ALIBABA CLOUD

Alibaba Cloud

Web应用防火墙

Product Introduction

Document Version: 20201015

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of 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.Editions and features

This topic describes the Pro, Business, Enterprise, and Exclusive editions of Web Application Firewall (WAF) and related features. If you want to purchase the Exclusive edition, you must submit a ticket. Each edition applies to a different business scale and provides specific protection features. You can purchase WAF instances by using the subscription billing method.

Editions and supported business scales

The following table lists the business scales supported by each edition. We recommend that you choose the Business or Enterprise edition for medium-sized enterprise websites.

> **Note** If you want to purchase the Exclusive edition, you must submit aticket.

Business specification	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
Website scale	Small- and medium-sized websites that do not have special security requirements	Medium-sized enterprise websites that provide services to all Internet users and have high data security requirements	Medium- and large-sized enterprise websites that have custom security requirements	Large-sized enterprise websites that require business-specific configurations
Peak queries per second (QPS)	2,000	5,000	Higher than 10,000	5,000
Maximum bandwidth, in Mbit/s (The origin server is deployed on Alibaba Cloud.)	50	100	200	100
Maximum bandwidth, in Mbit/s (The origin server is not deployed on Alibaba Cloud.)	10	30	50	30
Default number of second-level domains that can be protected	1	1	1	1,000

Business specification	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
Default number of subdomains of the second-level domains that can be protected in total (Wildcard domains are supported.)	10	10	10	1,000

For more information about how to activate WAF, see Purchase a WAF instance.

Editions and supported features (in mainland China)

The following table describes the features that are supported by each edition of WAF in mainland China. A WAF instance is billed on a subscription basis.

Symbol descriptions:

- √: indicates that the feature is supported.
- ×: indicates that the feature is not supported.
- Value-added: indicates a value-added service. If you want to use a value-added service, you must enable it when you purchase or upgrade a WAF instance.
- Supported after configuration: indicates a feature that must be separately enabled on the **Feature Settings** page for a pay-as-you-go WAF instance.

Feature	Description	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
Website access					
HTTPS protection	Allows you to implement HTTPS protection for websites with a few clicks.	√	√	√	√
Non-standard port protection	Protects traffic over the ports other than standard ports 80, 8080, 443, and 8443.	×	√	√	√

Feature	Description	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
Intelligent load balancing	Connects to multiple SLB service nodes to implement automatic disaster recovery and optimal routing with low latency.	Value-added	Value-added	Value-added	Value-added
Exclusive IP addresses	Provides exclusive IP addresses to protect specific domains.	Value-added	Value-added	Value-added	Value-added
Exclusive cluster	Allows you to customize service access and protection capabilities based on business requirements.	×	×	×	√
Website protection					
RegEx Protection Engine	Protects against common web attacks, such as SQL injection and cross-site scripting (XSS).	√	√	√	√
	Enables automatic update of protection rules against web zero-day vulnerabilities.	√	√	√	√
Protection rule group	Allows you to customize protection rule groups.	×	√	√	√
Big Data Deep Learning Engine	Detects web zero-day vulnerabilities.	×	√	√	√
Positive security model	Provides positive defense capabilities based on deep learning of website traffic.	×	×	√	√
Website tamper-proofing	Locks web pages to prevent tampering with content.	√	√	√	√
Data leak prevention	Prevents against the leak of sensitive data, such as ID card numbers, mobile numbers, and bank card numbers.	√	√	√	√

Feature	Description	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
HTTP flood protection	Protects against common HTTP flood attacks in Prevention or Prevention-emergency mode.	√	√	√	√
IP address blacklist	Blocks access requests from specific IP addresses or CIDR blocks.	√	√	√	√
	Supports the above blocking capability and also blocks access requests from IP addresses in specific regions.	×	√	√	√
Scan protection	Blocks the IP addresses where web attacks and path traversal are frequently initiated and the IP addresses of scanning tools, and provides collaborative defense. Default rules are used to block the first type of IP addresses.	√	√	√	√
	Supports the above protection capability and allows you to customize blocking rules for high-frequency web attacks and path traversal.	×	√	√	√
	Implements ACL-based access control by using basic fields, such as IP, URL, Referer, User-Agent, and Params.	√	√	√	√
	Supports the above protection capability and advanced fields, such as Cookie, Content-Type, Header, and Http-Method.	×	√	√	√

Custom protection policy Feature	Description	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
	Allows you to customize rules for HTTP flood protection. You can define a throttling policy, where the request frequency can be measured based on IP addresses or sessions.	×	√	√	√
	Allows you to measure the request frequency based on IP addresses, sessions, or custom fields.	×	×	√	√
Data risk control	Protects crucial website services, such as registrations, logons, activities, and forums, against fraud.	Value-added	Value-added	Value-added	Value-added
Bot management	Provides intelligent protection for bot traffic and against automated attacks. This feature is suitable for human-machine identification, scalping, and spam registration scenarios.	Value-added	Value-added	Value-added	Value-added
Application protection	Provides trusted communications and anti-bot protection for native applications to identify proxies, emulators, and requests with invalid signatures.	Value-added	Value-added	Value-added	Value-added
Account security	Detects credential stuffing, brute-force attacks, spam registration, weak passwords, and SMS interface abuse on service endpoints, such as registration and logon endpoints.	√	√	√	√
API request security	Allows upload of custom API definition files to ensure that only API requests that comply with the definitions are processed.	×	√	√	√

Feature	Description	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
Security analysis and support					
Log Service for WAF	Collects and stores all logs, enables near-real-time query and analysis, and provides online reports.	Value-added	Value-added	Value-added	Value-added

Editions and supported features (outside mainland China)

The following table describes the features that are supported by each edition of WAF outside mainland China. A WAF instance is billed on a subscription basis.

标识说明：

- **√：表示在当前套餐中支持。**
- **×：表示在当前套餐中不支持。**
- **增值：表示需要在开通WAF时额外开启的特性，或者在开通WAF后需要使用升级功能单独购买的特性。**
- **配置后支持：表示需要在开通按量计费WAF后，通过功能与规格设置单独开启的特性。**

Feature	Description	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
Website access					
HTTPS protection	Allows you to implement HTTPS protection for websites with a few clicks.	√	√	√	√
Non-standard port protection	Protects traffic over the ports other than standard ports 80, 8080, 443, and 8443.	×	√	√	√

Feature	Description	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
Intelligent load balancing	Connects to multiple SLB service nodes to implement automatic disaster recovery and optimal routing with low latency.	×	Value-added	Value-added	Value-added
Exclusive IP addresses	Provides exclusive IP addresses to protect specific domains.	Value-added	Value-added	Value-added	Value-added
Exclusive cluster	Allows you to customize service access and protection capabilities based on business requirements.	×	×	×	√
Website protection					
RegEx Protection Engine	Protects against common web attacks, such as SQL injection and XSS.	√	√	√	√
	Enables automatic update of protection rules against web zero-day vulnerabilities.	√	√	√	√
Protection rule group	Allows you to customize protection rule groups.	×	×	√	√
Big Data Deep Learning Engine	Detects web zero-day vulnerabilities.	×	×	×	×
Positive security model	Provides positive defense capabilities based on deep learning of website traffic.	×	×	×	×
Website tamper-proofing	Locks web pages to prevent tampering with content.	×	×	√	√
Data leak prevention	Prevents against the leak of sensitive data, such as ID card numbers, mobile numbers, and bank card numbers.	×	√	√	√

Feature	Description	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
HTTP flood protection	Protects against common HTTP flood attacks in Prevention or Prevention-emergency mode.	√	√	√	√
IP address blacklist	Blocks access requests from specific IP addresses or CIDR blocks.	√	√	√	√
	Supports the above blocking capability and also blocks access requests from IP addresses in specific regions.	×	×	√	√
Scan protection	Blocks the IP addresses where web attacks and path traversal are frequently initiated and the IP addresses of scanning tools, and provides collaborative defense. Default rules are used to block the first type of IP addresses.	√	√	√	√
	Supports the above protection capability and allows you to customize blocking rules for high-frequency web attacks and path traversal.	×	√	√	√
	Implements ACL-based access control by using basic fields, such as IP, URL, Referer, User-Agent, and Params.	√	√	√	√
	Supports the above protection capability and advanced fields, such as Cookie, Content-Type, Header, and Http-Method.	×	√	√	√

Custom protection policy Feature	Description	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
	Allows you to customize rules for HTTP flood protection. You can define a throttling policy, where the request frequency can be measured based on IP addresses or sessions.	×	√	√	√
	Allows you to measure the request frequency based on IP addresses, sessions, or custom fields.	×	×	√	√
Data risk control	Protects crucial website services, such as registrations, logons, activities, and forums, against fraud.	×	×	×	×
Bot management	Provides intelligent protection for bot traffic and against automated attacks. This feature is suitable for human-machine identification, scalping, and spam registration scenarios.	Value-added	Value-added	Value-added	Value-added
Application protection	Provides trusted communications and anti-bot protection for native applications to identify proxies, emulators, and requests with invalid signatures.	Value-added	Value-added	Value-added	Value-added
Account security	Detects credential stuffing, brute-force attacks, spam registration, weak passwords, and SMS interface abuse on service endpoints, such as registration and logon endpoints.	√	√	√	√
API request security	Allows upload of custom API definition files to ensure that only API requests that comply with the definitions are processed.	×	×	√	√

Feature	Description	Pro edition	Business edition	Enterprise edition	Exclusive edition (can be purchased only by submitting a ticket)
Security analysis and support					
Log Service for WAF	Collects and stores all logs, enables near-real-time query and analysis, and provides online reports.	×	Value-added	Value-added	Value-added

4.Benefits

This topic describes what you can get from Alibaba Cloud WAF.

More than 10 years of web security experience

- Built from over a decade's worth of web security experience from Alibaba Group involving successful online businesses in China, such as Taobao, Tmall, and Alipay.
- Professional security team consisting of security experts from around the globe.
- Resists existing OWASP known threats, and updates for the latest vulnerabilities.

HTTP flood mitigation and bot protection

- Effective mitigation of HTTP and HTTPS floods.
- Prevents web crawlers and other bots from consuming website's resources.
- Detects and blocks suspicious requests that may cause negative impacts on your server, such as bandwidth consumption, database/SMS/API interface exhaustion, increased latency, or even a breakdown.
- Customizable rules for varying business scenarios.

Big data ability

- Alibaba Cloud hosts more than 37% of China-based websites.
- Alibaba Cloud mitigates more than 800 million attacks every day.
- Alibaba Cloud maintains the most popular accessed IP database in China.
- Numerous case studies on the patterns, methods, and signatures of the popular web attacks.
- Analysis through the Alibaba Cloud big data platform in combination with the latest technologies.

Easy and reliable

- Setup and activation within 5 minutes.
- No hardware or software installation, or router and switch configuration.
- Works as a defense cluster to avoid single point failure and redundancy.
- Excellent processing ability.

5.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.

6.Terms

This topic introduces the common terms related to WAF.

back-to-origin IP address

A back-to-origin IP address is an IP address that WAF uses to establish network connections with an origin server.

WAF uses specified back-to-origin CIDR blocks to forward service traffic back to the origin server. After you activate WAF to protect your website, we recommend that you configure the WAF back-to-origin CIDR blocks on the origin server to prevent service traffic from being blocked. For more information, see Allow access from WAF back-to-origin CIDR blocks.

origin server

An origin server is a backend server that provides services.

web application

A web application is an application that users can access through a web browser.

Layer 4 proxy

A Layer 4 proxy is a proxy server that analyzes only destination address and port information in a request. The Layer 4 proxy forwards the request to an origin server based on specified rules.

Layer 7 proxy

A Layer 7 proxy is a proxy server that analyzes the application content and specific fields in a request. The Layer 7 proxy forwards the request to the origin server based on specified rules.