Leveraging Google Cloud Armor, Security Scanner and the Data Loss Prevention API

USING CLOUD ARMOR TO PROTECT AGAINST DDOS ATTACKS

Janani Ravi
CO-FOUNDER, LOONYCORN

www.loonycorn.com

Overview

Cloud Armor works with HTTP(S) load balancers

Mitigates DDoS attacks

Allows creation and enforcement of policies with allow/deny lists

Restricts malicious traffic to the edge of Google’s network

Prerequisites and Course Outline

Software and Skills

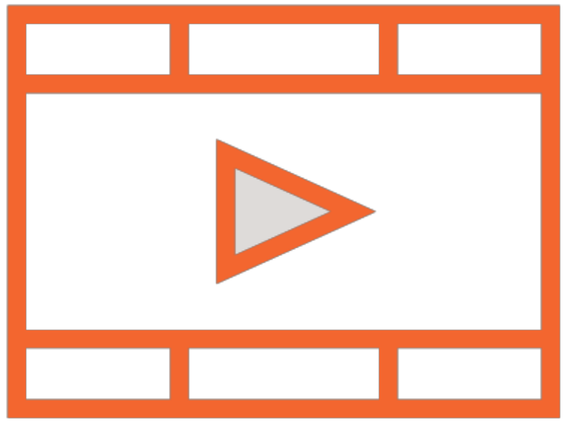
Cloud computing and networking basics

Web security basics

Working with RESTful APIs

Using the command line terminal

Prerequisites: Basic Cloud Computing



Choosing and Implementing Google Cloud Compute Engine Solutions

Architecting Global Private Clouds with VPC Networks

Building Scalable Compute Solutions Using Managed Instance Groups

Course Outline

Cloud Armor to protect against DDoS

- Edge security with allow and deny lists
- Associate security policies with load balancers

Cloud Security Scanner to identify app vulnerabilities

- Scan for XSS, Flash injection, mixed content usage, outdated and insecure libraries
- Install and use the open source Forseti security tools

Cloud Data Loss Prevention (DLP) API

- Classify and redact sensitive data
- Predefined and custom detectors for sensitive data

Scenarios: SpikeySales.com

Hypothetical online retailer

- Flash sales of trending products
- Spikes in user traffic

SpikeySales on the GCP

- Cloud computing fits perfectly
- Pay-as-you-go
- No idle capacity during off-sale periods

Introducing Cloud Armor

Cloud Armor

Security policies and IP allow and deny lists that work with HTTP(S) load balancing on the GCP

Features

Works with HTTP(S) load balancer

Provides built-in defense against DDoS

Used by Google Search, Gmail, YouTube

Security Policies

Apply policies to services

One or more security policies per service

Each has hierarchy of rules

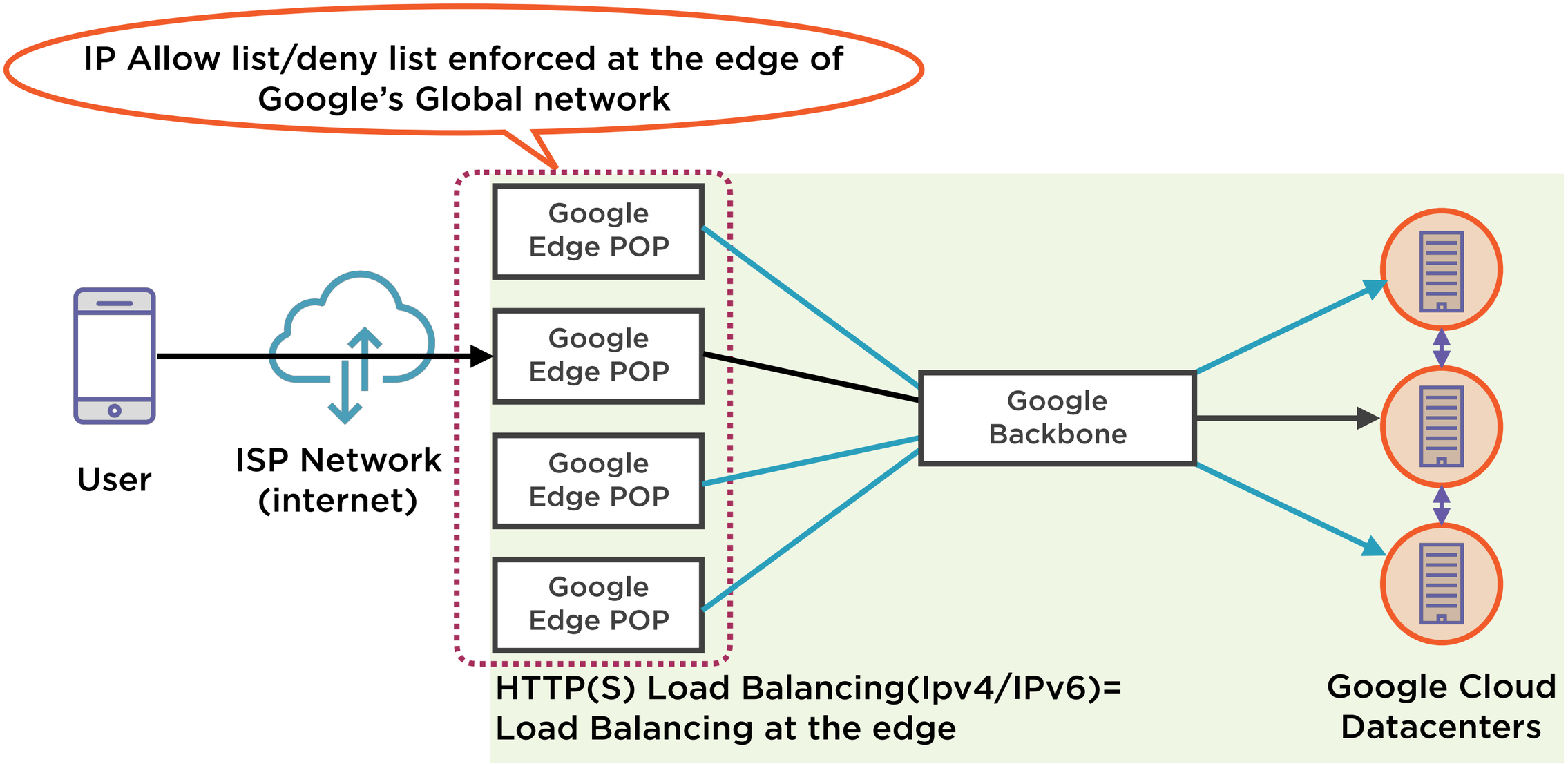
IP Deny/Allow Lists

Control access at edge of GCP

Enable or restrict access to HTTP(S) load balancer

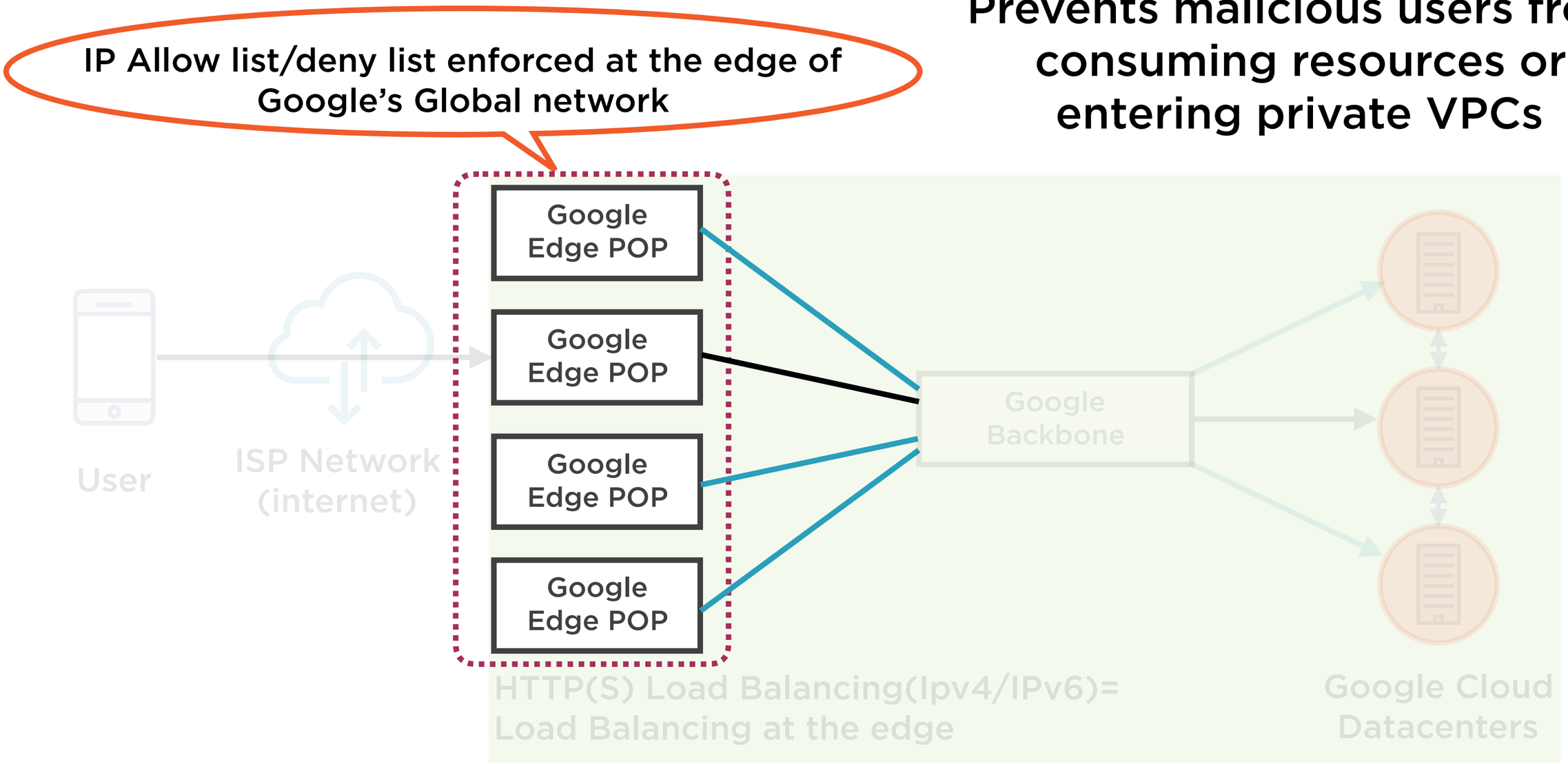
Prevents malicious traffic from consuming resources or entering core

Edge Security



Policies Applied Close to Users

Prevents malicious users from consuming resources or entering private VPCs



IP Deny/Allow Lists

Cloud Armor security policies for HTTP(S) Load Balancing

- Create security policies with deny list and allow list rules
- Associate security policy with one or more HTTP(S) Load Balancing backend services

IP Deny/Allow Lists

Deny listing to block a source IP address or CIDR range from accessing HTTP(S) load balancers

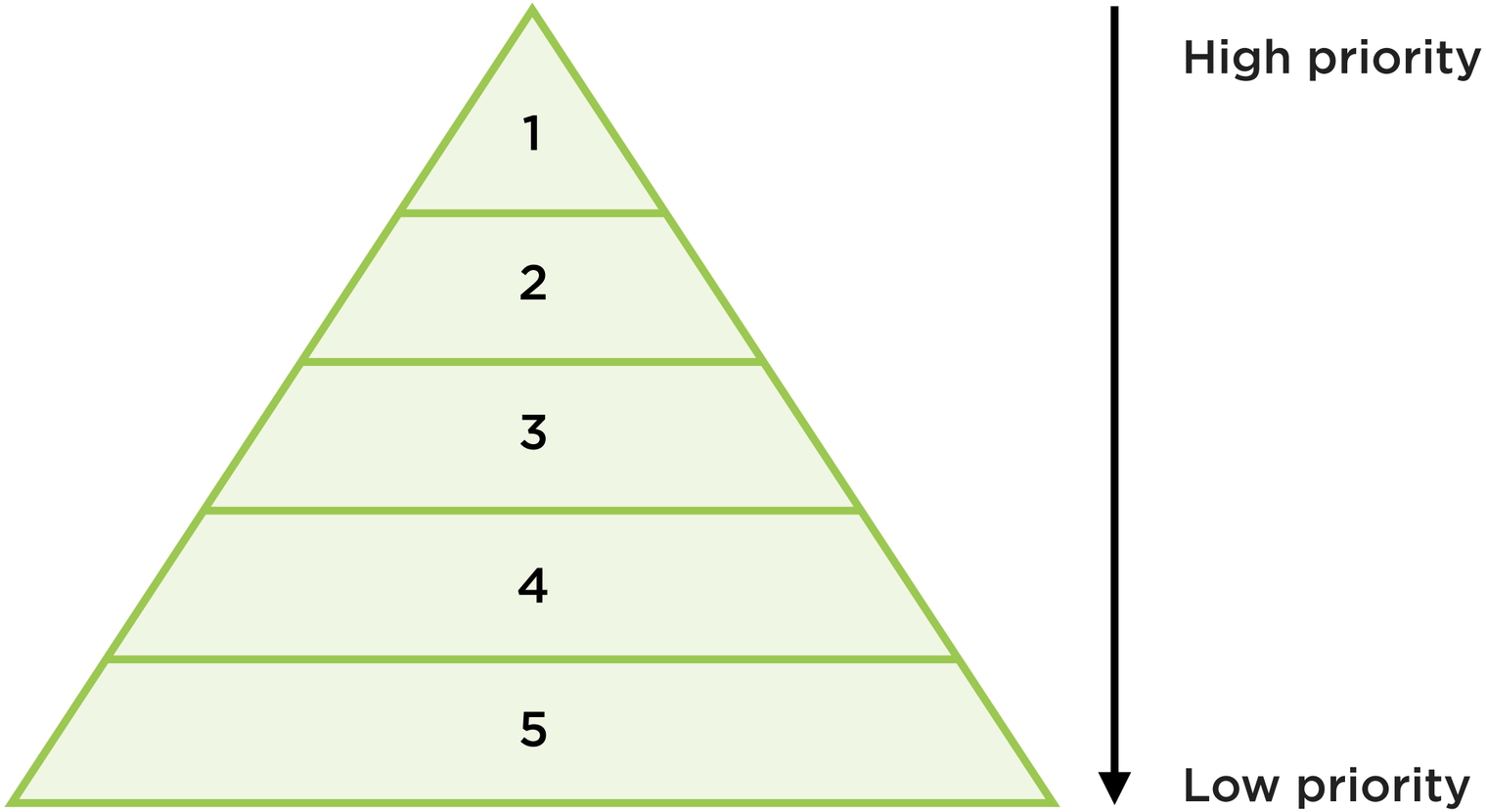
Allow listing to allow a source IP address or CIDR range to access HTTP(S) load balancers

IP Deny/Allow Lists

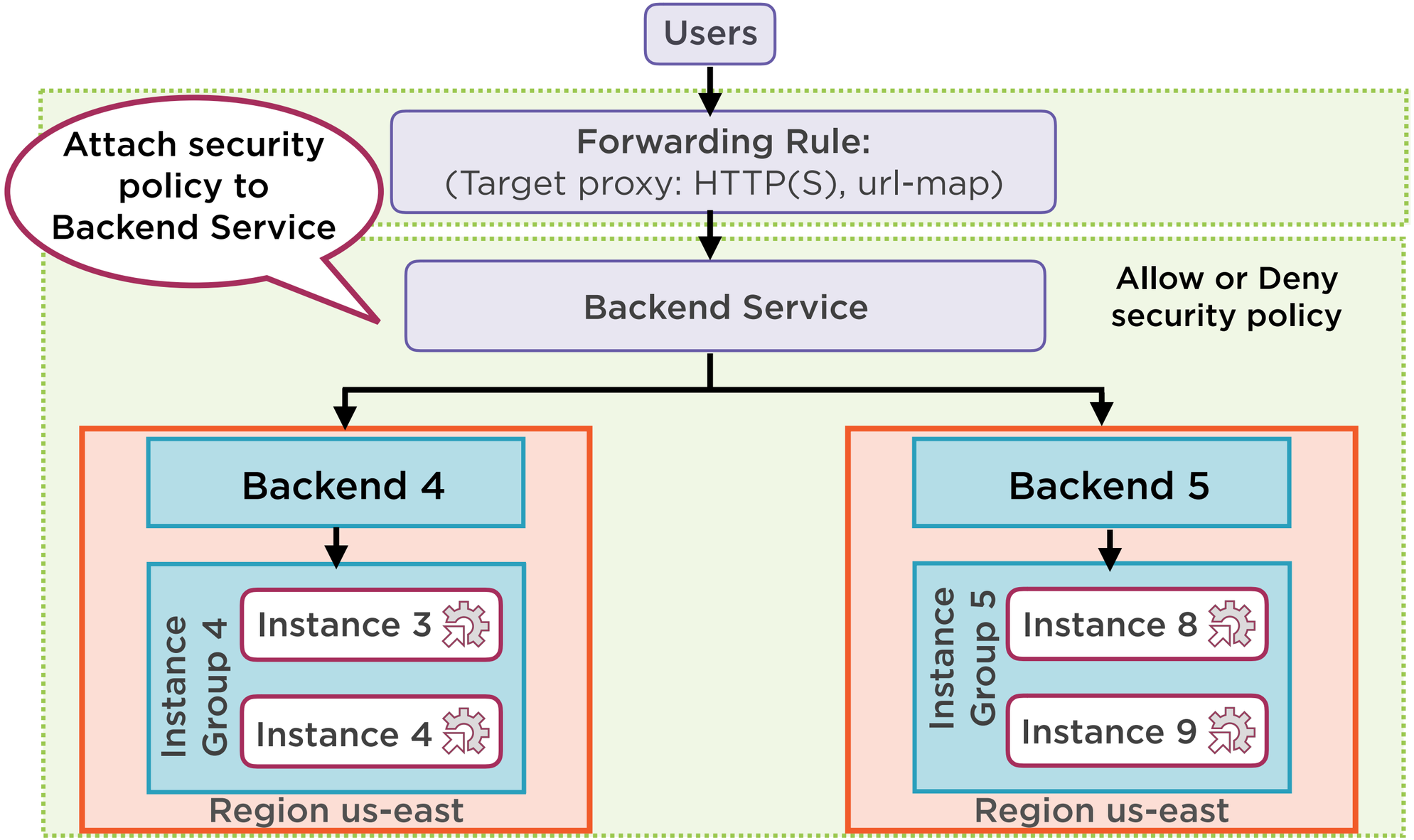
Can configure a deny rule to display a 403, 404, or 502 error code

If multiple rules present, can designate the order in which the rules are evaluated

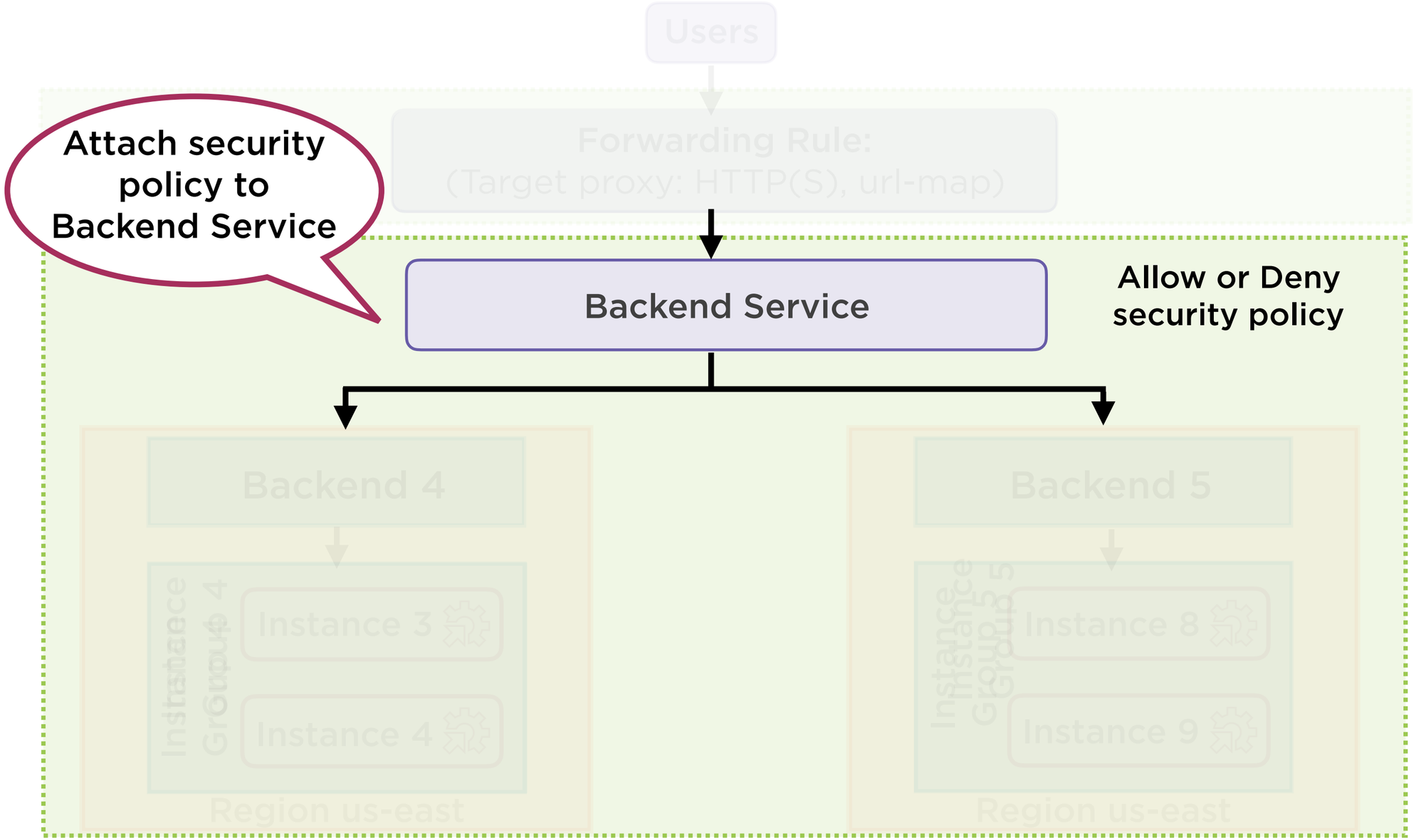
Cloud Armor Security Policies



Edge Security with IP Allow/Deny Lists



Applied Before Traffic Reaches Instances



Limits, Restrictions and Pricing

Limits

Each project is limited to a maximum of 200 security rules

Each project is limited to a maximum of 10 Cloud Armor security policies

Each rule is limited to a maximum of 5 IP addresses or IP address ranges

Limit of 20,000 requests per second per project across all backends

Restrictions

Not supported for Cloud CDN in the Beta release

Not supported for HTTP(S) Load Balancing with Google Cloud Storage backends

Cloud Armor Pricing

Policy Charge	$5 per Cloud Armor policy per month
Per Rule Charge	$1 per rule per month
Incoming Request Charge	$0.75 per million HTTP(S) requests

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

Demo

Creating Cloud Armor policies with allow and deny rules

Demo

Associating a Cloud Armor security policy with a load balancer to blacklist malicious traffic

Summary

Cloud Armor works with HTTP(S) load balancers

Mitigates DDoS attacks

Allows creation and enforcement of policies with allow/deny lists

Restricts malicious traffic to the edge of Google's network