Alibaba Cloud
Web应用防火墙

User Guide (Old Engines)

Issue: 20200702

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 individual s 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 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 contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
⛔	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.
⚠	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.
ⓘ	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.
📋	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]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

1 Protection engine is upgraded

From March 11, 2020, Web Application Firewall upgrades the protection engine for all users, to provide you with more comprehensive protection and more convenient operation experience.

When you upgrade to the new protection engine, you will experience the following upgrades:

- Improved protection experience

  The protection module is aggregated to provide comprehensive protection for your business, including web intrusion prevention, data security, Bot management, and access control and throttling.

  The new protection engine also provides powerful precision traffic limiting and account security capabilities to help you defend against illegal access attacks, HTTP flood attacks , credential stuffing, weak password attacks, and brute-force attacks. After the upgrade, trend analysis reports show you the protection effects in a more intuitive and secure way .
- Custom protection policies meet the needs of refined throttling

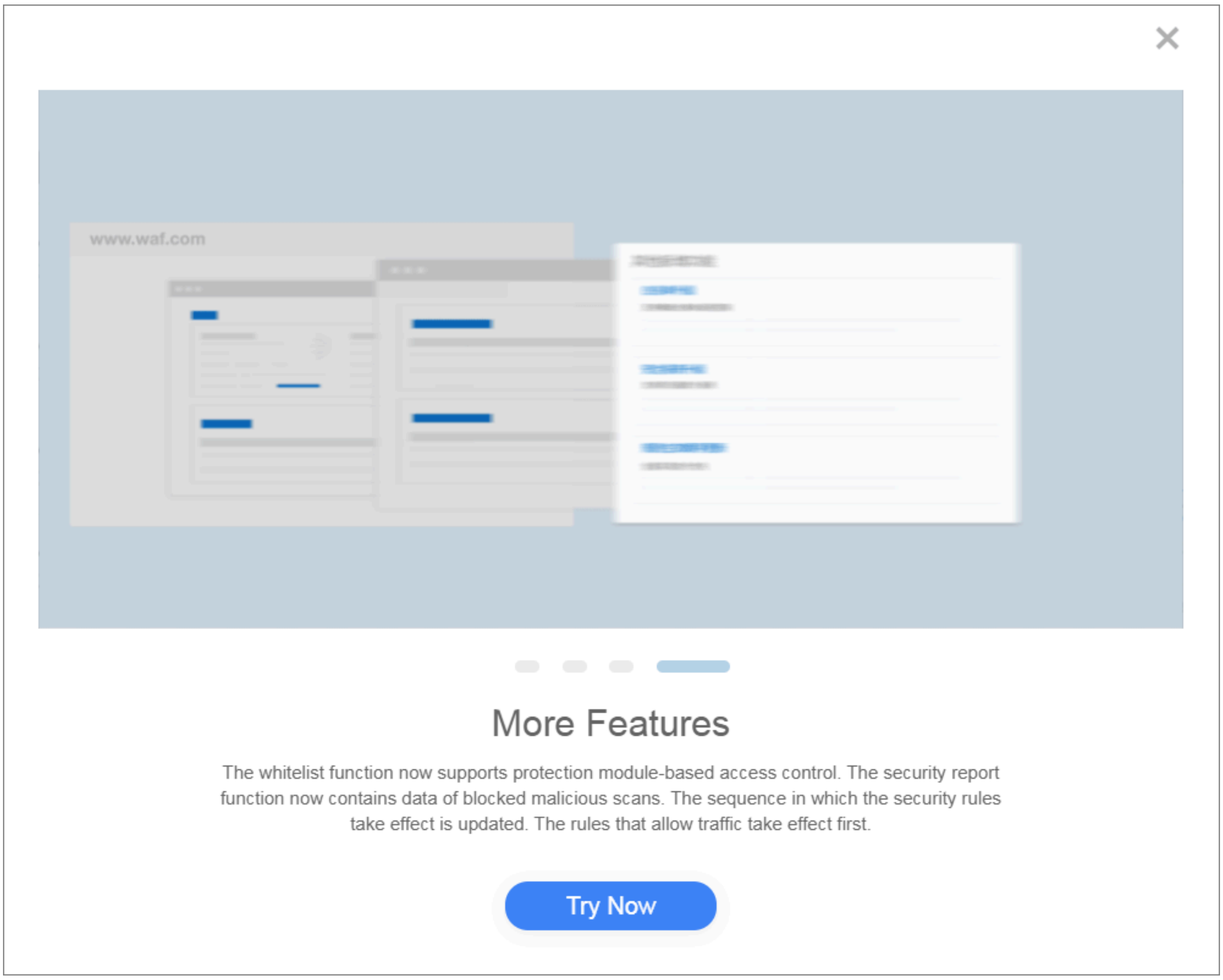
  The custom policy protection feature supports more fields and processes for precise access control, and provides you with the accurate access control under complex conditions. It can meet the management requirements for illegal access requests in various business scenarios.

  - Original Custom HTTP flood protection rules are integrated into custom protection policies to provide more precise throttling capabilities.
  - In the original HTTP ACL policy, the whitelist rule configuration for specific traffic is changed to that for each protection module, providing a more convenient way to configure legitimate traffic.
- Configure an IP address blacklist

  You can easily add IP addresses, IP address segments, and region blacklists to implement quick access control and quickly intercept specific traffic.

How to upgrade

We will arrange protection engine upgrades for all customers who have enabled Web Application Firewall before January 2020. After the backend protection engine has been upgraded, you will receive an upgrade notification when logging on to the Web Application Firewall console. Click **Try now** you can enjoy the upgraded experience of the new protection engine.



More Features

The whitelist function now supports protection module-based access control. The security report function now contains data of blocked malicious scans. The sequence in which the security rules take effect is updated. The rules that allow traffic take effect first.

2 Website protection (old engines)

2.1 Web application protection

Web application protection provides different levels of protection policies, including loose, normal, and strict, to prevent common Web application attacks such as SQL injection and XSS attacks.

Context

After you add your domain to the WAF protection list, you can enable Web applicatio n protection for this domain, and select a protection policy. This feature takes effect immediately after you enable it. You can disable it at any time.

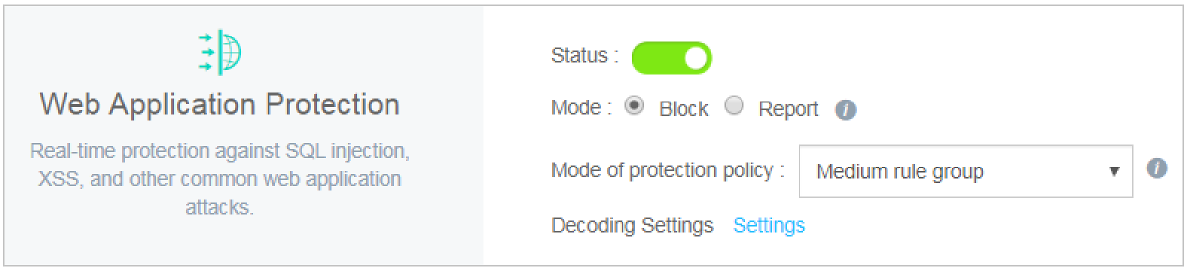
Before you perform the following operations, make sure that you have added the domain to WAF for protection. For more information, see Use WAF CNAME to add domains for protection.

Procedure

1. Log on to the WAF console.
2. In the left-side navigation pane, choose **Management** > **Website Configuration**. On the Website Configuration page, select the region of your WAF instance. The options include Mainland China and International.
3. In the domain list, find the domain to be configured, and click **Policies** in the Operation column.
4. Enable **Web Application Protection**, and select a mode.

Note:

You can disable this feature on this page.



Web Application Protection

Real-time protection against SQL injection, XSS, and other common web application attacks.

Status : on

Mode : ● Block ○ Report

Mode of protection policy : Medium rule group

Decoding Settings Settings

- **Prevention mode**: detects and blocks attacks.
- **Detection mode**: detects attacks and generates alerts.

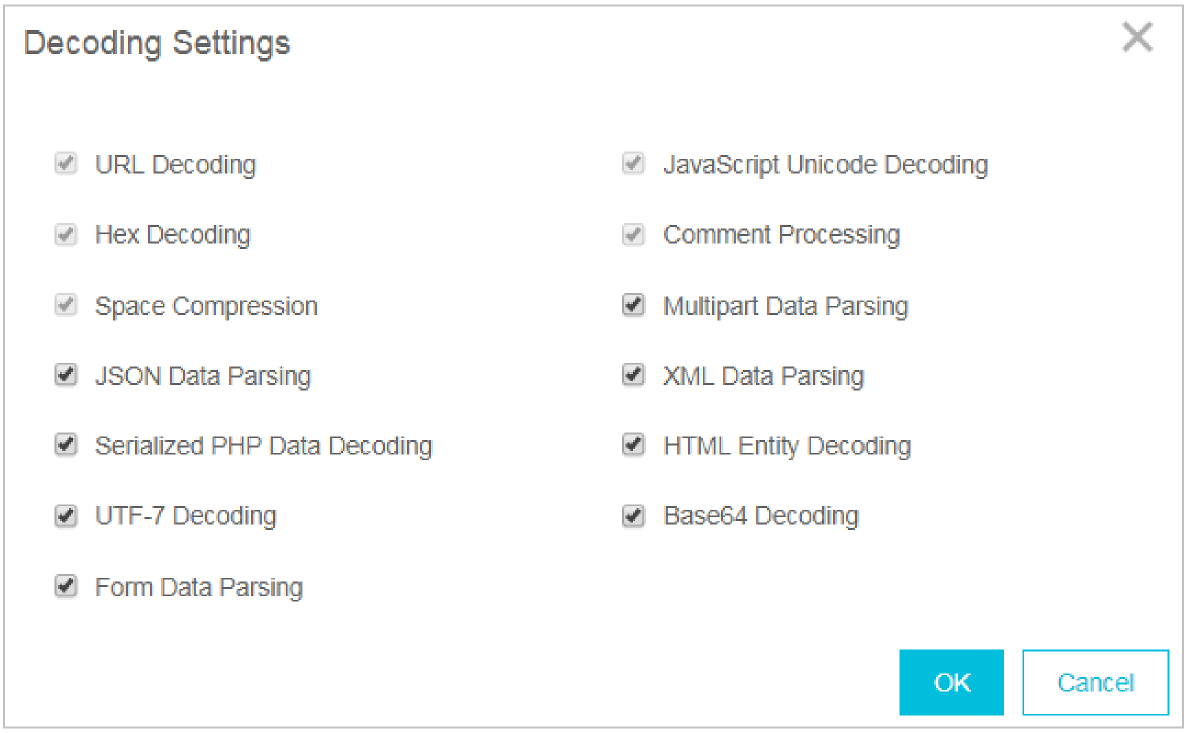
5. In the **Policy** drop-down list, select a protection policy.

    - By default, the **Normal** policy is selected.
    - In the normal policy mode, if many normal requests are blocked or many uncontrollable user inputs are detected, such as rich text editors and technology forums, we recommend that you use the **Loose** policy.
    - If you require stricter protection against path traversal, SQL injections, and command execution attacks, we recommend that you use the **Strict** policy.

6. Click **Settings** on the right of Decoding Settings. In the **Decoding Settings** dialog box, select the data formats to be decoded and analyzed by the Web application protection feature. If this feature often blocks normal requests with data of a specific format, open the **Decoding Settings** dialog box, clear the check box of this format, and click **OK**.

Note:

To ensure high performance, the feature decodes and analyzes the request data of all formats by default. You cannot clear URL decoding, JavaScript Unicode decoding, hex decoding, comment processing, or space compression.



Decoding Settings

☑ URL Decoding
☑ JavaScript Unicode Decoding
☑ Hex Decoding
☑ Comment Processing
☑ Space Compression
☑ Multipart Data Parsing
☑ JSON Data Parsing
☑ XML Data Parsing
☑ Serialized PHP Data Decoding
☑ HTML Entity Decoding
☑ UTF-7 Decoding
☑ Base64 Decoding
☑ Form Data Parsing

2.2 Big data deep learning engine

Through supervised learning, the big data deep learning engine of web application firewall relies on the neural network system built by Alibaba Cloud powerful algorithm team, Alibaba Cloud conducts classification training for hundreds of millions of attack data each day, and finally detects and intercepts unknown risk requests online in real time through the model. This makes up for other defense engines to detect unknown 0day vulnerabilities.

Prerequisites

Make sure that you have added the target domain in WAF for protection. For more information, see Implement Alibaba Cloud WAF.

Context

With the development of the Internet, web attack methods are constantly evolving. Traditional single-means protection methods cannot meet the security needs of complex Internet services. Only collaborative protection by multiple detection engines can achieve the best protection effect.

Based on continuous learning and modeling of normal business models, the big data deep learning engine identifies and warns of abnormal and risky behaviors in real time, providing users with the fastest and most comprehensive protection capabilities.

> **Note:**
> The big data deep learning engine mainly targets web attack requests without obvious features, rather than HTTP flood attacks. If you have high web attack protection requirements, we recommend that you enable the big data deep learning engine.

The main features of the big data deep learning engine are as follows:

- Semantics: New intelligent protection engine merges the similar behavior characteristics of similar attacks and aggregates the attack behaviors and characteristics of a single attack class into an attack feature. By grouping the multiple behavioral characteristics of attacks into specific permutations and combinations to represent individual attack classes, this function creates a semantic structure for attack behavior.
- Exception and attack set: Leveraging Alibaba Cloud Security's massive volume of operations data, this function models normal web applications, so that abnormalities can be detected. It extracts exception and attack models from a large volume of web application attacks to form an exception and attack set.

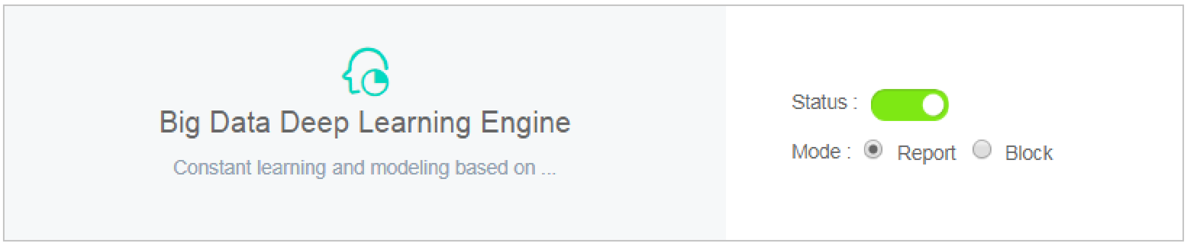
Procedure

1. Log on to the Web Application Firewall console.
2. Go to the **Management** > **Website Configuration** page and select the region of your WAF instance (**Mainland China** or **International**).
3. Locate to the domain name to be configured and click **Policies**.
4. In the **Big Data Deep Learning Engine** area, turn on the feature and select the protection mode.

   - **Report**: Only alert you of the detected attack.
   - **Block**: Block the detected attack directly.

   > **Note:**

If you do not require the big data deep learning engine feature, you can turn off it on this page.



Big Data Deep Learning Engine

Constant learning and modeling based on ...

Status : ON

Mode : ● Report ○ Block

2.3 HTTP flood protection

HTTP Flood protection helps you block HTTP flood attacks against your website.

Function description

HTTP Flood protection helps you block HTTP flood attacks in different modes, including Normal and Emergency. After adding your website to the WAF protection list, you can enable HTTP Flood protection and select an appropriate protection mode for the website . Upon identifying an HTTP flood attack, WAF disconnects from the client to protect your origin.

The Business and Enterprise editions support advanced HTTP flood protection. For more information, see FAQ.

Note:
The Emergency mode is applicable to web pages, but not to API/Native Apps, because it may result in a large number of false positives. For API/Native Apps, you can use Custom HTTP Flood Protection.

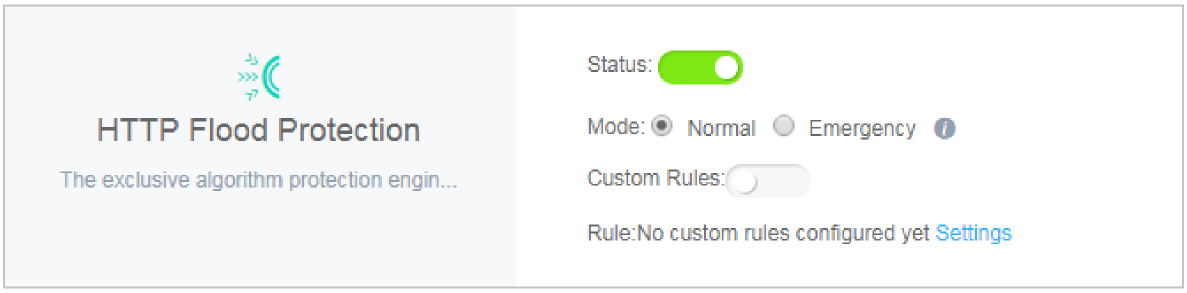
Procedure

Follow these steps to configure HTTP flood protection mode:

Note:
Make sure that you have added your domain to the WAF protection list before proceeding with the following operations. For more information, see WAF deployment guide.

1. Log on to the Alibaba Cloud WAF console.
2. Go to the **Management** > **Website Configuration** page, and select the region of your WAF instance (Mainland China or International).
3. Select the domain to be configured and click **Policies**.

4. Enable **HTTP Flood Protection** and select the protection mode:



HTTP Flood Protection

The exclusive algorithm protection engin...

Status: ●

Mode: ● Normal ○ Emergency

Custom Rules: ○

Rule:No custom rules configured yet Settings

- **Normal**: Used by default. In Normal mode, WAF only blocks extremely suspicious requests, and the amount of false positives is relatively small. We recommend that you use this mode when there is no apparent traffic exception to your website to avoid false positives.
- **Emergency**: When you find many HTTP flood attacks are not blocked in the Normal mode, you can switch to the Emergency mode. In Emergency mode, WAF imposes strict inspection rules against HTTP flood attacks, but it may cause false positives.

Note:

- If many attacks are still missed out in the Emergency mode, check if the source IP addresses are WAF's back-to-Source IP addresses. If the origin is directly attacked, see Protect your origin server to only allow WAF's back-to-Source IP addresses to access the server.
- For better protection effects and lower false positive rate, you can use the Business Edition or Enterprise Edition to customize or request security experts to customize targeted protection algorithms for your website.

FAQ

What is the difference between HTTP flood protection capability for different WAF editions?

WAF is categorized based on the capacity to provide protection against the complex HTTP flood attacks.

- **Pro Edition**: supports default protection modes (Normal and Emergency), and blocks HTTP flood attacks with obvious attack characteristics.
- **Business Edition**: supports custom access control rules, and defends against HTTP flood attacks with certain attack characteristics. For more information, see Custom HTTP flood protection.

- **Enterprise Edition**: offers protection rules customized by security experts to guarantee solid protection effects.

For more information on how to upgrade WAF, see Renewal and upgrade.

Why must I upgrade WAF to the Business Edition to defend against certain HTTP flood attacks?

Alibaba Cloud WAF identifies attacks by using human identification, big data analysis, model analysis, and other techniques, and blocks attacks accordingly. Different from program interaction, security attack and defense is the confrontation between people. Each website has its own performance bottleneck. If hackers find a type of attack to be ineffectiv e, they may analyze the website and then start a targeted attack. In this case, Alibaba Cloud Security experts can analyze the attack to provide a higher level protection and a better protect effect.

2.4 Custom HTTP flood protection

The Business and Enterprise editions of Alibaba Cloud WAF support customizing HTTP flood protection rules to apply rate-based access control.

Context

The frequency of certain URLs can be restricted from accessing your server by applying custom protection rules in the console. For example, you can define the following rule: when a single source IP address accesses www.yourdomain.com/login.html for more than 20 times within 10 seconds, then block this IP address for one hour.

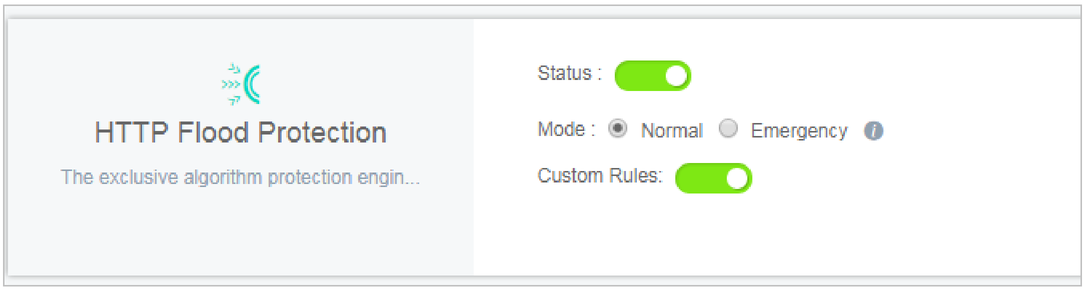
You must upgrade WAF to the Business or Enterprise edition to use this function. For more information, see Renewal and upgrade.

Make sure that you have added your domain to the WAF protection list before proceeding with the following operations. For more information, see WAF deployment guide.

Procedure

1. Log on to the Alibaba Cloud WAF console.
2. Go to the **Management** > **Website Configuration** page, and select the region of your WAF instance (Mainland China or International).
3. Select the domain to be configured, and click **Policies**.

4. Enable **HTTP Flood Protection** (**Normal** mode) and Custom Rules, and click **Settings**.



HTTP Flood Protection

The exclusive algorithm protection engin...

Status :

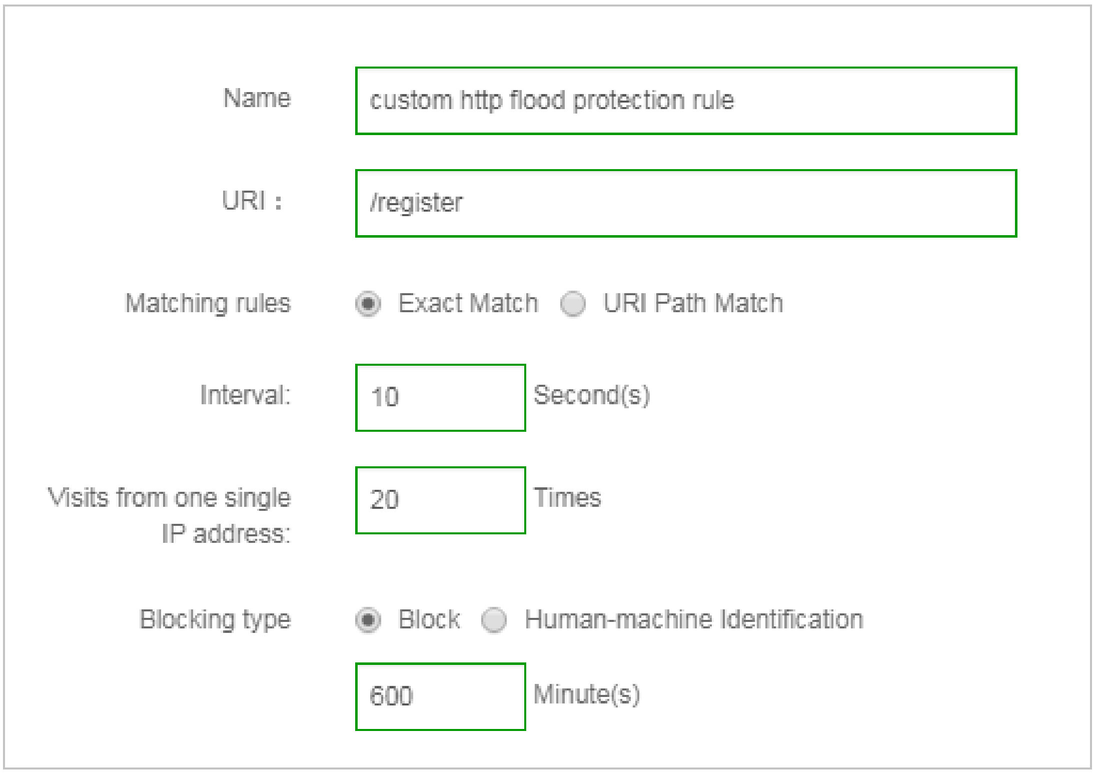
Mode : ● Normal ○ Emergency

Custom Rules:

5. Click **New Rule** to add a rule. The parameters include:

Configuration	Description
Name	The name of this rule.
URI	The URI path to be protected. For example, /register. The path can contain parameters connected by "?" . For example, you can use /user? action=login.
Matching rule	• **Exact Match**: The request URI must be exactly the same as the configured URI here to get counted. • **URI Path Match**: When the request URI starts with the URI value configured here, the request is counted. For example, /register.html is counted if you use /register as the URI.
Interval	The cycle for calculating the number of visits. It works in sync with **Visits from one single IP address**.
Visits from a single IP address	The number of visits allowed from a single source IP address to the URL during the **Interval**.

Configuration	Description
Blocking type	The action to be performed after the condition is met. The operations can be Block or Human-Machine Identification. • **Block**: blocks accesses from the client after the condition is met. • **Man-Machine Identification**: accesses the client with redirection after the condition is met. Only the verified requests are forwarded to the origin.



Name: custom http flood protection rule

URI : /register

Matching rules: ● Exact Match ○ URI Path Match

Interval: 10 Second(s)

Visits from one single IP address: 20 Times

Blocking type: ● Block ○ Human-machine Identification

600 Minute(s)

Consider the configurations in the preceding figure: a single IP address can access the target address (Exact Match) more than 20 times in 10 seconds, after which the IP is blocked for 600 minutes.

Since WAF collects data from multiple servers in the cluster to calculate the frequency of access from a single IP, a certain delay may exist in the statistical process.

Result

Once the rule is added successfully, you can **Edit** or **Delete** the rule.

2.5 HTTP ACL policy

With HTTP ACL policy, you can customize access control rules to filter HTTP requests by client IP, request URL, and commonly used HTTP fields.

Function description

HTTP ACL Policy supports customizing HTTP access control to filter HTTP requests based on a combination of criteria of commonly used HTTP fields, such as IP, URL, Referer, UA, and parameters. This feature applies to different business scenarios, such as anti-leech protection and website admin console protection.

HTTP ACL policy rule

Each HTTP ACL policy rule consists of a **Matching condition** and **Action**. When creating a rule, you define the matching condition by configuring matching fields, logical operators, and the corresponding match content, and select the action to be triggered in a match case.

Matching condition

A match condition is composed of matching fields, logical operators, and matching content . The matching content does not support regular expression descriptions, but is allowed to be set to null.

The following table lists all matching fields supported by HTTP ACL policy rules.

Note:
For WAF Pro instances, only IP, URL, Referer, User-Agent, and Params are supported in matching fields, and a maximum of 20 rules are allowed for each domain name. For WAF Business or Enterprise instances, all the listed matching fields are supported, and you can define up to 100 or 200 rules for each domain name respectively.

Matching field	Description	Supported logical operators
IP	The client IP address. **Note:** You can add up to 50 IPs or IP segments, separated by commas (,).	• Has • Does not have

URL	The requested URL.	• Includes • Does not include • Equals to • Does not equal to
Referer	The address of the previous web page with a link to the current request page.	• Includes • Does not include • Equals to • Does not equal to • Length less than • Length equals • Length more than • Does not exist
User-Agent	The user agent string that identifies information about the client's browser.	• Includes • Does not include • Equals to • Does not equal to • Length less than • Length equals • Length more than
Params	The parameters in the request URL, which start after "?". For example, the parameter of the URL www.abc.com/index.html?action=login is action=login.	• Includes • Does not include • Equals to • Does not equal to • Length less than • Length equals • Length more than
Cookie	The cookie in the request URL.	• Includes • Does not include • Equals to • Does not equal to • Length less than • Length equals • Length more than • Does not exist

Content-Type	The Media type of the body of the request (used with POST and PUT requests).	• Includes • Does not include • Equals to • Does not equal to • Length less than • Length equals • Length more than
X-Forwarded-For	The x-forward-for field in the request URL . X-Forwarded-For (XFF) identifies the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer.	• Includes • Does not include • Equals to • Does not equal to • Length less than • Length equals • Length more than • Does not exist
Content-Length	The length of the request body in octets (8-bit bytes).	• Value less than • Value equals • Value more than
Post-Body	The response content of the request.	• Includes • Does not include • Equals to • Does not equal to
Http-Method	The request method, such as GET, POST.	• Equals to • Does not equal to
Header	The customized header field.	• Includes • Does not include • Equals to • Does not equal to • Length less than • Length equals • Length more than • Does not exist

Note:

Each rule allows a combination of three conditions at most. Multiple conditions in a rule are connected by “AND”, that is, a request must satisfy all the conditions to match the rule.

Action

The following actions can be performed after a rule is matched:

- **Block**: blocks the request that matches the condition.
- **Allow**: allows the request that matches the condition.
- **Warn**: allows the request that matches the condition and triggers an alarm.

Note:

After specifying **Allow** or **Warn**, you can further decide whether to proceed to perform Web application protection, HTTP flood protection, new intelligent protection, regional blocking, and data risk control.

Sort rules

Matching rules follow a specific order. The rule with the higher ranking is matched first.

You can adjust the order of the rules to achieve the optimal protection performance.

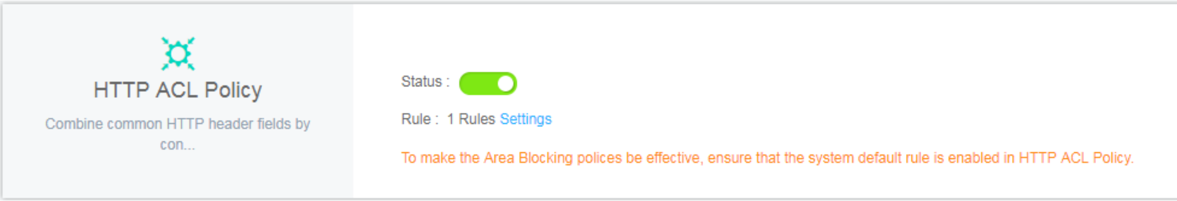
Procedure

Follow these steps to add a HTTP ACL policy rule for the protected domain name:

Note:

Before you perform the following operations, make sure that you have added the domain to WAF for protection. For more information, see WAF deployment guide.

1. Log on to the Alibaba Cloud WAF console.
2. Go to the **Management** > **Website Configuration** page, and select the region of your WAF instance (Mainland China or International).
3. Select the domain to be configured, and click **Policies**.
4. Enable **HTTP ACL Policy**, and click **Settings**.



HTTP ACL Policy

Combine common HTTP header fields by con...

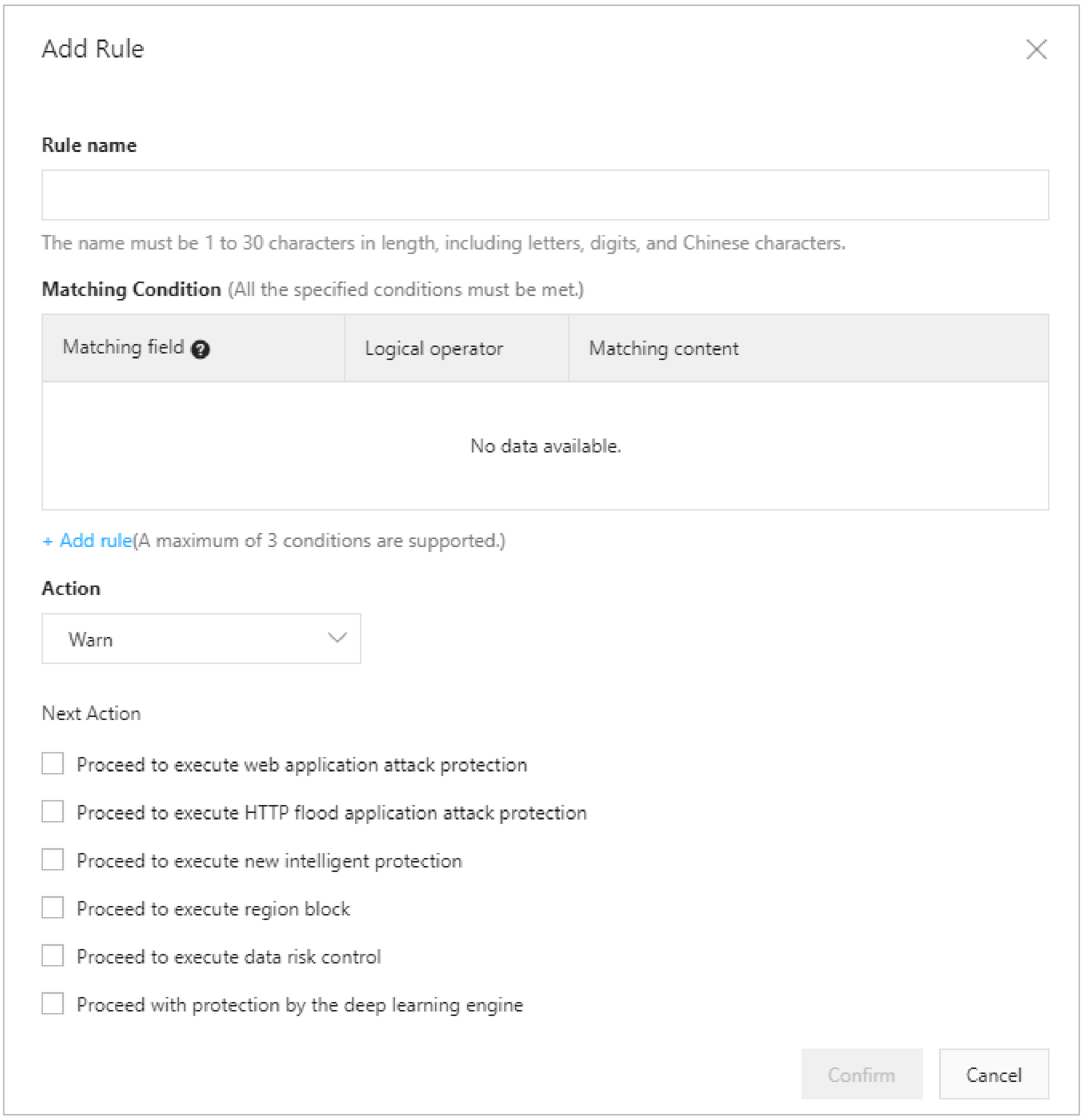
Status :

Rule : 1 Rules Settings

To make the Area Blocking polices be effective, ensure that the system default rule is enabled in HTTP ACL Policy.

5. Click **Add Rule**, configure the expected rule, and click **OK**.

> **Note:**
>
> For more information about the configuration, see HTTP ACL policy rule. For more information about configuration examples, see Configuration examples.



Add Rule

Rule name

The name must be 1 to 30 characters in length, including letters, digits, and Chinese characters.

Matching Condition (All the specified conditions must be met.)

Matching field	Logical operator	Matching content
No data available.		

+ Add rule(A maximum of 3 conditions are supported.)

Action

Warn

Next Action

□ Proceed to execute web application attack protection

□ Proceed to execute HTTP flood application attack protection

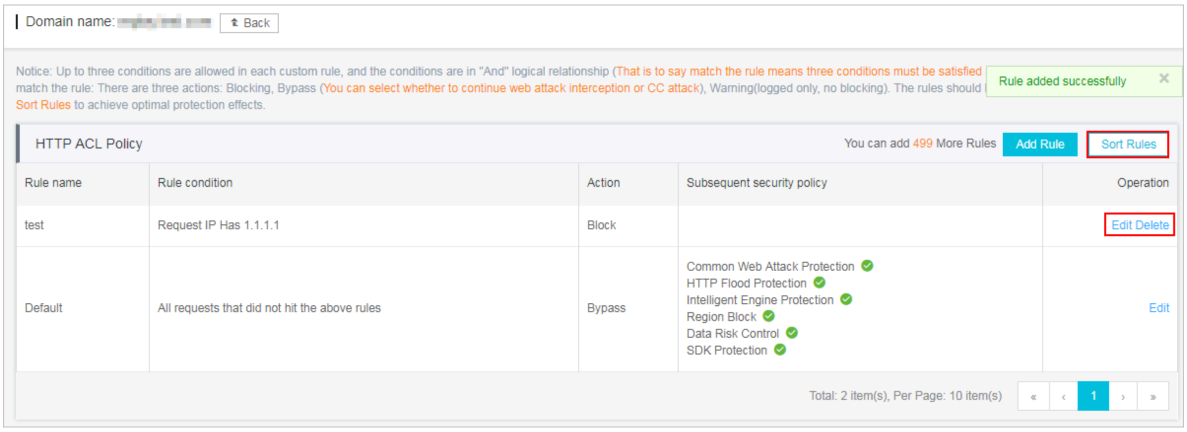
□ Proceed to execute new intelligent protection

□ Proceed to execute region block

□ Proceed to execute data risk control

□ Proceed with protection by the deep learning engine

6. For a created rule, you can either **Edit** its content or **Delete** it. If multiple rules are created, you can click **Sort Rules** to change the default order of them. By using **Move up**, **Move down**, **Move to top**, and **Move to bottom**, you decide which rule is matched first.



Domain name: [redacted] Back

Notice: Up to three conditions are allowed in each custom rule, and the conditions are in "And" logical relationship (That is to say match the rule means three conditions must be satisfied match the rule: There are three actions: Blocking, Bypass (You can select whether to continue web attack interception or CC attack), Warning(logged only, no blocking). The rules should Sort Rules to achieve optimal protection effects.

Rule added successfully

HTTP ACL Policy

You can add 499 More Rules

Rule name	Rule condition	Action	Subsequent security policy	Operation
test	Request IP Has 1.1.1.1	Block		Edit Delete
Default	All requests that did not hit the above rules	Bypass	Common Web Attack Protection ✓ HTTP Flood Protection ✓ Intelligent Engine Protection ✓ Region Block ✓ Data Risk Control ✓ SDK Protection ✓	Edit

Total: 2 item(s), Per Page: 10 item(s)

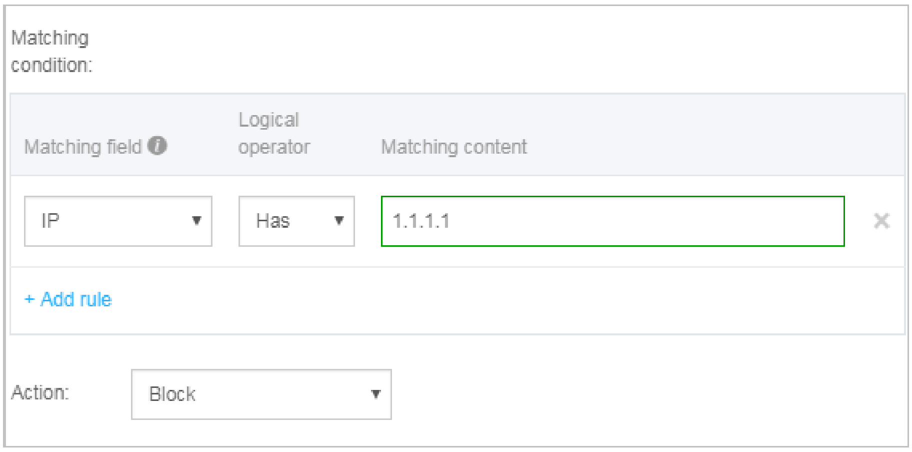
Configuration examples

HTTP ACL Policy supports various configuration methods. You can work out the best rules based on your business characteristics. You can also use HTTP ACL policy to fix certain Web vulnerabilities.

Some examples are as follows.

Configure IP blacklist and whitelist

Use the following configuration to block all access from 1.1.1.1.

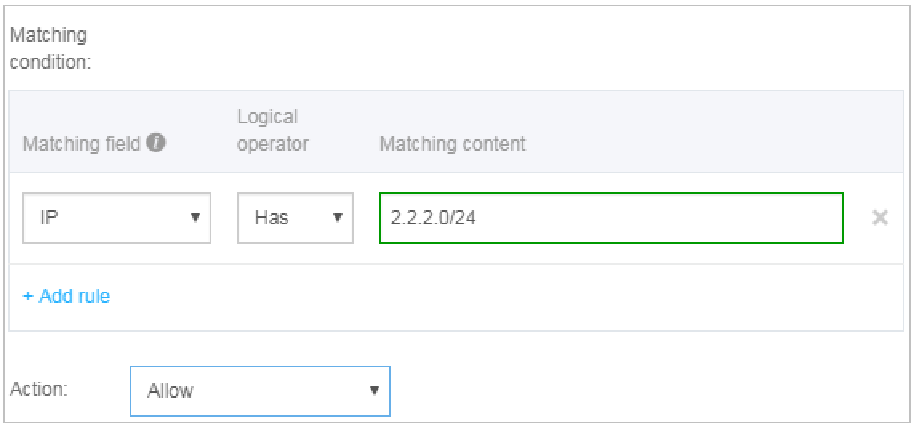


Matching condition:

Matching field	Logical operator	Matching content
IP	Has	1.1.1.1

Action: Block

Use the following configuration to allow all access from 2.2.2.0/24.



Matching condition:

Matching field	Logical operator	Matching content
IP	Has	2.2.2.0/24

Action: Allow

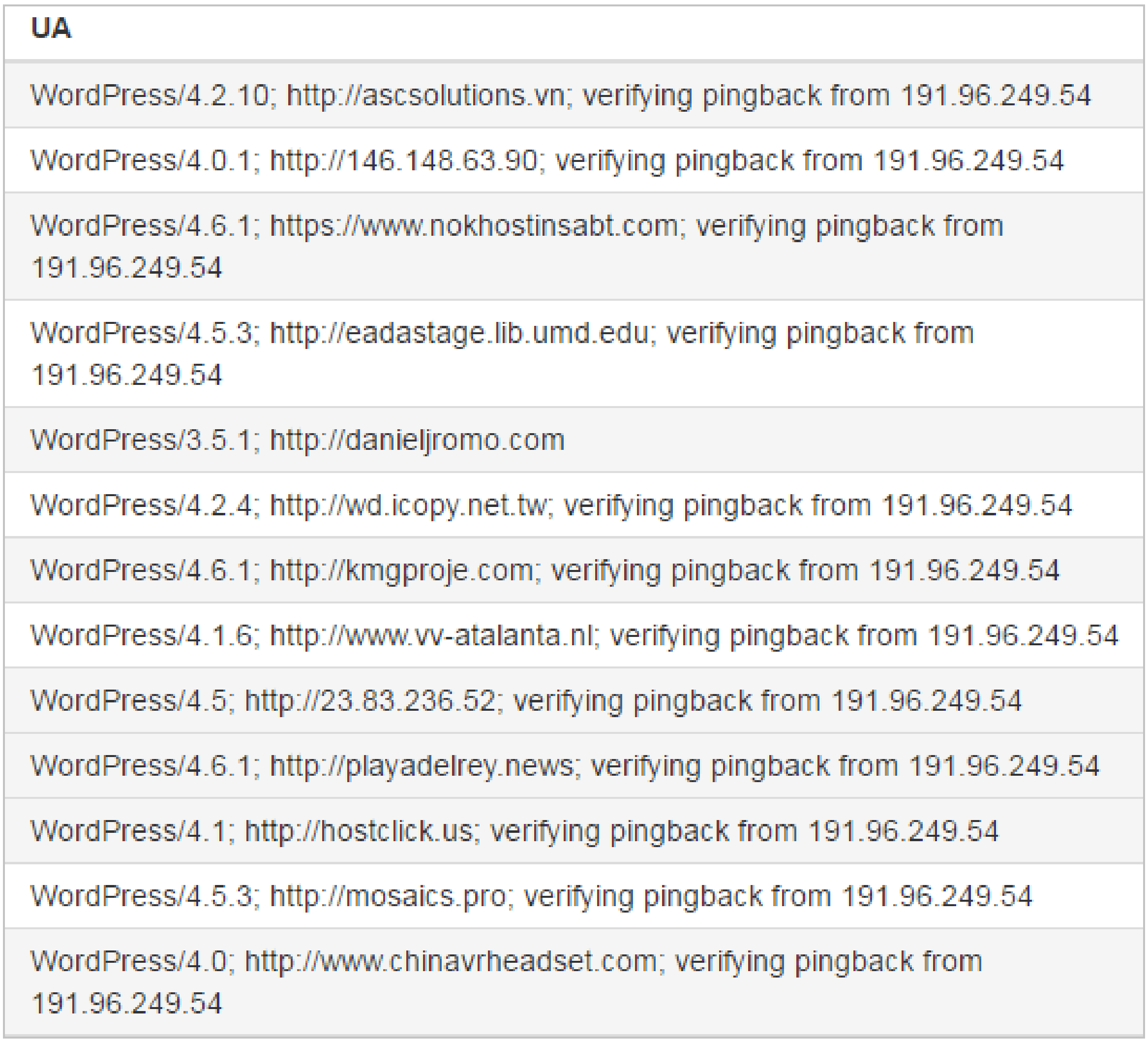
Note:

Do not check **Proceed to execute web application attack protection** or **Proceed to execute HTTP flood attack protection**.

For more information, see Set up IP whitelist and blcaklist.

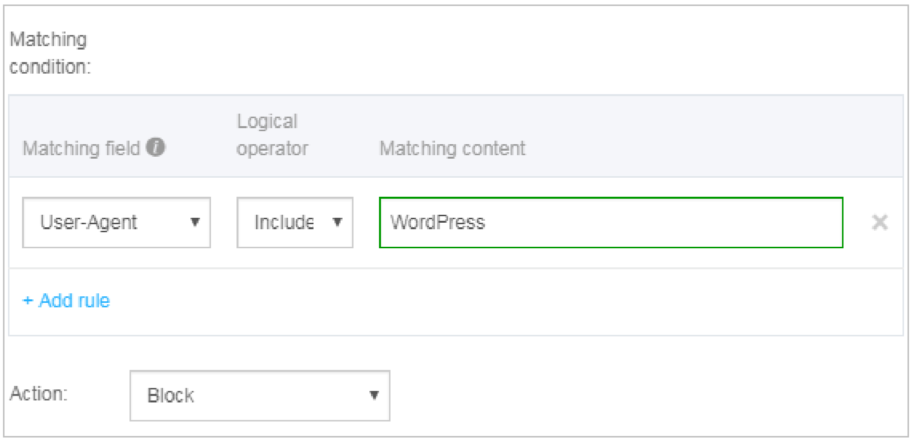
Block malicious requests

The following figure shows an example of WordPress bounce attack, featuring that the UA contains WordPress.



UA
WordPress/4.2.10; http://ascsolutions.vn; verifying pingback from 191.96.249.54
WordPress/4.0.1; http://146.148.63.90; verifying pingback from 191.96.249.54
WordPress/4.6.1; https://www.nokhostinsabt.com; verifying pingback from 191.96.249.54
WordPress/4.5.3; http://eadastage.lib.umd.edu; verifying pingback from 191.96.249.54
WordPress/3.5.1; http://danieljromo.com
WordPress/4.2.4; http://wd.icopy.net.tw; verifying pingback from 191.96.249.54
WordPress/4.6.1; http://kmgproje.com; verifying pingback from 191.96.249.54
WordPress/4.1.6; http://www.vv-atalanta.nl; verifying pingback from 191.96.249.54
WordPress/4.5; http://23.83.236.52; verifying pingback from 191.96.249.54
WordPress/4.6.1; http://playadelrey.news; verifying pingback from 191.96.249.54
WordPress/4.1; http://hostclick.us; verifying pingback from 191.96.249.54
WordPress/4.5.3; http://mosaics.pro; verifying pingback from 191.96.249.54
WordPress/4.0; http://www.chinavrheadset.com; verifying pingback from 191.96.249.54

Use the following configuration to defend against this type of attack.



Matching condition:

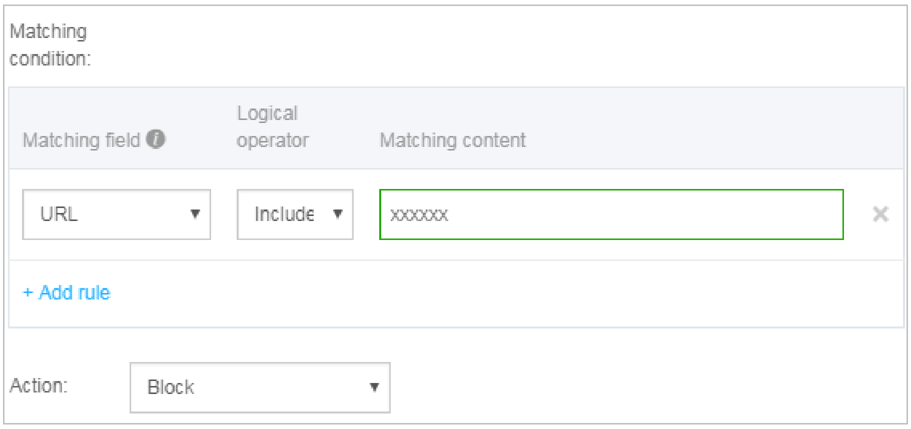
Matching field	Logical operator	Matching content
User-Agent	Include	WordPress

Action: Block

For more information, see Prevent Wordpress pingback attacks.

Block specific URLs

If a large number of IP addresses are requiring a specific but nonexistent URL, you can use the following configuration.



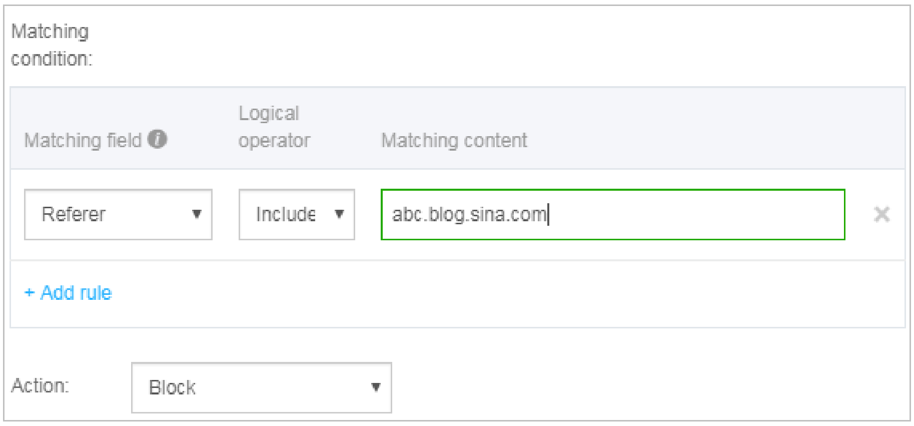
Matching condition:

Matching field	Logical operator	Matching content
URL	Include	xxxxxx

Action: Block

Anti-Leech

You can configure a Referer-based access condition. For example, if you find abc.blog .sina.com is using a large quantity of pictures on your site, you can use the following configuration.



Matching condition:

Matching field	Logical operator	Matching content
Referer	Include	abc.blog.sina.com

Action: Block

2.6 Blocked regions

Use this feature to add specific areas of Mainland China, Hong Kong, Macao and Taiwan, and up to 247 countries in the world to the region blacklist. All requests from the specified areas are blocked.

Context

To enable the Blocked Regions feature, you must upgrade WAF to Business Edition or above. For more information about the upgrade, see Renewal and upgrade.

Note:

WAF instances created in International regions must be upgraded to the Enterprise edition.

To enable and specify blocked regions, follow these steps:

Note:

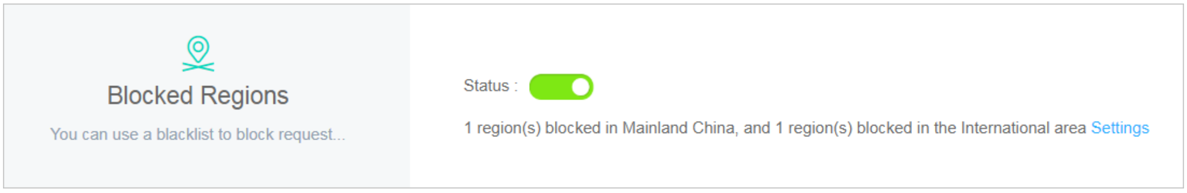
Ensure that you have added the target domain in WAF for protection. For more information, see CNAME access guide.

Procedure

1. Log on to the Web Application Firewall console.
2. Go to the **Management** > **Website Configuration** page, and select the region of your WAF instance (Mainland China or International).
3. Select the domain to be configured, and click **Policies**.
4. Enable the **Blocked Regions** option.

   Note:

   To make the Area Blocking polices be effective, ensure that the system default rule is enabled in HTTP ACL Policy.

   Blocked Regions

   You can use a blacklist to block request...

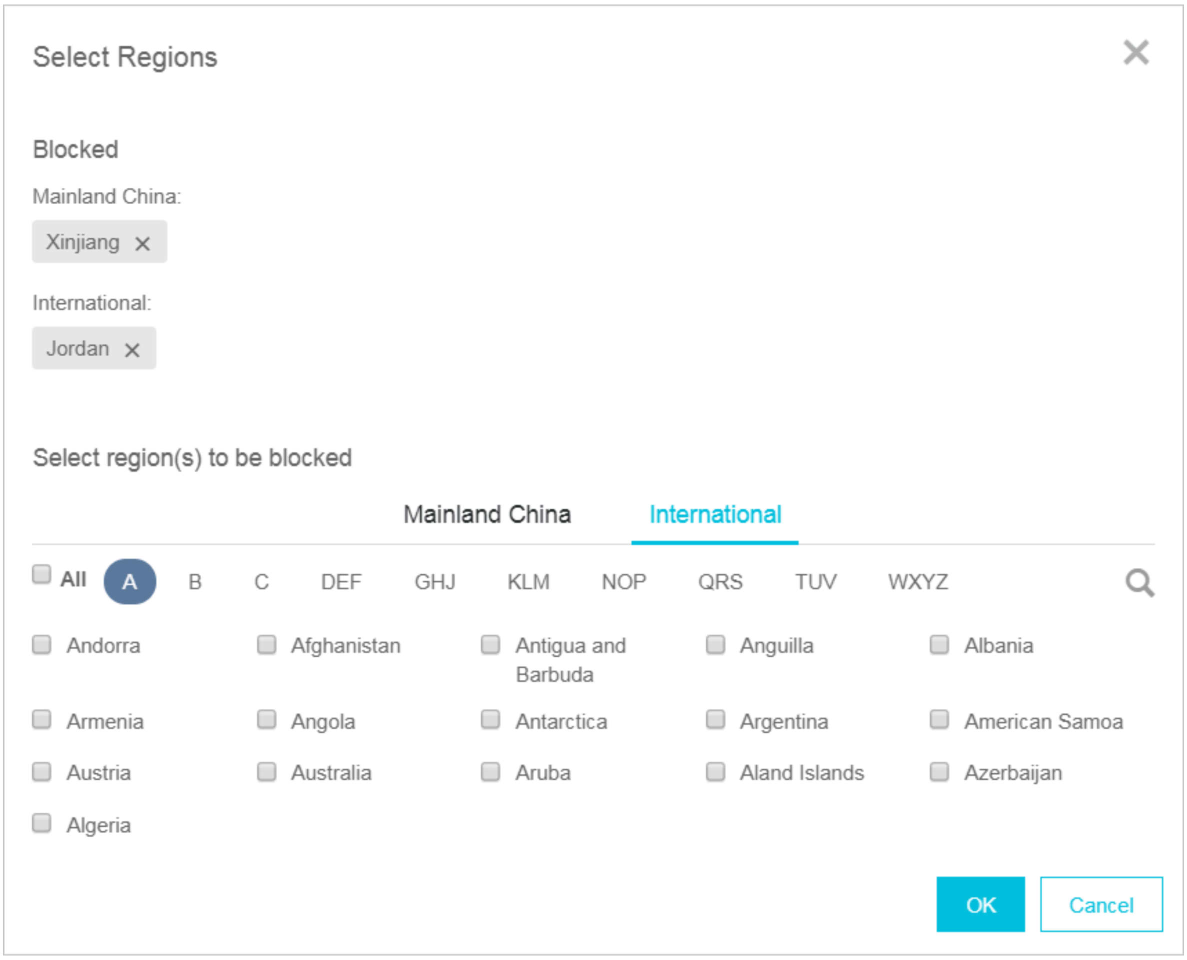
   Status :

   1 region(s) blocked in Mainland China, and 1 region(s) blocked in the International area Settings

5. Click **Settings**, select the **Mainland China** or **International** scope, and select the areas that you want to block. Then, click **OK**.

   Note:

When you select the **International** scope, you can quickly find the country or area through the initial letter of the country name or the quick search.



Select Regions

Blocked

Mainland China:

Xinjiang ×

International:

Jordan ×

Select region(s) to be blocked

□ Andorra
□ Armenia
□ Austria
□ Algeria
□ Afghanistan
□ Angola
□ Australia
□ Antigua and Barbuda
□ Antarctica
□ Aruba
□ Anguilla
□ Argentina
□ Aland Islands
□ Albania
□ American Samoa
□ Azerbaijan

Result

After you confirm the settings, all requests from the IP addresses in the blocked areas are blocked by WAF.

Note:

The source area information of the IP is based on the Alibaba Taobao IP address Library.

2.7 Configure a whitelist or blacklist

You can set a whitelist or blacklist by configuring HTTP ACL policies in WAF. The whitelist and blacklist are only effective on the specific domain that has the HTTP ACL policy configured.

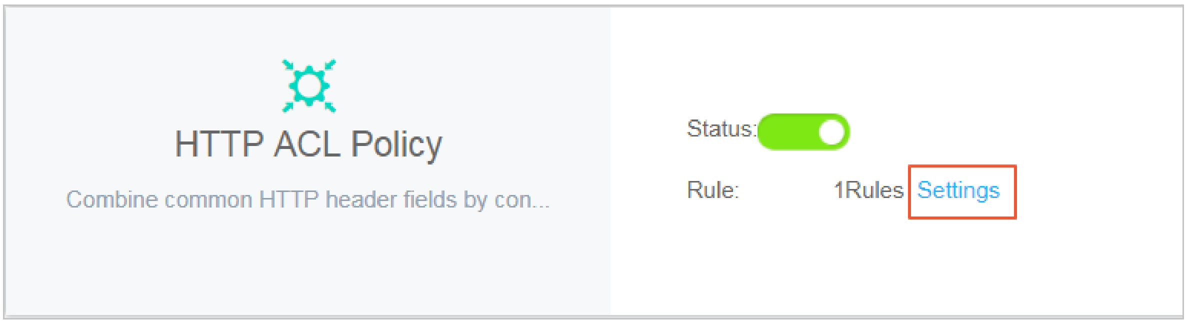
Procedure

Follow these steps to configure a whitelist or blacklist:

Note:

Make sure that you have added your domain to the WAF protection list before proceeding with the following operations. For more information, see WAF deployment guide.

1. Log on to the Alibaba Cloud WAF console.
2. Go to the **Management** > **Website Configuration** page, and select the region of your WAF instance (Mainland China or International).
3. Select the domain to be configured, and click **Policies**.
4. Enable **HTTP ACL Policy**, and click **Settings**.



HTTP ACL Policy

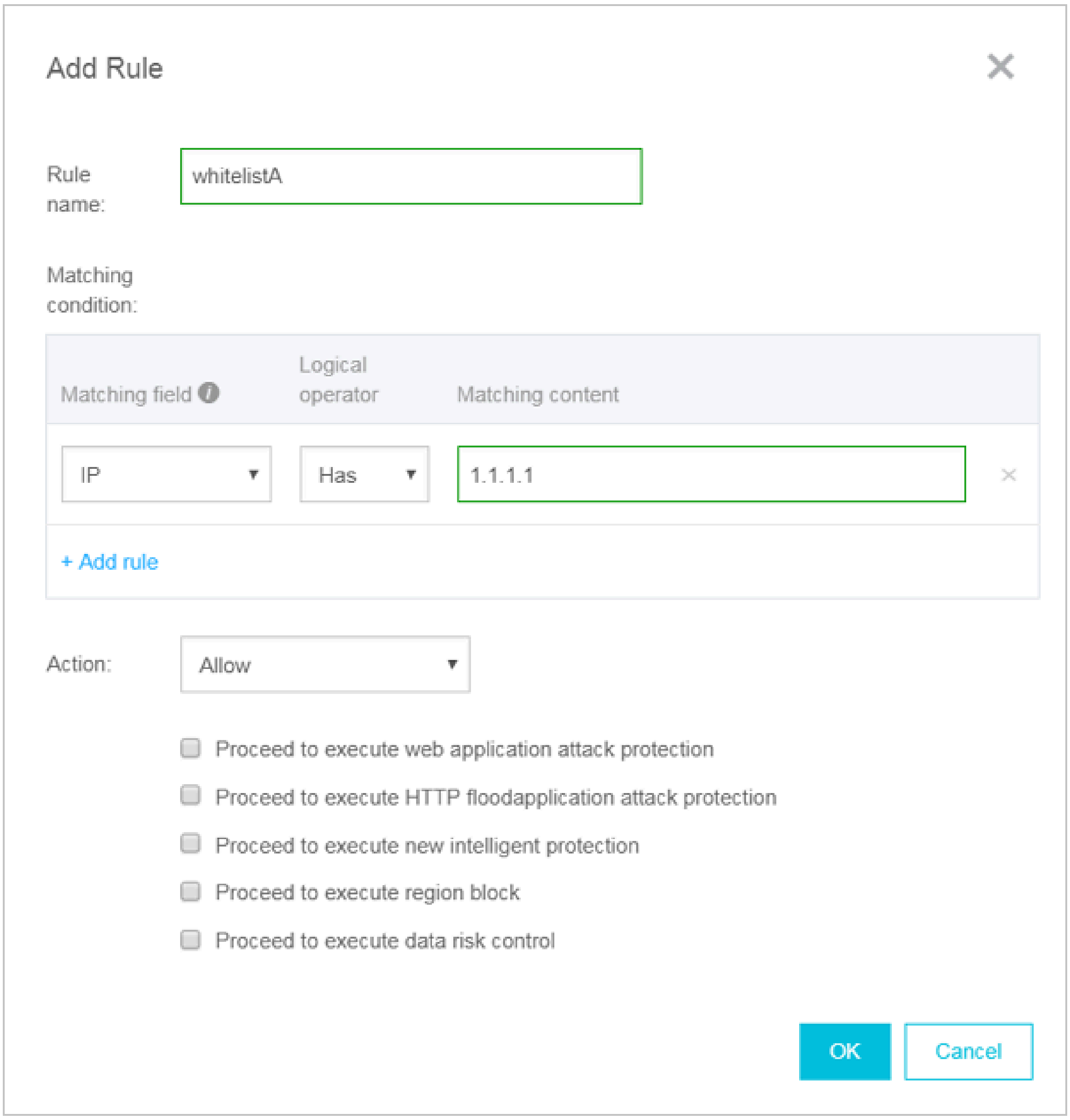
Combine common HTTP header fields by con...

Status:

Rule: 1Rules Settings

5. Click **Add Rule**.

- Whitelist configuration example. Use the following configuration to allow all requests from IP 1.1.1.1.



Add Rule

Rule name: whitelistA

Matching condition:

Matching field	Logical operator	Matching content
IP	Has	1.1.1.1

Action: Allow

□ Proceed to execute web application attack protection

□ Proceed to execute HTTP floodapplication attack protection

□ Proceed to execute new intelligent protection

□ Proceed to execute region block

□ Proceed to execute data risk control

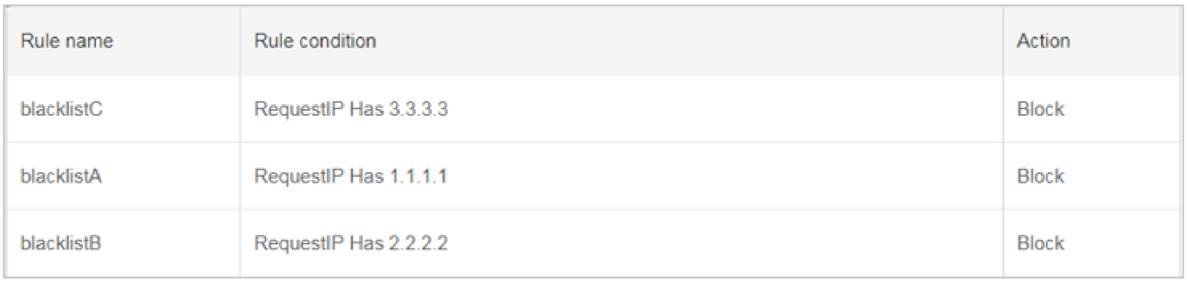
Note:

If you want to allow all requests from this IP, do not select any “Proceed to ...” protection option in the Add Rule dialog box. If any protection option is selected, some requests from this IP can still be blocked.

- Similarly, you can also follow this procedure to set blacklist for a specific domain.

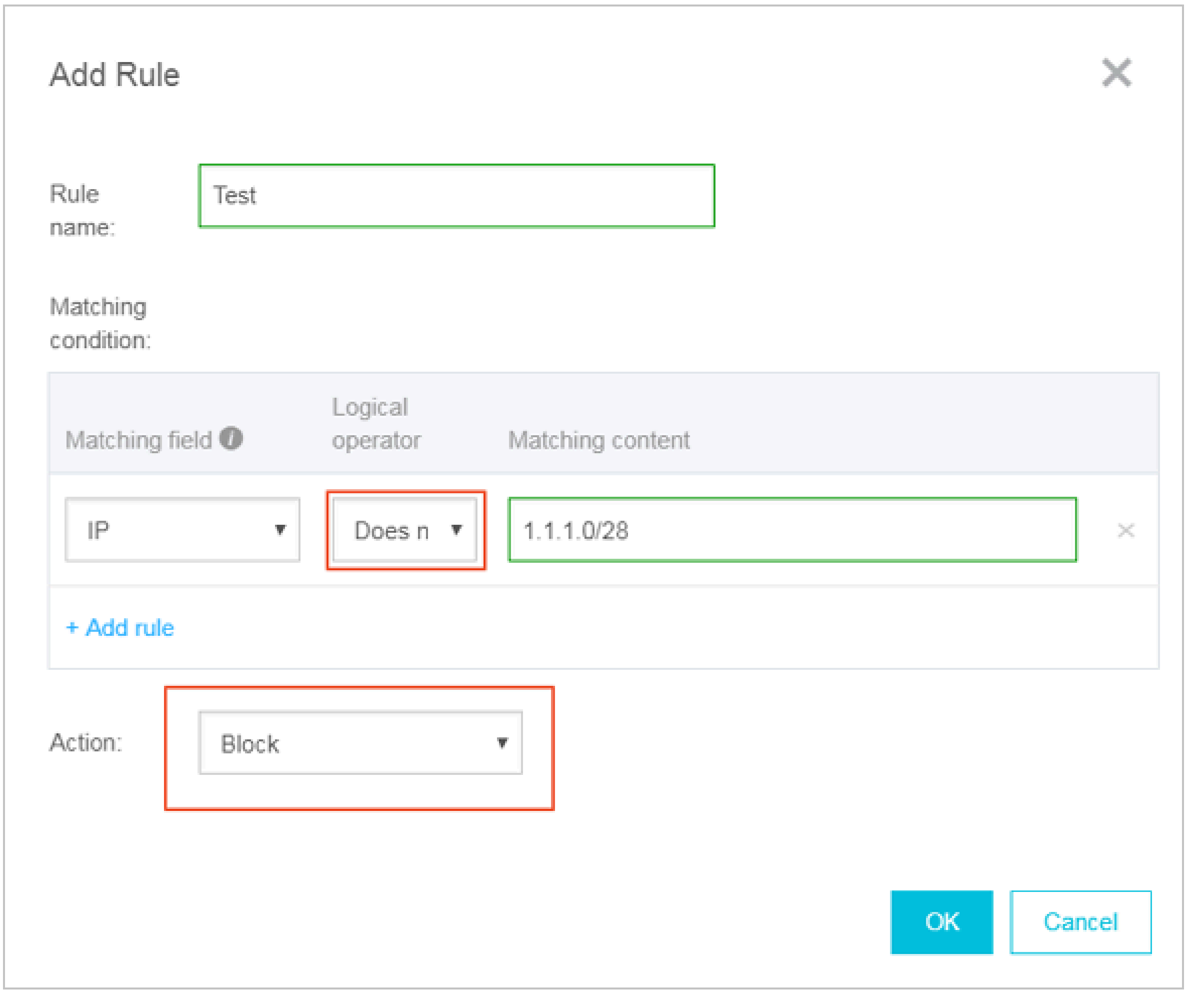
Note

- A rule supports up to three matching conditions. All conditions in a rule must be matched to trigger the rule. If you want to whitelist or blacklist multiple discrete IP addresses/IP segments, you must configure multiple HTTP ACL rules. For example, to block access requests from 1.1.1.1, 2.2.2.2, and 3.3.3.3, you must configure three rules separately.



Rule name	Rule condition	Action
blacklistC	RequestIP Has 3.3.3.3	Block
blacklistA	RequestIP Has 1.1.1.1	Block
blacklistB	RequestIP Has 2.2.2.2	Block

- The IP matching filed in HTTP ACL rules supports mask format (for example, 1.1.1.0/24), and the logical operator supports "does not have". For example, you can use the following configuration to only allow requests from specific IP segment to one domain.



Add Rule

Rule name: Test

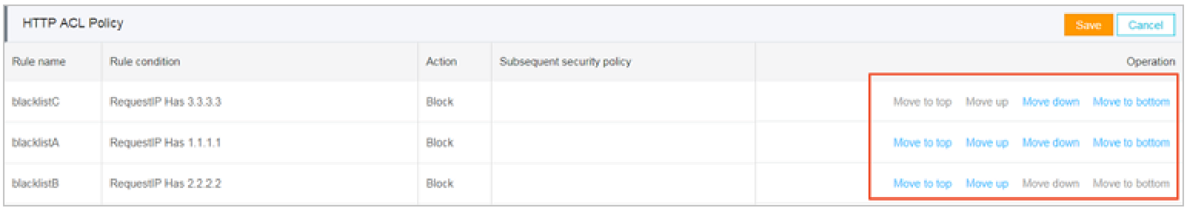
Matching condition:

Matching field	Logical operator	Matching content
IP	Does n	1.1.1.0/28

+ Add rule

Action: Block

- Priority exists among multiple HTTP ACL rules. WAF applies the HTTP ACL rules according to the displayed sequence (from top to bottom) of HTTP ACL rules in the HTTP ACL Policy list. Additionally, you can click **Sort Rules** to change the priority among the HTTP ACL rules.



HTTP ACL Policy

Rule name	Rule condition	Action	Subsequent security policy	Operation
blacklistC	RequestIP Has 3.3.3.3	Block		Move to top Move up Move down Move to bottom
blacklistA	RequestIP Has 1.1.1.1	Block		Move to top Move up Move down Move to bottom
blacklistB	RequestIP Has 2.2.2.2	Block		Move to top Move up Move down Move to bottom

2.8 Data risk control

Data risk control helps you protect critical business interfaces (such as registration, login, activity, and forum) on your website against fraud.

Function description

Based on Alibaba Cloud's big data capabilities, Data risk control leverages industry-leading risk decision engines and human-machine identification technologies to protect critical businesses from fraud in different situations. By implementing Alibaba Cloud WAF (WAF) for your website, you can access data risk control without any modification to the server or client.

Note:

Currently, the Data risk control feature is only available in the WAF instance of the Mainland China region.

Data risk control is applicable to (but not limited to) the following scenarios:

- Zombie accounts
- SMS verification code floods
- Credential stuffing and brute force cracking
- Malicious snatching, flash sales, bonus hunting, and snatching of red packets
- Ticket scalping by machines, vote cheating, and malicious voting
- Spam messages

Procedure

Follow these steps to enable and configure data risk control:

Note:

Make sure you have implemented Alibaba Cloud WAF for your website before doing this configuration. For more information, see Implement Alibaba Cloud WAF.

1. Log on to the Alibaba Cloud WAF console.
2. Go to the **Management** > **Website Configuration** page and select the region of your WAF instance (Mainland China or International).
3. Locate to the domain name to be configured and click **Policies**.
4. Under **Data Risk Control**, turn on the Status switch and confirm enabling this feature.

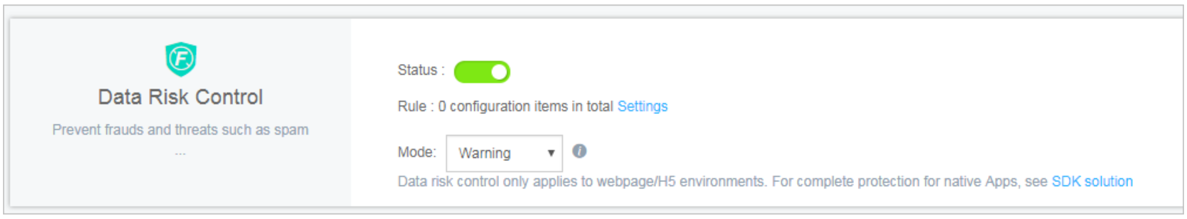
   Note:

   When enabled, Data risk control will inject JavaScript code into your webpage for detecting malicious behaviors, and disable all gzip compression settings. Even if your website uses a non-standard port, no additional configuration is required in data risk control. The JavaScript can be inserted into all webpages (default) or specific webpages. For more information, see Insert JavaScript into specific webpages.
5. Select a protection **Mode**:

   - **Warning**: Allow all requests and record suspicious requests in logs.
   - **Protection**: For suspicious requests, ask the client to finish the slider verification to continue.

   Note:

   The warning mode is used by default. Data risk control does not block any request, but injects JavaScript code into webpages to analyze behaviors on the client.



Data Risk Control

Prevent frauds and threats such as spam

...

Status :

Rule : 0 configuration items in total Settings

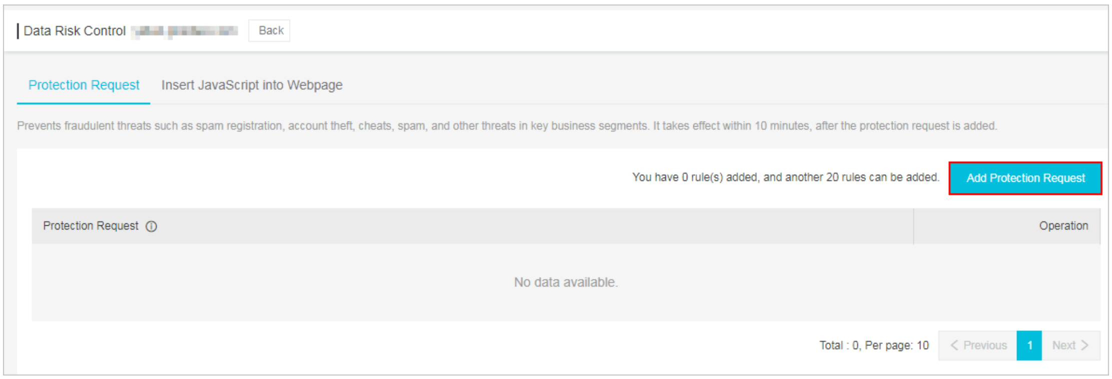
Mode: Warning

Data risk control only applies to webpage/H5 environments. For complete protection for native Apps, see SDK solution

6. Click **Settings** to add protection requests or specify the webpages to insert JavaScript.

- Add a protection request

  a. On the **Protection Request** tab page, click **Add Protection Request**.



Data Risk Control [redacted]

Protection Request | Insert JavaScript into Webpage

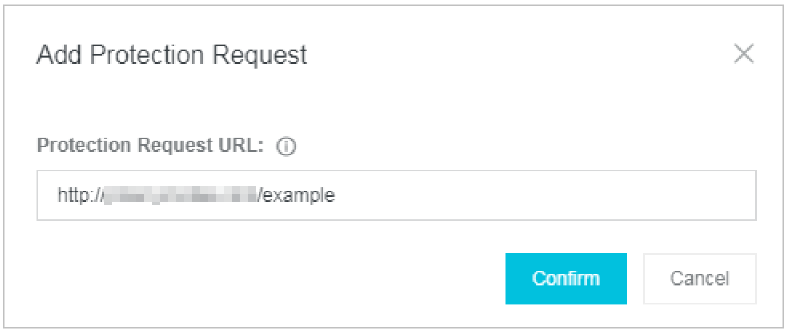
Prevents fraudulent threats such as spam registration, account theft, cheats, spam, and other threats in key business segments. It takes effect within 10 minutes, after the protection request is added.

You have 0 rule(s) added, and another 20 rules can be added.

Protection Request	Operation
No data available.	

Total : 0, Per page: 10

  b. In the **Add Protection Request** dialog box, enter the exact **Protection Request URL** to be protected.



Add Protection Request

Protection Request URL: http://[redacted]/example

What is the Protection Request URL

Protection Request URL is the interface address where business actions are performed instead of the webpage's address. Take the following registration page as an example.

In this example, the registration page is www.abc.com/new_user where users can submit a registration request. To submit a registration request, users must perform the SMS verification and agree to registration. The business interfaces that work in this scenario are www.abc.com/getsmscode and www.abc.com/register.do.

In this case, you can add two protection requests to protect URL www.abc.com/getsmscode and www.abc.com/register.do against SMS interface abuse and zombie registration.

If you configure the request URL as www.abc.com/new_user, a validation slider will pop up when a user accesses the registration page. This will affect the user experience.

Note on specifying the Protection Request URL

- The request URL must be an exact URL. A fuzzy match is not supported.

  For example, if www.test.com/test is specified, the protection only applied to the www.test.com/test interface. Any subdomain page (for example www.test.com/test/abc) is not affected.
- You can use /* to apply data risk control to all paths under a web directory.

  For example, if www.test.com/book/* is specified, the protection applied to all paths under www.test.com/book. We recommend that you do not apply data risk control to full site (for example, use www.abc.com/* as the protection request URL). Because users will be required to finish the slider verification even on the homepage, which may reduce the user experience.
- We recommend that you do not configure a URL that is normally accessed directly by users without a series of previous visits. Because the user experience will be affected if the user is required to complete the slider verification without a series of previous visits.
- Data risk control does not apply to the direct API call scenario, and such calls may be blocked by data risk control. Because API calls are directly initiated machine actions, these calls cannot pass the human-machine identification of

data risk control. If the API service is called by a user operation (such as clicking a button in the console), data risk control can be applied.

c. Click **Confirm**.

The successfully added protection request takes effect in about ten minutes.

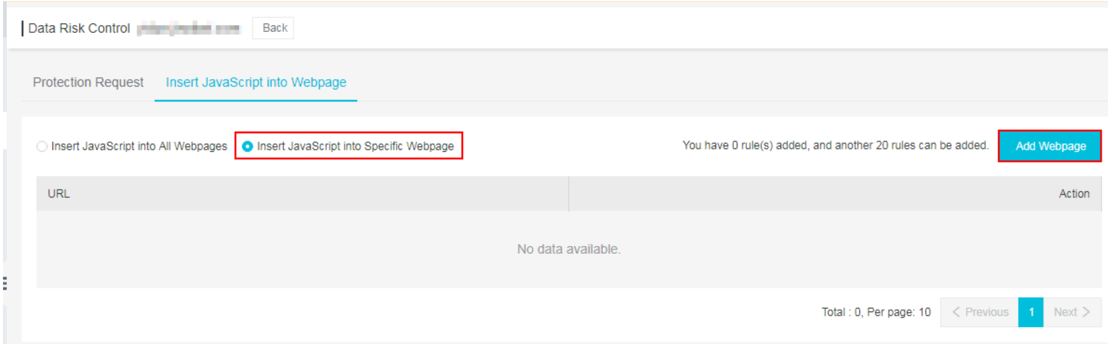
- Specify a webpage to insert the Data risk control JavaScript

In case not all your webpages are compatible with the Data risk control JavaScript, you can insert JavaScript into specific webpages.

Note:

Not inserting Data risk control JavaScript into all webpages may weaken the protection effectiveness, because data risk control cannot perceive all user behaviors.

a. On the **Insert JavaScript into Webpage** tab page, click **Insert JavaScript into Specific Webpage**.



Data Risk Control [redacted]

○ Insert JavaScript into All Webpages ● Insert JavaScript into Specific Webpage

You have 0 rule(s) added, and another 20 rules can be added.

URL	Action
No data available.	

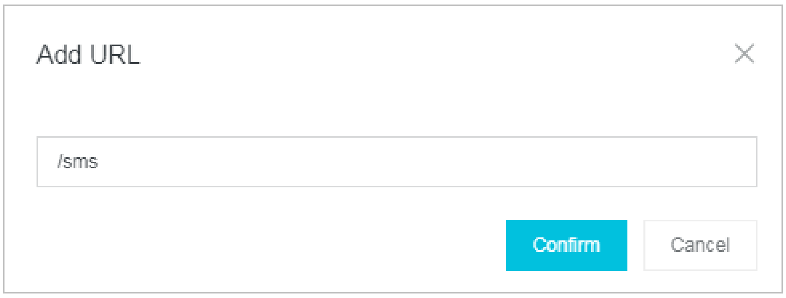
Total : 0, Per page: 10

b. Click **Add Webpage**.

Note:

You can add up to 20 webpages.

c. In the **Add URL** dialog box, enter a specific URI (starting with “/?) under the domain name to protect, and click **Confirm**.



Add URL

/sms

Data risk control only inserts the JavaScript into the specified paths.

After data risk control is enabled, you can use the logs feature of Alibaba Cloud WAF to view the protection results. For more information about a log example, see Data risk control logs.

Use case

A user, Tom, has a website with the domain name `www.abc.com`. Common users can register as members at `www.abc.com/register.html`.

Recently, Tom found out that hackers frequently submit registration requests by using malicious scripts. The hackers register a large number of zombie accounts to participate in the prize draw activity that Tom organizes. (These hackers are known as econnoisseurs.) These requests are similar to normal requests, where the frequency is not high. Traditional HTTP flood protection methods have problems identifying malicious requests of this kind.

Tom adds the website to WAF for protection, and enables data risk control for the domain name `www.abc.com`. As the business at `www.abc.com/register.html` is the most important to Tom, he configures specific request protection for this URL.

From the moment the configuration takes effect, WAF will do the following:

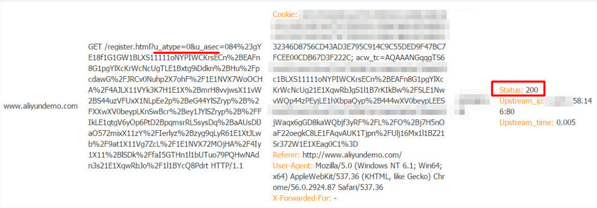
- Observes and analyzes whether the behaviors of users who access the domain name `www.abc.com` (including the homepage and its subpaths) are abnormal. WAF refers to Alibaba Cloud's reputation database to determine whether this source IP address is risky.
- A user submits a registration request to `www.abc.com/register.html`. Because this URL is configured for request protection in WAF, WAF will determine if the user is suspicious based on user behavior and reputation from the moment the user accesses the webpage to when the user submits the registration request. For example, if a user doesn't perform any prior actions but directly submits a registration request, the user is suspicious.
    - If WAF finds the request to be suspicious or this client IP address has a bad record, a validation slider pops up for user authentication. The authenticated user can continue to register.
        - If the user passes the slider validation in a suspicious way (for example, use scripts to simulate a real person's sliding process), WAF will continue to perform other validation tests.
        - If the user cannot pass the validation, WAF will block this request.
    - If WAF finds this is a common user based on the preceding behaviors, he or she can finish the registration process without any intervention.

Data risk control is enabled for the entire domain name (www.abc.com) during the process. This means that **WAF will insert JavaScript into all the pages with this domain name to determine whether the client is trusted**. The real protection and validation are targeted at the interface www.abc.com/register.html. WAF will intervene when this interface is requested. If the preceding behaviors of the client are trusted, WAF will not intervene. Otherwise, the user must pass the validation to continue the operation.

Data risk control logs

You can use the Logs feature of Alibaba Cloud WAF to troubleshoot the monitoring and blocking situations of data risk control. For example,

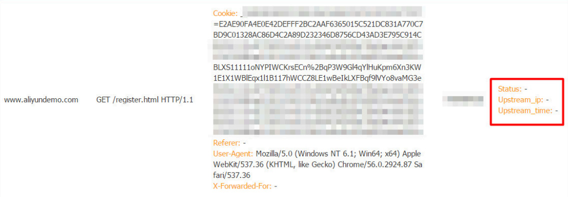
- The following figure shows the log that the user passed the validation test of data risk control.



```
www.aliyundemo.com

GET /register.html?u_atype=0&u_asec=084%23gY
E18f1G1GW1BLXS11111oNYPIWCKrsECn%2BEAFn
8G1pgYlXcKrWcNcUgTLE1Bxtg9iDdkn%2BHu%2Fp
cdawG%2FJRCv0Nuhp2X7ohF%2F1E1NVX7WoOCH
A%2F4AJLX11VYk3K7H1E1X%2BmrH8vvjwsX11vW
2BS44uzVFUxX1NLpEe2p%2BeG44YlSZryp%2B%2
FXXwXV0beypLKnSwBcr%2Bey1JYlSZryp%2B%2FF
IkLE1qtgV6yOp6PtD2BpqmsrRL5sysDq%2BaAUsDlJ
aO572mixX11zY%2FIerlyz%2Bzyg9qLyR61E1XtJLw
b%2F9at1X11Vg7ZcL%2F1E1NVX72MOjHA%2F4Iy
1X11%2BlSDk%2FfaI5GTHn1l1bUTuo79PQHwNAd
n3s21E1XqwRbJo%2F1l1BYcQ8Pdrt HTTP/1.1

Cookie: [redacted]
32346D8756CD43AD3E795C914C9C55DED9F47BC7
FCEE00CDB67D3F222C; acw_tc=AQAAANGqqgTS6
[redacted]
c1BLXS11111oNYPIWCKrsECn%2BEAFn8G1pgYlXc
KrWcNcUg21E1XqwRbJgS1l1B7rKIkBw%2FSLE1Nw
vWQp44zPEyjLE1hXbpaQyp%2B444wXV0beypLEES
[redacted]
jWaqx6gGD8kaWQbjf3yRF%2FL%2FO%2Bj7H5nO
aF22oegkC8LE1FAqvAUK1Tjpn%2FUlj16Mx1l1BZ21
Sr372W1E1XEag0C1%3D
Referer: http://www.aliyundemo.com/
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
ome/56.0.2924.87 Safari/537.36
X-Forwarded-For: -

[redacted]

Status: 200
Upstream_ip: [redacted]58.14
6:80
Upstream_time: 0.005
```

When a common user who has passed the data risk control validation requests a URL, the URL has a parameter that begins with ua. This request will be sent to the origin and get a normal response.

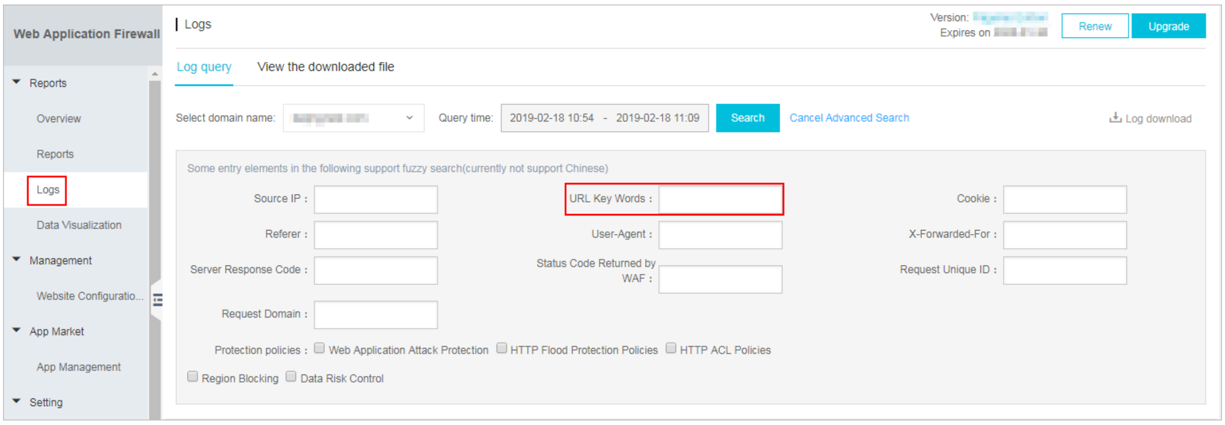
- The following figure shows the blocking logs of data risk control.



```
www.aliyundemo.com    GET /register.html HTTP/1.1

Cookie: _[redacted]
=E2AE90FA4E0E42DEFFF2BC2AAF6365015C521DC831A770C7
BD9C01328AC86D4C2A89D232346D8756CD43AD3E795C914C
[redacted]
BLXS11111oNYPIWCKrsECn%2BqP3W9Gl4qYlHuKpm6Xn3KW
1E1X1WBlEqx1l1B117hWCCZ8LE1wBeIkLXFBqf9lVYo8vaMG3e
[redacted]
Referer: -
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) Apple
WebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Sa
fari/537.36
X-Forwarded-For: -

[redacted]

Status: -
Upstream_ip: -
Upstream_time: -
```

If the user directly requests this interface, the URL typically does not have a parameter that begins with ua (or a parameter with forged ua). The request will be blocked by WAF , and the origin response cannot be seen in the corresponding logs.

You can use the Logs feature to configure and enable the data risk control interface in **Advanced Search** > **URL Key Words**. You can use this interface to troubleshoot the blocking logs.



Web Application Firewall

- Reports
  - Overview
  - Reports
  - Logs
  - Data Visualization
- Management
  - Website Configuratio...
- App Market
  - App Management
- Setting

| Logs

Version: [redacted]
Expires on [redacted]
Renew Upgrade

Log query View the downloaded file

Select domain name: [redacted] Query time: 2019-02-18 10:54 - 2019-02-18 11:09 Search Cancel Advanced Search Log download

Some entry elements in the following support fuzzy search(currently not support Chinese)

Source IP :
URL Key Words :
Cookie :
Referer :
User-Agent :
X-Forwarded-For :
Server Response Code :
Status Code Returned by WAF :
Request Unique ID :
Request Domain :

Protection policies : □ Web Application Attack Protection □ HTTP Flood Protection Policies □ HTTP ACL Policies
□ Region Blocking □ Data Risk Control

2.9 Website tamper-proofing

Website tamper-proofing allows you to lock specific web pages and manually cache the intact content as the server response to prevent malicious tampering. When a locked web page is requested, Alibaba Cloud WAF (WAF) responds with the cached content.

Context

Note:

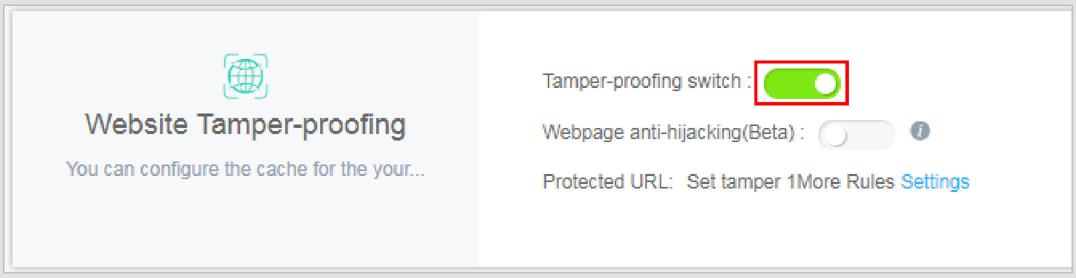
Make sure that you have implemented WAF for your website before performing this configuration. For more information, see Implement Alibaba Cloud WAF.

Procedure

1. Log on to the Alibaba Cloud WAF console.
2. Go to the **Management** > **Website Configuration** page and select the region of your WAF instance (Mainland China or International).
3. Locate to the domain name to be configured and click **Policies**.
4. Enable **Website Tamper-proofing** and click **Settings**.

   Note:

   If you no longer need the website tamper-proofing feature, you can disable it on this page.



Website Tamper-proofing

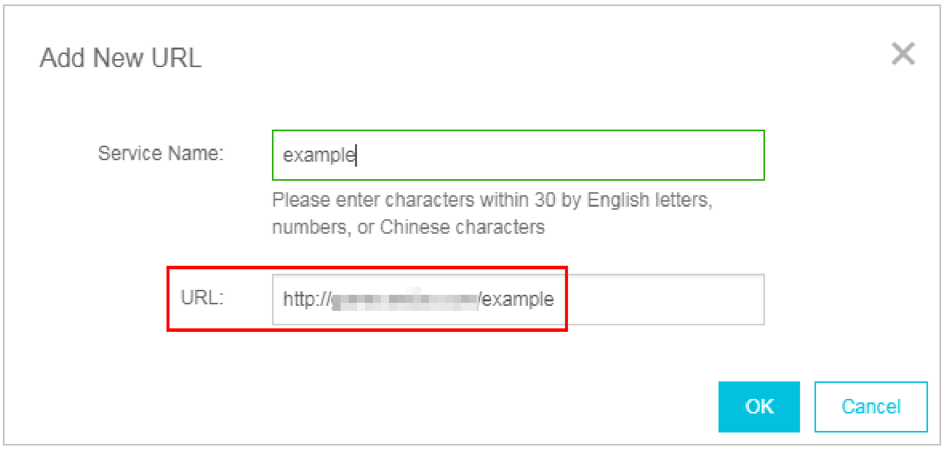
You can configure the cache for the your...

Tamper-proofing switch :

Webpage anti-hijacking(Beta) :

Protected URL: Set tamper 1More Rules Settings

5. Click **New Rule** and complete the configuration in the **Add New URL** dialog box.



Add New URL

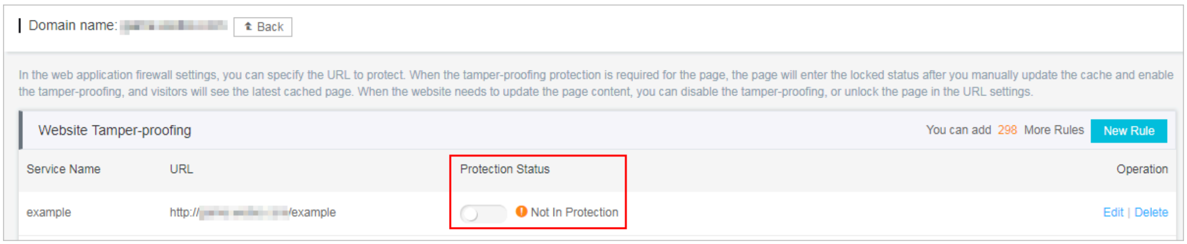
Service Name: example

Please enter characters within 30 by English letters, numbers, or Chinese characters

URL: http://[redacted]/example

- **Service Name**: Name this rule.
- **URL**: Specify the exact path of the web page to be protected. Wildcard characters (such as /*) or parameters (such as /abc? xxx=) are not supported. WAF can protect all text, HTML, and pictures under this path against tampering.

6. When the rule is successfully added, turn on the **Protection Status** switch to enable it, that it, lock the specified web page and cache the latest content as the server response. If you do not enable the rule, the settings do not take effect.



Domain name: [redacted]

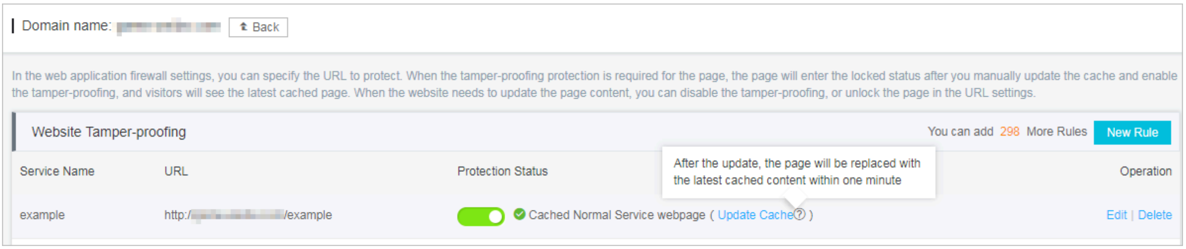
In the web application firewall settings, you can specify the URL to protect. When the tamper-proofing protection is required for the page, the page will enter the locked status after you manually update the cache and enable the tamper-proofing, and visitors will see the latest cached page. When the website needs to update the page content, you can disable the tamper-proofing, or unlock the page in the URL settings.

Website Tamper-proofing

You can add 298 More Rules

Service Name	URL	Protection Status	Operation
example	http://[redacted]/example	Not In Protection	Edit | Delete

7. When the locked web page is updated, you must click **Update Cache** to cache the latest content. If you do not perform this operation, WAF always returns the last cached content.



Domain name: [redacted]

In the web application firewall settings, you can specify the URL to protect. When the tamper-proofing protection is required for the page, the page will enter the locked status after you manually update the cache and enable the tamper-proofing, and visitors will see the latest cached page. When the website needs to update the page content, you can disable the tamper-proofing, or unlock the page in the URL settings.

Website Tamper-proofing

You can add 298 More Rules

After the update, the page will be replaced with the latest cached content within one minute

Service Name	URL	Protection Status	Operation
example	http:/[redacted]/example	Cached Normal Service webpage (Update Cache)	Edit | Delete

2.10 Data leakage prevention

The data leakage prevention function allows Web Application Firewall (WAF) to comply with China's Cyber Security Law that stipulates that "network operators should take technical measures and other necessary measures to guarantee the security of personal information they collect and prevent information leaks, damages, and loss. In the event of, or possible occurrence of, any personal information leaks, damages, or loss, the network operators involved shall immediately take remedial measures, notify users in a timely manner, and report the case to competent authorities in accordance with the provisions.”

Function description

The data leakage prevention function provides desensitization and warning measures for sensitive information leaks on websites (especially mobile phone numbers, ID card numbers, and credit card information) and the leakage of sensitive keywords. It also allows you to block specified HTTP status codes.

You must upgrade WAF to the Business or Enterprise edition to use this function. For more information, see Renewal and upgrade.

Common information leak situations faced by websites include:

- Unauthorized access to a URL, such as unauthorized access to the website management background.
- Excessive permission access vulnerabilities, such as horizontal excessive permission access vulnerabilities and vertical excessive permission access vulnerabilities.
- Sensitive information crawled by malicious crawlers on webpages.

The data leakage prevention function can do the following tasks for you:

- Detects and identifies private and sensitive data generated on the webpage and offers protection measures, such as early warnings and the shielding of sensitive information, to avoid website operation data leaks. This sensitive and private data includes, but is not limited to, ID card numbers, mobile phone numbers, and bank card numbers.
- Supports one-click blocking of sensitive server information that may expose the web application software, operating systems, and versions used by the website to avoid leaks of sensitive server information.
- Using a built-in illegal and sensitive keyword library, the function provides warnings , illegal keyword shielding, and other protective measures to deal with illegal and sensitive keywords that appear on webpages.

How it works

The data leakage prevention function detects if response pages have ID card numbers , mobile phone numbers, bank card numbers, and other types of sensitive information

. If it discovers a sensitive information match, it sends a warning or filters the sensitive information based on the action configured for the matching rule. When sensitive information is filtered, the sensitive portion of the information is replaced by asterisks (*) to protect it.

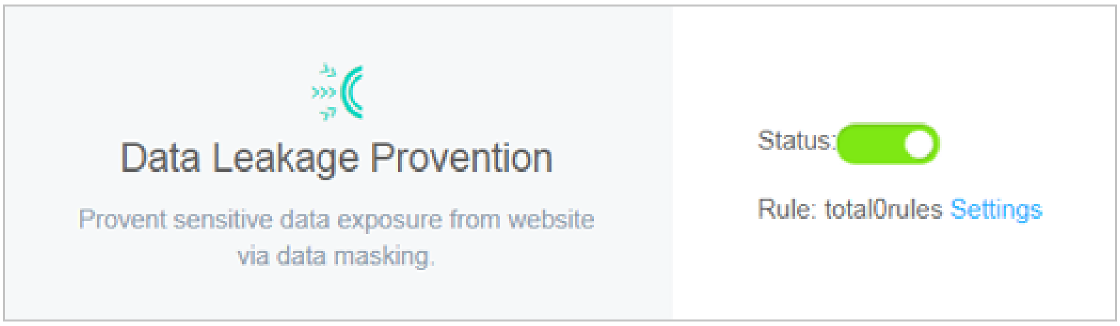
The data leakage prevention function supports Content-Types including text/*, image/*, and application/* and covers web terminals, app terminals, and API interfaces.

Procedure

Follow these steps to enable and configure Data Leakage Prevention:

Note:
Make sure that you have added your domain to the WAF protection list before proceeding with the following operations. For more information, see CNAME access guide.

1. Log on to the Web Application Firewall console.
2. Go to the **Management** > **Website Configuration** page, and select the region of your WAF instance (Mainland China or International).
3. Select the domain to be configured, and click **Policies**.
4. Enable the **Data Leak Prevention** function and click **Settings**.



Data Leakage Provention

Provent sensitive data exposure from website via data masking.

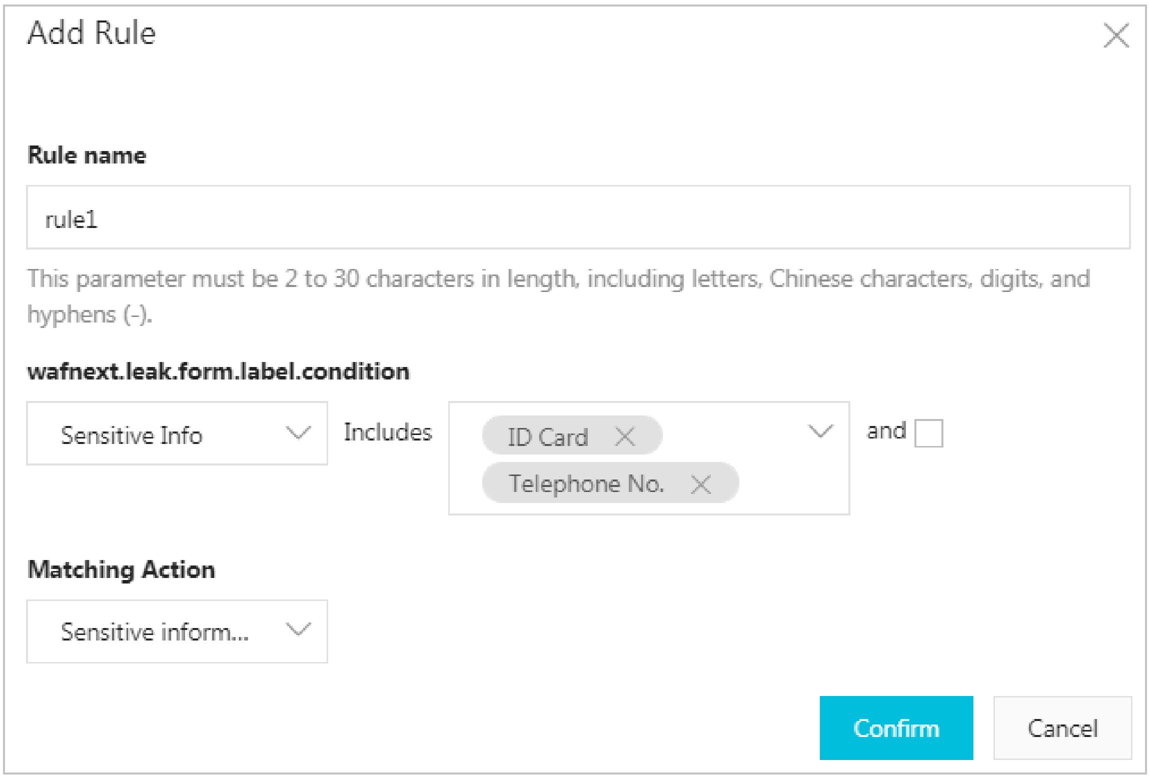
Status:

Rule: total0rules Settings

5. Click **Add Rule** to add a sensitive information protection rule.

Note:
In the Add Rule dialog box, you can click **and** to add more URL matching conditions.

- **Sensitive information masking**: For webpages that may display mobile phone numbers, ID card numbers, and other sensitive information, configure the relevant rules to mask this information or provide warnings. For example, you can set the following protection rule to protect mobile phone numbers and ID card numbers by data masking.



Add Rule

Rule name

rule1

This parameter must be 2 to 30 characters in length, including letters, Chinese characters, digits, and hyphens (-).

wafnext.leak.form.label.condition

Sensitive Info Includes ID Card, Telephone No. and □

Matching Action

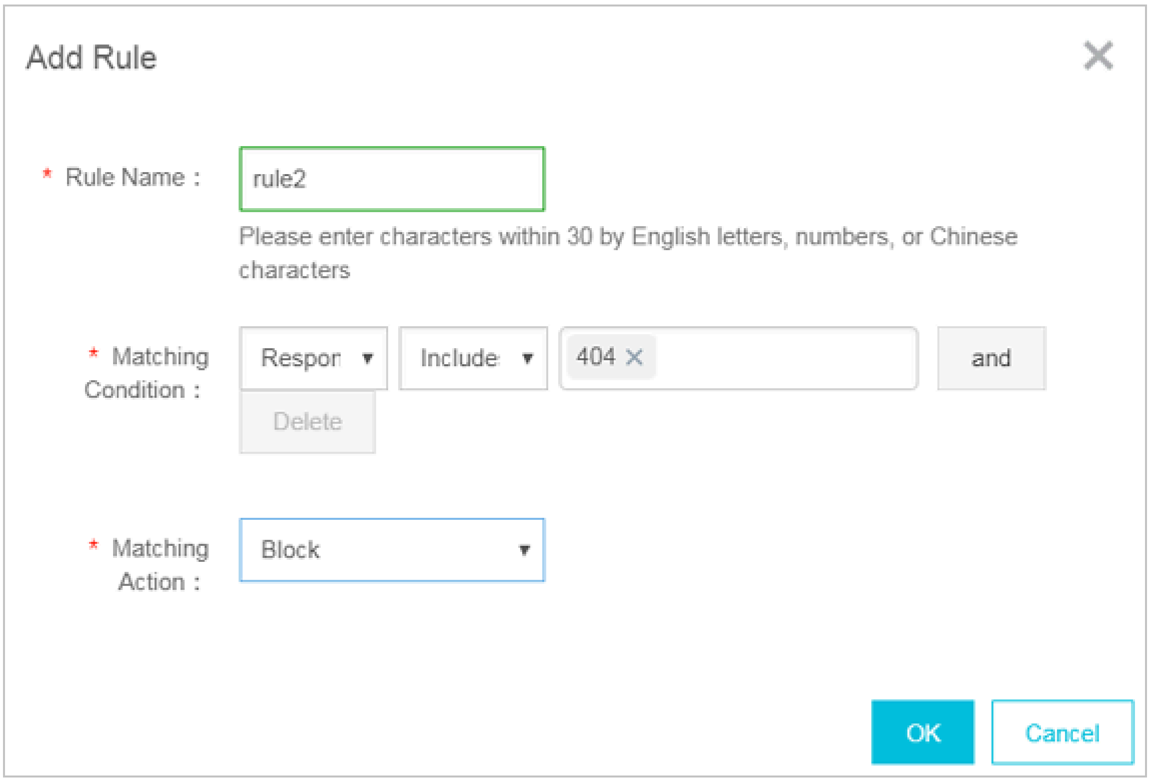
Sensitive inform...

After setting this protection rule, mobile phone and ID card numbers displayed on all webpages in this website are automatically desensitized.

Note:

When a webpage has business contact phone numbers, support hotline numbers, and other mobile phone numbers that are to be provided to the public, these may also be filtered out by the configured mobile phone number sensitive information filtering rule.

- **Status code blocking**: You can set rules to block or warn of specific HTTP request status codes to avoid leaking sensitive server information. For example, you can set the following protection rule to block HTTP 404 status codes.



Add Rule

* Rule Name : rule2

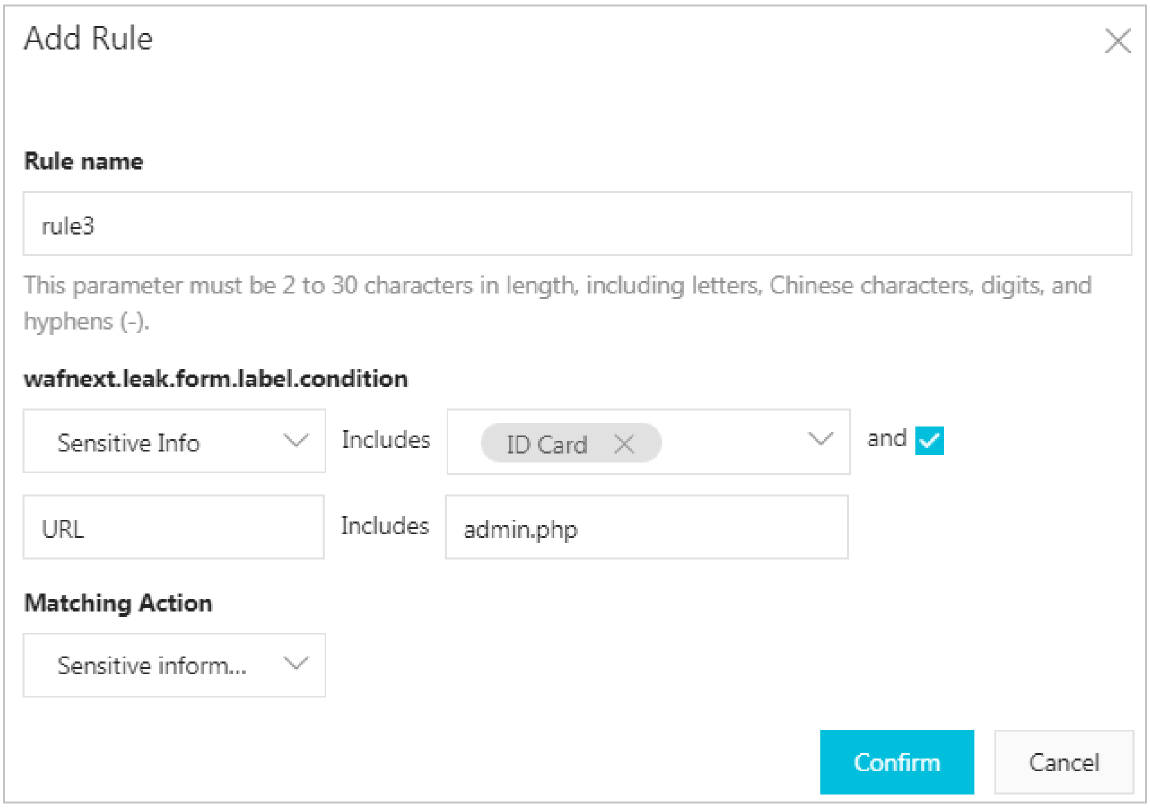
Please enter characters within 30 by English letters, numbers, or Chinese characters

* Matching Condition : Respon Include 404

* Matching Action : Block

After setting this protection rule, when users request a page that does not exist under this website, the specified page is returned.

- **Filter sensitive information of specified URLs**: For specified webpage URLs that may display mobile phone numbers, ID card numbers, and other sensitive information, configure the relevant rules to filter this information or provide warnings. For example, you can set the following protection rule to filter ID card numbers on the webpage admin.php.



Add Rule

Rule name

rule3

This parameter must be 2 to 30 characters in length, including letters, Chinese characters, digits, and hyphens (-).

wafnext.leak.form.label.condition

Sensitive Info Includes ID Card and ☑

URL Includes admin.php

Matching Action

Sensitive inform...

After setting this protection rule, ID card numbers are desensitized on the admin.php webpage.

6. For an added rule, you can also **Edit** or **Delete** it.

After enabling the Data Leak Prevention function, you can log on to the Web Application Firewall console, and go to the **Reports** > **Attack Protection** page to view protection reports. This report allows you to query logs of access requests filtered out or blocked by data leakage prevention rules.

2.11 IP blocking

IP blocking helps you automatically block client IP addresses that launch multiple Web attacks on your domain within a short period of time.

Prerequisites

You can enable this feature in Web Application Firewall (WAF) only when the following conditions are met:

- You have bought a monthly or yearly subscription WAF service. For more information, see Activate Alibaba Cloud WAF.

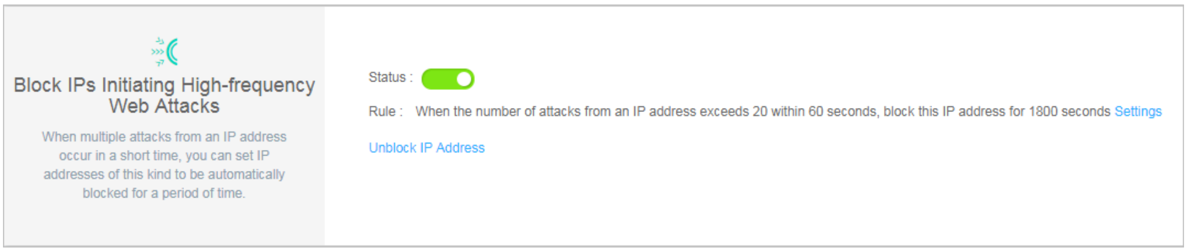
- You have added your domain to WAF for protection. For more information, see #unique_26.
- You have enabled Web application protection and HTTP flood protection. For more information, see Web application protection and HTTP flood protection.

Context

You can enable the IP blocking feature to automatically detect and block client IP addresses that launch multiple Web attacks on your domain within a short period of time. Requests from the blocked IP addresses are rejected during the blocking period. After the blocking period expires, the blocked IP addresses are automatically unblocked. After enabling IP blocking, you can customize a protection rule. For more information, see Step 5. You can also unblock IP addresses manually. For more information, see Step 6.

Procedure

1. Log on to the WAF console.
2. In the left-side navigation pane, choose **Management** > **Website Configuration**. On the Website Configuration page that appears, select the region of your WAF instance (Mainland China or International).
3. Find the domain to be configured in the domain list, and click **Policies** in the Operation column.
4. On the page that appears, scroll down to the **Block IPs Initiating High-frequency Web Attacks** area and turn on Status to enable IP blocking.



Block IPs Initiating High-frequency Web Attacks

When multiple attacks from an IP address occur in a short time, you can set IP addresses of this kind to be automatically blocked for a period of time.

Status :

Rule : When the number of attacks from an IP address exceeds 20 within 60 seconds, block this IP address for 1800 seconds Settings

Unblock IP Address

After IP blocking is enabled, the following protection rule takes effect by default: If WAF detects that a client IP address has launched more than 20 Web attacks on the specified domain within 60 seconds, WAF blocks the IP address for 1,800 seconds.

5. Optional: You can perform the following steps to customize a protection rule:

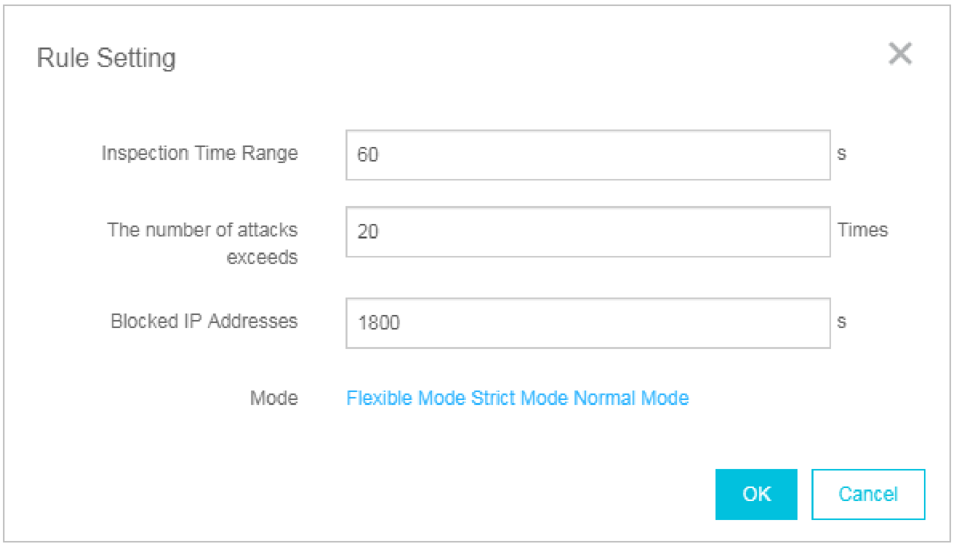
a) In the **Block IPs Initiating High-frequency Web Attacks** area, Click **Settings**.

b) In the **Rule Setting** dialog box that appears, set the following parameters.

Note:

If you do not know how to set these parameters, set **Mode** to one of the following values: **Flexible Mode**, **Strict Mode**, and **Normal Mode**. Each of these values correspond to a default protection rule that is configured to a certain degree of strictness. You can adjust the settings in these rules to customize the degree of strictness.

Parameter	Description
Inspection Time Range	The period of time at which WAF checks for Web attacks from client IP addresses on the specified domain. Unit: second.
The number of attacks exceeds	The maximum number of Web attacks that a client IP address can launch on the specified domain within the specified period of time. If the number of Web attacks from a client IP address exceeds the value of this parameter, WAF blocks this IP address.
Blocked IP Addresses	The period of time over which a client IP address is blocked. Unit: second.


Rule Setting

Inspection Time Range: 60 s

The number of attacks exceeds: 20 Times

Blocked IP Addresses: 1800 s

Mode: Flexible Mode Strict Mode Normal Mode

c) Click **OK**.

6. Optional: To manually unblock client IP addresses, click **Unblock IP Address** in the **Block IPs Initiating High-frequency Web Attacks** area.

2.12 Directory traversal protection

Directory traversal protection helps you automatically block client IP addresses that launch multiple directory traversal attacks on your domain within a short period of time.

Prerequisites

You can enable this feature in Web Application Firewall (WAF) only when the following conditions are met:

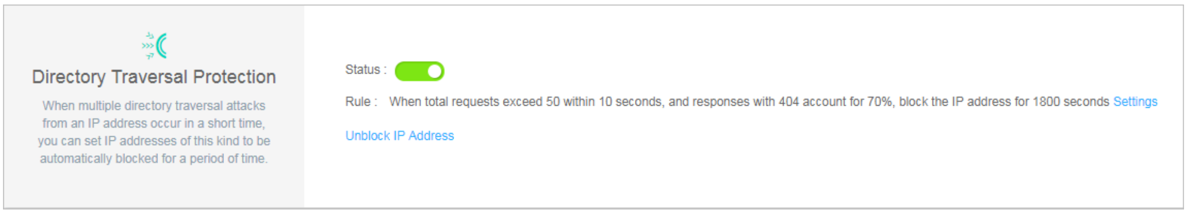
- You have bought a monthly or yearly subscription WAF service. For more information, see Activate Alibaba Cloud WAF.
- You have added your domain to WAF for protection. For more information, see #unique_26.
- You have enabled Web application protection and HTTP flood protection. For more information, see Web application protection and HTTP flood protection.

Context

You can enable the directory traversal protection feature to automatically detect and block client IP addresses that launch multiple directory traversal attacks on your domain within a short period of time. Requests from the blocked IP addresses are rejected during the blocking period. After the blocking period expires, the blocked IP addresses are automatically unblocked. After enabling directory traversal protection, you can customize a protection rule. For more information, see Step 5. You can also unblock IP addresses manually. For more information, see Step 6.

Procedure

1. Log on to the WAF console.
2. In the left-side navigation pane, choose **Management** > **Website Configuration**. On the Website Configuration page that appears, select the region of your WAF instance (Mainland China or International).
3. Find the domain to be configured in the domain list, and click **Policies** in the Operation column.
4. On the page that appears, scroll down to the **Directory Traversal Protection** area and turn on Status to enable directory traversal protection.



Directory Traversal Protection

When multiple directory traversal attacks from an IP address occur in a short time, you can set IP addresses of this kind to be automatically blocked for a period of time.

Status :

Rule : When total requests exceed 50 within 10 seconds, and responses with 404 account for 70%, block the IP address for 1800 seconds Settings

Unblock IP Address

After directory traversal protection is enabled, the following protection rule takes effect by default: If WAF detects more than 50 access requests from a client IP address to the specified domain within 10 seconds and that more than 70% of the responses to these requests contain the 404 response code , WAF blocks the IP address for 1,800 seconds.

5. Optional: You can perform the following steps to customize a protection rule:

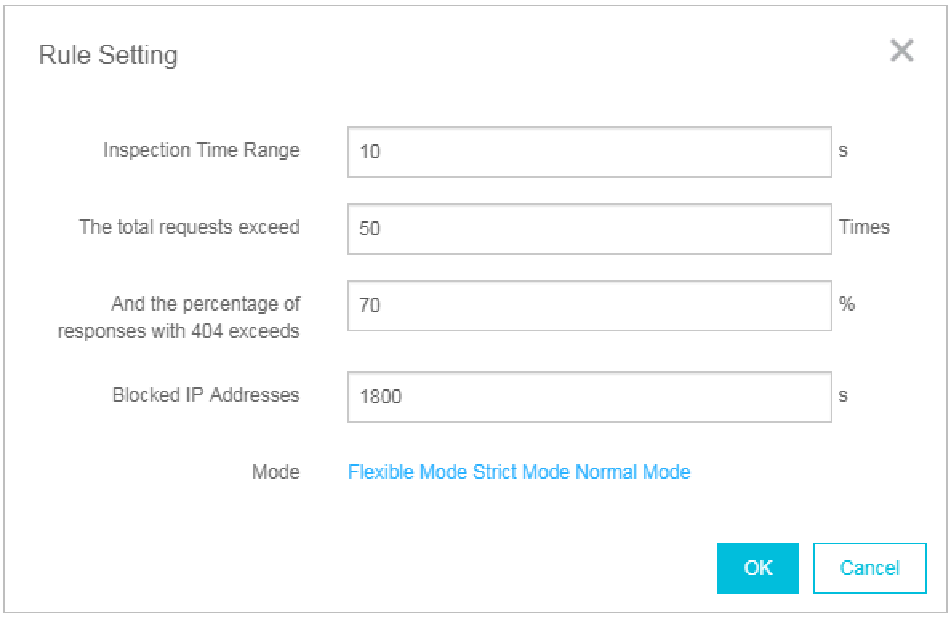
    a) In the **Directory Traversal Protection** area, click **Settings**.

    b) In the **Rule Setting** dialog box that appears, set the following parameters.

> **Note:**
>
> If you do not know how to set the parameters, set **Mode** to one of the following values: **Flexible Mode**, **Strict Mode**, and **Normal Mode**. Each of these values correspond to a default protection rule that is configured to a certain degree of strictness. You can adjust the settings in these rules to customize the degree of strictness.

Parameter	Description
Inspection Time Range	The period of time at which WAF checks for directory traversal attacks from client IP addresses on the specified domain. Unit: second.
The total requests exceeds	The maximum number of access requests that can be sent from a client IP address to the specified domain within the specified period of time. WAF blocks a client IP address when both of the following conditions are met: The number of access requests from the IP address to the specified domain within the specified period of time is greater than the value of this parameter, and the percentage of responses to these requests with the 404 response code exceeds the specified threshold.
And the percentage of responses with 404 exceeds	

Parameter	Description
Blocked IP Addresses	The period of time over which a client IP address is blocked. Unit: second.



Rule Setting

Inspection Time Range: 10 s

The total requests exceed: 50 Times

And the percentage of responses with 404 exceeds: 70 %

Blocked IP Addresses: 1800 s

Mode: Flexible Mode Strict Mode Normal Mode

c) Click **OK**.

6. Optional: To manually unblock client IP addresses, click **Unblock IP Address** in the **Directory Traversal Protection** area.

2.13 Threat intelligence

Threat intelligence helps you automatically block access requests from common vulnerability scanners or from IP addresses in the Alibaba Cloud library of identified port scan attackers.

Prerequisites

You can enable this feature only when the following conditions are met:

- You have bought a monthly or yearly subscription WAF service. For more information, see Activate Alibaba Cloud WAF.
- You have added your domain to WAF for protection. For more information, see #unique_26.
- You have enabled Web application protection and HTTP flood protection. For more information, see Web application protection and HTTP flood protection.

Context

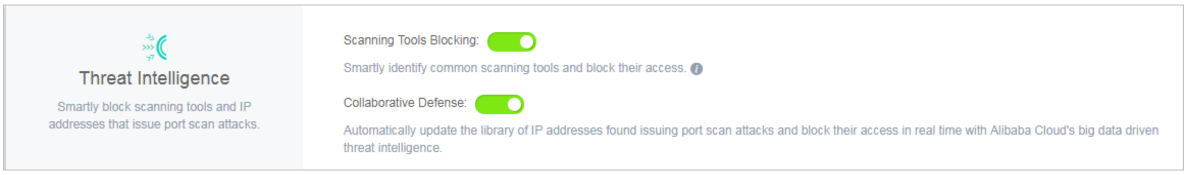
You can enable the threat intelligence feature to automatically block access requests from common vulnerability scanners, including sqlmap, Acunetix Web vulnerability scanner (AWVS), Nessus, AppScan, WebInspect, Netsparker, Nikto, and RSAS. You can also use the collaborative defense function of this feature to automatically block access requests from all IP addresses in the Alibaba Cloud global library of identified port scan attackers.

Procedure

1. Log on to the WAF console.
2. In the left-side navigation pane, choose **Management** > **Website Configuration**. On the Website Configuration page that appears, select the region of your WAF instance (Mainland China or International).
3. Find the domain to be configured in the domain list, and click **Policies** in the Operation column.
4. On the page that appears, scroll down to the **Threat Intelligence** area and enable or disable the protection functions as required.

   The following protection functions are available in threat intelligence:

   - **Scanning Tool Blocking**: identifies common vulnerability scanners and blocks their access requests.
   - **Collaborative Defense**: automatically blocks access requests from all IP addresses in the Alibaba Cloud global library of identified port scan attackers.



Threat Intelligence

Smartly block scanning tools and IP addresses that issue port scan attacks.

Scanning Tools Blocking: on

Smartly identify common scanning tools and block their access.

Collaborative Defense: on

Automatically update the library of IP addresses found issuing port scan attacks and block their access in real time with Alibaba Cloud's big data driven threat intelligence.

2.14 Positive security model

A positive security model is also known as a whitelist. The positive security model of Web Application Firewall (WAF) applies Alibaba Cloud machine learning to network traffic to generate security rules, block malicious requests, and allow benign network traffic to pass through.

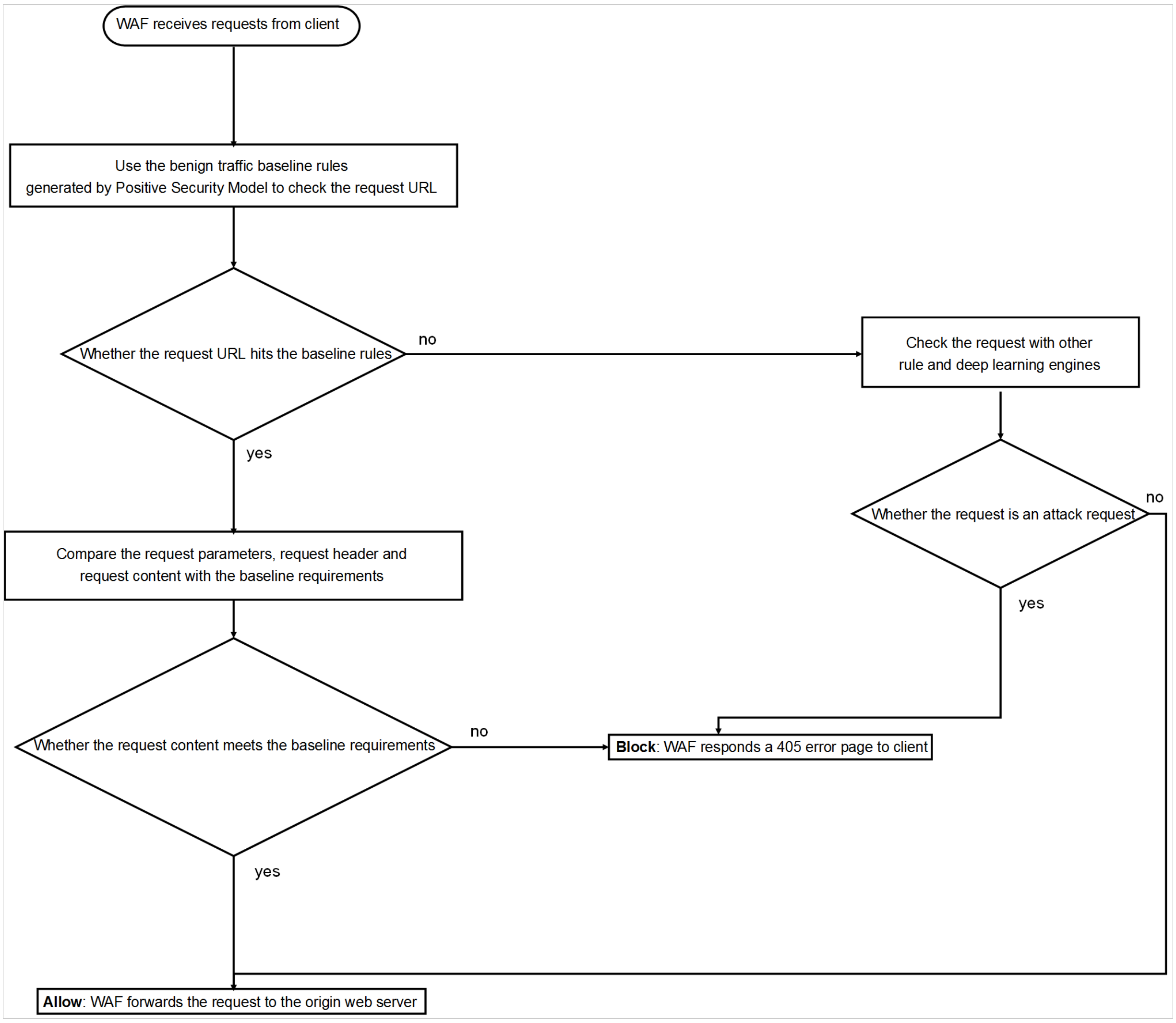
Prerequisites

- Before you use the positive security model, make sure that you have added your domain to WAF for protection. For more information, see #unique_26

- If you are using the WAF Pro or Enterprise edition, you must upgrade WAF to the Ultimate edition. For more information about how to upgrade WAF, see Renew and upgrade.

Context

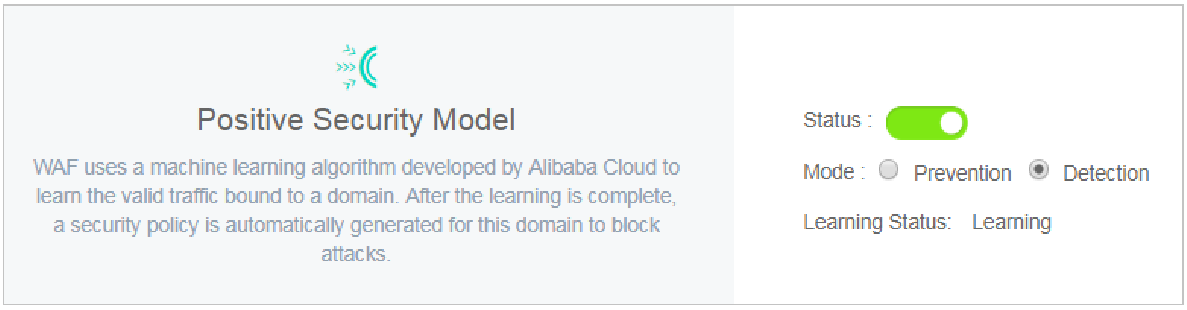
Traditional security models use predefined security rules to detect malicious network traffic . The positive security model of WAF applies machine learning to network traffic in an unsupervised way. Deep learning models are trained based on benign network data and then used to generate security rules. Only requests that reach the baselines of benign traffic in these rules are allowed to pass through. The positive security model works with other detection modules of WAF to prevent attacks at different network layers.


WAF receives requests from client
Use the benign traffic baseline rules generated by Positive Security Model to check the request URL
Whether the request URL hits the baseline rules
no
yes
Check the request with other rule and deep learning engines
Whether the request is an attack request
no
yes
Compare the request parameters, request header and request content with the baseline requirements
Whether the request content meets the baseline requirements
no
yes
Block: WAF responds a 405 error page to client
Allow: WAF forwards the request to the origin web server

Procedure

1. Log on to the WAF console.

2. In the left-side navigation pane, choose **Management** > **Website Configuration**. On the top of the Website Configuration page, select the region of your WAF instance: Mainland China or International.
3. In the domain list, find the domain that you want to manage, and click **Policies** in the Operation column.
4. In the **Positive Security Model** area, click the switch to enable the positive security model.



Positive Security Model

WAF uses a machine learning algorithm developed by Alibaba Cloud to learn the valid traffic bound to a domain. After the learning is complete, a security policy is automatically generated for this domain to block attacks.

Status :

Mode : ○ Prevention ● Detection

Learning Status: Learning

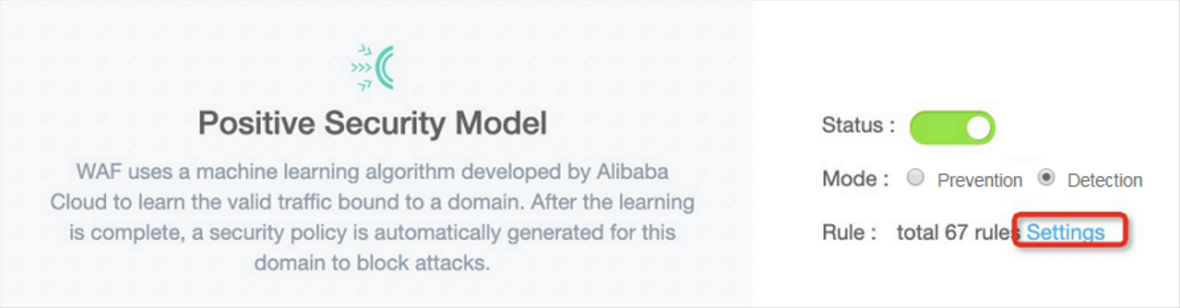
If this is the first time that you have enabled the positive security model for your domain, WAF automatically uses historical network traffic data and deep learning to train machine learning models. WAF then generates security rules to protect your domain.

Note:
The entire machine learning process may be time-consuming depending on the total amount of the network traffic data. Typically it takes up to one hour for WAF to complete learning and generating security rules. After WAF completes learning, you will receive an internal message, SMS message, and email.

5. After the machine learning process is complete, click **Settings** in the **Positive Security Model** area to check the generated security rules.

Note:
By default, the positive security model is set to the Detection mode. This mode only reports requests that fail to match the security rules. These requests are not blocked. Before you set the mode to Prevention, we recommend that you go to the Reports page and check the statistics for a period of time to make sure that the security rule does not incur any false positives.

For security rules in Prevention mode to block malicious requests, you must first set the protection mode of the positive security model to Prevention. When the positive security model is set to Detection, even if your security rules are set to Prevention, malicious requests are not blocked.



Positive Security Model

WAF uses a machine learning algorithm developed by Alibaba Cloud to learn the valid traffic bound to a domain. After the learning is complete, a security policy is automatically generated for this domain to block attacks.

Status :

Mode : ○ Prevention ● Detection

Rule : total 67 rules Settings

6. Optional: In the security rules list, click **Edit** in the Actions column to edit the protection mode of a security rule generated by the positive security model. Click **Delete** to delete a security rule.

Note:
To ensure that the positive security model is protecting your domain efficiently, we recommend that you do not modify or delete security rules. Before you set a security rule to **Prevention**, set it to **Detection**, go to the WAF security reports page, and make sure that the security rule does not incur any false positives.

Fields of security rules

Note:
Currently, you can only change the **Protection Mode** field for a security rule.

Field	Description
Rule name	The name of the security rule.
Mode	Specifies the URL of HTTP requests. Request parameters are excluded. For example, for URL /index.php? a = 122, enter /index.php into this field. Security rules generated by the positive security model use regular expressions to match requests.
Method	Specifies the methods of HTTP requests. You can specify one or more methods.

Field	Description
Parameters	Specifies the request parameters in the URL. For example, the URL `/index.php? a =122` contains the parameter a. The value of the parameter is 122. Security rules generated by the positive security model use regular expressions to match requests.
Protection Mode	The protection mode of the security rule. Valid values: • **Prevention**: Before you set a security rule to Prevention to filter network traffic, you must set the mode of the positive security model to Block. Otherwise, the security rule does not block malicious requests. • **Detection**: If a security rule is set to this mode, malicious requests are only reported. You can check the detailed information about malicious requests on the Reports page. **Note:** We recommend that you set the mode of a newly added rule to Detection and then check the statistics on the Reports page for a period of time. Make sure that the security rule does not incur any false positives before you set the rule to Prevention.

2.15 Account security

WAF supports the account security feature that detects account risks. This feature monitors endpoints related to user authentication, such as registration and logon endpoints, and detects events that may pose a threat to user credentials. Detectable risks include credential stuffing, brute-force attacks, account registration launched by bots, weak password sniffing, and SMS interface abuse. To use the account security feature, add endpoints that need to be monitored to WAF. You can view detection results in WAF security reports.

Context

- Before you enable account security, obtain the endpoint information that is required for configuration. For example, you must provide the domain name, the URL where user credentials are submitted, and the parameters that specify the username and password.
- The business is protected by WAF. For more information, see Website configuration.

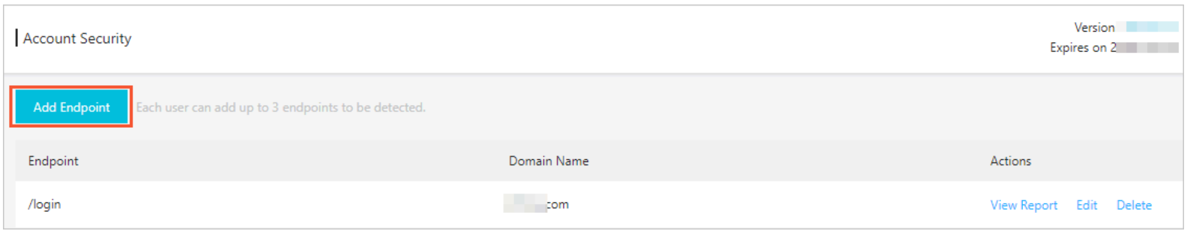
Limits

Each WAF instance supports up to three endpoints.

Add an endpoint

1. Log on to the WAF console.
2. In the upper-left corner, select the region where the WAF instance is deployed. You can select **Mainland China** or **International**.
3. In the left-side navigation pane, choose **Management** > **Account Security**.
4. On the **Account Security** page, click **Add Endpoint**.

> **Note:**
> Each WAF instance supports up to three endpoints. If the number of endpoints has reached the upper limit, the **Add Endpoint** icon turns grey, which indicates that you cannot add more endpoints.



Account Security

Version

Expires on 2

Each user can add up to 3 endpoints to be detected.

Endpoint	Domain Name	Actions
/login	com	View Report Edit Delete

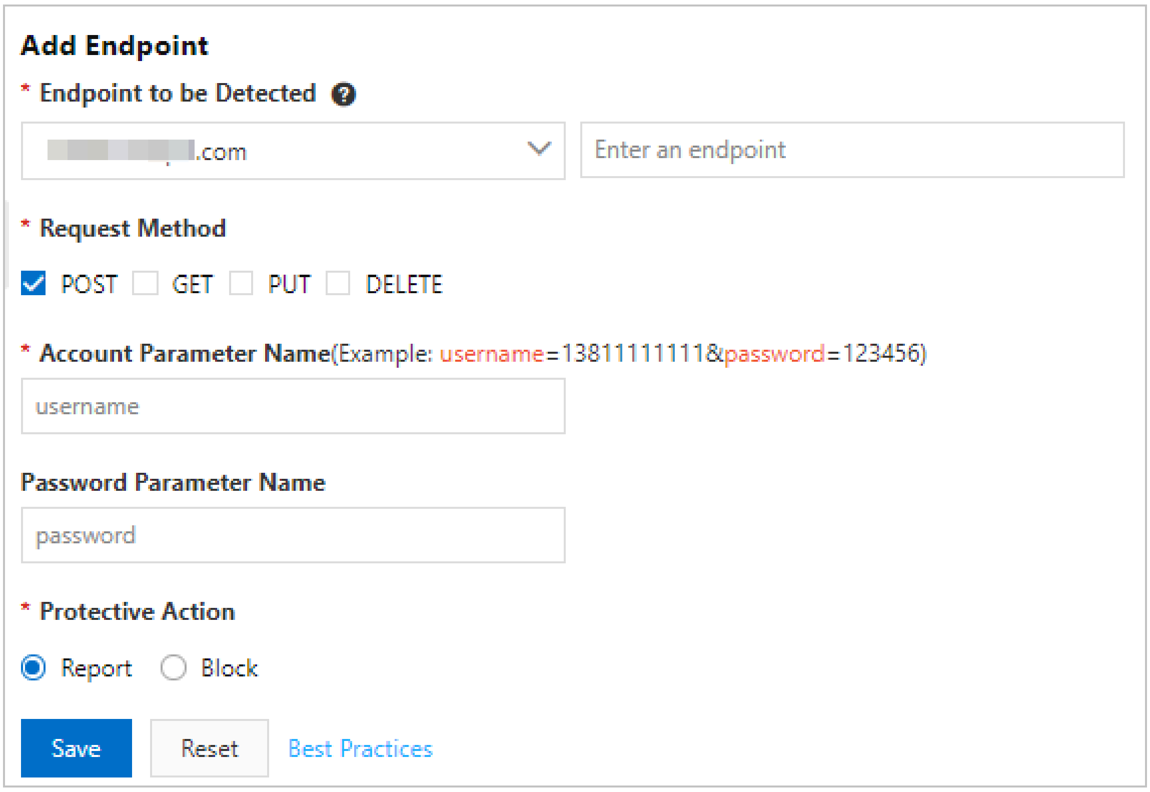
5. In the **Add Endpoint** dialog box that appears, set the parameters, and then click **Save**. The following table lists the parameters and descriptions.

Parameter	Description
Endpoint to be Detected	Select the domain name that needs to be monitored by WAF, and enter the URI where user credentials are submitted. Do not enter the endpoint where users log on, for example, /login.html. Enter the endpoint where usernames and passwords are submitted.
Account Parameter Name	Enter the parameter that specifies usernames.

Parameter	Description
Password Parameter Name	Enter the parameter that specifies passwords. If passwords are not required on the endpoint, do not set this parameter.

Sample configuration

- For example, the logon endpoint is /login.do, and the body of the submitted POST request is username=Jammy&pwd=123456. In this case, you must set **Account Parameter Name** to username and **Password Parameter Name** to pwd, as shown in the following figure.



Add Endpoint

* Endpoint to be Detected

[redacted].com | Enter an endpoint

* Request Method

☑ POST □ GET □ PUT □ DELETE

* Account Parameter Name(Example: username=13811111111&password=123456)

username

Password Parameter Name

password

* Protective Action

● Report ○ Block

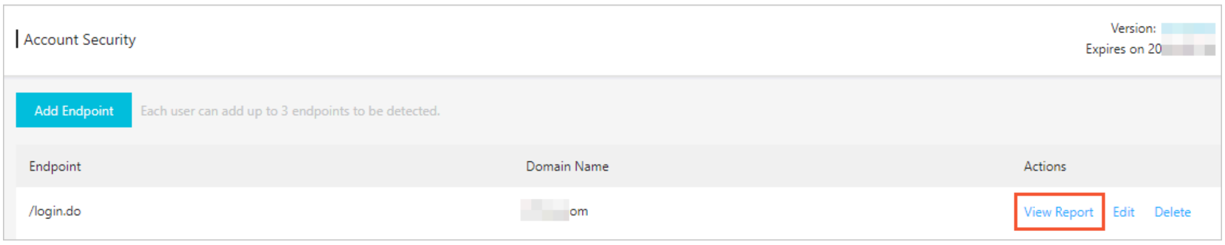
- If the parameters that specify user credentials are included in the URL of a GET request, for example, /login.do? username=Jammy&pwd=123456, set the parameters as shown in the preceding figure.
- If passwords are not required on the endpoint, for example, a registration endpoint, set the **Account Parameter Name** parameter. Do not set the **Password Parameter Name** parameter.
- If phone numbers are used as user credentials on the endpoint, enter the parameter that specifies phone numbers in the Account Parameter Name field. For example, the URL is /sendsms.do? mobile=13811111111. In this case, you must set **Endpoint**

to be Detected to /sendsms.do and **Account Parameter Name** to mobile. Do not set **Password Parameter Name**.

The endpoint is added. After the endpoint is added, WAF automatically dispatches detection tasks. If the network traffic of the endpoint meets the detection conditions, account risks are reported within a few hours.

View account security reports

To view account security reports, navigate to the **Account Security** page, find the target endpoint, and then click **View Report** in the Actions column. You can also view security reports on the **Reports** page.

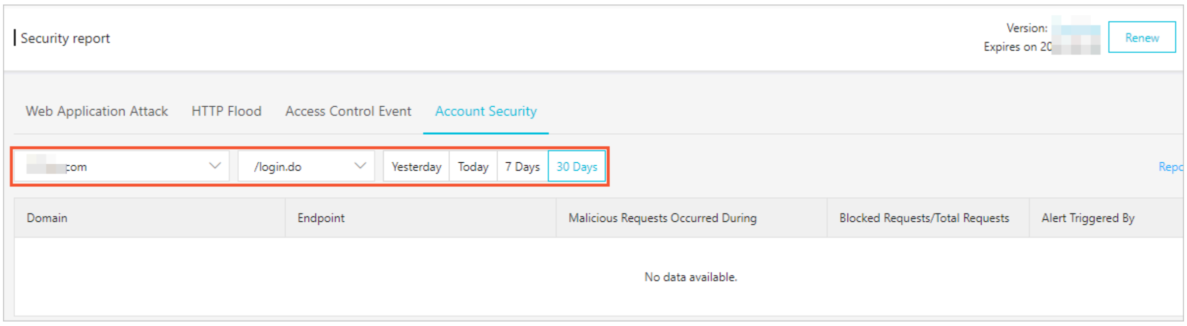


Each user can add up to 3 endpoints to be detected.

Endpoint	Domain Name	Actions
/login.do	[redacted]om	View Report Edit Delete

The following procedure shows how to view security reports on the **Reports** page.

1. Log on to the WAF console.
2. In the upper-left corner, select the region where the WAF instance is deployed. You can select **Mainland China** or **International**.
3. In the left-side navigation pane, choose **Reports** > **Reports**.
4. On the **Account Security** tab, select the domain, endpoint, and time period (**Yesterday**, **Today**, **Last 7 Days**, or **Last 30 Days**) to view detected account risks.



Domain	Endpoint	Malicious Requests Occurred During	Blocked Requests/Total Requests	Alert Triggered By

No data available.

The following table lists the fields and descriptions in an account security report.

Field	Description
Endpoint	The URI where account risks are detected by WAF.
Domain	The domain to which the endpoint belongs.

Field	Description
Malicious Requests Occurred During	The time period during which account risks are detected.
Blocked Requests	The number of requests blocked by WAF protection rules during the time period displayed in the **Malicious Requests Occurred During** column. WAF protection rules indicate all the protection rules that are currently effective, including Web application protection rules, HTTP ACL policies, HTTP flood protection rules, and blocked regions. The proportion of the blocked requests reflects the account security status of the endpoint.
Total Requests	The total number of requests sent to the endpoint during the time period displayed in the **Malicious Requests Occurred During** column.
Alert Triggered By	The reason why the alert is triggered. Possible reasons include: • A request fits the behavior model of credential stuffing or brute-force attacks. • The traffic baseline of the endpoint is exceeded during the displayed time period. • A large number of requests sent to the endpoint fit the rules described in the threat intelligence library during the displayed time period. • Weak passwords are detected in a large number of requests sent to the endpoint during the displayed time period. In this case, credential stuffing and brute-force attacks may occur.

Additional information

The account security feature only detects account risks. Due to the variation of businesses and technologies, we recommend that you choose security services based on your actual business requirements to better safeguard your business. For more information, see Account security best practices.

3 WAF security reports

Alibaba Cloud WAF provides security reports for you to view and understand all protection actions of WAF. You can view the attack protection and risk warning statistics.

Background information

Alibaba Cloud WAF security reports include attack protection report and risk warning report.

- The attack protection report gives you an overall view of all Web application attacks, HTTP flood attacks, and HTTP ACL events.
- The risk warning report records and summarizes common attacks that occur on your network assets, and provides you with risk warning information. You can view the following risk warnings: known hacker attack, WordPress attack, suspected attack, robots script, crawler access, and SMS abuse.

Procedure

Follow these steps to view WAF security reports:

1. Log on to the Alibaba Cloud WAF console.
2. Go to the **Reports** > **Reports** page.
3. Go to the **Attack Protection** or **Risk Warning** tab page to view the corresponding report.

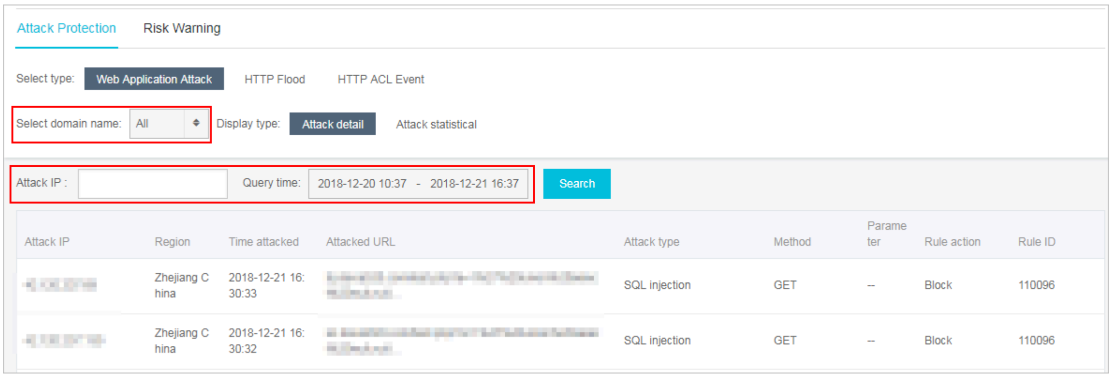
   - View attack protection report

     On the **Attack Protection** tab page, select the attack type to view the detailed records. You can view the following records:

     - **Web Application Attack**: displays records of all Web attacks inspected by WAF. You can filter the records based on domain names, attack IP addresses, and attack time.

       Note:

For more information about web attack protection, see Web application attack protection.



Attack Protection Risk Warning

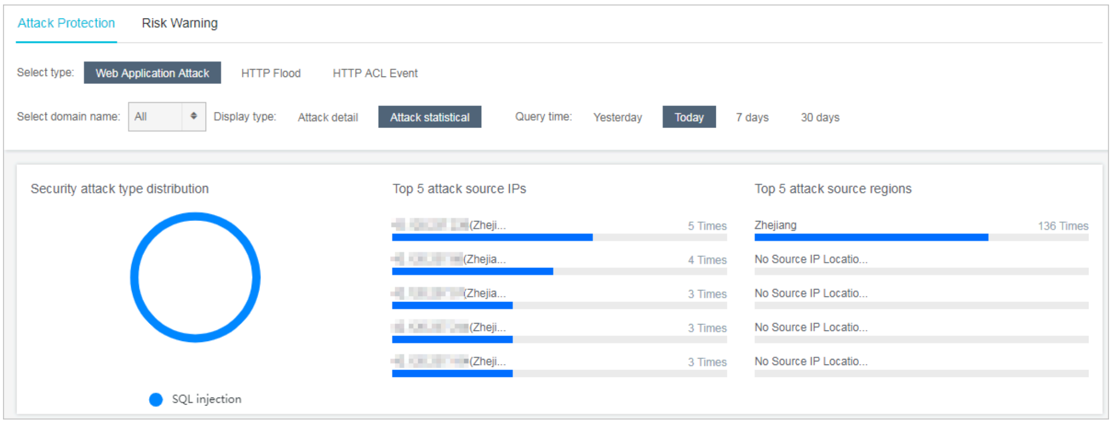
Select type: Web Application Attack HTTP Flood HTTP ACL Event

Select domain name: All Display type: Attack detail Attack statistical

Attack IP : Query time: 2018-12-20 10:37 - 2018-12-21 16:37 Search

Attack IP	Region	Time attacked	Attacked URL	Attack type	Method	Parameter	Rule action	Rule ID
[redacted]	Zhejiang China	2018-12-21 16:30:33	[redacted]	SQL injection	GET	--	Block	110096
[redacted]	Zhejiang China	2018-12-21 16:30:32	[redacted]	SQL injection	GET	--	Block	110096

By default, the records are displayed in details. You can also view the attack statistics. Attack statistics displays the distribution of security attack types, top 5 attacker source IP addresses, and top 5 attacker source regions.



Attack Protection Risk Warning

Select type: Web Application Attack HTTP Flood HTTP ACL Event

Select domain name: All Display type: Attack detail Attack statistical Query time: Yesterday Today 7 days 30 days

Security attack type distribution

● SQL injection

Top 5 attack source IPs

[redacted](Zheji...	5 Times
[redacted](Zhejia...	4 Times
[redacted](Zhejia...	3 Times
[redacted](Zheji...	3 Times
[redacted](Zheji...	3 Times

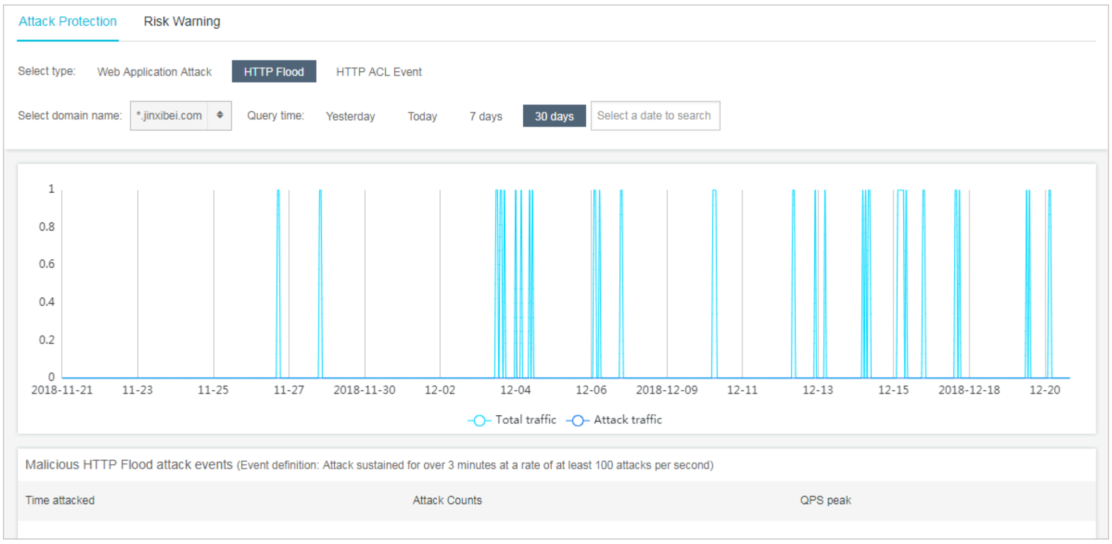
Top 5 attack source regions

Zhejiang	136 Times
No Source IP Locatio...	
No Source IP Locatio...	
No Source IP Locatio...	
No Source IP Locatio...	

- **HTTP Flood**: displays the records of HTTP flood attacks inspected by WAF. You can select the domain name and query time to view the corresponding records.

Note:

For more information about HTTP flood attack protection, see HTTP flood protection.



Select type: HTTP Flood

Select domain name: *.jinxibei.com

Query time: 30 days

Malicious HTTP Flood attack events (Event definition: Attack sustained for over 3 minutes at a rate of at least 100 attacks per second)

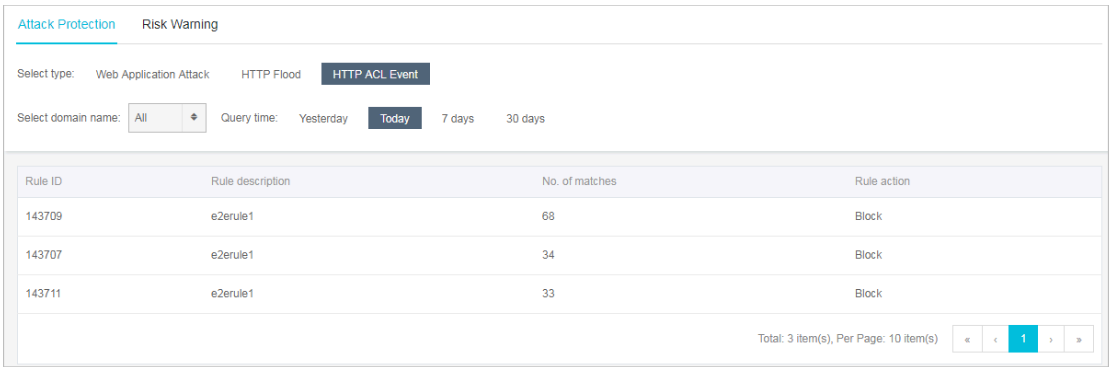
Time attacked	Attack Counts	QPS peak

The real-time total QPS and attack QPS records are displayed at the top of the page, and all HTTP flood events are displayed at the bottom of the page. Alibaba Cloud WAF defines the HTTP flood attack as follows: attack duration > 3 minutes and attack frequency (per second) > 100.

- **HTTP ACL Event**: displays the ACL events for a domain name. You can select the domain name and query time to view the corresponding records.

Note:

For more information about the HTTP ACL events, see HTTP ACL events.



Select type: HTTP ACL Event

Select domain name: All

Query time: Today

Rule ID	Rule description	No. of matches	Rule action
143709	e2erule1	68	Block
143707	e2erule1	34	Block
143711	e2erule1	33	Block

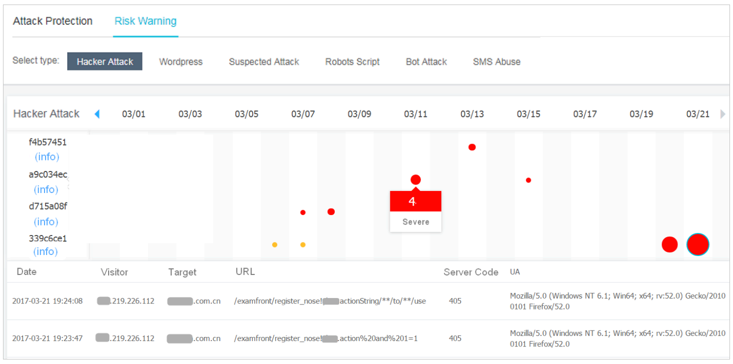
Total: 3 item(s), Per Page: 10 item(s)

- View risk warning report

  On the **Risk Warning** tab page, select a risk type to view details. You can view the following risk records:

  - **Hacker attack**

    Risk warning provides the hacker profiling function based on Alibaba Cloud big data analytics and the attack source tracing capability. This function identifies and records the malicious behaviors and activities of recognized hackers on your website. These behaviors include footprints, scans, and attacks. A hacker can be an individual or it can be a group of hackers, with real identities. When you receive such alarms, it means your website is hacked by a known hacker.



Date	Visitor	Target	URL	Server Code	UA
2017-03-21 19:24:08	[redacted].219.226.112	[redacted].com.cn	/examfront/register_nose![redacted]actionString/**/to/**/use	405	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
2017-03-21 19:23:47	[redacted].219.226.112	[redacted].com.cn	/examfront/register_nose![redacted].action%20and%201=1	405	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0

Dots in the figure indicate the activity of hackers on the corresponding date. Click a specific dot to view the detailed attack record. Here,

- Different lines stand for different hackers. Click hacker information to view the characteristics of the hacker.
- The severity of the hazard is gauged by the color of the dot. Darker the color, more severe is the hazard.
- The size of the dots indicates the frequency of attacks during the day. Bigger dots indicate more attacks and smaller dots, lesser attacks.

Defense: The attack displayed in the report is intercepted by WAF. You do not need to worry about it. We recommend that you pay attention to non-web services security on the server because the hackers may try various options (for example, SSH and database port) to penetrate into your website.

- **Wordpress**

Risk warning detects WordPress attacks according to attack features described in Prevent WordPress bounce attacks. If the number of such warnings keeps increasing, your server may encounter this kind of HTTP Flood attacks these days.

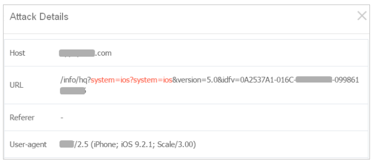
Defense: Configure HTTP flood protection according to the defense suggestions provided in the preceding document.

- **Suspected attack**

Based on the exception detection algorithm of big data analytics, WAF screens suspicious access requests, which may include abnormal parameter names, types

, sequences, special symbols, and statements, for you to perform further analysis and provide protection based on service features.

The risk warnings highlight the abnormal portion. For example, the request shown in the following figure includes two repeated parameters and is not connected with the conventional “&” symbol.



Attack Details

Host	[redacted].com
URL	/info/hq?system=ios?system=ios&version=5.0&idfv=0A2537A1-016C-[redacted]-099861 [redacted]
Referer	-
User-agent	[redacted]/2.5 (iPhone; iOS 9.2.1; Scale/3.00)

Defense: The alarm here reports a suspicious request, which may be a normal request of a special service or a variant attack. Analyze the alarm based on features of your service.

- **Robot Script**

  WAF supports detecting features of common machine script tools, such as Python2.2 and HttpClient. If you have not submitted a large number of requests through the test tool recently, the alarm number indicates the number of malicious requests received or detected from some machine script tools. It may also include the tools used to test the traffic pressure or initiate HTTP flood attacks.

  Defense: Check whether HTTP flood attacks exist by analyzing logs and intercept malicious attacks based on protection algorithms such as HTTP ACL Policy, HTTP flood protection emergency mode, and blocked region.

- **Bot Attack**

  WAF supports detecting crawler requests (including valid crawlers such as Baidu spider). If the number of this alarms is high, the number of requests increases abnormally on the server, and the CPU usage increases, the website may encounter malicious crawler requests or HTTP flood attacks that are masqueraded as crawlers.

  Defense: Based on logs and server performance analysis, check whether HTTP flood attacks or malicious crawler requests exist. For more information, see

Intercept malicious crawlers. WAF does not incept valid crawler (for example, Baidu crawler) requests.

- **SMS Abuse**

  WAF supports detecting requests on interfaces such as the short message registrati on interface and short message verification interface. If you receive more alarms , your short message interface is being abused (causing high short message overhead).

  Defense: Click **View Details** to view specific requests. You can analyze whether the invocation is normal service invocation based on the source IP address and interface to which most requests are sent. If not, we recommend that you use Data Risk Control and Custom HTTP flood protection to protect the abused interfaces.

4 API reference

4.1 Legacy engine

4.1.1 API overview

This topic describes the API operations provided by Web Application Firewall (WAF).

instance information

Name	Description
DescribeRegions	You can call this operation to query the regions supported by WAF.
DescribePayInfo	You can call this operation to query the information of the WAF instance in a specified region.
DescribeWafSourceIpSegment	Queries DescribeWafSourceIpSegment CIDR blocks of the WAF instance.

Domain configurations

Name	Description
DescribeDomainNames	You can call this operation to obtain a list of domains that have been added to a specified WAF instance.
DescribeDomainConfig	You can call this operation to query the forwarding configurations of a specified domain name.
DescribeDomainConfigStatus	You can call this operation to query whether the forwarding configuration of a specified domain name takes effect.
CreateDomainConfig	Adds CreateDomainConfig domain name configuration information.
ModifyDomainConfig	You can call this operation to modify the configuration of a specified domain name.
DeleteDomainConfig	You can call this operation to delete the configurations of a specified domain name.
CreateCertAndKey	You can call this operation to upload CreateCertAndKey and private key information for a specified domain configurat ion record.

Configure Web attack protection

Name	Description
ModifyWafSwitch	Call the ModifyWafSwitch API to enable or disable Web attack protection.

Configure access control list

Name	Description
CreateAclRule	Adds an HTTP-based ACL rule for a specified domain.
DeleteAclRule	Deletes a specified ACL rule.
ModifyAclRule	Modifies a specified ACL rule.
DescribeAclRules	You can call this operation to query the list of precise access control rules for a specified domain name.

Asynchronous task information

Name	Description
DescribeAsyncTaskStatus	You can call this operation to query the DescribeAs yncTaskStatus of a WAF task.

4.1.2 Request method

To send a Web Application Firewall (WAF) API request, you must send an HTTP GET request to the WAF endpoint. You must add the request parameters that correspond to the API operation being called. After you call the API, the system returns a response. The request and response are encoded in UTF-8.

Request syntax

WAF API operations use the RPC protocol. You can call WAF API operations by sending HTTP GET requests.

The request syntax is as follows:

```
https://Endpoint/?Action=xx&Parameters
```

In the request:

- **Endpoint**: The endpoint of the WAF API is wafopenapi.cn-hangzhou.aliyuncs.com.
- **Action**: The operation that you want to perform. For example, to obtain a list of the domains added to WAF, you must set the Action parameter to **DescribeDomainNames**.

- **Version**: The version of the API to be used. The current WAF API version is 2018-01-17.
- **Parameters**: The request parameters for the operation. Separate multiple parameters with ampersands (&).

  Request parameters include both common parameters and operation-specific parameters. Common parameters include the API version and authentication information. For more information, see Common parameters.

The following example demonstrates how to call the **DescribeDomainNames** operation to obtain a list of the domains added to WAF.

Note:

To improve readability, the API request is displayed in the following format:

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Format=xml
&Version=2018-01-17
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
...
```

API authorization

To ensure the security of your account, we recommend that you call the WAF API as a RAM user. To call the WAF API as a RAM user, you must create an account for the RAM user and grant the account required permissions.

Signature method

You must sign all API requests to ensure security. WAF uses the request signature to verify the identity of the API caller.

WAF implements symmetric encryption with an AccessKey pair to verify the identity of the request sender. An AccessKey pair is an identity credential issued to Alibaba Cloud accounts and RAM users that is similar to a logon username and password. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. The AccessKey ID is used to verify the identity of the user, while the AccessKey secret is used to encrypt and verify the signature string. You must keep your AccessKey secret strictly confidential.

You must add the signature to the Cloud Firewall API request in the following format:

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=
CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-
4e0ad82fd6cf
```

Take the **DescribeDomainNames** operation as an example. If the AccessKey ID is `testid` and the AccessKey secret is `testsecret`, the original request URL is as follows:

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2018-01-17
&SignatureVersion=1.0
```

Perform the following operations to calculate the signature:

1. Use the request parameters to create a string-to-sign:

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeDomainNames&Region%3Dcn
&InstanceId%3Dwaf_elasticity-cn-0xldbqtm005&Format%3DXML&SignatureMethod
%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&
SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A46%253A24Z&Version
%3D2018-01-17
```

2. Calculate the HMAC value of the string-to-sign.

   Add an ampersand (&) to the end of the AccessKey secret, and use the result as the key to calculate the HMAC value. In this example, the key is `testsecret&`.

```
CT9X0VtwR86fNWSnsc6v8YGOjuE=
```

3. Add the signature to the request parameters:

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2018-01-17
&SignatureVersion=1.0
```

```
&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

4.1.3 Common parameters

Common request parameters

Common request parameters must be included in all WAF API requests.

Table 4-1: Common request parameters

Parameter	Type	Require	Description
Region	String	Yes	The ID of the region to which the WAF instance belongs. Set the value to: • CN: indicates mainland China. • cn-hongkong: indicates the overseas region.
InstanceId	String	Yes	The ID of the WAF instance. **Note:** You can call **DescribePayInfo** to view your WAF instance ID.
Format	String	No	The format in which to return the response. Valid values: • JSON (default) • XML
Version	String	Yes	The version number of the API, in the format of YYYY-MM-DD. Set the value to: 2018-01-17
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud
Signature	String	Yes	The signature string in the API request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to HMAC-SHA1
Timestamp	String	Yes	The UTC time when the request is signed. Specify the time in the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format. The time must be in UTC. For example, 20:00:00 on January 10, 2013 in China Standard Time (UTC +8) is written as 2013-01-10T12:00:00Z.

Parameter	Type	Require	Description
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to 1.0.
SignatureNonce	String	Yes	A unique, random number used to prevent replay attacks. You must use different numbers for multiple requests.
ResourceOwnerAccount	String	No	The account that owns the resource to be accessed by the current request.

Sample requests

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2018-01-17
&SignatureVersion=1.0
&Signature=Signature
```

Common response parameters

API responses use the HTTP response format where a 2xx status code indicates a successful call and a 4xx or 5xx status code indicates a failed call. Response data can be returned in either the JSON or XML format. You can specify the response format when you are making the request. The default response format is XML.

Every response returns a unique **RequestId** (request ID) regardless of whether the call is successful.

- XML format

```
<?xml xml version="1.0" encoding="utf-8"? >
   <!--Result Root Node-->
   <Operation Name+Response>
      <!-Return Request Tag-->
      <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
      <!-Return Result Data-->
   </Operation Name+Response>
```

- JSON format

```
{
    "RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
    /*Return Result Data*/
    }
```

4.1.4 Call examples

When you call a WAF API, an HTTP GET request is sent to the WAF API end point. You must add the Web Application Firewall in the request based on the API operation description. After the call, the system returns a response.

The following Python Sample code demonstrates how to add common parameters and interface request parameters, how to use request parameters to construct a canonicalized query string, how to construct a StringToSign string, and how to obtain an OpenAPI server address. The system sends an HTTP request by using the Get method to obtain the response .

Download the Python Sample code

Note:

To use the following examples, you need to replace common request parameters and request parameters in request parameters examples.

Define common parameters

```
#! /usr/bin/env python
# -*- coding: utf-8 -*-
import hashlib
import urllib
import requests
import hmac
import random
import datetime
import sys

class OpenAPI(object):
    def __init__(self, signature_version='1.0', api_url=None, ak=None, sk=None, api_version
=None):
        assert api_url is not None
        assert ak is not None
        assert sk is not None
        assert api_version is not None

        self.signature_once = 0
        self.signature_method = 'HMAC-SHA1'
        self.signature_version = signature_version
        self.api_version = api_version
        self.format = 'json'
        self.signature_method = 'HMAC-SHA1'
        self.api_url = api_url
        self.access_key = ak
        self.access_secret = sk
    def __gen_common_params(self, req_type, api_version, access_key, access_secret,
http_params):
        while 1:
            rand_int = random.randint(10, 999999999)
            if rand_int! =self.signature_once:
                self.signature_once = rand_int
                break

        # Indicates whether the current step contains the AccessKey parameter.
        if access_key == None:
            return None

        http_params.append(('AccessKeyId', access_key))
        http_params.append(('Format', self.format))
        http_params.append(('Version', api_version))
        timestamp = datetime.datetime.utcnow().strftime("%Y-%m-%dT%H:%M:%SZ")
        http_params.append(('Timestamp', timestamp))
        http_params.append(('SignatureMethod', self.signature_method))
        http_params.append(('SignatureVersion', self.signature_version))
        http_params.append(('SignatureNonce', str(self.signature_once)))
        # Signature
        http_params = self.sign(req_type, http_params, access_secret)
        return urllib.urlencode(http_params)

    def get(self, http_params=[], host=None, execute=True):
        data = self.__gen_common_params('GET', self.api_version, self.access_key, self.
access_secret, http_params)
        api_url = self.api_url

        if data == None:
            url = "%s" % (api_url)
        else:
            url = "%s/? " % api_url + data
        print ("URL: %s"%url)
        if execute is False:
            return url
        ret = {}
        try:
            if host is not None:
                response = requests.get(url,headers={'Host':host}, verify=False)
            else:
                response = requests.get(url, verify=False)
            ret['code'] = response.status_code
            ret['data'] = response.text
        except Exception as e:
            ret['data'] = str(e)

        return ret

    def __get_data(self, http_params):
        params = self.__gen_common_params('POST', self.api_version, self.access_key, self.
access_secret, http_params)
        if params == []:
            data = None
        else:
            data = params.replace("+", "%20")
            data = data.replace("*", "%2A")
            data = data.replace("%7E", "~")
        return data

    def post(self, http_params=[], out_fd=sys.stdout):
        data = self.__get_data(self.api_version, self.access_key, self.access_secret,
http_params)
        api_url = self.api_url
        out_fd.write(u"[%s] --> (POST):%s\n%s\n" % (datetime.datetime.now(), api_url, data
))
        ret = requests.post(api_url, data, verify=False)
        print (ret.text)
        return ret

    def sign(self, http_method, http_params, secret):
        list_params = sorted(http_params, key=lambda d: d[0])
        # print list_params
        url_encode_str = urllib.urlencode(list_params)
        # print url_encode_str
        url_encode_str = url_encode_str.replace("+", "%20")
        url_encode_str = url_encode_str.replace("*", "%2A")
        url_encode_str = url_encode_str.replace("%7E", "~")
        string_to_sign = http_method + "&%2F&" + urllib.quote(url_encode_str)
        # print string_to_sign
        hmac_key = str(secret + "&")
        sign_value = str(hmac.new(hmac_key, string_to_sign, hashlib.sha1).digest().encode
('base64').rstrip())
        http_params.append(('Signature', sign_value))
        return http_params
```

Generate an API call request

Note:

The following code example is used to call the **ModifyWafSwitch** example: enable Web application protection through the API.

```
from open_api import OpenAPI

class Waf(OpenAPI):
    def __init__(self, api_url, ak, sk, api_version, instance_id, region):

        super(Waf, self).__init__(api_url=api_url, ak=ak, sk=sk, api_version=api_version)
        self.instance_id = instance_id
        self.region = region

    def ModifyWafSwitch(self,domain, instance_id=None, region='cn', service_on=1,
execute=True):
        if instance_id is None:
            instance_id = self.instance_id
        if region is None:
            region = self.region

        params = [
            ('Action', 'ModifyWafSwitch'),
            ('InstanceId', instance_id),
            ('Domain', domain),
            ('Region',region),
            ('ServiceOn', service_on)
        ]

        print (params)

        return self.get(http_params=params,execute=execute)

if __name__ == "__main__":
    api_url = "https://wafopenapi.cn-hangzhou.aliyuncs.com"
    # Enter the accesskey ID of your account
    ak = ""
    # Enter the AccessKeyScecret information of your account.
    sk = ""
    # Enter the ID of your WAF instance. You can obtain the instance ID by calling the
GetPayInfo operation.
    instance_id = ""
    # Enter the region information of your WAF instance.
    region = ""
    api_version = "2018-01-17"

    t = Waf(api_url=api_url, ak=ak, sk=sk, api_version=api_version, instance_id=instance_id
, region=region)
    print (t.ModifyWafSwitch(domain="", service_on=1))
```

Send an HTTP GET request

You can use the preceding code to obtain an HTTP request and send the HTTP GET request to the WAF API endpoint.

Sample requests

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=ModifyWafSwitch&Domain=
www.aliyun.com&ServiceOn=1&Region=cn&InstanceId=waf_elasticity-cn-0xldbqtm005&
TimeStamp=2018-08-23T12:46:24Z&Format=JSON&AccessKeyId=testid&SignatureMethod
=HMAC-SHA1&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&Version=2018-
01-17&SignatureVersion=1.0&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

Get response results

Finally, a response is received from the WAF API server.

Sample responses

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
 "Result":{
   "Status":2,
   "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 }
}
```

4.1.5 Instance information

4.1.5.1 DescribePayInfo

You can call this operation to query the information of the WAF instance in a specified region.

Note:

You do not need to specify the **InstanceId** common request parameters.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribePayInfo	The operation that you want to perform. Valid values: **DescribePayInfo**.
InstanceSource	String	Yes	waf-cloud	The source of the instance. Default value: **waf-cloud**.
Region	String	Yes	cn	The ID of the region. Valid values: • **cn**: mainland China (default) • **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	Cost	The ID of the request.
Result			The returned result.
EndDate	Long	1512921600	The time when an instance expires. **Note:** For a pay-as-you-go instance, the trial period ends.

Parameter	Type	Example	Description
InDebt	Integer	1	Whether the current instance is overdue: • **0**: The instance has overdue payments. • **1**: indicates normal. **Note:** This parameter takes effect for pay-as-you-go WAF instances.
InstanceId	String	waf_elasticity-cn-0xldbqtm005	The ID of the instance whose type or storage space is modified.
PayType	Integer	env	The type of the WAF instance: • **0**: indicates that the ECS instance is not purchased or activated. • **1**: A subscription instance. • **2**: A pay-as-you-go instance.
Region	String	cn	Region: • **CN**: indicates mainland China. • **cn-hongkong**: indicates the overseas region.
RemainDay	Integer	0	The number of days before the trial period of the WAF instance expires. **Note:** This parameter is only valid for pay-as-you-go WAF instances.

Parameter	Type	Example	Description
Status	Integer	0	The status of the WAF instance. Valid values: • **0**: indicates that the API has expired. • **1**: indicates normal. **Note:** This parameter is only valid for WAF subscription instances.
Trial	Integer	0	Indicates whether this is a trial instance. Valid value: • **0**: false • **1**: true **Note:** This parameter is only valid for pay-as-you-go WAF instances.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribePayInfo
&Region=cn
&Common request parameters
```

Sample success responses

XML format

```
<DescribePayInfoResponse>
    <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
    <Result>
        <Status>1</Status>
        <Trial>0</Trial>
        <InstanceId>waf_elasticity-cn-0xldbqtm005</InstanceId>
        <InDebt>1</InDebt>
        <Region>cn</Region>
        <RemainDay>0</RemainDay>
        <PayType>2</PayType>
        <EndDate>1512921600</EndDate>
    </Result>
```

```
</DescribePayInfoResponse>
```

JSON format

```
{
 "Result":{
  "Status":1,
  "EndDate":1512921600,
  "Region":"cn",
  "InDebt":1,
  "Trial":0,
  "InstanceId":"waf_elasticity-cn-0xldbqtm005",
  "RemainDay":0,
  "PayType":2
 },
 "RequestId":"276D7566-31C9-4192-9DD1-51B10DAC29D2"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.5.2 DescribeRegions

You can call this operation to query the regions supported by WAF.

Note:

You do not need to specify the **Region** and **InstanceId** these two public request parameters.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribeRegions	The operation that you want to perform. Set the value to **DescribeRegions**.

Response parameters

Parameter	Type	Example	Description
Regions			The list of regions.

Parameter	Type	Example	Description
Region			The list of regions.
Display	String	ture	Indicates whether the WAF service is available in the specified region. • **true**: indicates yes. • **false**: indicates no.
Region	String	cn	The region ID.
RequestId	String	Cost	The ID of the request.

Samples

Sample request

```

https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeRegions
&Common request parameters
```

Sample success responses

XML format

```
<DescribeRegionsResponse>
    <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
    <Regions>
         <Region>
            <Region>cn</Region>
            <Display>true</Display>
        </Region>
        <Region>
            <Region>cn-hongkong</Region>
            <Display>true</Display>
        </Region>
    </Regions>
</DescribeRegionsResponse>
```

JSON format

```
{
 "RequestId":"276D7566-31C9-4192-9DD1-51B10DAC29D2",
 "Regions":{
  "Region":[
   {
    "region":"cn",
    "display":"true"
   },
   {
    "region":"cn-hongkong",
    "display":"true"
    }
   ]
  }
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.5.3 DescribeWafSourceIpSegment

Queries DescribeWafSourceIpSegment CIDR blocks of the WAF instance.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribeWafSourceIpSegment	The operation that you want to perform. Valid values: **DescribeWafSourceIpSegment**.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
Ips	String	121.43.18.0/24, 120.25.115.0/24, 101.200.106.0/24	The CIDR blocks used by WAF. Separate the CIDR blocks with commas (,).
RequestId	String	9087 ADDC-9047-4D02-82A7-33021B58083C	The ID of the request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeWafSourceIpSegment
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Region=cn
& <Common request parameters>
```

Sample success responses

XML format

```
<DescribeWafSourceIpSegmentResponse>
    <Ips>121.43.18.0/24,120.25.115.0/24,101.200.106.0/24</Ips>
    <RequestId>9087ADDC-9047-4D02-82A7-33021B58083C</RequestId>
</DescribeWafSourceIpSegmentResponse>
```

JSON format

```
{
 "RequestId":"9087ADDC-9047-4D02-82A7-33021B58083C",
 "Ips":"121.43.18.0/24,120.25.115.0/24,101.200.106.0/24"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.6 Domain configuration

4.1.6.1 DescribeDomainNames

You can call this operation to obtain a list of domains that have been added to a specified WAF instance.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribeDomainNames	The operation that you want to perform. Set the value to **DescribeDomainNames**.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: - **cn**: mainland China (default) - **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	Cost	The ID of the request.
Result		rstest.cdn.com	The returned result. The structure is described as follows: - **DomainNames** A list of domain names that have been added. It is a string array.

Parameter	Type	Example	Description
DomainNames			The returned result. The structure is described as follows: • **DomainNames** A list of domain names that have been added. It is a string array.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Common request parameters
```

Sample success responses

XML format

```
<DescribeDomainNamesResponse>
    <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
    <Result>
        <DomainNames>rstest.cdn.com</DomainNames>
        <DomainNames>rstest1.cdn.com</DomainNames>
        <DomainNames>rstest2.cdn.com</DomainNames>
        <DomainNames>rstest3.cdn.com</DomainNames>
    </Result>
</DescribeDomainNamesResponse>
```

JSON format

```
{
 "Result":{
  "DomainNames":[
   "rstest.cdn.com",
   "rstest1.cdn.com",
   "rstest2.cdn.com",
   "rstest3.cdn.com"
  ]
 },
 "RequestId":"56B40D30-4960-4F19-B7D5-2B1F0EE6CB70"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.6.2 DescribeDomainConfig

You can call this operation to query the forwarding configurations of a specified domain name.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribeDomainConfig	The operation that you want to perform. Valid values: **DescribeDomainConfig**.
Domain	String	No	rstest.cdn.com	The domain name that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	Cost	The ID of the request.
Result			The returned result.

Parameter	Type	Example	Description
DomainConfig			Domain name configuration structure.
Cname	String	xxxxxxxxxxxxxxx. fakewaf.com	The WAF CNAME address.
ProtocolType	Integer	env	Protocol type: • **0**: indicates that HTTP is supported. • **1**: indicates that HTTPS is supported. • **2**: indicates that both HTTP and HTTPS are supported.
SourceIps	String	1.1.1.1	The IP address of the origin server.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf. 2018071218 0229702.Y6re3d	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeDomainConfig
&Domain=www.aliyun.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Common request parameters
```

Sample success responses

XML format

```
<DescribeDomainConfigResponse>
    <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
    <Result>
        <Status>2</Status>
        <DomainConfig>
            <ProtocolType>2</ProtocolType>
            <SourceIps>x.x.x.x</SourceIps>
            <SourceIps>x.x.x.x</SourceIps>
            <Cname>xxxxxxxxxxxxxx.fakewaf.com</Cname>
        </DomainConfig>
        <WafTaskId>aliyun.waf.20180712180229702.Y6re3d</WafTaskId>
    </Result>
</DescribeDomainConfigResponse>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712180229702.Y6re3d",
  "DomainConfig":{
   "Cname":"xxxxxxxxxxxxx.fakewaf.com",
   "ProtocolType":2,
   "SourceIps":[
    "x.x.x.x",
    "x.x.x.x"
   ]
  }
 },
 "RequestId":"56B40D30-4960-4F19-B7D5-2B1F0EE6CB70"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.6.3 DescribeDomainConfigStatus

You can call this operation to query whether the forwarding configuration of a specified domain name takes effect.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribeDomainConfigStatus	The operation that you want to perform. Valid values: **DescribeDomainConfigStatus**.
Domain	String	No	rstest.cdn.com	The domain name that has been added to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: - **cn**: mainland China (default) - **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
DomainConfig			Domain name forwarding configuration structure.
ConfigStatus	String	1	Domain name forwarding configuration effective Status: - **0**: indicates that it does not take effect. - **1**: indicates that the alert has taken effect. - **-1**: indicates that the detection has not been completed.

Parameter	Type	Example	Description
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeDomainConfigStatus
&Domain=www.aliyun.com
&Common request parameters
```

Sample success responses

XML format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
<Result>
    <Status>2</Status>
    <DomainConfig>
        <ConfigStatus>1</ConfigStatus>
    </DomainConfig>
    <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
</Result>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a",
  "DomainConfig":{
   "ConfigStatus":1
  }
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.6.4 CreateDomainConfig

Adds CreateDomainConfig domain name configuration information.

To ensure Web application security when you add your domain name to WAF, perform the following steps:

1. Call CreateDomainConfig to add domain name configuration information.

2. Based on the information in the returned result **WafTaskId** value, call DescribeAsyncTaskStatus to view the execution progress of the configuration task for adding a domain name. When the task is completed, the domain name configuration information is added.

3. Call DescribeDomainConfigStatus to check whether the domain name configuration takes effect.

> **Note:**
> In the returned result, you can switch the business traffic to the WAF instance only after the configurations take effect.

4. Call DescribeDomainConfig to view the WAF CNAME address.

5. In the domain name DNS resolution service provider, modify the parsing records of the domain name, switch the business traffic to WAF.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	CreateDomainConfig	The operation that you want to perform. Valid values: **CreateDomainConfig**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
IsAccessProduct	Integer	Yes	0	Indicates whether a layer -7 proxy, such as anti-DDoS pro or CDN, has been configured for the domain name in front of the WAF instance. Valid values: • **0**: indicates none. • **1**: indicates yes.
Protocols	String	No	["http"]	The access protocol supported by the domain name. Valid values: • **HTTP**: indicates that HTTP is supported. • **HTTPS**: indicates that HTTPS is supported. • **http,https**: supports both HTTP and HTTPS.
SourceIps	String	Yes	["1.1.1.1"]	The origin IP address. Multiple IP addresses can be specified. Array type. Example values: ["1.1.1.1"].

Parameter	Type	Required	Example	Description
HttpPort	String	Yes	[80]	The HTTP ports. When multiple HTTP ports are specified, separate them with commas (,). Example value: [80]. **Note:** This parameter is required if the Protocols parameter is set to http. Default value: **80**. **HttpPort** and **HttpsPort** fill in at least one of the two request parameters.
HttpsPort	String	Yes	[443]	The HTTPS ports. When multiple HTTPS ports are specified, separate them with commas (,). Example value: [443]. **Note:** This parameter is required if the Protocols parameter is set to https. Default value: **443**. **HttpPort** and **HttpsPort** fill in at least one of the two request parameters.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: - **cn**: mainland China (default) - **cn-hongkong**: areas outside mainland China
LoadBalancing	String	Optional	0	The back-to-source SLB policy. Valid values: - **0**: represents IP Hash mode. - **1**: Round robin

Parameter	Type	Required	Example	Description
HttpToUserIp	String	Optional	0	Indicates whether to enable HTTP-based back-to-origin for HTTPS requests. Valid values: - **0**: Disabled (default) - **1**: indicates enabled **Note:** If your website does not support HTTPS back-to-origin, enable the HTTP back-to-origin feature (port 80 is selected by default) to enable HTTPS access through WAF.
HttpsRedirect	String	Optional	0	Specifies whether to redirect HTTP requests as HTTPS requests. Valid values: - **0**: Disabled (default) - **1**: indicates enabled **Note:** You need to specify this request parameter only if the Protocols parameter is set to https. After you enable this feature, HTTP requests are redirected to HTTPS port 443.
RsType	String	Optional	0	The origin address type of the domain name. Valid values: - **0**: indicates a back-to-origin IP address. - **1**Indicates the back-to-origin domain name.
ResourceGroupId	String	Yes	rs1234	The ID of the resource group.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result	Struct		The returned result.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.
Status	Integer	2	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=CreateDomainConfig
&Domain=www.aliyun.com
&SourceIps=["x.x.x.x","x.x.x.x"]
&Protocols=["http","https"]
&HttpPort=[80]
&HttpsPort=[443]
&RsType=0
&IsAccessProduct=0
&LoadBalancing=0
&HttpsRedirect=1
&HttpToUserIp=0
&Common request parameters
```

Sample success responses

XML format

```
<CreateDomainConfigResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
```

```
</CreateDomainConfigResponse>
```

JSON format

```
{
   "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
   "Result":{
      "Status":2,
      "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
   }
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.6.5 ModifyDomainConfig

You can call this operation to modify the configuration of a specified domain name.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	ModifyDomainConfig	The operation that you want to perform. Valid values: **ModifyDomainConfig**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.

Parameter	Type	Required	Example	Description
IsAccessProduct	Integer	Yes	0	Indicates whether a layer -7 proxy, such as anti-DDoS pro or CDN, has been configured for the domain name in front of the WAF instance. Valid values: - **0**: indicates none. - **1**: indicates yes.
Protocols	String	No	["http"]	The access protocol supported by the domain name. Valid values: - **HTTP**: indicates that HTTP is supported. - **HTTPS**: indicates that HTTPS is supported. - **http,https**: supports both HTTP and HTTPS.
HttpPort	String	Yes	[80]	The HTTP ports. When multiple HTTP ports are specified, separate them with commas (,). Example value: [80]. **Note:** This parameter is required if the Protocols parameter is set to http. Default value: **80**. **HttpPort** and **HttpsPort** fill in at least one of the two request parameters.

Parameter	Type	Required	Example	Description
HttpToUserIp	String	Optional	0	Indicates whether to enable HTTP -based back-to-origin for HTTPS requests. Valid values: • **0**: Disabled (default) • **1**: indicates enabled **Note:** If your website does not support HTTPS back-to-origin, enable the HTTP back-to-origin feature (port 80 is selected by default) to enable HTTPS access through WAF.
HttpsPort	String	Yes	[443]	The HTTPS ports. When multiple HTTPS ports are specified, separate them with commas (,). Example value: [443]. **Note:** This parameter is required if the Protocols parameter is set to https. Default value: **443**. **HttpPort** and **HttpsPort** fill in at least one of the two request parameters.
HttpsRedirect	String	Optional	1	The Https status. Set the value to: • **1:** Log backup is enabled. • **0**: Off (default)
LoadBalancing	String	Optional	0	The load balancing method. Valid values: • **0**:IP hash • **1**: Polling

Parameter	Type	Required	Example	Description
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: - **cn**: mainland China (default) - **cn-hongkong**: areas outside mainland China
SourceIps	String	Yes	["1.1.1.1"]	The origin IP address. Multiple IP addresses can be specified. Example: ["1.1.1.1"].

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
Status	Integer	env	Request execution status: - **0**: indicates that the request is pending execution. - **1**: indicates that the request is being executed. - **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=ModifyDomainConfig
&Domain=www.aliyun.com
&SourceIps=["x.x.x.x","x.x.x.x"]
&Protocols=["http","https"]
&HttpPort=[80]
```

```
&HttpsPort=[443]
&IsAccessProduct=0
&HttpsRedirect=1
&HttpToUserIp=0
&Common request parameters
```

Sample success responses

XML format

```
<ModifyDomainConfigResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</ModifyDomainConfigResponse>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.6.6 DeleteDomainConfig

You can call this operation to delete the configurations of a specified domain name.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DeleteDomainConfig	The operation that you want to perform. Valid values: **DeleteDomainConfig**.
Domain	String	No	rstest.cdn.com	The domain name that has been added to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DeleteDomainConfig
&Domain=www.aliyun.com
```

```
&Common request parameters
```

Sample success responses

XML format

```
<DeleteDomainConfigResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</DeleteDomainConfigResponse>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.6.7 CreateCertAndKey

You can call this operation to upload CreateCertAndKey and private key information for a specified domain configuration record.

Note:

You can also call this operation to update the uploaded certificate and private key for a specified domain.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	CreateCertAndKey	The operation that you want to perform. Valid values: **CreateCertAndKey**.

Parameter	Type	Required	Example	Description
Cert	String	No	----- BEGIN CERTIFICATE ----------END CERTIFICATE -----	The content of the certificate.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.
HttpsCertName	String	No	www.aliyun.com	The name of the certificate.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Key	String	No	----- BEGIN RSA PRIVATE KEY ----------END RSA PRIVATE KEY -----	Private key
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: - **cn**: mainland China (default) - **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.

Parameter	Type	Example	Description
Status	Integer	env	Request execution status: - **0**: indicates that the request is pending execution. - **1**: indicates that the request is being executed. - **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DeleteDomainConfig
&Domain=www.aliyun.com
&Cert="-----BEGIN CERTIFICATE----------END CERTIFICATE-----"
&Key="-----BEGIN RSA PRIVATE KEY----------END RSA PRIVATE KEY-----"
&HttpsCertName=www.aliyun.com
&Common request parameters
```

Sample success responses

XML format

```
<CreateCertAndKeyResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</CreateCertAndKeyResponse>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Errors

For a list of error codes, visit the API Error Center.

4.1.7 Configure web attack protection

4.1.7.1 ModifyWafSwitch

Call the ModifyWafSwitch API to enable or disable Web attack protection.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	ModifyWafSwitch	The operation that you want to perform. Valid values: **ModifyWafSwitch**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
ServiceOn	Integer	Yes	1	The Web attack protection switch . Valid values: - **0**: indicates closing. - **1**: indicates enabled.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: - **cn**: mainland China (default) - **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=ModifyWafSwitch
&Domain=www.aliyun.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&ServiceOn=1
&Common request parameters
```

Sample success responses

XML format

```
<ModifyWafSwitchResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</ModifyWafSwitchResponse>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Errors

For a list of error codes, visit the API Error Center.

4.1.8 Configure access control list

4.1.8.1 DescribeAclRules

You can call this operation to query the list of precise access control rules for a specified domain name.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribeAclRules	The operation that you want to perform. Valid values: **DescribeAclRules**.
CurrentPage	Integer	Yes	1	The number of the page to return. For example, to query the returned results on the first page, enter **1**.
Domain	String	No	www.aliyun.com	The domain that you want to add to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.

Parameter	Type	Required	Example	Description
PageSize	Integer	Yes	10	The number of entries returned per page.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
AclRules			The list of HTTP-based ACL rules. Each ACL rule is described as a sub-parameter of AclRule. The AclRule sub-parameter is a JSON string.
AclRule			The list of HTTP-based ACL rules. Each ACL rule is described as a sub-parameter of AclRule. The AclRule sub-parameter is a JSON string.

Parameter	Type	Example	Description
Action	Integer	1	The matching action of the rule. Valid values: - **0**: indicates blocking, that is, the access request is blocked if the matching condition of the rule is met. - **1**: allows the access request to pass, that is, the access request that meets the matching condition of the rule. - **2**: indicates an alert. That is, when the matched condition of the rule is matched, the access request is allowed, but the request is recorded and an alert is generated.
Conditions			The structure of rule matching conditions.
condition			The structure of rule matching conditions.

Parameter	Type	Example	Description
Contain	String	1	Logical operator: • **0**: indicates that the rule is not included. • **1**: indicates include. • **2**: indicates that it does not exist. • **10**: indicates a value that is not equal to the passed value. • **11**: indicates equal to. • **20**: indicates that the length is less than the specified value. • **21**: indicates a character with a length equal to the value of • **22**: indicates that the length is greater than. • **30**: indicates that the value is less than. • **31**: indicates that the value is equal to. • **32**: indicates a value greater than.
Key	String	url	The matching field. Valid values: IP , URL, Referer, User-Agent, Params, Cookie, Content-Type, X-Forwarded-For, Content-Length, Post-Body, Http-Method, and Header. **Note:** Note: WAF instances of different versions support different fields. You can view the supported fields in the Web Application Firewall console.
Value	String	login.	The matching content.
ContinueBlockGeo	Integer	1	Indicates whether to continue region blocking. Valid values: • **0**: false • **1**: true

Parameter	Type	Example	Description
ContinueCc	Integer	1	Indicates whether to proceed with the HTTP flood detection. Valid values: • **0**: false • **1**: true
ContinueDataRiskControl	Integer	1	Indicates whether to continue data risk control protection. Valid values: • **0**: false • **1**: true
ContinueSA	Integer	1	Indicates whether to perform the smart protection engine rule check. Valid values: • **0**: false • **1**: true
ContinueSdk	Integer	1	Indicates whether to continue SDK protection. Valid values: • **0**: no • **1**: true
ContinueWaf	Integer	1	Indicates whether to proceed with the Web attack protection rule detection. Valid values: • **0**: false • **1**: true
Id	Long	1111	The ID of the ACL rule.
IsDefault	Integer	1	Indicates whether the rule is a default rule. Valid values: • **0**: false • **1**: true
Name	String	test	The name of the rule.

Parameter	Type	Example	Description
Order	Integer	1	The order of the rules. **Note:** Note: the greater the value, the higher the priority of the rule.
Total	Interger	1	The total number of rules.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeAclRules
&Domain=www.aliyun.com
&CurrentPage=1
&PageSize=50
&Common request parameters
```

Sample success responses

XML format

```
<DescribeAclRulesResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <AclRules>
            <AclRule>
                <IsDefault>1</IsDefault>
                <Order>0</Order>
                <ContinueBlockGeo>1</ContinueBlockGeo>
                <Action>1</Action>
                <ContinueWaf>1</ContinueWaf>
                <ContinueSdk>0</ContinueSdk>
                <Id>16572</Id>
                <ContinueCc>1</ContinueCc>
                <Conditions>
                    <condition>
                        <key>URL</key>
                        <contain>1</contain>
                        <value>asfas</value>
                    </condition>
                </Conditions>
                <Name>default</Name>
                <ContinueDataRiskControl>1</ContinueDataRiskControl>
                <ContinueSA>1</ContinueSA>
            </AclRule>
        </AclRules>
        <Total>1</Total>
    </Result>
```

```
</DescribeAclRulesResponse>
```

JSON format

```
{
 "Result":{
  "AclRules":{
   "AclRule":[
    {
     "Name":"default",
     "Conditions":{
      "condition":[
       {
        "contain":1,
        "value":"asfas",
        "key":"URL"
       }
      ]
     },
     "ContinueDataRiskControl":1,
     "Action":1,
     "ContinueSdk":0,
     "ContinueWaf":1,
     "IsDefault":1,
     "Order":0,
     "Id":16572,
     "ContinueCc":1,
     "ContinueSA":1,
     "ContinueBlockGeo":1
    }
   ]
  },
  "Total":1
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.8.2 CreateAclRule

Adds an HTTP-based ACL rule for a specified domain.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	CreateAclRule	The operation that you want to perform. Valid values: **CreateAclRule**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.

Parameter	Type	Required	Example	Description
Rules	String	No	{"conditions":[{"key":"URL","contain":1,"value":"asfas"}],"continueComponent":{"post_action_cc":1,"post_action_waf":1,"post_action_sa":1,"post_action_block_geo":"0","post_action_data_risk_control":"1"},"action":"1","name":"lei123"}	The details of the HTTP-based ACL rule, in JSON format. The following table describes the structure. • **Id**: Optional. The ID of the rule. The value is of the Long type. • **Name**: the name of the rule. This parameter is required and of String type. • **Action** the matching action of the rule. This parameter is required and of Integer type. Valid values: - **0**: indicates blocking, that is, the access request is blocked if the matching condition of the rule is met. - **1**: allows the access request to pass, that is, the access request that meets the matching condition of the rule. - **2**: indicates an alert. That is, when the matched condition of the rule is matched, the access request is allowed, but the request is recorded and an alert is generated. • **ContinueComponent**: Optional. The String type. This parameter specifies whether to run other WAF protection policies in JSON format. The following table describes the structure. - **post_action_cc**(Optional) The Integer type. Specifies whether to proceed with the HTTP flood detection. Valid values: ■ **0**: false ■ **1**: true - **post_action_waf**(Optional)

Parameter	Type	Required	Example	Description
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China

Specifies the mapping between a field and logical operators.

Field	Logical operator
IP	Belongs to, does not belong to
Referer	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
User-Agent	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
Param	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
Cookie	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist
Content-Type	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
X-Forwarded-For	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist

Field	Logical operator
Content-Length	Value less than, value equal to, and value greater than
Post-Body	Contains, does not contain, equals, is not equal to
Http-Method	Equal to, not equal to
Header	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The GUID generated by Alibaba Cloud for the request.
Result			The returned result.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=CreateAclRule
&Domain=www.aliyun.com
&ServiceOn=1
&Rules={...}
```

```
&Common request parameters
```

Sample success responses

XML format

```
<CreateAclRuleResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</CreateAclRuleResponse>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.8.3 ModifyAclRule

Modifies a specified ACL rule.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	ModifyAclRule	The operation that you want to perform. Valid values: **ModifyAclRule**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.

Parameter	Type	Required	Example	Description
Rules	String	No	{"conditions":[{"key":"URL","contain":1,"value":"asfas"}],"continueComponent":{"post_action_cc":1,"post_action_waf":1,"post_action_sa":1,"post_action_block_geo":"0","post_action_data_risk_control":"1"},"action":"1","name":"lei123","id":65899}	The details of the HTTP-based ACL rule, in JSON format. The following table describes the structure. • **Id** the ID of the rule. Required. The ID is of the Long type. • **Name**: the name of the rule. This parameter is required and of String type. • **Action** the matching action of the rule. This parameter is required and of Integer type. Valid values: - **0**: indicates blocking, that is, the access request is blocked if the matching condition of the rule is met. - **1**: allows the access request to pass, that is, the access request that meets the matching condition of the rule. - **2**: indicates an alert. That is, when the matched condition of the rule is matched, the access request is allowed, but the request is recorded and an alert is generated. • **ContinueComponent**: Optional. The String type. This parameter specifies whether to run other WAF protection policies in JSON format. The following table describes the structure. - **post_action_cc**(Optional) The Integer type. Specifies whether to proceed with the HTTP flood detection. Valid values: ■ **0**: false ■ **1**: true - **post_action_waf**(Optional)

Parameter	Type	Required	Example	Description
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China

Specifies the mapping between a field and logical operators.

Field	Logical operator
IP	Belongs to, does not belong to
Referer	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
User-Agent	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
Param	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
Cookie	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist
Content-Type	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
X-Forwarded-For	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist

Field	Logical operator
Content-Length	Value less than, value equal to, and value greater than
Post-Body	Contains, does not contain, equals, is not equal to
Http-Method	Equal to, not equal to
Header	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result	Struct		The returned result.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.
Status	Integer	2	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=ModifyAclRule
&Domain=www.aliyun.com
&ServiceOn=1
&Rules={...}
```

```
&Common request parameters
```

Sample success responses

XML format

```
<ModifyAclRuleResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</ModifyAclRuleResponse>
```

JSON format

```
{
   "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
   "Result":{
      "Status":2,
      "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
   }
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.8.4 DeleteAclRule

Deletes a specified ACL rule.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DeleteAclRule	The operation that you want to perform. Valid values: **DeleteAclRule**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
RuleId	Long	Yes	65899	The ID of the HTTP-based ACL rule.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: - **cn**: mainland China (default) - **cn-hongkong**: areas outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
Status	Integer	env	Request execution status: - **0**: indicates that the request is pending execution. - **1**: indicates that the request is being executed. - **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DeleteAclRule
&Domain=www.aliyun.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&RuleId=65899
&Common request parameters
```

Sample success responses

XML format

```
<DeleteAclRuleResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</DeleteAclRuleResponse>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

4.1.9 Asynchronous task information

View the WAF API task status.

4.1.9.1 DescribeAsyncTaskStatus

You can call this operation to query the DescribeAsyncTaskStatus of a WAF task.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribeAsyncTaskStatus	The operation that you want to perform. Valid values: **DescribeAsyncTaskStatus**.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
WafRequestId	String	No	aliyun.waf.20180719140433783.SvaZeY	The ID of the WAF task.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	12EF3845-CCEB-4B84-AE60-2B49B2FF1EE5	The ID of the request.
Result			Responses
AsyncTaskStatus	String	env	Asynchronous task execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.

Parameter	Type	Example	Description
Data	String	xx	The business data returned by asynchronous tasks.
ErrCode	String	400	Error code. **Note:** This parameter is only returned when an error occurs during request execution.
ErrMsg	String	xx	The description of the error message. **Note:** This parameter is only returned when an error occurs during request execution.
Progress	Integer	90	The progress of the asynchronous task . Unit: percentage.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeAsyncTaskStatus
&InstanceId=waf_elasticity-cn-0xldbqtm005
&WafRequestId=aliyun.waf.20180719140433783.SvaZeY
&Common request parameters
```

Sample success responses

XML format

```
<DescribeAsyncTaskStatusResponse>
    <RequestId>12EF3845-CCEB-4B84-AE60-2B49B2FF1EE5</RequestId>
    <Result>
        <DomainConfig>
            <Progress>100</Progress>
            <AsyncTaskStatus>2</AsyncTaskStatus>
        </DomainConfig>
    </Result>
</DescribeAsyncTaskStatusResponse>
```

JSON format

```
{
 "Result":{
  "DomainConfig":{
   "AsyncTaskStatus":2,
   "Progress":100
  }
 },
 "RequestId":"12EF3845-CCEB-4B84-AE60-2B49B2FF1EE5"
}
```

Errors

For a list of error codes, visit the API Error Center.