Cloud Armor

#GCPSketchnote

@PVERGADIA THECLOUDGIRL.DEV

10.29.2020

ERIN: User traffic on our internet facing service is growing rapidly!

We need a solution to get protection from DDoS & Web attacks.

SAM: And so are the malicious attacks!

Cloud Armor!

What is Cloud Armor?

Defend against application layer attacks (SQLi, XSS, etc). Use in combination with IAP.

Mitigate infrastructure DDoS attacks with Global HTTP(s) Load Balancing (TCP SYN floods, Amplification attacks, IP fragmentation attacks, etc.

Telemetry: Decisions sent to Cloud logging, monitoring and Security command center.

Allow or block traffic based on IP, Geo, and custom match parameters (L3-L7, etc).

How do security policies apply?

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: SECURITY POLICIES

PROJECT web-frontend

- CLOUD ARMOR Policy P1 → backend-service-1
- CLOUD ARMOR Policy P2 → backend-service-2
- CLOUD ARMOR Policy P3 → backend-service-3, backend-service-4

How does Cloud Armor work?

CLOUD ARMOR: DDOS PROTECTION & WAF

Defense against L3/L4 volumetric and protocol DDoS attacks

HTTPs

Cloud CDN

HTTP(s) Load Balancing

- IP Allow/Deny
- Geo
- WAF
- Custom rules (L3-L7)

Internet

Internet

Cloud Provider / Customer Datacenter: External Application

GKE Cluster

Autoscaling: App Instance

Hybrid or Multi Cloud Workload

Google Cloud Platform

L3/L4 Volumetric DDoS Protection

- DNS Amplification
- SYN Flood
- ICMP Flood
- Slowloris

Cloud Armor

Geography Based Access Controls

- origin: US
- origin: UK
- origin: SG

Cloud Load Balancing

Layer 7 Traffic Filtering & WAF

Google Cloud

- www.website.com
- www.website.com
- website.com/admin
- SQL Injection
- Cross-Site Scripting

Application/ Service

What do I get in visibility & telemetry?

Cloud Security Command Center

Finding & Assets

Pre request logging

Cloud Armor

Real time telemetry

Cloud Logging

Cloud Monitoring