Google Cloud Armor overview

Google Cloud Armor helps you protect your Google Cloud deployments from multiple types of threats, including distributed denial-of-service (DDoS) attacks and application attacks like cross-site scripting (XSS) and SQL injection (SQLi). Google Cloud Armor features some automatic protections and some that you need to configure manually. This document provides a high-level overview of these features, several of which are only available for global external HTTP(S) load balancers and global external HTTP(S) load balancer (classic)s.

Security policies

Use Google Cloud Armor security policies to protect applications running behind a load balancer from distributed denial-of-service (DDoS) and other web-based attacks, whether the applications are deployed on Google Cloud, in a hybrid deployment, or in a multi-cloud architecture. Security policies can be configured manually, with configurable match conditions and actions in a security policy. Google Cloud Armor also features preconfigured security policies, which cover a variety of use cases. For more information, see Google Cloud Armor security policy overview (/armor/docs/security-policy-overview).

Rules language

Google Cloud Armor enables you to define prioritized rules with configurable match conditions and actions in a security policy. A rule takes effect, meaning that the configured action is applied, if the rule is the highest priority rule whose attributes match the attributes of the incoming request. For more information, see Google Cloud Armor custom rules language reference (/armor/docs/rules-language-reference).

Preconfigured WAF rules

Google Cloud Armor preconfigured rules help protect your web applications and services from common attacks from the internet and help mitigate the OWASP Top 10 risks (https://owasp.org/www-project-top-ten/). The rules allow Google Cloud Armor to evaluate distinct traffic signatures by referring to conveniently-named rules, rather than requiring you to define each signature manually. The rule source is ModSecurity Core Rule Set 3.0.2 (https://modsecurity.org/crs/) (CRS).

These preconfigured rules can be tuned to disable noisy or otherwise unnecessary signatures. For more information, see Tuning Google Cloud Armor WAF rules (/armor/docs/rule-tuning).

Google Cloud Armor Managed Protection

Managed Protection is the managed application protection service that helps protect your web applications and services from distributed denial-of-service (DDoS) attacks and other threats from the internet. Managed Protection features always-on protections for your load balancer, and gives you access to WAF rules.

DDoS protection is automatically provided for global external HTTP(S) load balancers, global external HTTP(S) load balancer (classic)s, external SSL proxy load balancers, and external TCP proxy load balancers, regardless of tier. The HTTP, HTTPS, HTTP/2, and QUIC protocols are all supported.

For more information, see Managed Protection overview (/armor/docs/managed-protection-overview).

Threat Intelligence

Google Cloud Armor Threat Intelligence lets you secure your traffic by allowing or blocking traffic to your global external HTTP(S) load balancers and global external HTTP(S) load balancer (classic)s based on several categories of threat intelligence data. For more information about Threat Intelligence, see Configuring Threat Intelligence features (/armor/docs/threat-intel).

Named IP address lists

Google Cloud Armor named IP address lists let you reference lists of IP addresses and IP ranges. You can configure a security policy rule with named IP address lists. You do not have to manually specify each IP address or IP range individually. For more information, see Named IP address lists (/armor/docs/armor-named-ip).

Google Cloud Armor Adaptive Protection

Adaptive Protection helps you protect your applications and services from L7 distributed denial-of-service (DDoS) attacks by analyzing patterns of traffic to your backend services, detecting and alerting on suspected attacks, and generating suggested WAF rules to mitigate such attacks. These rules can be tuned to meet your needs. Adaptive Protection can be enabled on a per- security policy basis, but it requires an active Managed Protection subscription in the project.

For more information, see Google Cloud Armor Adaptive Protection overview (/armor/docs/adaptive-protection-overview).

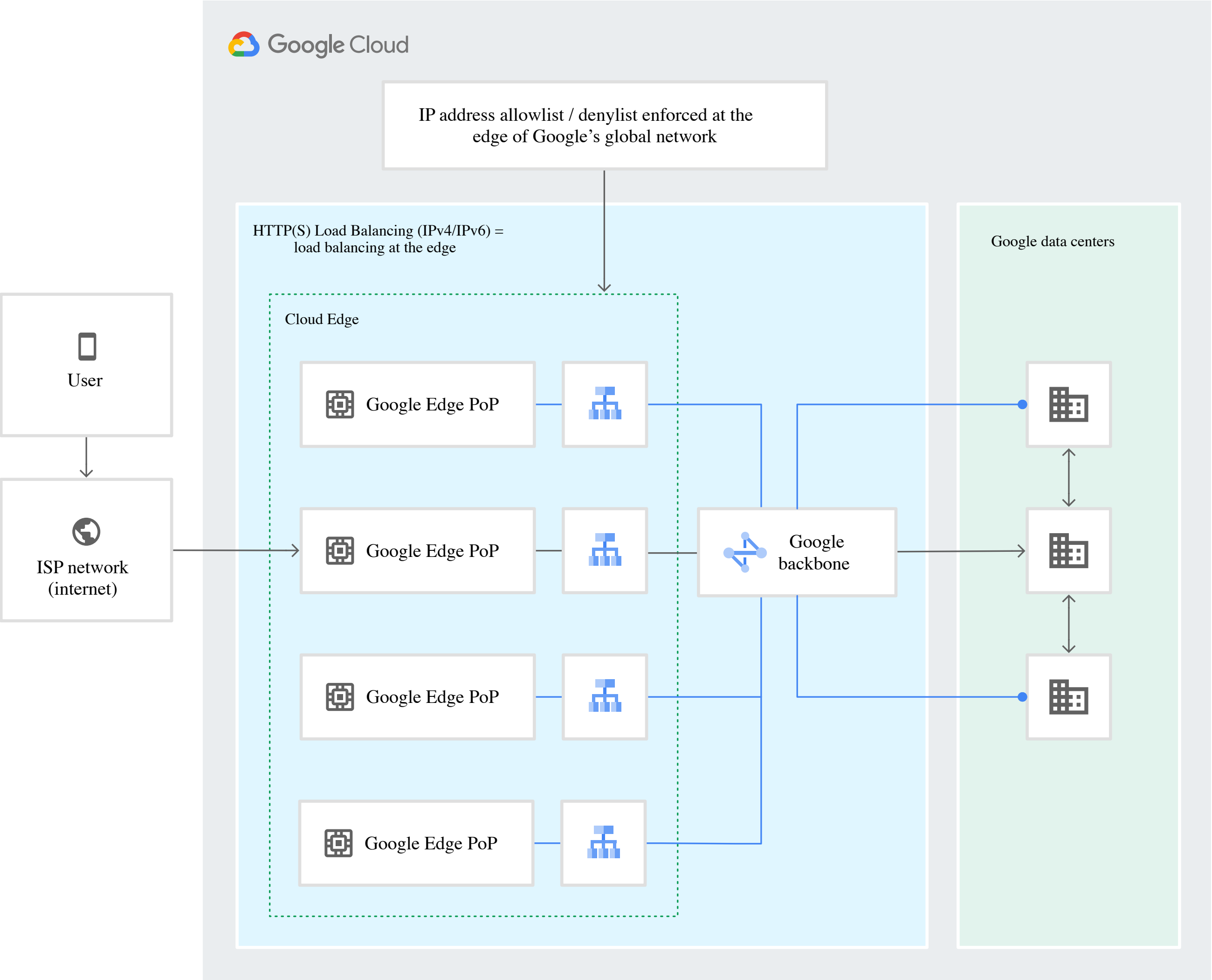
How Google Cloud Armor works

Google Cloud Armor provides always-on DDoS protection against network or protocol-based volumetric DDoS attacks. This protection is for applications or services behind load balancers. It is able to detect and mitigate network attacks in order to allow only well-formed requests through the load balancing proxies. You can attach security policies to the backend services of the following load balancers. The security policies enforce custom Layer 7 filtering policies, including pre-configured WAF rules that mitigate OWASP top 10 web application vulnerability risks:

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

Google Cloud Armor security policies enable you to allow or deny access to your deployment at the Google Cloud edge, as close as possible to the source of incoming traffic. This prevents unwelcome traffic from consuming resources or entering your Virtual Private Cloud (VPC) networks.

The following diagram illustrates the location of the global external HTTP(S) load balancers, global external HTTP(S) load balancer (classic)s, the Google network, and Google data centers.


Google Cloud
IP address allowlist / denylist enforced at the edge of Google's global network
HTTP(S) Load Balancing (IPv4/IPv6) = load balancing at the edge
Google data centers
Cloud Edge
User
ISP network (internet)
Google Edge PoP
Google Edge PoP
Google Edge PoP
Google Edge PoP
Google backbone

(/static/armor/images/ip-bl-wl-1.svg)

Google Cloud Armor policy at network edge (click to enlarge)

You can use some or all of these features to protect your application. You can use security policies to match against known conditions, create WAF rules to protect against common attacks like those found in the ModSecurity Core Rule Set 3.0.2 (https://modsecurity.org/crs/), and use Google Cloud Armor Managed Protection's built-in protections against DDoS attacks.

What's next

- Examine common use cases for Google Cloud Armor (/armor/docs/common-use-cases)
- Learn about Google Cloud Armor Managed Protection (/armor/docs/managed-protection-overview)
- Learn about Google Cloud Armor Adaptive Protection (/armor/docs/adaptive-protection-overview)

Last updated 2022-09-28 UTC.