**DDOS Mitigation Using Cloud Armor**

What is DDOS?

DDoS stands for Distributed Denial of Service. It is a type of cyber attack in which multiple compromised computers or devices are used to flood a target system, network, or website with a massive amount of traffic, overwhelming its resources and making it unavailable to legitimate users.

There are three types of DDOS Attacks-

Protocol Attacks: These attacks are usually on Layer 3&4 in the OSI model.

Application Attacks: These attacks are usually on Layer 7 in the OSI model.

Volumetric Attacks: These attacks aim to use all the available bandwidth of the Internet Pipe.

**Cloud Armor**

Cloud Armor protects customers against all kinds of DDOS attacks. Cloud Armor has inbuilt Security Policies which help protect against DDOS attacks. You can use the predefined or custom ruleset to protect against the attacks. Google Cloud Armor is delivered at the edge of Google’s network providing protection against attacks close to the source.

It works in combination with another load balancer. It can be attached to:

* Global external HTTP(S) load balancer
* Global external HTTP(S) load balancer (classic)
* External TCP proxy load balancer
* External SSL proxy load balancer

**Mitigation Strategy**

Custom Rules: Create custom rules using a combination of L3–L7 parameters and geolocation to protect your deployment. These flexible rules language allow you to define specific criteria for filtering incoming traffic.

Preview Mode: Deploy Cloud Armor rules in preview mode to assess their effectiveness and impact on production traffic before enabling active enforcement. This helps you understand how the rules will affect your system and fine-tune them accordingly.

Security Policies: Configure one or more security policies with a hierarchical structure. You can create rules at different levels of granularity and apply them to individual or multiple workloads, providing tailored security for each.

Filtering Based on IP: Filter incoming traffic based on IPv4 and IPv6 addresses or CIDRs. This allows you to control access by allowing or denying traffic from specific IP ranges or individual addresses.

Geolocation-Based Access Control: Enforce access control based on the geographic location of incoming traffic. You can specify rules to allow or deny traffic based on the country or region from which it originates.

DDoS and Web Attack Protection: Defend your applications from DDoS attacks and web attacks. Cloud Armor helps you mitigate these threats and enforce Layer 7 security policies, regardless of whether your application is deployed on Google Cloud or in a hybrid or multi-cloud architecture.

Named IP List: Allow or deny traffic through a Cloud Armor security policy using a curated Named IP List. This feature provides a convenient way to manage and control access based on predefined lists of IP addresses.

Monitoring and Visibility: Easily monitor the metrics associated with your security policies in the Cloud Monitoring dashboard. You can also view suspicious application traffic patterns directly in the [Security Command Center dashboard](https://cloud.google.com/security-command-center), which provides visibility into Cloud Armor decisions, implicated policies, and rules on a per-request basis.

Logging: Gain insights into Cloud Armor decisions, as well as the specific policies and rules implicated in each request, through [Cloud Logging.](https://cloud.google.com/logging) This allows you to review and analyze the behavior and impact of your security policies.

**Cloud Armor Adaptive Protection**

Google Cloud Armor Adaptive Protection is a feature powered by machine learning that helps safeguard your Google Cloud applications, websites, and services against L7 distributed denial-of-service (DDoS) attacks, specifically targeting HTTP floods and other high-frequency layer 7 (application-level) malicious activities.

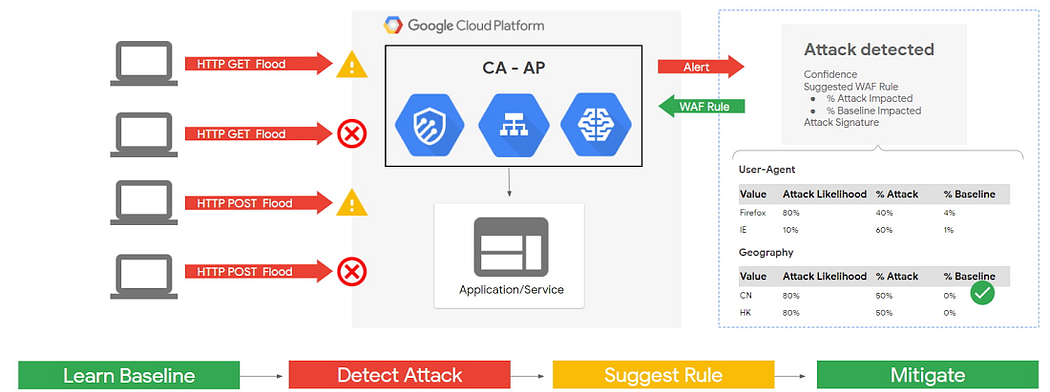
The underlying mechanism of Adaptive Protection involves constructing machine learning models to:

* Identify and raise alarms for abnormal activities.
* Generate a descriptive signature that characterizes the potential attack.
* Produce a customized Google Cloud Armor WAF rule to block the identified signature.

When a potential attack is detected by Adaptive Protection, it generates an alert comprising the following details:

* The attack traffic's signature.
* A suggested Google Cloud Armor WAF rules to obstruct the attack traffic.
* A confidence score, indicating the likelihood that the attack is genuine.
* A projected impacted baseline rate, representing the percentage of traffic that the suggested rule would block.

You can utilize the information from the alert to determine whether to implement the suggested rule. If you choose to deploy the rule, it will be applied to the Google Cloud Armor security policy associated with the protected resource.



Cloud Armor — Advanced Protection

When configuring DDoS mitigation with Cloud Armor, there are several key rules and settings one can consider to enhance the protection. Here are some recommended best practices:

1. Rate Limiting:

* Implement rate limiting rules to restrict the number of requests per second from a single IP address or subnet. This helps prevent overwhelming your application or infrastructure.
* Set appropriate rate limits based on your expected traffic patterns, ensuring a balance between legitimate requests and potential DDoS attacks.

2. IP Whitelisting/Blacklisting:

* Utilize IP whitelisting to allow only trusted IP addresses or IP ranges to access your application or service. This helps mitigate DDoS attacks originating from unknown or suspicious sources.
* Consider IP blacklisting to block known malicious IP addresses or ranges associated with DDoS attacks or other security threats.

3. Geo-Blocking:

* Employ geo-blocking rules to restrict traffic from specific countries or regions where you don't expect legitimate users or clients. This can help mitigate DDoS attacks originating from certain geographical areas known for malicious activities.

4. HTTP Flood Protection:

* Configure Cloud Armor to detect and mitigate HTTP flood attacks, which involve overwhelming your application with a large number of HTTP requests.
* Define thresholds for the maximum number of requests per second or minute from a single IP or subnet, and configure appropriate actions such as rate limiting, IP blocking, or challenge pages for suspicious traffic.

5. SYN Flood Protection:

* Enable SYN flood protection to defend against SYN flood attacks that exploit the TCP handshake process.
* Set SYN cookie thresholds to automatically drop or rate limit connections that exceed the defined limit, preventing the exhaustion of server resources.

6. CAPTCHA Challenges:

* Implement CAPTCHA challenges for suspicious or potentially malicious traffic, forcing users to solve a challenge before accessing your application.
* Configure Cloud Armor to present CAPTCHA challenges based on various triggers, such as abnormal traffic patterns or suspicious behavior.

7. Monitoring and Logging:

* Enable logging and monitoring features provided by Cloud Armor to analyze traffic patterns, detect anomalies, and respond to potential DDoS attacks in real time.
* Use Cloud Monitoring or other logging and analysis tools to gain insights into traffic behavior and identify potential attack vectors.