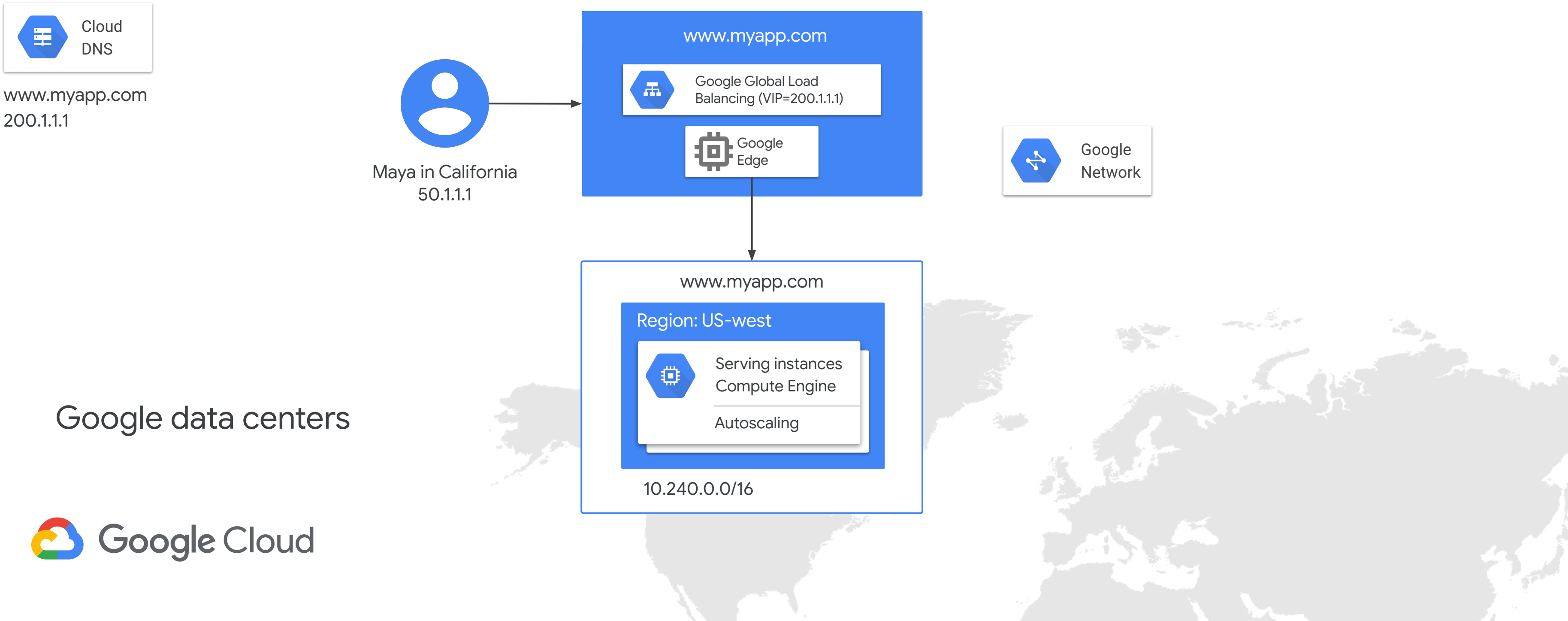
HTTP(S) LB

SSL Proxy

TCP Proxy

Google Cloud

Google Global LB



Cloud DNS

www.myapp.com
200.1.1.1

Maya in California
50.1.1.1

www.myapp.com

Google Global Load Balancing (VIP=200.1.1.1)

Google Edge

Google Network

www.myapp.com

Region: US-west

Serving instances
Compute Engine

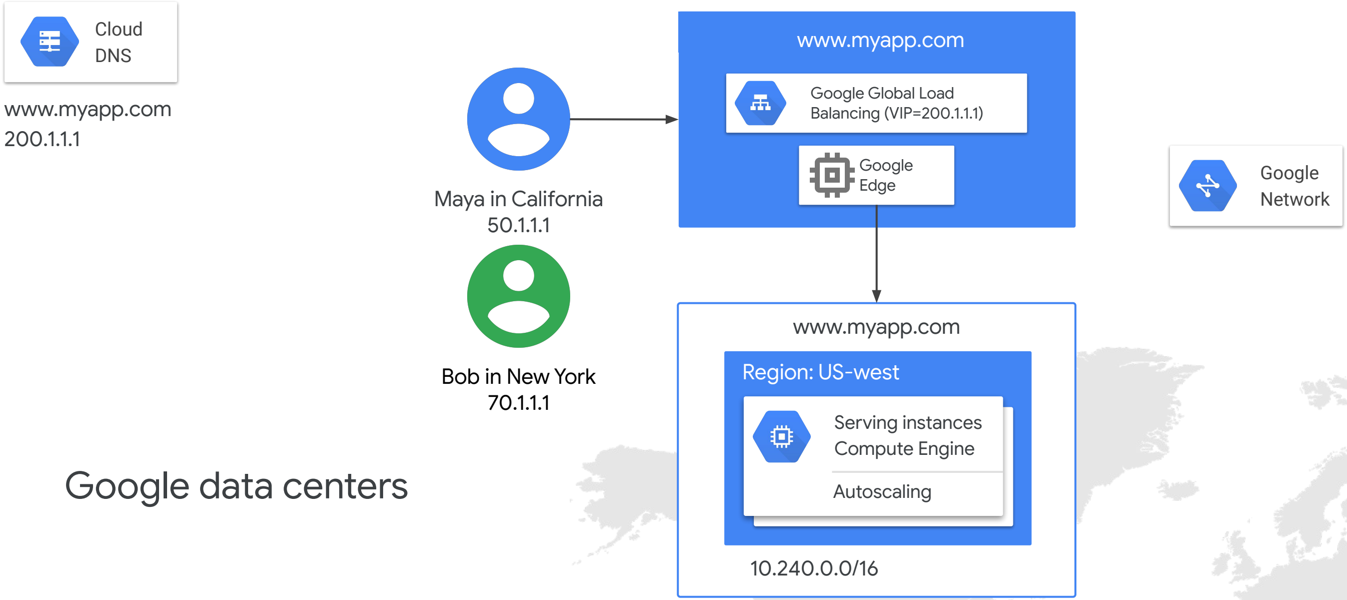
Autoscaling

10.240.0.0/16

Google data centers

Google Cloud

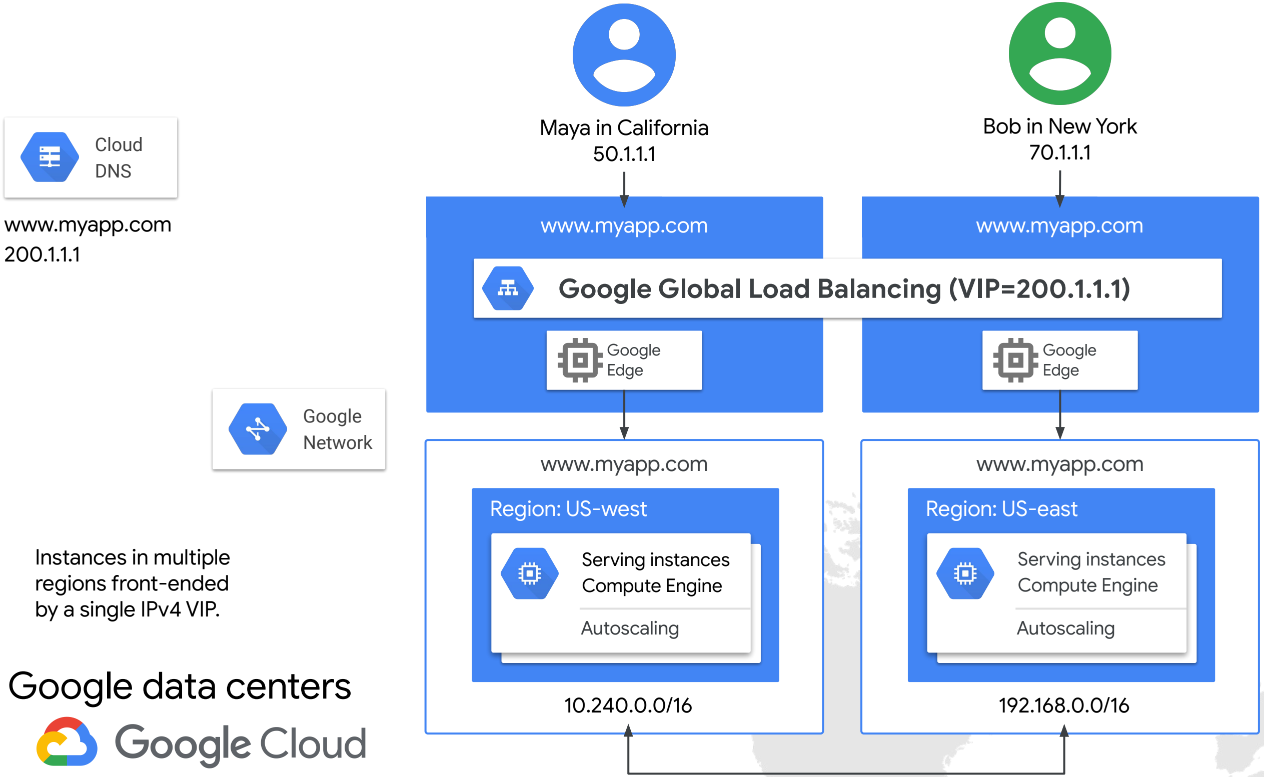
Global LB: Expand seamlessly



Google data centers

Google Cloud

Global LB: Expand seamlessly

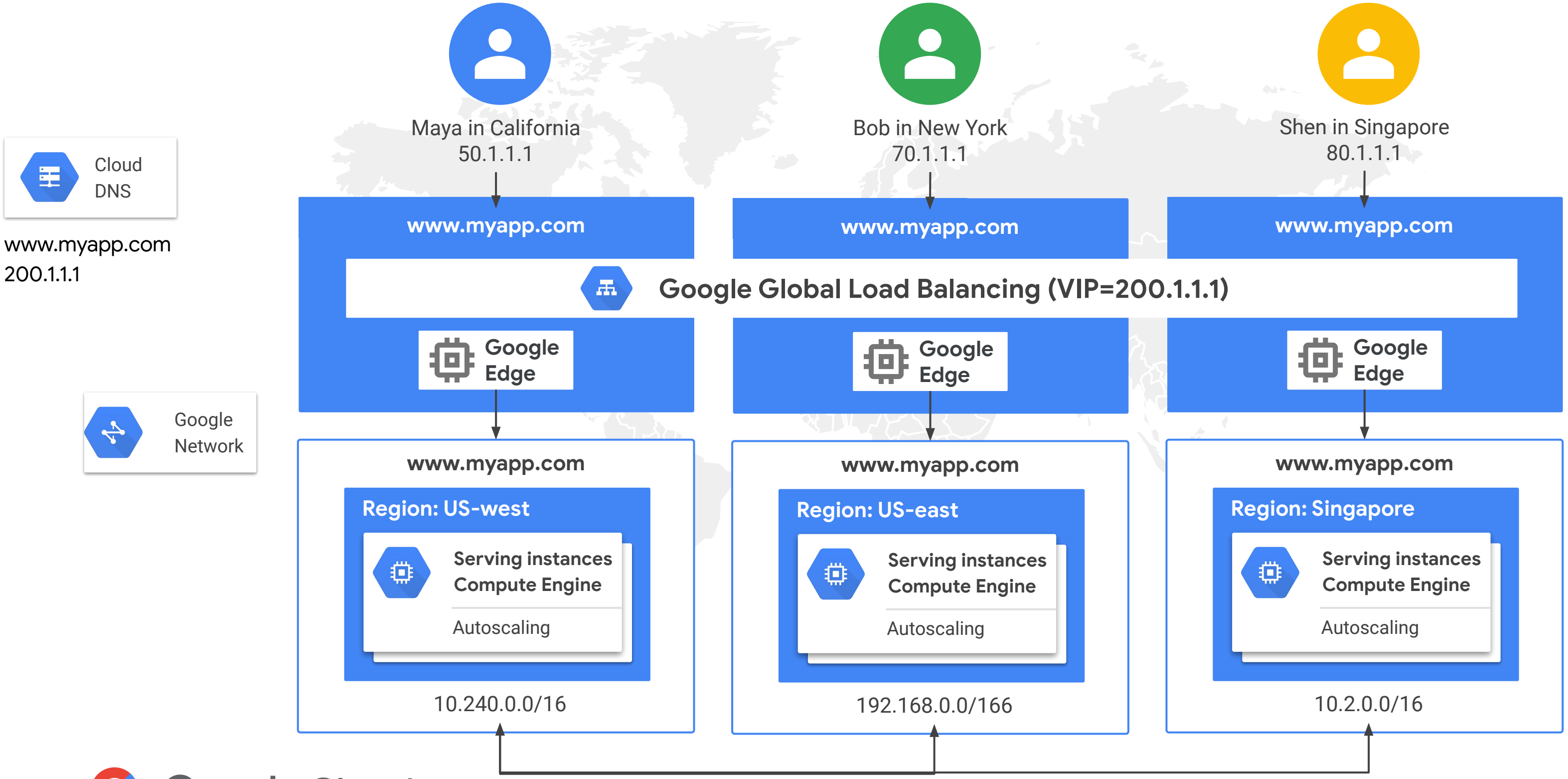


Instances in multiple regions front-ended by a single IPv4 VIP.

Google data centers

Google Cloud

Global LB: Expand seamlessly



Cloud DNS

www.myapp.com
200.1.1.1

Google Network

Maya in California
50.1.1.1

Bob in New York
70.1.1.1

Shen in Singapore
80.1.1.1

www.myapp.com

www.myapp.com

www.myapp.com

Google Global Load Balancing (VIP=200.1.1.1)

Google Edge

Google Edge

Google Edge

www.myapp.com

Region: US-west

Serving instances
Compute Engine

Autoscaling

10.240.0.0/16

www.myapp.com

Region: US-east

Serving instances
Compute Engine

Autoscaling

192.168.0.0/166

www.myapp.com

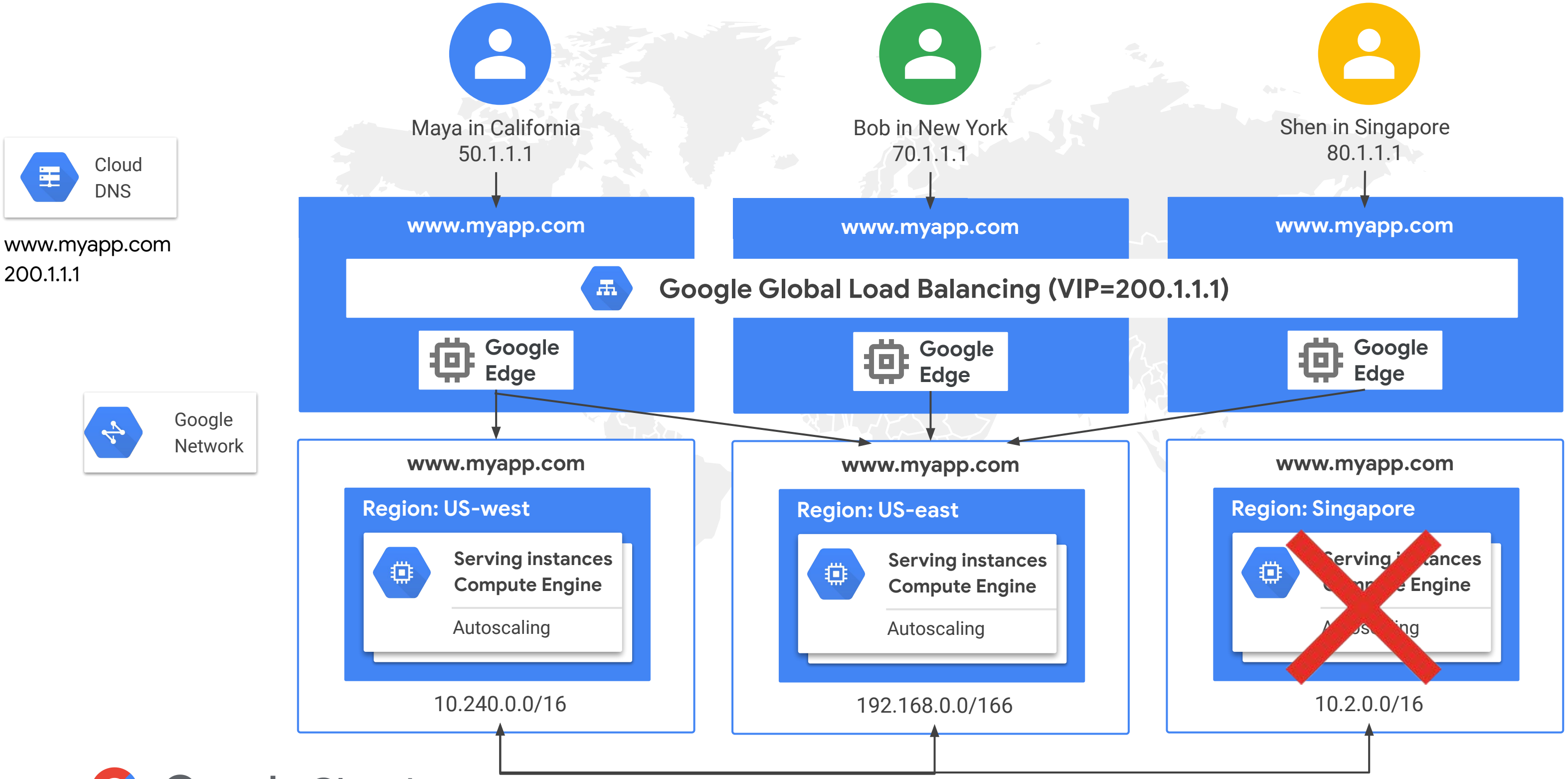
Region: Singapore

Serving instances
Compute Engine

Autoscaling

10.2.0.0/16

Global LB: Cross-region failover, overflow



Cloud DNS

www.myapp.com
200.1.1.1

Google Network

Maya in California
50.1.1.1

Bob in New York
70.1.1.1

Shen in Singapore
80.1.1.1

www.myapp.com

www.myapp.com

www.myapp.com

Google Global Load Balancing (VIP=200.1.1.1)

Google Edge

Google Edge

Google Edge

www.myapp.com

Region: US-west

Serving instances
Compute Engine

Autoscaling

10.240.0.0/16

www.myapp.com

Region: US-east

Serving instances
Compute Engine

Autoscaling

192.168.0.0/166

www.myapp.com

Region: Singapore

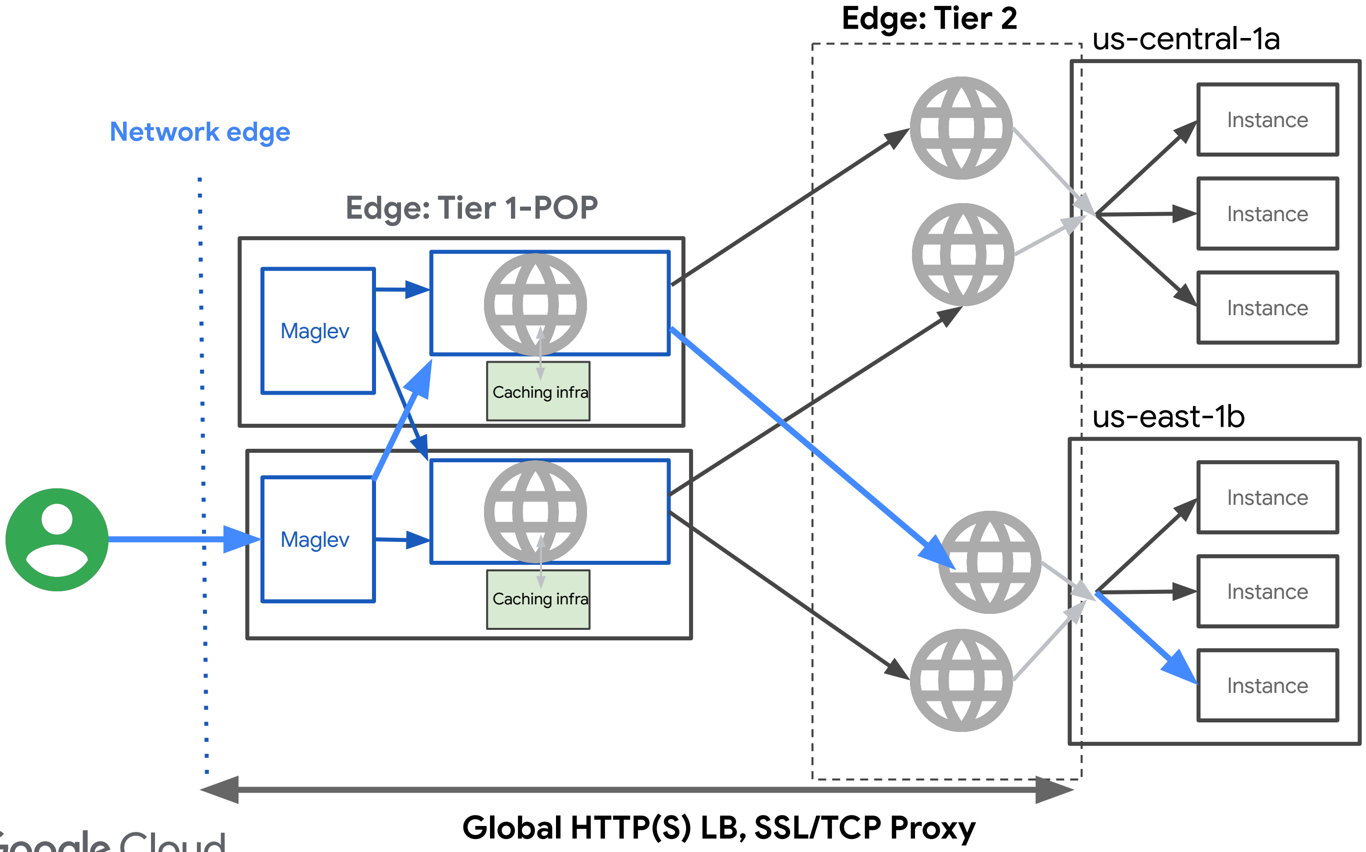
Serving instances
Compute Engine

Autoscaling

10.2.0.0/16

Google Cloud

Global LB under the hood



Google Cloud

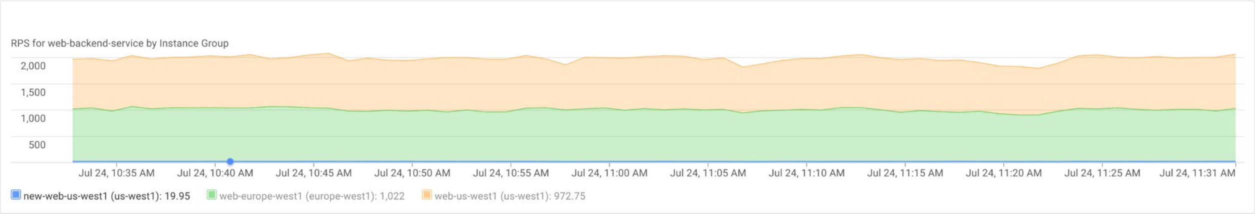
Global traffic distribution

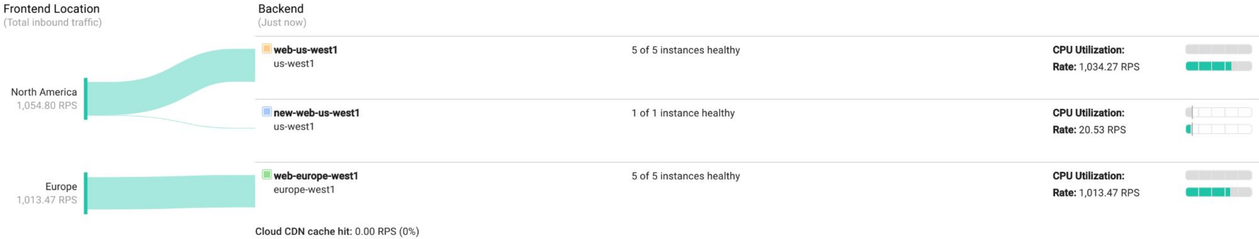
Compute worldwide capacity

- If worldwide load > worldwide capacity { scale up worldwide capacity }

For each zone where traffic is coming from

- Assign local zone up to capacity
- Fill in local region up to capacity, load zones equally within a region
- Overflow to next closest region, undrained with available capacity
- Within zone - RoundRobin





Backend
(Just now)

web-us-west1 us-west1 — 5 of 5 instances healthy — **CPU Utilization:** **Rate:** 1,034.27 RPS

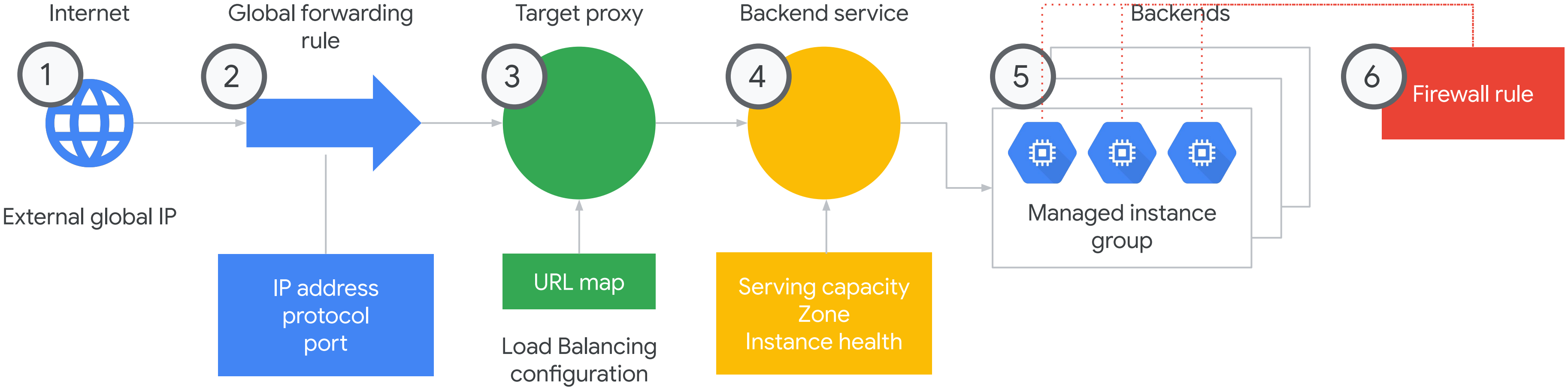
new-web-us-west1 us-west1 — 1 of 1 instance healthy — **CPU Utilization:** **Rate:** 20.53 RPS

web-europe-west1 europe-west1 — 5 of 5 instances healthy — **CPU Utilization:** **Rate:** 1,013.47 RPS

Cloud CDN cache hit: 0.00 RPS (0%)

Google Cloud

Global HTTP(S) Load Balancing Data Model

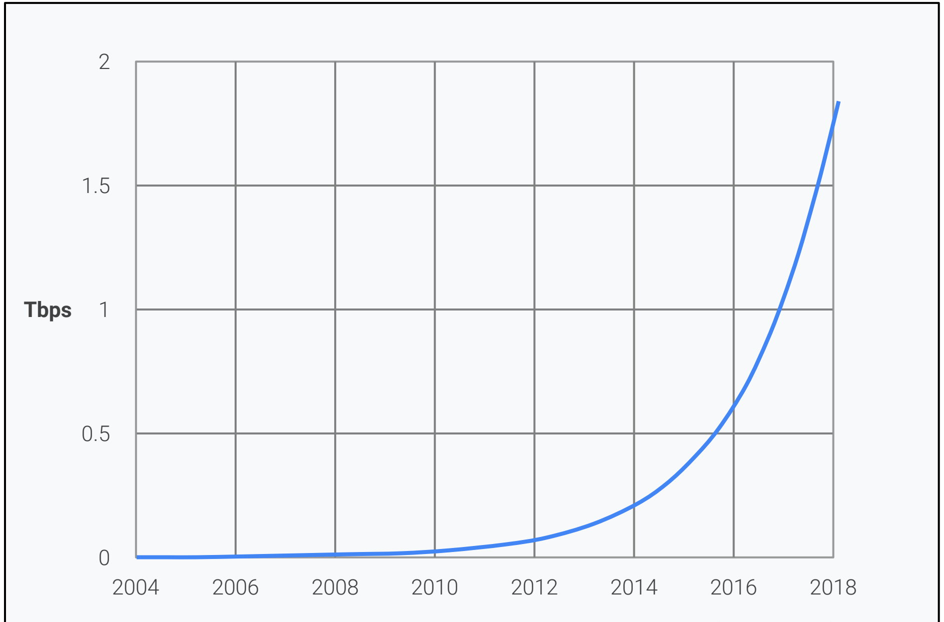


Google Cloud

Cloud Armor and DDos Defense

03

DDoS trends based on attacks on Google



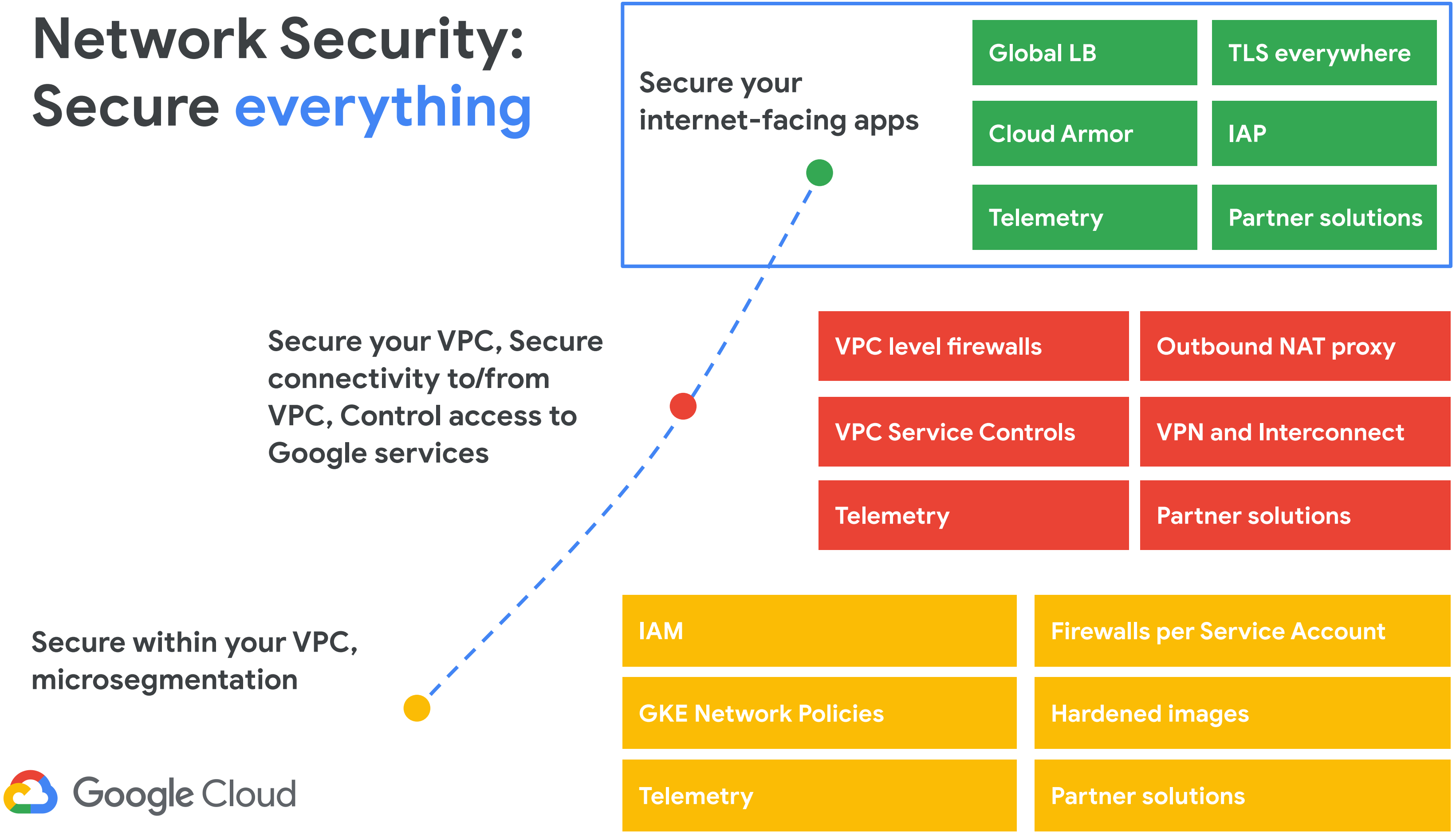
Source- Google

"Absorbing the largest attacks requires the bandwidth needed to watch half a million YouTube videos at the same time… in HD."

Dr. Damian Menscher
DDoS Defense Team, Google

Google Cloud

Network Security: Secure everything



Secure your internet-facing apps

- Global LB
- TLS everywhere
- Cloud Armor
- IAP
- Telemetry
- Partner solutions

Secure your VPC, Secure connectivity to/from VPC, Control access to Google services

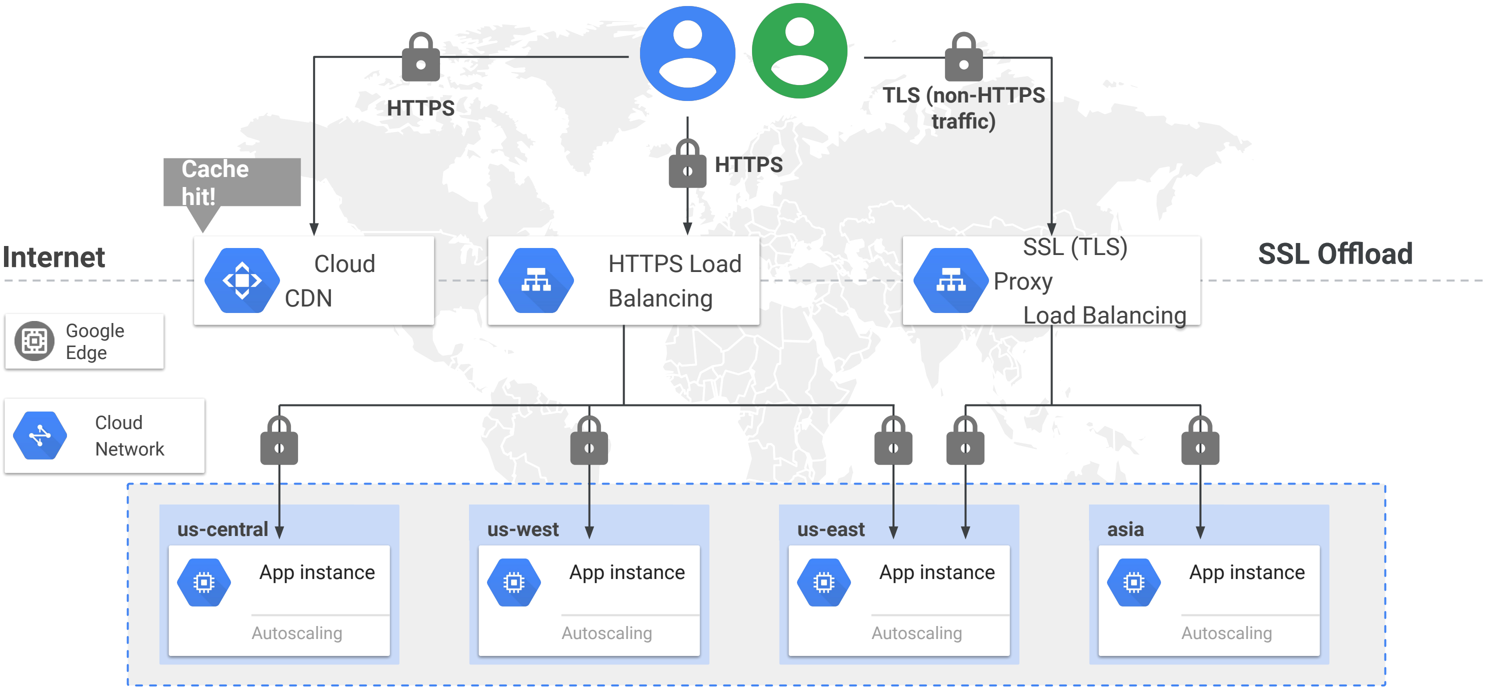
- VPC level firewalls
- Outbound NAT proxy
- VPC Service Controls
- VPN and Interconnect
- Telemetry
- Partner solutions

Secure within your VPC, microsegmentation

- IAM
- Firewalls per Service Account
- GKE Network Policies
- Hardened images
- Telemetry
- Partner solutions

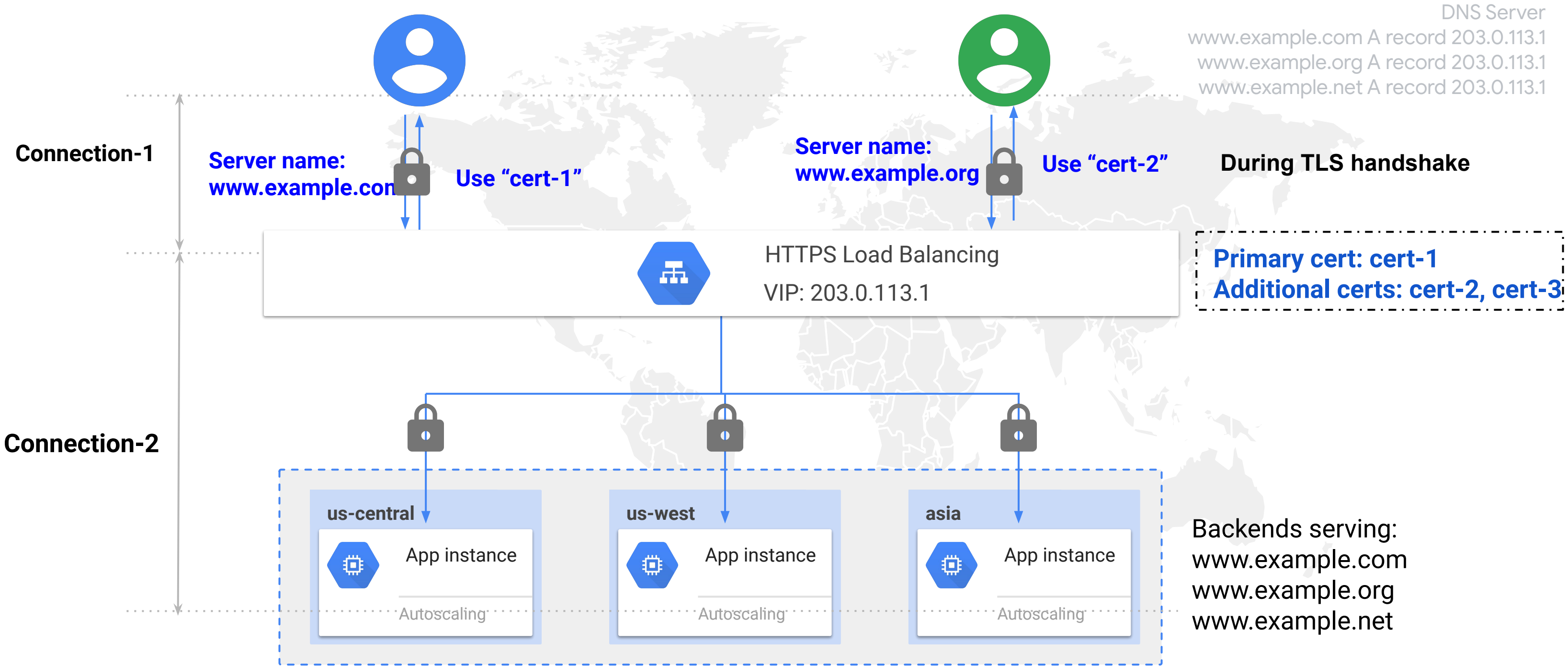
Google Cloud

Best practice: TLS everywhere



Google Cloud

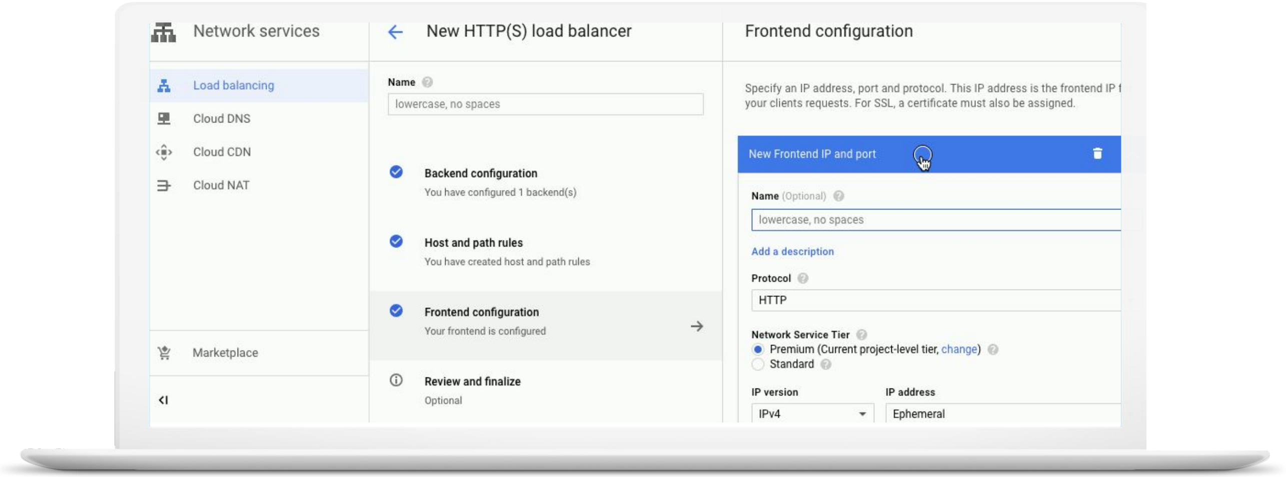
Multiple SSL certs



Google Cloud

Managed SSL certs

★ Beta



Network services

- Load balancing
- Cloud DNS
- Cloud CDN
- Cloud NAT
- Marketplace

New HTTP(S) load balancer

Name
lowercase, no spaces

✓ Backend configuration
You have configured 1 backend(s)

✓ Host and path rules
You have created host and path rules

✓ Frontend configuration
Your frontend is configured

ⓘ Review and finalize
Optional

Frontend configuration

Specify an IP address, port and protocol. This IP address is the frontend IP f
your clients requests. For SSL, a certificate must also be assigned.

New Frontend IP and port

Name (Optional)
lowercase, no spaces

Add a description

Protocol
HTTP

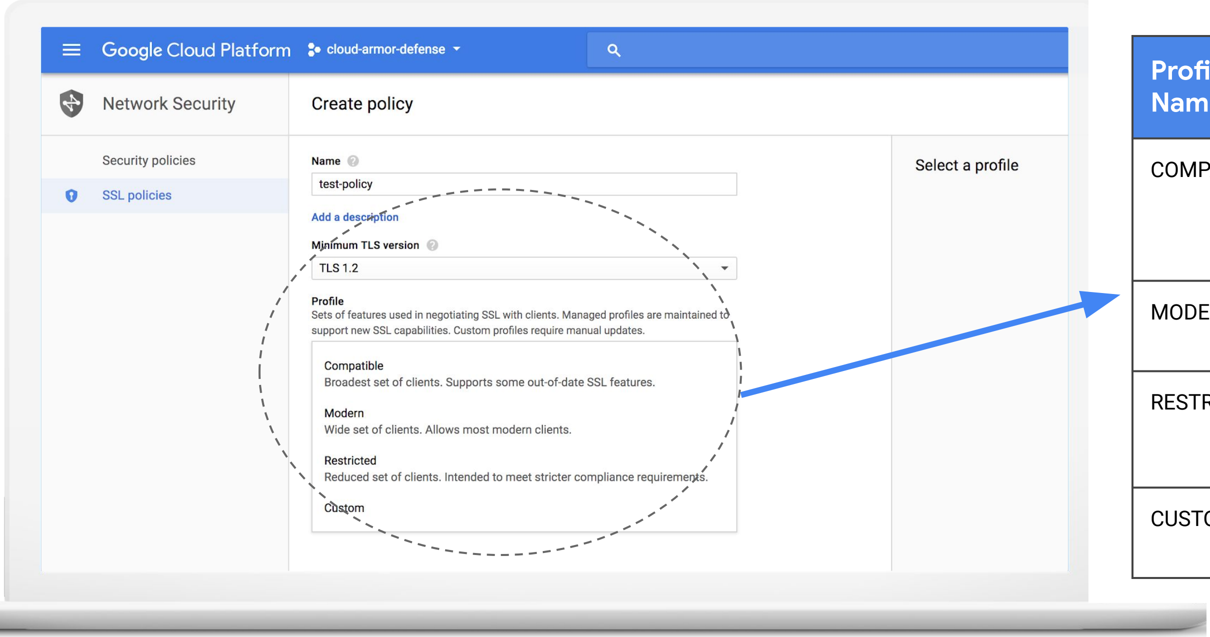
Network Service Tier
● Premium (Current project-level tier, change)
○ Standard

IP version	IP address
IPv4	Ephemeral

- Remove toil of procuring certs
- Remove toil of managing lifecycle of certs
- Domain Validation Certificates supported

Google Cloud

GCP-Managed and Custom SSL policies



Name

test-policy

Add a description

Minimum TLS version

TLS 1.2

Profile

Sets of features used in negotiating SSL with clients. Managed profiles are maintained to support new SSL capabilities. Custom profiles require manual updates.

Compatible
Broadest set of clients. Supports some out-of-date SSL features.

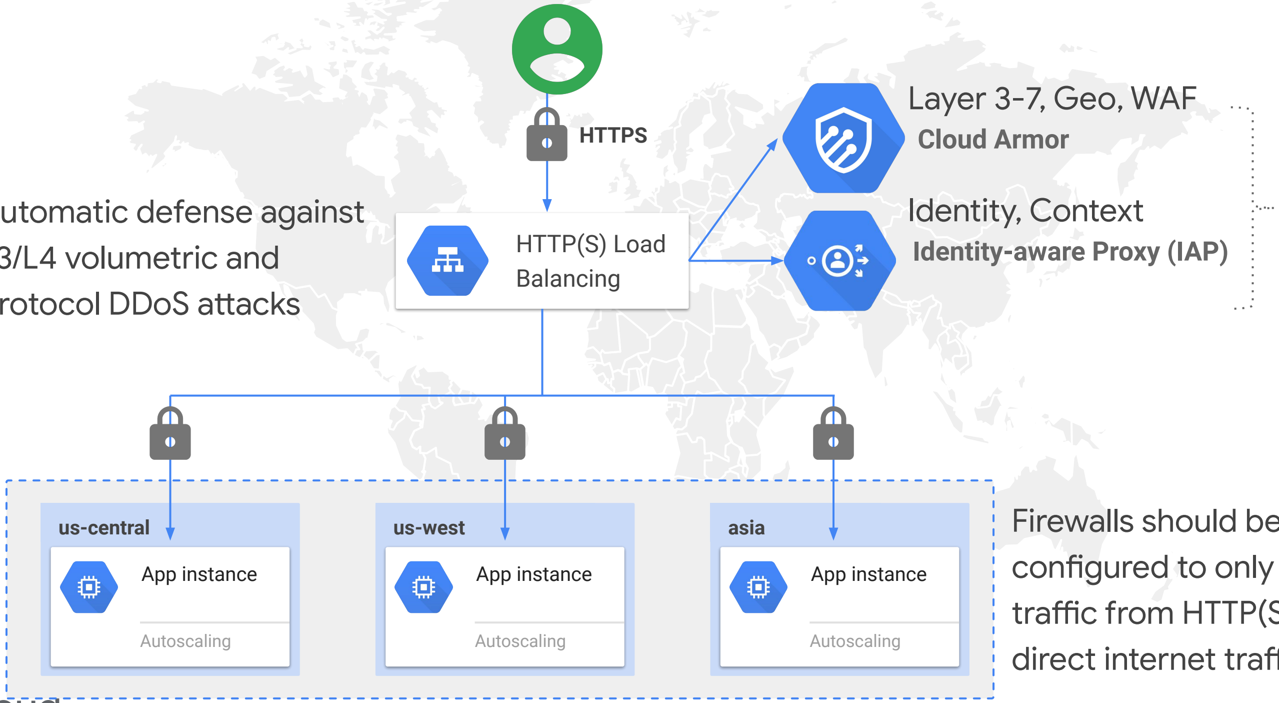
Modern
Wide set of clients. Allows most modern clients.

Restricted
Reduced set of clients. Intended to meet stricter compliance requirements.

Custom

Profile Name	Description
COMPATIBLE	Allows the broadest set of clients, including those which support only out-of-date SSL features, to negotiate SSL with the load balancer.
MODERN	Supports a wide set of SSL features, allowing modern clients to negotiate SSL
RESTRICTED	Supports a reduced set of SSL features, intended to meet stricter compliance requirements.
CUSTOM	Allows you to specify exactly the set of features to be enabled with your SSL policy

Best practice: Global LB + Cloud Armor + IAP



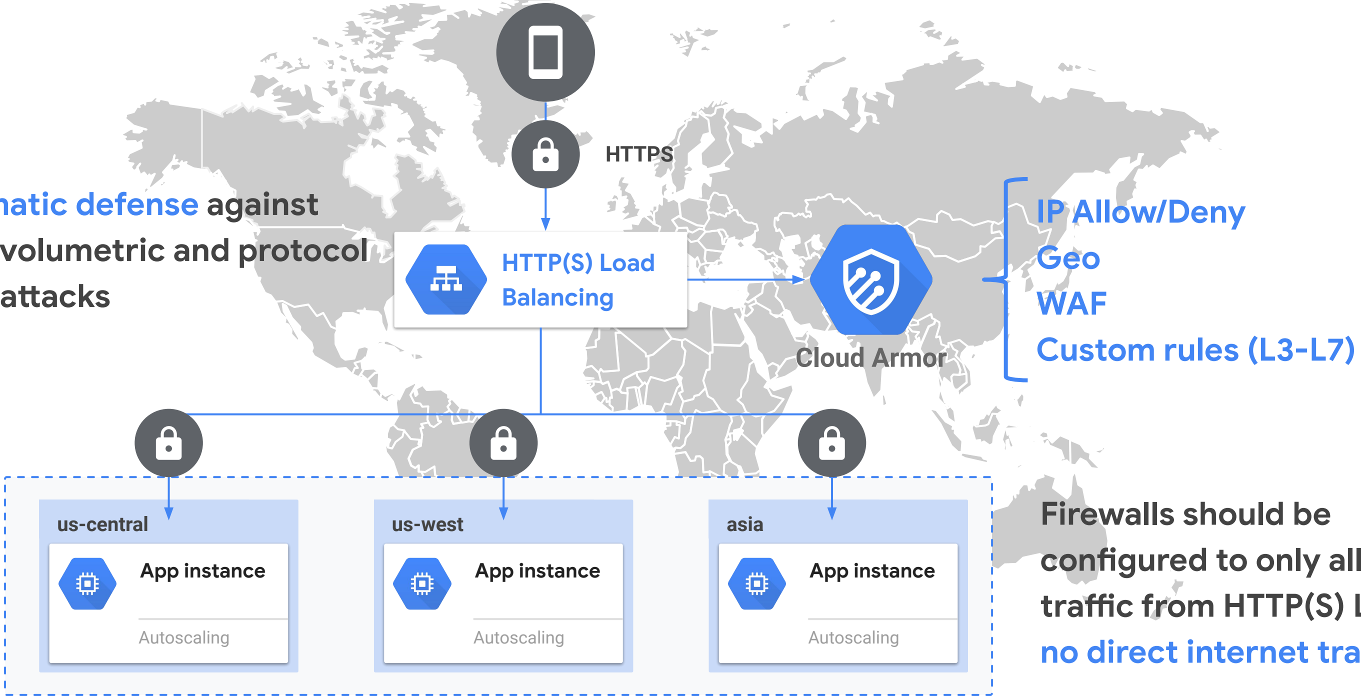
Automatic defense against L3/L4 volumetric and protocol DDoS attacks

Traffic is allowed only if Cloud Armor and IAP both allow it

Firewalls should be configured to only allow traffic from HTTP(S) LB, no direct internet traffic

Google Cloud Armor: DDoS Protection & WAF

Automatic defense against L3/L4 volumetric and protocol DDoS attacks



Firewalls should be configured to only allow traffic from HTTP(S) LB, no direct internet traffic

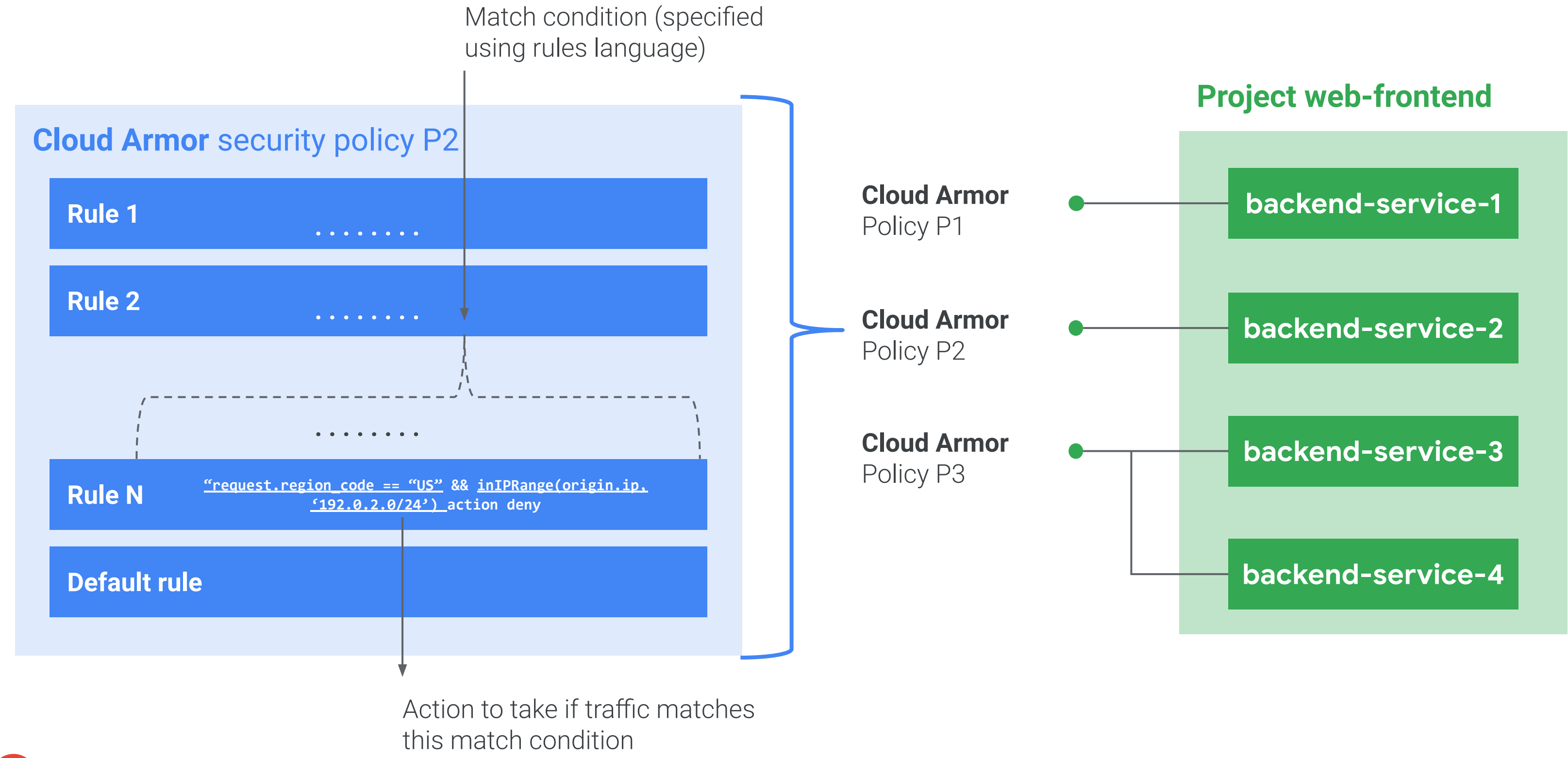
Google Cloud

Google Cloud Armor

- **Mitigate infrastructure DDoS attacks** with Global HTTP(S) Load Balancing (TCP SYN floods, Amplification attacks, IP fragmentation attacks, etc)
- **Allow or block traffic** based on IP, Geo, and custom match parameters (L3-L7 etc)
- **Defend against application layer attacks** (SQLi, XSS etc). Use in combination with IAP.
- **Telemetry:** Decisions logged to StackDriver and Monitoring dashboard

https://cloud.google.com/armor/

Google Cloud Armor Security Policies



Match condition (specified using rules language)

Cloud Armor security policy P2

Rule 1 ....

Rule 2 ....

....

Rule N

```
“request.region_code == “US” && inIPRange(origin.ip,
‘192.0.2.0/24’) action deny
```

Default rule

Action to take if traffic matches this match condition

Cloud Armor Policy P1

Cloud Armor Policy P2

Cloud Armor Policy P3

Project web-frontend

backend-service-1

backend-service-2

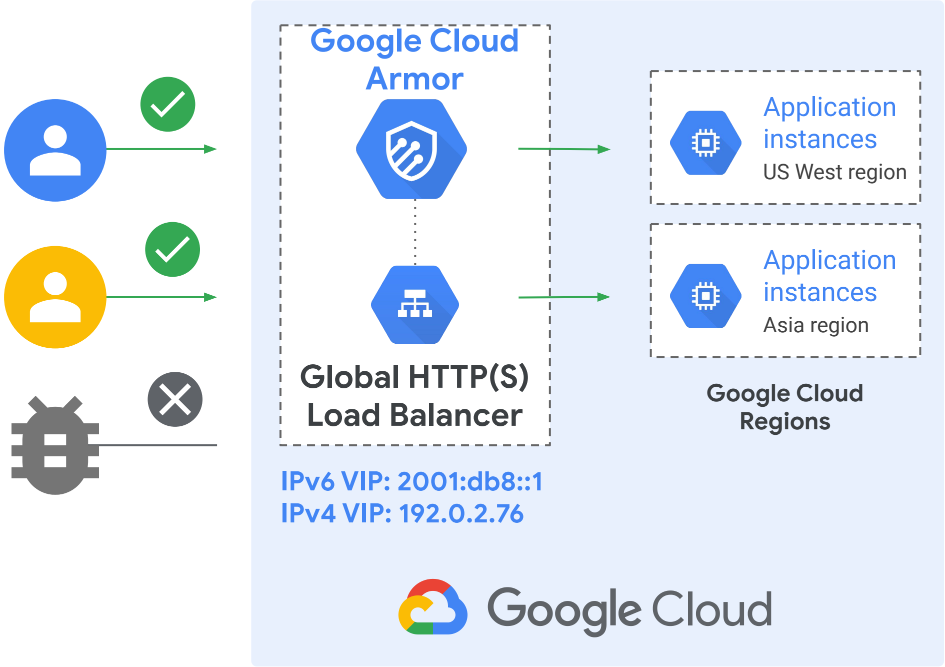
backend-service-3

backend-service-4

Google Cloud

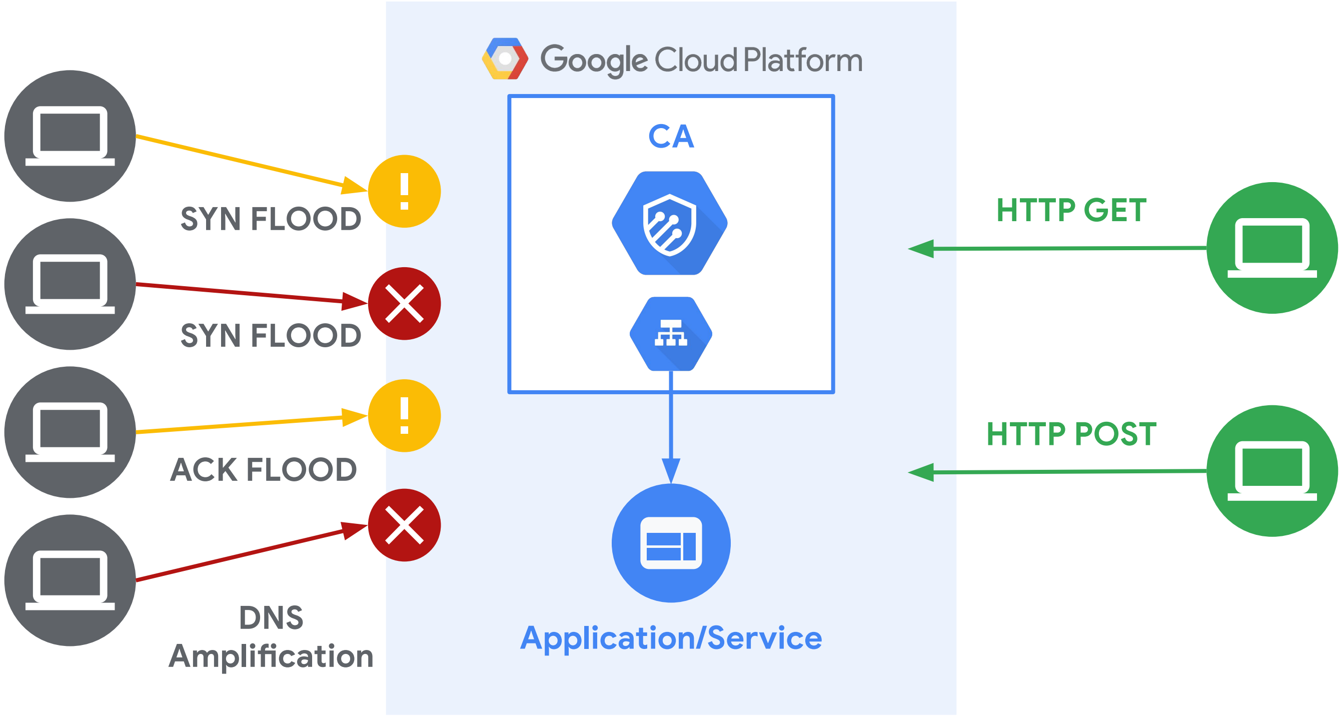
Google Cloud Armor Current Capabilities

Capability	Status
L3/L4 DDoS Defense	GA
Policy framework	GA
IP Allow/Deny List	GA
Geo-based access control	Alpha
Rules Language	Alpha
OWASP ModSecurity (SQLi & XSS) Rules	Alpha
Custom Rules L3-L7	Alpha
Cloud Armor Telemetry	GA



Google Cloud

Use Case: L3/L4 DDoS Protection

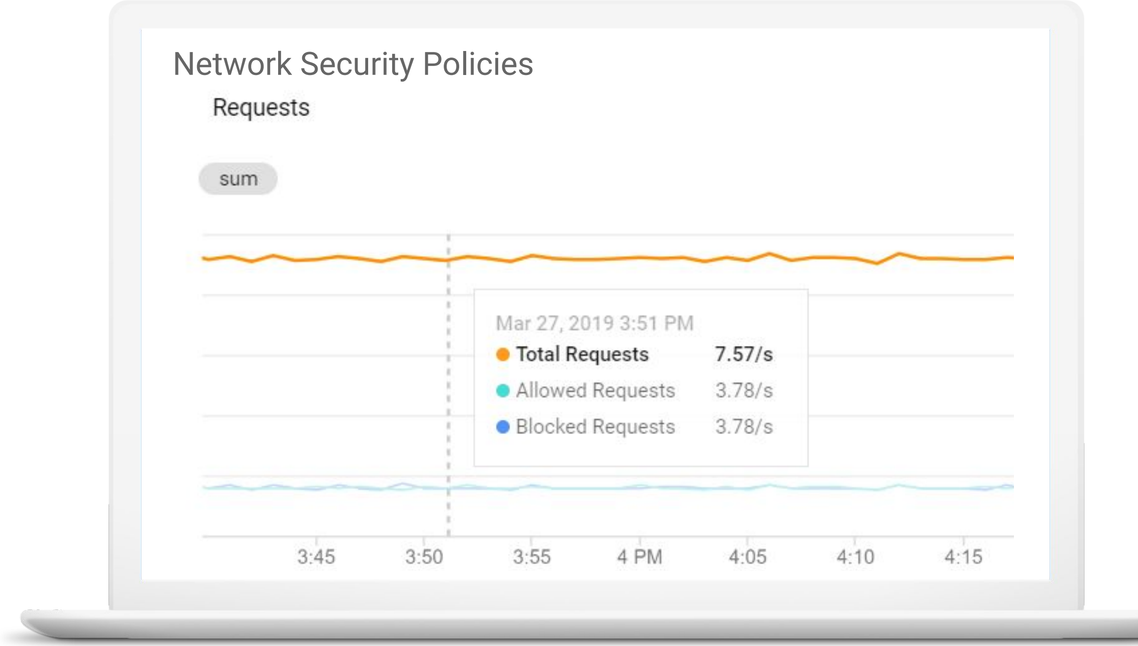


Google Cloud

Use Case: Real Time Monitoring & Alerting

Stackdriver Monitoring

- Granular Visibility
- Blocked & allowed traffic
- Impact of rules in preview
- Custom Alerting Policies



Network Security Policies

Requests

Mar 27, 2019 3:51 PM

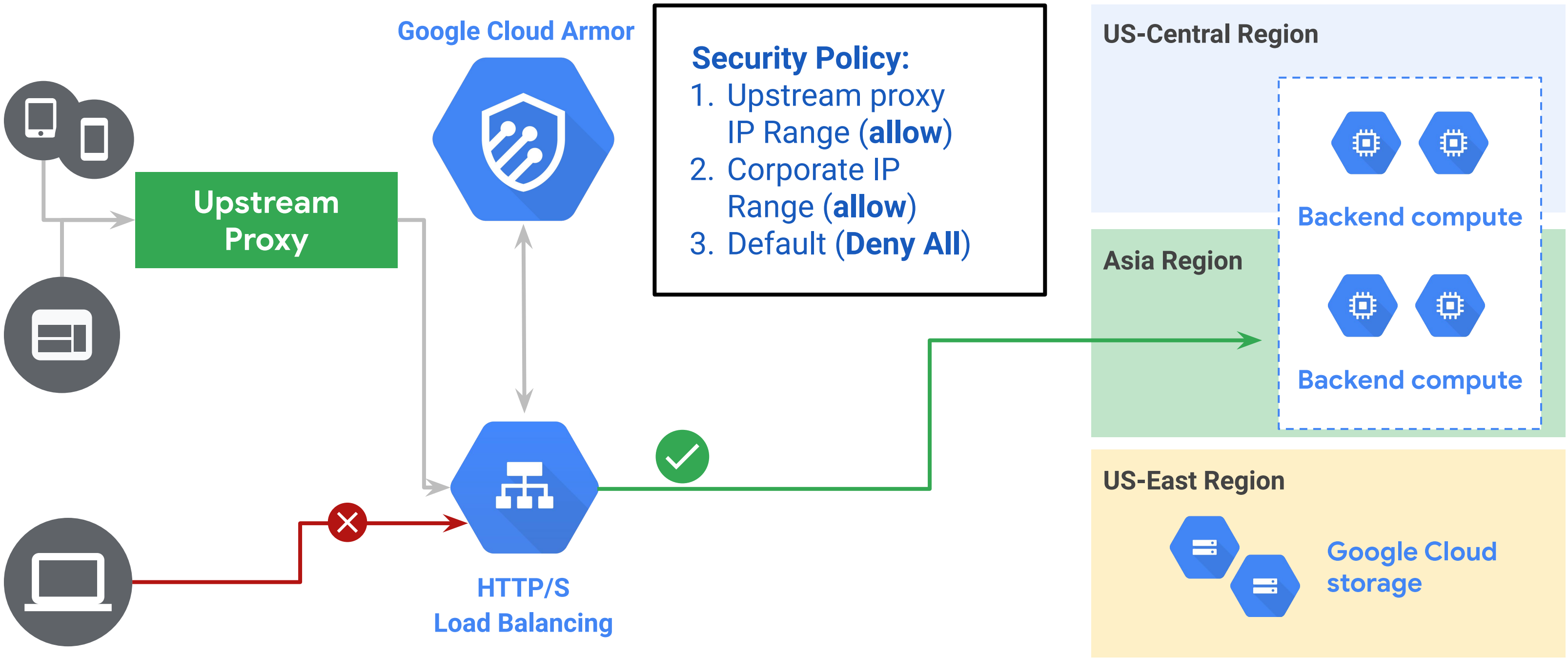
● Total Requests 7.57/s

● Allowed Requests 3.78/s

● Blocked Requests 3.78/s

Google Cloud

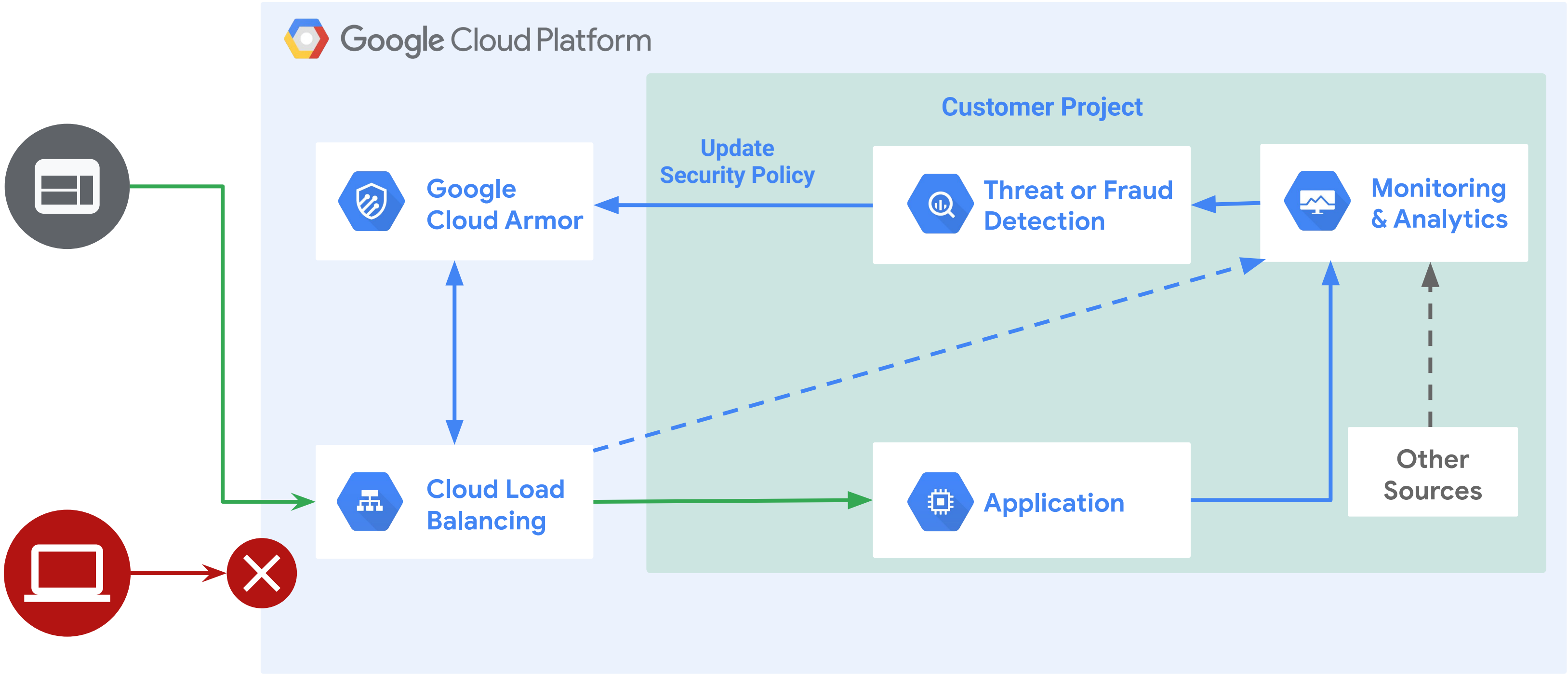
Use Case: Restricting Source IPs



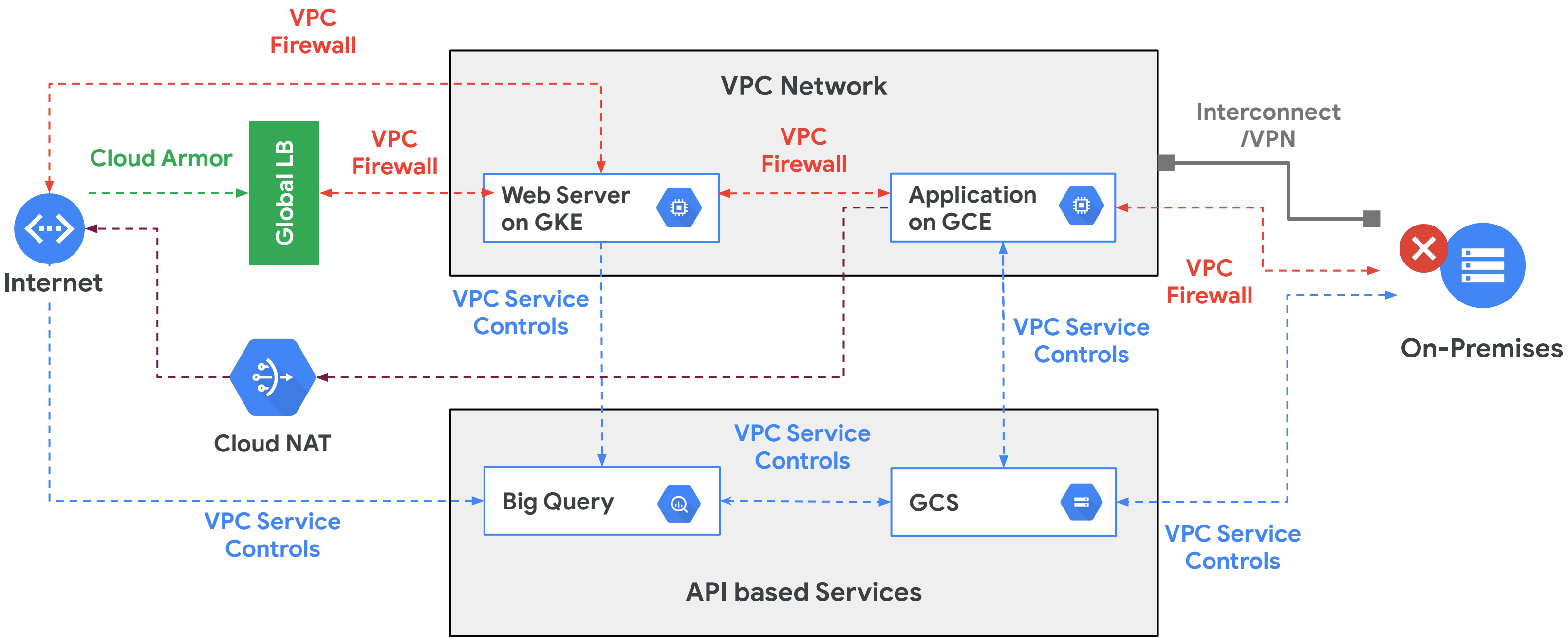
Security Policy:

1. Upstream proxy IP Range (**allow**)
2. Corporate IP Range (**allow**)
3. Default (**Deny All**)

Use Case: Upstream enforcement at the edge



Network Security Wrap-Up



Google Cloud

Thank you

Google Cloud