

Web Application Firewall

Introduction

Introduction

Overview

Web Application Firewall (also known as WAF) is a dedicated firewall that filters, monitors, and blocks HTTP traffic to and from web application. By inspecting the traffic, WAF protects your network contents from attacks originated from web application vulnerabilities.

As a key component of Alibaba Cloud Security, WAF effectively applies to most common web attacks, such as SQL injections, XSS, web shell, Trojan, etc. Besides, it improves your website performance through HTTP or HTTPS floods mitigation, and bad hot protection. Meanwhile, through it, customized security policies are available for various scenarios.

Compared to traditional hardware devices, Alibaba Cloud WAF can be set up to protect your web service within 10 minutes, with no complicated hardware deployment or tedious settings of appliances such as routers and switches.

Benefits

WAF provides a strong protection for most HTTP based web services.

General website protection

Function	Description
Common vulnerabilities protection	Protects content against SQL injection, cross-site scripting (XSS), command execution, code execution, local file include, remote file include, illegal file upload and so on.
Web shell protection	Prevents popular web shell and Trojan upload.
Sensitive information protection	Prevents leaking sensitive information, such as username and password.
Scanner & Hack tools protection	Identifies and blocks scanners or hack tools.

HTTP flood mitigation

Function	Description
Challenge	Reverse probes a client by inserting a cookie and a redirection challenge, tools or scripts cannot respond the challenge successfully.
Speed limitation	Speed limitation based on source IP' s query per second.
Bot protection	Identifies and blocks malicious bots or spiders to avoid unnecessary consumption of bandwidth and performance.
Customized rules	Customized rules against massive requests which have a specific pattern, such as user-agent, referrer URL.
IP reputation database	Up-to-date malicious IP database maintained by Alibaba Cloud helps to identify more malicious requests.
HTTP status codes	Analyzes the distribution of HTTP status code and block the abnormal IPs.
SSL encryption	Entire secure channel encrypted by SSL.
Specific path or Parameters statistic	Dynamically blacklists abnormal IPs which query specific interfaces, application, or paths with extremely fast speed.

Customized access control

Function	Description
Multiple factor based ACL	IP, URL, referrer, user-agent.
Flexible combination	Combines multiple rules as an integrated rule.
Customized scenario protection	Leeching, CSRF, management backend protection and so on.
Customized priorities	Free change of the consequences of the rules.

Key features

More than 10 years of web security experience

Built on more than a decade' s web security experience of Alibaba Group and hundreds of

most famous online businesses in China such as Taobao, Tmall and Alipay.

Professional security team consisting of top security experts worldwide.

Resist all existing OWASP attacks, and keep up with the latest vulnerabilities.

HTTP flood mitigation and bot protection

Effective mitigation of HTTP and HTTPS floods.

Prevent malicious spiders or bots from consuming website' s resources.

Detect and block suspicious requests that may exert negative impacts on your server, such as bandwidth consumption, database/SMS/API interface exhaustion, increased latency or even breakdown.

Customable rules for special business scenarios.

Big data ability

Alibaba Cloud hosts more than 37% websites in China.

Alibaba Cloud deals with more than 0.8 billion times of attacks every day.

Alibaba Cloud maintains the most popular malicious IP database in China.

Plentiful case studies on popular patterns, methods, and signatures of web attacks.

Analysis through big data platform of Alibaba Cloud and combined with latest technologies.

Easy and Reliable

Quick setup and activation within 5 minutes.

No hardware or software installation or router and switch configuration.

Work as defense cluster to avoid single point failure and provide redundancy.

Excellent processing ability that successfully addresses the massive requests of the world' s

largest e-shopping day (\$ 14.3 billion GMV in 11th November, 2015).