Alibaba Cloud
Web Application Firewall

Product Introduction

MORE THAN JUST CLOUD | ⊂-⊃ Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	**It indicates that it is a required value, and only one item can be selected.**	swich *{stand | slave}*

Contents

1 What is Alibaba Cloud WAF?

Alibaba Cloud WAF is a web application firewall that monitors, filters, and blocks HTTP traffic to and from web applications. Based on the big data capacity of Alibaba Cloud Security, Alibaba Cloud WAF helps you to defend against common web attacks such as SQL injections, Cross-site scripting (XSS), web shell, Trojan, and unauthorized access, and to filter out massive HTTP flood requests. It protects your web resources from being exposed and guarantees your website security and availability.

Alibaba Cloud WAF is easy to deploy. You can enable WAF protection for your website by subscribing to Alibaba Cloud WAF, configuring the website on the WAF console, and updating the website's DNS records using the WAF Cname address . When WAF is deployed on your website, all network traffic to the website is inspected by WAF. WAF identifies and filters out malicious traffic, and only returns valid traffic to the origin server.

Follow the *WAF learning path* to get started with WAF.

2 Features

Alibaba Cloud WAF (Web Application Firewall) helps to protect your website against various web attacks and to guarantee website security and availability. It leverages both core defense capabilities and big data capabilities to achieve reliable web security. Alibaba Cloud WAF offers the following features:

Request monitoring

Monitors the HTTP and HTTPS (only for WAF Business and Enterprise editions) requests that are forwarded to your website.

Web application protection

Protects your website against common web application attacks

- Defense against common OWASP threats, such as SQL injection, XSS attacks, Webshell uploading, command injection, illegal HTTP protocol requests, common Web server vulnerability attacks, unauthorized access to core files, and path traversing. Also provides backdoor isolation and scanning protection services.
- Websites stealth: Keeps the website address invisible to attackers to avoid direct attacks that bypass WAF.
- Regular and timely patches against 0day vulnerabilities: The protection rules used by Alibaba WAF are tried and tested and cover the latest vulnerability patches, which are updated in a timely manner and synchronized globally immediately after release.
- User-friendly observation mode: Provides observation mode for newly launched businesses on the website. In this mode, a suspected attack only triggers a warning, instead of a blocking action, in a bid to facilitate the statistics of business false alarms.

Protection against HTTP flood attacks

- Manages the access frequency from a single source IP address by using re-direction verification and human/machine identification.
- Prevents massive and slow request attacks based on precise access control policies and recognition of exceptional response code, URL request distribution, Referer, and User-Agent requests.

· Establishes threat intelligence and trustful access analysis models to quickly identify malicious requests by making full use of Alibaba Group's big data security advantages.

HTTP ACL Policy

· Provides a user-friendly configuration console that supports condition combinations of common HTTP fields such as IP, URL, Referer, and User-Agent to form precise access control policies. Also supports anti-leech protection, website backend protection, and so on.

· Combined with common web attack protection and HTTP flood protection, access control helps to create multiple layers of protection to suit a variety of needs to identify legitimate and malicious requests.

Virtual patches

Adjusts web protection policies to enable swift protection before patches are released for rectification of web application vulnerabilities.

Attack event management

Supports centralized management and analysis of attack events, attack traffic, and attack scales.

Reliability

· Load balancing: Provides services in cluster mode, with load balancing among multiple devices. Supports multiple load balancing policies.

· Smooth capacity expansion: Reduces or increases the number of cluster devices based on actual traffic and performs flexible capacity expansion of service.

· No single-point issues: Even if a single device breaks down or is offline for repair, services are not affected at all.

For more information, see the *Web Application Firewall product detail* page.

3 Scenarios

Alibaba Cloud WAF is applicable to Web application security protection of various websites, such as finance, e-commerce, o2o Internet+, games, government, and insurance.

You can use Alibaba Cloud WAF to solve the following problems:

· Prevent data leaks and avoid intrusions from malicious injections that may lead to core database leaks from the website.

· Prevent malicious HTTP flood attacks. Alibaba Cloud WAF can block large-volume malicious requests to safeguard website availability.

· Prevent Trojans from being uploaded to webpages with the intention of tampering with the content, and maintain the credibility of the website.

· Provide virtual patches to address the latest known website vulnerabilities and provide quick fixes wherever required.

3 Scenarios