CLOUD GATEWAY

Web Application Firewall (WAF)

What is it?

Cloud Gateway WAF is a highly sophisticated, configurable firewall that protects customers' web applications from malicious attacks. Equipped with a comprehensive suite of protective features, WAF sits between external consumers and the web applications, safeguarding critical business data from a host of potential threats.

How does it work?

The internet is an increasingly common vehicle for service consumption, with many applications using web-based technologies, often built in public cloud environments. Many cloud providers offer default WAF services that may not be sufficient to protect the business, or cannot be configured to follow enterprise-specific rule sets. Cloud Gateway WAF works at layers 4-7, and provides an enhanced set of protections that can be configured to secure web applications, whether hosted in the cloud or on-premise.

Onboarding

Cloud Gateway work closely with the client to set up the rules and policies that govern WAF for each supported web application. To do this, we first establish the certificate management process, to make sure important badges of authenticity are preserved and renewed. Secondly, mapping sessions establish the necessary connections between individual front-end applications and their counterpart location within the network. Finally, these mapped connections are customised, so that WAF knows what a malformed or anomalous packet looks like, ensuring traffic is inspected and sanitised effectively.

Key benefits

Dependable security - A sophisticated set of protections to safeguard the customer's applications. All features come as standard, and can be reconfigured to suit evolving requirements.

Simple costing model - One fully mapped instance of Cloud Gateway WAF is charged at an annual fee, billed monthly. Additional consultation services are available too, priced on request.

The Agile Network - WAF protects web applications based in the cloud, but also those hosted on legacy infrastructure. Customers have the freedom to operate hybrid networks with a blend of cloud and on-prem services.

Bespoke security policy - Cloud Gateway WAF affords granular control over how specific web applications are protected. Connections are mapped and customised in accordance with customer-defined rule sets.

Supports Digital Transformation - Cloud Gateway manages security on the client's behalf, allowing them to focus on their core business and keep pace with their cloud journey.
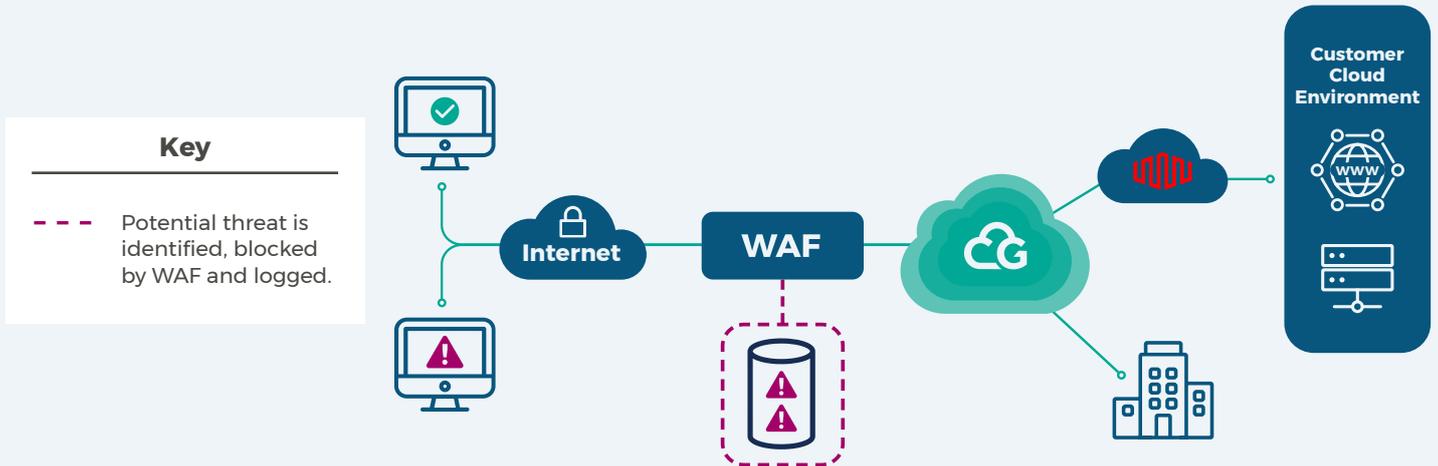
Use case

A company is running a front-end web application that makes product recommendations to its customers, alongside an e-commerce platform to handle transactions. At the back-end, a set of bespoke algorithms are used to set the service apart from its competitors. This intellectual property is critical to the company's success, and must be protected along with the personal client data submitted through the web application.

Cloud Gateway WAF is provisioned between the outward-facing web application and internal business systems. WAF sanitises every transaction at a deep level, inspecting every packet and its source for potential threats. During onboarding, we work with the client to establish the rules that WAF should obey, so that unusual strings of characters, untrusted users and other anomalies are recognised and blocked.

Features

- Blocks threats such as cross-site scripting, SQL injection, buffer overflows, file inclusion, denial of service, cookie poisoning, schema poisoning and countless other attacks.

- Protects against automated web attacks by identifying access from botnets and malicious sources, by using IP reputation, web application attack signatures, anti-virus and credential stuffing defence services.

- Intelligent Threat Detection identifies anomalous requests and determines if they are dangerous. Machine Learning eliminates false positives and false negatives with greater accuracy than Application Learning.

- Built-in Vulnerability Scanner to help protect web servers and web applications, assisting with the design of effective and efficient protection profiles.

- Layer 7 load balancing and content-based routing increases application speeds, improves server resource utilisation and stabilises applications.

- HTTPS/SSL Offloading including support for Client Certificate Authentication.

- Network and application layer DoS/DDoS protection.

- Full SNMP, Syslog and Email Logging/Monitoring support with integration into Customer SIEM platforms.

Key

- - - Potential threat is identified, blocked by WAF and logged.

Internet **WAF** Customer Cloud Environment