Alibaba Cloud Web Application Firewall

User Guide

Issue: 20190219

Legal disclaimer

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

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

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

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

Generic conventions

Table -1: Style conventions

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

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

Contents

1 Understand Alibaba Cloud WAF in five minutes

Alibaba Cloud WAF (WAF) is a web application firewall that helps you monitor HTTP and HTTPS requests to your website and implement website access control. You can use Alibaba Cloud WAF to customize ACL rules or enable the inbuilt scenario-based protection features.

Activate WAF

Alibaba Cloud WAF is a paid service and is billed with the Subscription method on a monthly or annually basis. To get started with WAF, you must subscribe to a suitable business plan and make the payment. After that, you can enjoy the protection service specified in the specs within the subscription duration.

> Note:
> When purchasing WAF, you must specify the normal business traffic you want WAF to inspect, so that WAF can distinguish abnormal traffic such as DDoS attacks. Different subscription plan has different bandwidth. If your normal business traffic exceeds the bandwidth in the specs, you can purchase *Extra bandwidth*.

For more information, see *Billing method*, *Subscription plans*, and *Purchase Alibaba Cloud WAF*.

After activating WAF, you are assigned with a WAF instance (one WAF IP address), with which you can associate one domain name and up to 10 related subdomain names for inspecting web traffic.

- If you want to protect more than one domain name, you must purchase *Extra domain quota*.
- If you have a key interface and want to associate it with an exclusive WAF IP other than the default one, which may be used by multiple subdomains, you can enable *Exclusive WAF IP*.

Implement WAF

To implement Alibaba Cloud WAF, you first create a website configuration in the WAF console to associate your domain name with the subscribed WAF instance, and then update the domain name’ s DNS (*Domain Name System*) settings to redirect web traffic to WAF for inspection.

- Create a website configuration

  Website configuration describes the forwarding routes of the websites that are deployed with Alibaba Cloud WAF. You can add a website configuration by using the automatic or manual method. In a website configuration, you specify a domain name to protect and configure the forwarding settings such as the server address. Alibaba Cloud WAF assigns a dedicated WAF CNAME address (*What is CNAME*) to each website configuration.

  For more information, see *Website configuration*.

- Update the DNS settings

  Only when you enable the WAF CNAME address for your domain name at the DNS provider will Alibaba Cloud WAF begin monitoring network traffic requesting the domain name. WAF helps you filter out malicious requests and forward valid requests back to the origin server address.

  For more information, see *WAF deployment guide*.

- Automatically implement Alibaba Cloud WAF

  If you use *Alibaba Cloud DNS* to host your domain name, when you are implementing WAF, WAF can read the existing forwarding settings (in particular, A records) to automatically create website configuration, and update the corresponding DNS settings on your behalf. You only have to select the domain name to protect. If not, you have to manually create a website configuration and update the DNS settings yourself.

Configure WAF protection policies

When implemented, Alibaba Cloud WAF inspects the HTTP and HTTPS requests to your website and applies access control rules to filter out malicious requests.

> **Note:**
> The following features may not be included in your subscription plan. For more information about whether a feature is available, see the feature description link.

- You can use HTTP ACL Policy to customize access control rules to filer requests based on specified client IP addresses, request URLs, and common request header fields. For more information, see *HTTP ACL Policy* and *Create a whitelist or blacklist*.

- You can also use the scenario-based Web protection features to protect against common Web attacks. These inbuilt protection features integrate precise filtering algorithms that are written based on Web attack characteristics and analysis of massive requests. They are ease of use and include the following:

   Note:
  Alibaba Cloud WAF enables multi-layer filtering. After you implement WAF and configure multiple protection policies, client requests have to go through multi-layer filtering. The default protection sequence is: HTTP ACL Policy > HTTP Flood Protection > Web Application Protection.

  - Web application protection: This feature helps you protect against common Web attacks such as SQL injection and XSS cross-site attacks. For more information, see *Web application protection*.
  - HTTP flood protection: This feature helps you protect against HTTP flood attacks. For more information, see *HTTP flood protection mode* and *Customize HTTP flood protection*.
  - New intelligent protection engine: This feature performs semantic analysis on web requests, detects malicious requests, and helps you protect against malicious attacks initiated by confusion attacks and variants. For more information, see *New intelligent protection engine*.
  - Malicious IP penalty: This feature helps you automatically block the client IP address that has launched multiple Web attacks in a short period of time. For more information, see *Enable malicious IP penalty*.
  - Blocked region: This feature helps you block IP access requests based on the geolocation vector and supports blocking all requests from one or more

specified China provinces and International countries. For more information, see *Blocked regions*.

- Data risk control: This feature helps you defend against machine frauds such as zombie accounts, credential stuffing, brute force cracking, vote cheating, and spam messages. For more information, see *Data risk control*.
- Website tamper-proofing: This feature helps you lock specified web pages to prevent content tampering. The locked pages only return the cached content. For more information, see *Website tamper-proofing*.
- Data leakage prevention: This feature helps you mask sensitive information in the server response, such as the ID number, bank card number, telephone number, and sensitive words. For more information, see *Data leakage prevention*.

View WAF security reports

Alibaba Cloud WAF provides convenient data visualization and statistics features:

- Security monitoring: You can view the business QPS data and security protection statistics on the *Overview* page.
- Reports: You can search for attack details and risk warning information on your domain name within 30 days. For more information, see *Attack protection reports* and *Risk warning reports*.
- Logs: You can search for your website logs and use online analysis to quickly locate requests. For more information, see *Alibaba Cloud WAF logging*.

Additional WAF best practices

For a website that is implemented with WAF, all valid web requests are forwarded to the origin server from the WAF instance, and the origin server address is invisible to clients.

- If you want to see the real client IP address, see *Get real client IP addresses*.
- If your origin IP address is exposed or unintentionally disclosed, an attacker can bypass WAF and attack your origin directly. To protect against this situation, you can *Configure origin protection*.
- If you are using Alibaba Cloud WAF with *DDoS Pro* or *CDN*, see the following topics for detailed implementation method:

 Note:

You must select yes for Any layer 7 proxy (e.g. Anti-DDoS/CNS) enabled ? in this case.

- *Deploy WAF and Anti-DDoS Pro together*
- *Deploy WAF and CDN together*

- **To protect your native apps and resolve issues such as HTTP flood attacks, malicious registrations, and fake orders, see *WAF SDK solution*.**

2 Access WAF

2.1 Website configuration

Website configuration describes the forwarding routes of the websites that are deployed with Alibaba Cloud WAF.

You can add a website configuration by using the *automatic* or *manual* method.

- Automatically create a website configuration. When you are creating a website configuration, WAF accesses your A record configurations in *Alibaba Cloud DNS* and lists all website domains and their origin server IP addresses. You can simply select the domains for which you want to enable WAF protection and let WAF do the rest of configurations. In this way, WAF also helps update the DNS settings to redirect web traffic to WAF for inspection.
- Manually create a website configuration. If no A record has been created in Alibaba Cloud DNS, you must manually create the website configuration. After that, you must log on to the DNS host's system to update the DNS settings to redirect web traffic to WAF for inspection.

  For more information about how to update the DNS settings, see *WAF deployment guide*.

> **Note:**
> The number of website configurations you can add to the Alibaba Cloud WAF instance depends on your subscription plan and the number of extra domains. For more information, see *Extra domain quota*.

When your origin server addresses, protocol types, or ports change, or you want to configure the HTTPS advanced settings, you can *edit the website configuration*.

For websites that do not need WAF protection any more, you can restore their DNS settings and *delete the website configuration*.

Automatically add a website configuration

Prerequisites

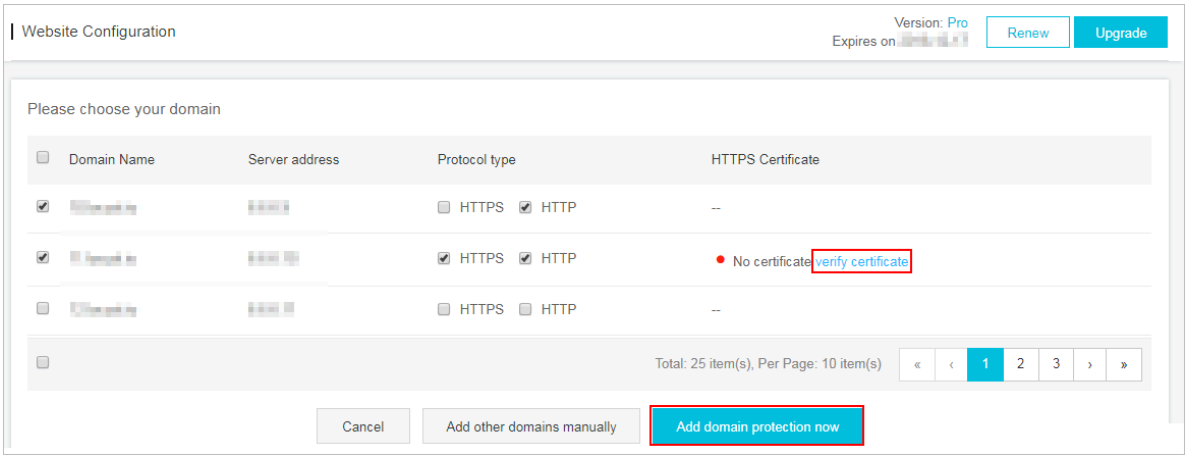
- The domain to be protected is hosted at Alibaba Cloud DNS. Besides, its DNS settings must include at least one valid A record.

  If you do not use Alibaba Cloud DNS, see *Website configuration* to manually add the website configuration.
- (For Mainland China region) The website is granted an ICP license by the Ministry of Industry and Information Technology (MIIT).
- (For HTTPS-enabled websites) You have access to a valid SSL certificate and private key of the website, or you have uploaded the certificate to Alibaba Cloud SSL Certificate Service.

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China, International.
3. On the Management > Website Configuration page, click Add Domain.

   WAF automatically lists all domain names that have an A record configured in Alibaba Cloud DNS of the current Alibaba Cloud account. If no A record has been created in Alibaba Cloud DNS, the Please choose your domain page does not appear. In this case, we recommend that you manually create a website configuration. For more information, see *Website configuration*.



4. On the Please choose your domain page, check the Domain Name for which you want to enable WAF protection and the Protocol Type.
5. (Optional) If the protocol type includes HTTPS, you must verify certificate first to add the configuration.

   Note:

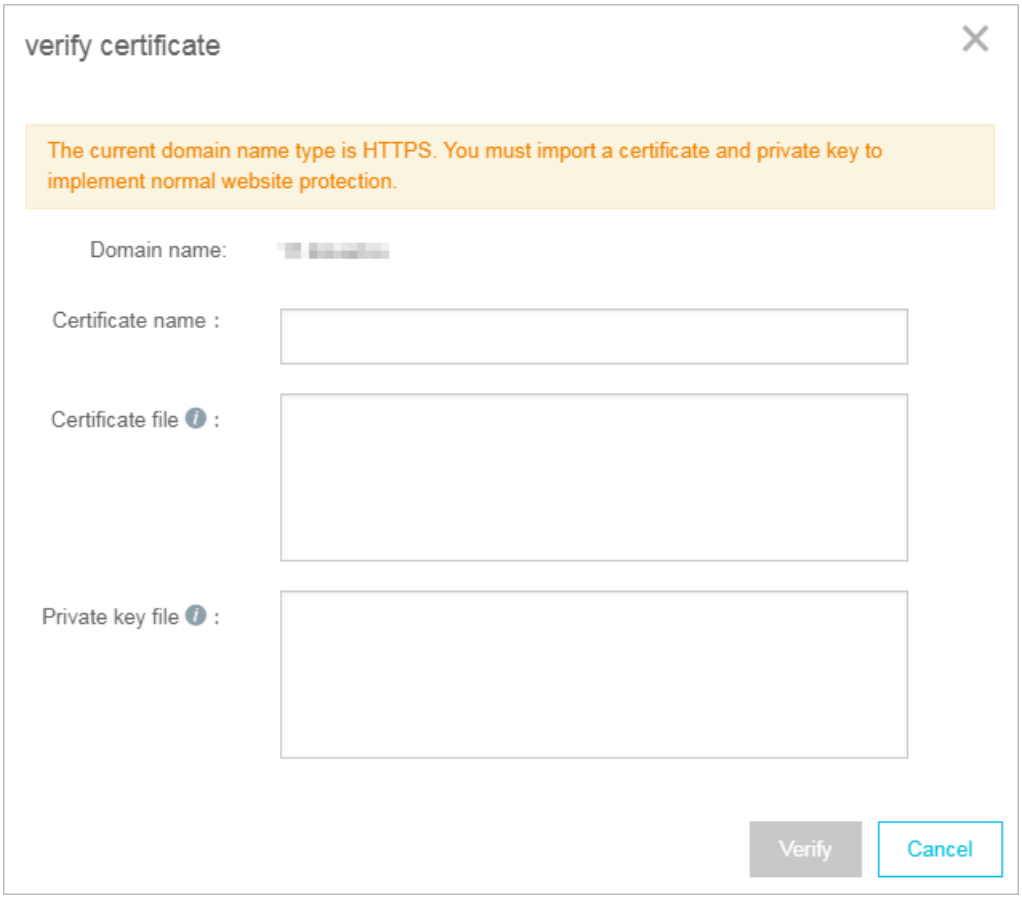
Alternatively, do not select HTTPS here, but edit the website configuration and upload the certificate after you create the configuration. For more information, see *Update HTTPS certificate*.

a. Click Verify Certificate.

b. In the Verify Certificate dialog box, upload the certificate and private key.

- If the certificate has been hosted in the *Alibaba Cloud SSL Certificate Service console*, you can click Select existing certificate in the Verity Certificate dialog box and select it to upload.
- Manual upload. Click Manual upload, enter the Certificate name, and paste the text content of the certificate and private key respectively to the Certificate file and Private key file boxes.

  For more information, see *Update HTTPS certificate*.



c. Click Verify to upload.

6. Click Add domain protection now.

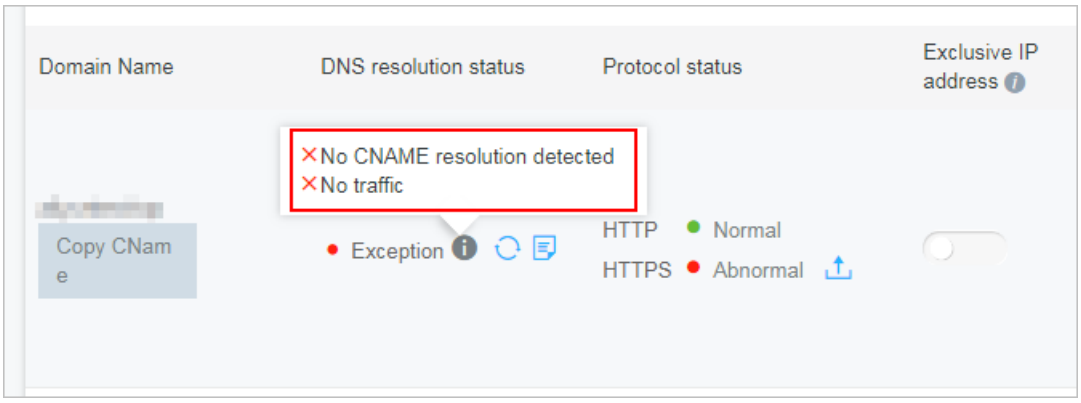
   After adding the website configuration, WAF automatically updates the DNS settings (CNAME record) of the domain name to redirect web requests to WAF for inspection. The whole process takes about 10 to 15 minutes.

   > Note:
   > If you are prompted to manually change the DNS settings, you must perform *Step 2: Update DNS settings* to redirect web traffic to WAF.

7. On the Management > Website Configuration page, view the newly added domain name and its DNS Resolution Status.

   - Normal indicates that Alibaba Cloud WAF has been successfully deployed for the website. Go on to perform *Step 3: Configure WAF protection policies*.
   - Exception indicates that you must wait for a while or check the DNS settings at your DNS service provider.

     If the DNS settings are incorrect, perform *Step 2: Update DNS settings*. For more information, see *DNS resolution status exception*.



Manually add a website configuration

Prerequisites

- Obtain the domain name of the website to be protected.
- Obtain the origin server IP address or other type of address that is supposed to receive the WAF-returned traffic.
- Determine whether the website is deployed with CDN, DDoS protection, or other proxy services.
- (For Mainland China region) The website is granted an ICP license by the Ministry of Industry and Information Technology (MIIT).

- (For HTTPS-enabled websites) You have access to a valid SSL certificate and private key of the website, or you have uploaded the certificate to Alibaba Cloud SSL Certificate Service.

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China, International.
3. On the Management > Website Configuration page, click Add Domain.

   WAF automatically lists all domain names that have an A record configured in Alibaba Cloud DNS of the current Alibaba Cloud account. If no A record has been created in Alibaba Cloud DNS, the Please choose your domain page does not appear.
4. (Optional) On the Please choose your domain page, click Add other domain manually.
5. In the task of Fill in the website information, complete the following configuration.

Configuration	Description
Domain name	Enter the domain name to be protected.  Note: · Supports wildcard domains, such as `*.aliyun.com`. When a wildcard domain is presented, all its associated subdomains are matched. · If you add website configurations for an exact domain (for example, `www.aliyun.com`) and a wildcard domain (for example, `*.aliyun.com`) that matches the exact domain, the configuration for the exact domain takes priority. · Does not support .edu domain names. If you want to use Alibaba Cloud WAF to protect domain names suffixed with .edu, submit a ticket to us.

Configuration	Description
Protocol type	Check the protocols used by the website. Optional values: HTTP, HTTPS. Note: · If your website is enabled with HTTPS, check HTTPS and see *Update HTTPS certificate* to upload a valid certificate and private key to let WAF inspect the HTTPS traffic. · When HTTPS is checked, you can configure the Advanced settings to enable HTTPS force redirect or HTTP back-to-source to smooth the website access. For more information, see *HTTPS advanced settings*.
Server address	Enter the origin server address, which can be one or more IP addresses or other addressees, such as an OSS CNAME address. When the website is deployed with Alibaba Cloud WAF, WAF returns the inspected web requests to this address. · (Recommended) Check IP and enter the public IP address of the origin server, such as the ECS instance IP or the SLB instance IP. Note: - Multiple IP addresses are separated by commas. Up to 20 IP addresses can be added. - If multiple IP addresses are presented, WAF performs health check and load balancing across them when returning the inspected web traffic. For more information, see *Load balancing across multiple origin servers*. · Check Other addresses and enter the server address used to receive the WAF-returned traffic, such as an OSS CNAME address. Note: - The server address (Other address) must not be same as the website domain name. - If you enter an OSS CNAME address, after you create the website configuration, you must log on to the Alibaba Cloud OSS console to associate the custom domain (in this case, the domain to be protected) for the specified OSS CNAME address. For more information, see *Associate a custom domain*.

Configuration	Description
Server port	Specify the server port. When the website is deployed with Alibaba Cloud WAF, WAF returns the inspected web requests to this port. · When Protocol type includes HTTP, the default HTTP port is 80. · When Protocol type includes HTTPS, the default HTTPS port is 443. · If you want to specify other ports, click custom to add them. Note: For more information, see *Supported non-standard ports*.
Any layer 7 proxy (e.g. Anti-DDoS/ CDN) enabled?	Check yes or no according to the actual condition. If any layer 7 proxy is deployed in front of Alibaba Cloud WAF, you must check yes. Otherwise, Alibaba Cloud WAF may not be able to obtain the real client IP address.
Load balancing algorithm	When multiple origin server addresses are specified, select the load balance method (IP HASH or Round-robin) for WAF to distribute traffic among these addresses.
Flow Mark	Enter an unoccupied Header Filed name and a custom Header Field Value to mark the web requests returned to the origin server by Alibaba Cloud WAF. WAF adds the specified header field into the inspected web requests for your web server to identify the WAF-returned traffic. Note: If the web request itself uses the specified header field, Alibaba Cloud WAF overwrites the original value with the specified value.

6. Click Next to complete the configuration.

   When the website configuration is created, you can perform the following tasks:

   · Follow the tutorial to perform the next task Change DNS Record. For more information, see *WAF deployment guide*.

   · (For HTTPS-enabled websites) Upload the HTTPS certificate and private key. For more information, see *Update HTTPS certificate*.

   · Go to the Management > Website Configuration page to view the newly added website configuration, and Edit or Delete it as you need.

Edit a website configuration

When your web server’ s configuration changes, such as server IP address changes , protocol type or port changes, or when you want to configure the HTTPS advanced settings, you can edit the website configuration.

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China, International.
3. On the Management > Website Configuration page, select the website configuration to be operated, and click Edit.
4. On the Edit page, complete the configuration by following *Step 5 in Manually add a website configuration*.

   Note:
   The Domain name cannot be modified. If you want to associate another domain name, we recommend that you add a new website configuration and delete the unnecessary one.
5. Click OK to complete the procedure.

Delete a website configuration

If you want to disable Alibaba Cloud WAF for your website, you can restore the DNS to redirect traffic to your web servers, and delete the website configuration on the Alibaba Cloud WAF console.

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China, International.
3. On the Management > Website Configuration page, select the website configuration to be deleted, and click Delete.

   Note:
   You must restore the DNS settings before deleting the website configuration. Otherwise, the website may become inaccessible.
4. In the Prompt message dialog box, click OK.

2.2 Whitelist Alibaba Cloud WAF IP addresses

When a website is deployed with Alibaba Cloud WAF, all web traffic is redirected to WAF for inspection, and WAF returns the inspected traffic to origin server.

From the origin server’ s perspective, all web requests arrive from a limited quantity of WAF IP addresses, which is suspicious. If the origin server has been installed with a security software such as FortiGate, the security software may trigger a blocking action against WAF IP address and web traffic returned by WAF. Therefore, you must whitelist all WAF IP addresses in the security software in origin server to avoid normal business interruption.

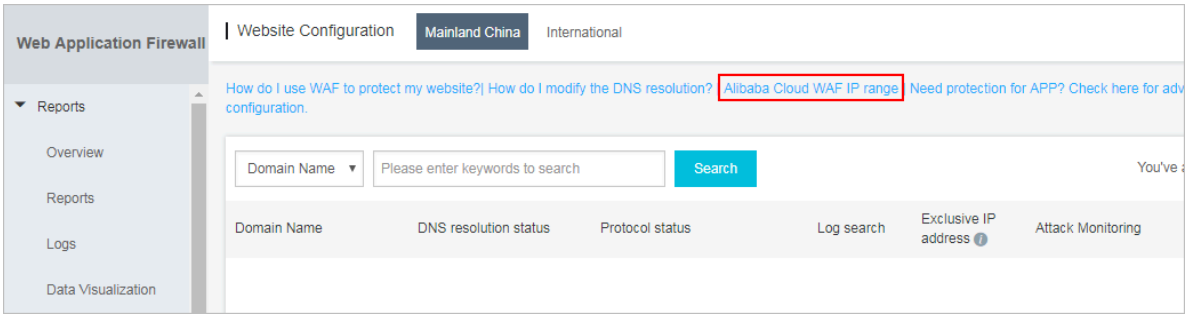
 Note:
We recommend that you uninstall other security software in origin server after Alibaba Cloud WAF is deployed.

Procedure

You can view the IP addresses of Alibaba Cloud WAF in the Alibaba Cloud WAF console. The procedure is as follows.

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China, International.
3. Go to the Management > Website Configuration page.

4. Click Alibaba Cloud WAF IP range to view and copy all WAF IP addresses.



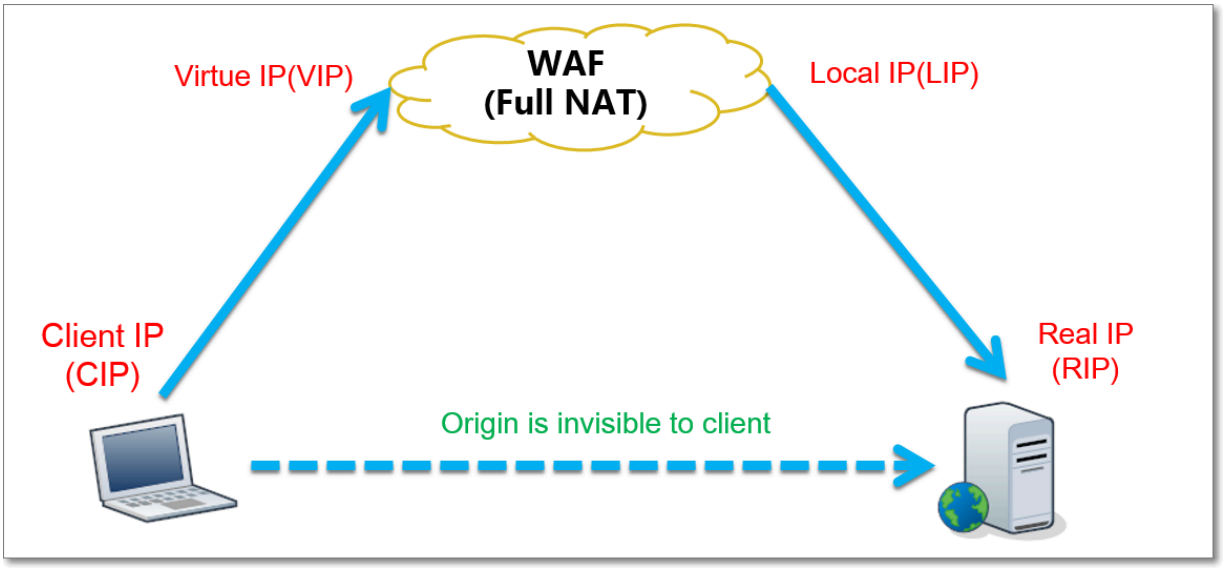
You can see the following result:

5. Open the security software in origin server, and add the copied WAF IP addresses to the IP whitelist.

FAQs

What is the Alibaba Cloud WAF IP address?

Alibaba Cloud WAF acts as a reverse proxy between your client and origin server. In origin server’ s eyes, all web requests originate from Alibaba Cloud WAF IP addresses and the real client IP addresses are written into the XFF (X-Forwarded-For) field of HTTP header.



Why must I whitelist Alibaba Cloud WAF IP addresses?

From origin server’ s perspective, web requests from the Alibaba Cloud WAF IP addresses are more concentrated and in a high frequency. The security software in origin server may determine that Alibaba Cloud WAF IP addresses are starting attacks , and trigger a blocking action against them. If Alibaba Cloud WAF IP addresses are blocked, the real client cannot get a response. Therefore, you must whitelist Alibaba Cloud WAF IP addresses once your website is deployed with WAF. Otherwise, normal web access may be affected, which leads to web pages cannot be opened or respond slowly.

We recommend that after deploying Alibaba Cloud WAF, you only allow web requests originate from WAF and block other requests to guarantee normal web business access and avoid direct-to-origin attacks. If the origin server IP address is disclosed, an attacker can bypass WAF to directly attack your origin server. For more information, see *Protect your origin server*.

2.3 Perform redirect check with a local computer

When you have created a website configuration in Alibaba Cloud WAF for your website and are going to update the DNS settings to redirect web traffic to WAF for inspection, we recommend that you perform a redirect check with a local computer to make sure that WAF can handle the traffic. Redirect check requires you to modify the local hosts file to make your local machine look directly at your Alibaba Cloud WAF instance. Therefore, you can test whether the WAF instance works properly.

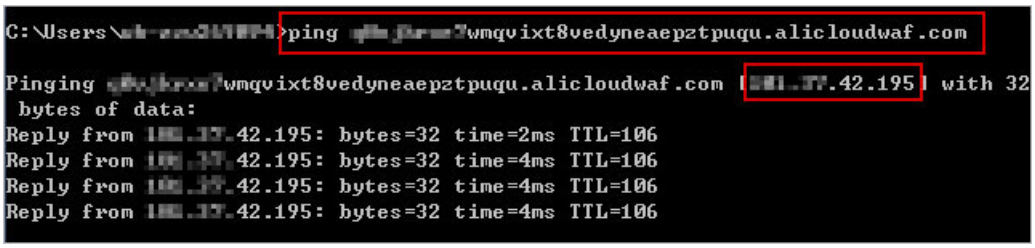
Modify the local hosts file

Modify the local *hosts* file (*What is the hosts file?*) to forward local requests to WAF. For Windows systems, the procedure is as follows:

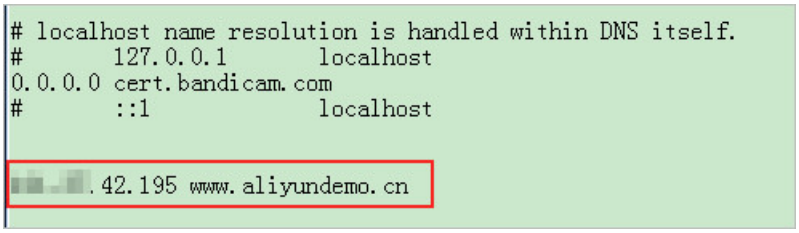
1. Open the *hosts* file with Notepad. The *hosts* file locates in the *C:\Windows\System32\drivers\etc\hosts* directory.
2. In the last line, add the following content: `WAF_IP_address Domain_name_protected`.

   Suppose that you have created a website configuration for `www.aliyundemo.cn`, and Alibaba Cloud WAF assigns the following CNAME address to it: `xxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com`.

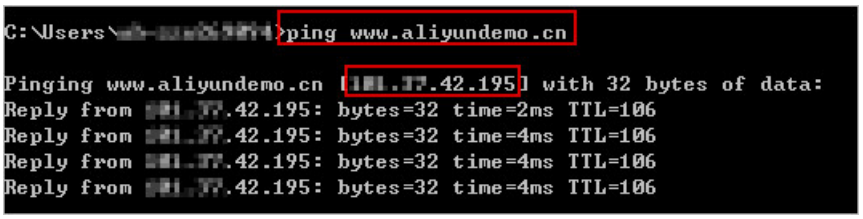
   a. Open the cmd command-line tool in Windows, and run the following command to obtain the WAF IP address: `ping xxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com`. You can view the WAF IP address in the response.



   b. Add the following line to *hosts*. The IP address is the WAF IP address obtained in the previous step, and the domain name is the protected domain name.



3. Save changes to *hosts*. Ping the protected domain name in cmd.



If WAF works properly, the IP address you see will be the WAF IP address configured in the previous step. If the origin IP address is displayed, try refreshing the local DNS cache. In Windows, you can run `ipconfig/flushdns` in cmd.

Verify WAF forwarding

Once the changes in the hosts file are effective, you can access the protected domain name from your local computer. If WAF is configured correctly, the website is expected to be normally accessed.

In addition, you can verify the protection effect by constructing some simple attack commands. For example, you can add `/? alert(xss)` to the URL to construct a Web attack request for testing. As you try to access `www.aliyundemo.cn/? alert(xss)`,

2.4 WAF deployment guide

Deploying Alibaba Cloud WAF for a website indicates updating the DNS records (CNAME or A type) after the website configuration is created, to redirect web requests to WAF for inspection.

You can use a *CNAME record* or *A record* to redirect web traffic. We recommend that you use CNAME. Using CNAME supports node switch or even redirecting traffic back to source in case of node failure or machine failure, which improves your business' s availability and failure recovery capacity.

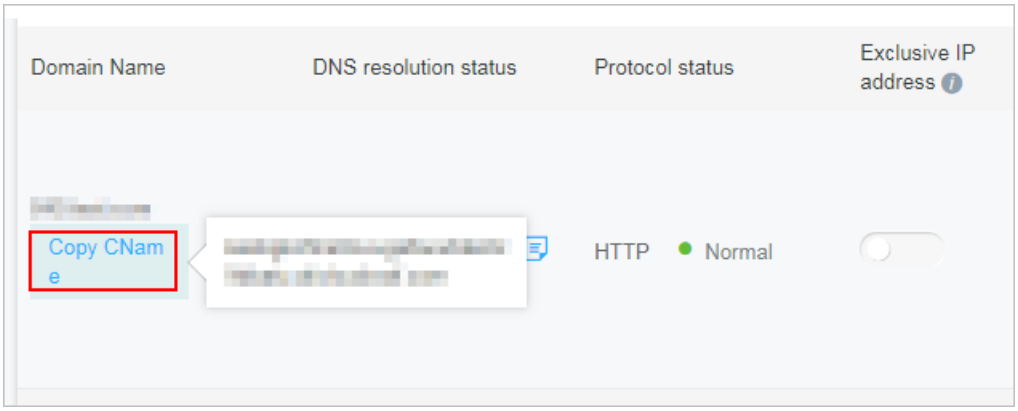
The following content applies to deploying Alibaba Cloud WAF exclusively for the website, that is, the website does not use CDN, DDoS protection, and other proxy services. For other scenarios, see the following documents:

- *Deploy Alibaba Cloud WAF and CDN together*: explains how to deploy CDN and WAF together for your website.
- *Deploy Alibaba Cloud WAF and DDoS protection together*: explains how to deploy DDoS protection and WAF together for your website.

(Recommended) Edit CNAME record to deploy WAF

Prerequisites

- Website configuration is successfully created. For more information, see *Website configuration*.
- Obtain the WAF CNAME address.
  1. Log on to the *Alibaba Cloud WAF console*.
  2. On the top of the page, select the region: Mainland China, International.
  3. On the Management > Website Configuration page, move the pointer onto the domain name you want to operate. You will see the Copy CName button.



  4. Click Copy CName to copy the WAF CNAME address to the Clipboard.

> **Note:**
> If you want to update A record to redirect web traffic to WAF, you can ping this CNAME address to obtain the corresponding WAF IP address. For more information, see *WAF deployment guide*. In general, the WAF IP address seldom changes.

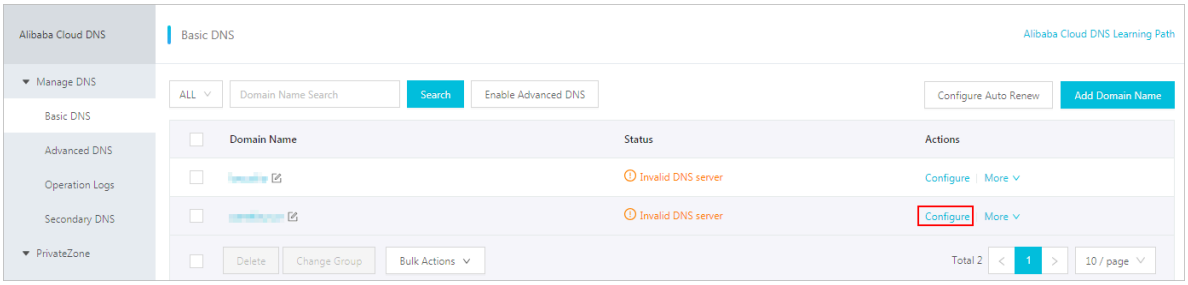
- You have permissions to update the domain's DNS settings in its DNS host's system.
- (Optional) Whitelist Alibaba Cloud WAF IP addresses. If your origin web server has enabled non-Alibaba Cloud security software (such as Fortinet FortiGate), you must whitelist WAF IP addresses in the software to prevent legitimate traffic returned by WAF from being blocked. For more information, see *Whitelist Alibaba Cloud WAF IP addresses*.
- (Optional) Perform redirect check with a local computer. Perform a redirect check to guarantee that all configuration is correct, before you change the DNS settings.

This helps avoid business interruption due to incorrect configuration. For more information, see *Perform redirect check with a local computer*.

Procedure

The following steps explain how to update the CNAME record in Alibaba Cloud DNS. If your domain is hosted in Alibaba Cloud DNS, follow these steps. Otherwise, you must log on to your DNS host's system to do the modification.

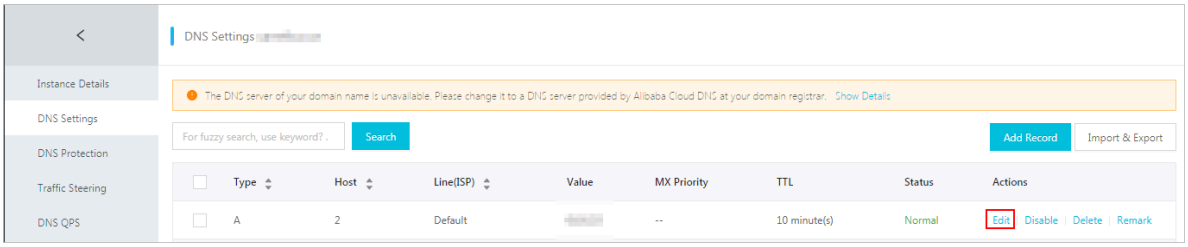
1. Log on to the *Alibaba Cloud DNS console*.
2. Select the domain to be operated and click Configure.



3. Select the Host (hostname) to be operated and click Edit.

   Take `abc.com` as an example. You can select hostname as follows:

   - www: matches the subdomain starting with www, in this case `www.abc.com`.
   - @: matches the root domain, in this case `abc.com`.
   - *: matches a wildcard domain name that includes both the root domain and all subdomains, in this case `blog.abc.com`, `www.abc.com`, `abc.com`, and so on.



4. In the Edit Record dialog box, do the following:

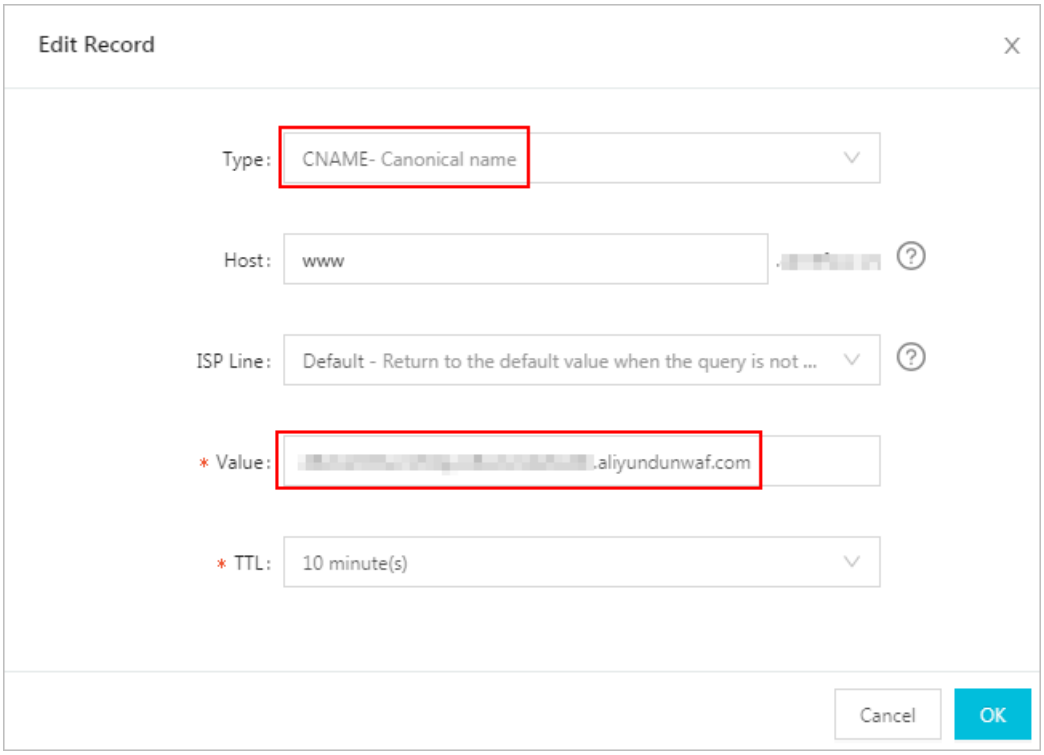
   - Type: Select CNAME.
   - Value: Enter the WAF CNAME address.
   - Leave other settings as they are. We recommend that you set TTL value to 10 minutes. The larger the TTL value, the slower the DNS propagation.

   Notes about editing DNS records:

   - For a hostname, the CNAME record is unique. You must edit it to the WAF CNAME address.
   - Different record type conflicts with each other. For example, for a hostname, the CNAME record cannot coexist with an A record, MX record, or TXT record. If you cannot change the record type directly, you can first delete the conflicting records and add a new CNAME record.

     Note:
     The whole process of deleting and adding must be performed in a short time. Otherwise, your domain becomes inaccessible.

   - If the MX record is being used, you can use an A record to redirect web traffic to WAF. For more information, see *WAF deployment guide*.



5. Click OK to complete the DNS settings and wait for the DNS change to take effect.

6. (Optional) Verify the DNS settings. You can ping the domain or use *DNS Check* to validate whether the DNS change is effective.

   Note:
   It takes a certain time for the setting to be in effect. If the validation fails, wait for about 10 minutes and re-validate it again.

7. Check the DNS resolution status.

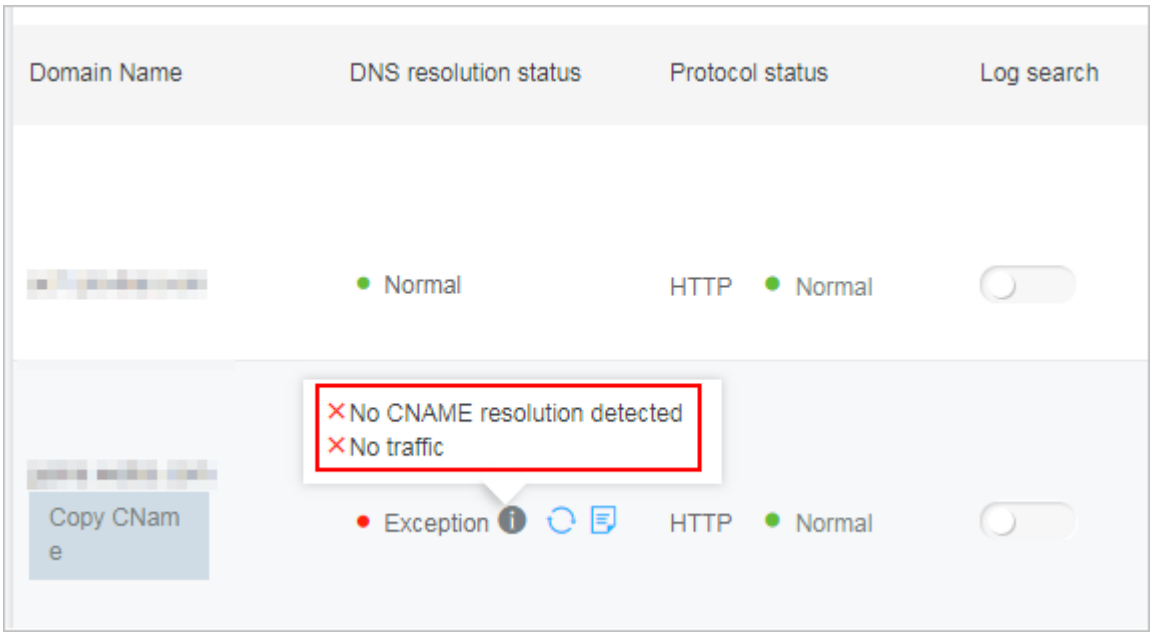
   a. Log on to the *Alibaba Cloud WAF console*.

   b. On the Management > Website Configuration page, check the DNS resolution status of the domain name.

   - Normal: Alibaba Cloud WAF has been successfully deployed and the web traffic is being monitored by WAF.
   - Exception: With the exception messages of NO CNAME resolution detected, No traffic, or DNS check failed, the DNS settings may be incorrect.

     In this case, check the DNS settings. If you confirm that the DNS settings are correct, wait for an hour and refresh the DNS resolution status. For more information, see *DNS resolution status exception*.

     Note:
     The exception here indicates that WAF is not properly deployed. Your website access is not affected.



Protect the origin

When the origin server IP address is exposed, attackers may exploit it to bypass Alibaba Cloud WAF and start direct-to-origin attacks. To prevent such attacks, we recommend that you configure the ECS security group or SLB whitelist to block all web requests that do not come from Alibaba Cloud WAF's IP addresses. For more information, see *Protect your origin server*.

Edit A record to deploy WAF

The A record method is same as the CNAME one, except the following differences.

- Prerequisites: After obtaining the WAF CNAME address, do the following to obtain the associated WAF IP address.
  1. In a Windows operating system, open the cmd command line tool.
  2. Run the following command: `ping "copied WAF Cname address"`.
  3. In the result, view the WAF IP address.
- Procedure: In step 4 editing record, do the following:
  - Type: Select A.
  - Value: Enter the WAF IP address.
  - Leave other settings as they are.

2.5 Update HTTPS certificates

To let Alibaba Cloud WAF inspect HTTPS traffic for your web business, you must include HTTPS in the protocol type in *website configuration*, and upload a valid HTTPS certificate to WAF. If the certificate changes, you must update the certificate in the Alibaba Cloud WAF console in a timely manner.

Context

If you have uploaded the certificate file to *Alibaba Cloud SSL Certificate Service* for integrated management, then in the following steps, you can reuse it directly instead of uploading it again.

Otherwise, you must have the certificate and private key files prepared, to complete the following operations.

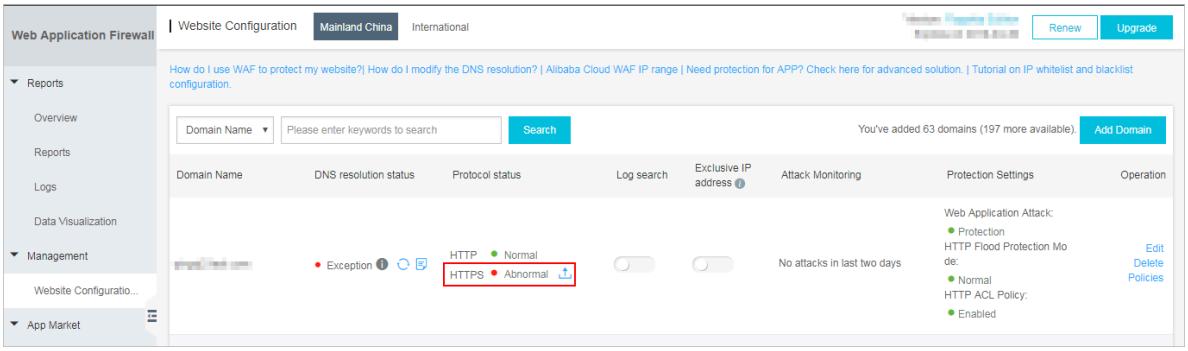
In general, the following files are required:

- *.crt (Public key) or *.pem (Certificate)

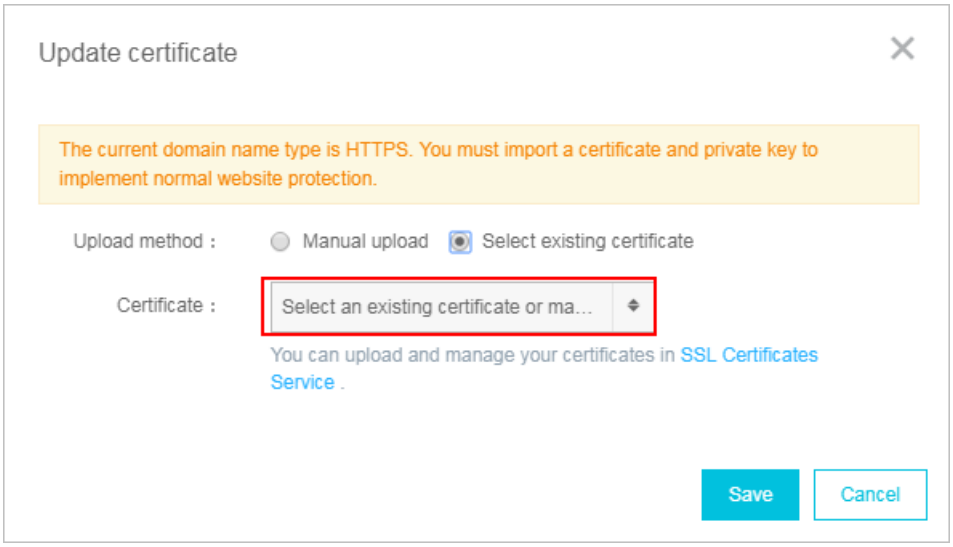
- *.key (Private key)

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China, International.
3. On the Management > Website Configuration page, locate the domain name to be operated, and click the Update Certificate button (↑) next to the HTTPS Protocol Status.



4. In the Update Certificate dialog box, select an Upload method.
   - If the HTTPS certificate to be uploaded is hosted in *Alibaba Cloud SSL Certificate Service*, you can check Select existing certificate and select it for upload.



   - Manual upload. Click Manual upload, enter a Certificate name, and paste the text context of the certificate file and private key file respectively to the Certificate file and Private key file boxes.

Note:

- For certificates in general formats, such as PEM, CER, and CRT, you can open the certificate file directly by using a text editor tool to copy the text content. For certificates in other formats, such as PFX and P7B, convert the certificate file to the PEM format, and then copy the text content from the converted certificate file.
- If the HTTPS certificate has multiple certificate files, such as a certificate chain file, merge the text contents from the multiple certificate files and paste them into the Certificate file box.

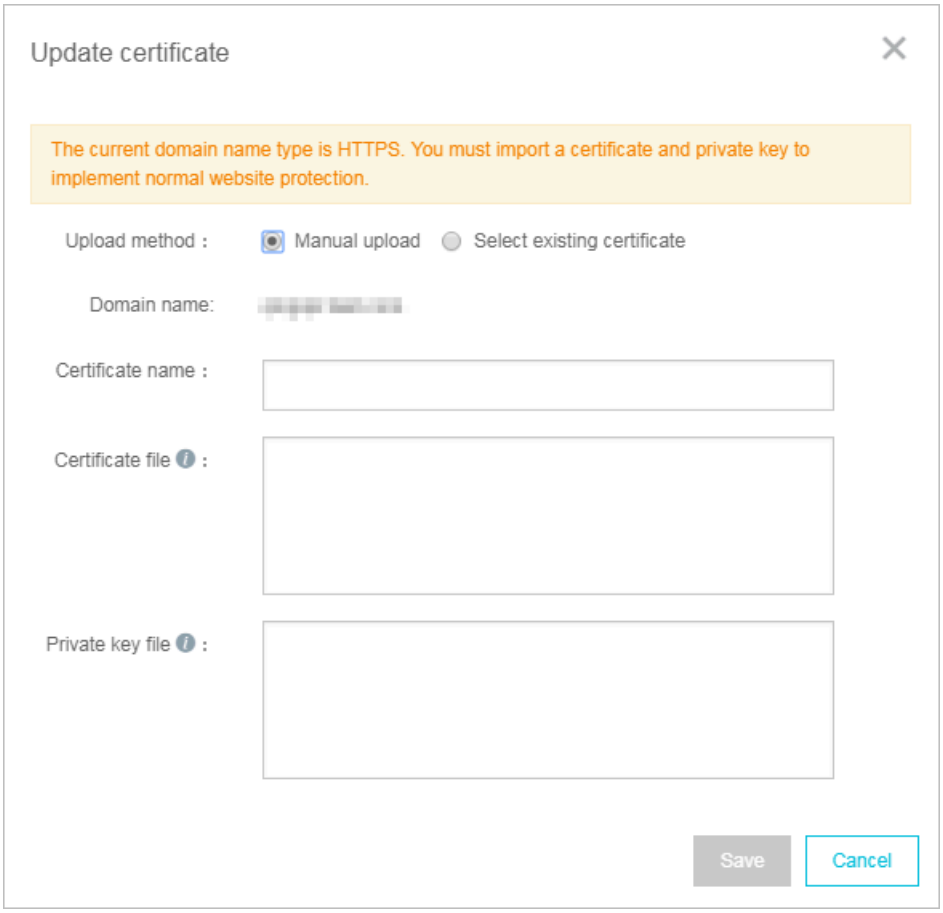
Example of the text content of a certificate file:

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx8ixZJ4krc+1M+
j2kcubVpsE2
cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOk
jgvhlqt9vc
65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9
nIrHsPl8YKk
vRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

Example of the text content of a private key file:

```
-----BEGIN RSA PRIVATE KEY-----
DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThL
yvsmLQKBgQ
Cr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJ
aiygoIYo
aMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDz
FdZ9Zujxvuh9o
4Vqf0YF8bv5UK5G04RtKadOw==
```

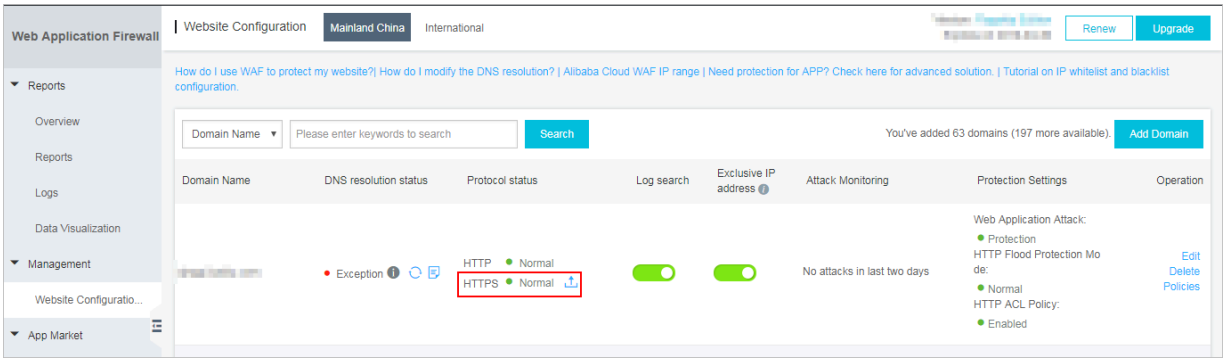
```
-----END RSA PRIVATE KEY-----
```



5. Click Save to complete the procedure.

Result

The HTTPS protocol status displays as Normal.

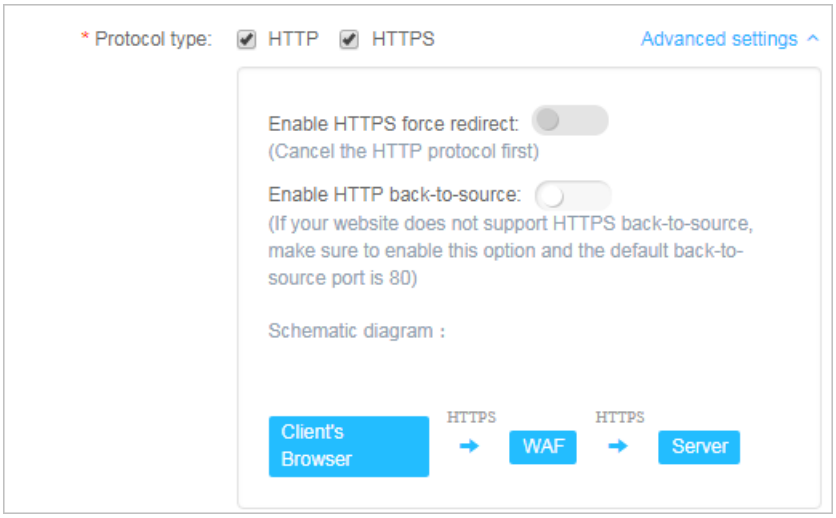


2.6 HTTPS advanced settings

Alibaba Cloud WAF provides convenient HTTPS options to help you implement HTTP back-to-source and HTTPS force redirect without re-constructing the origin.

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China, International.
3. On the Management > Website Configuration page, locate the domain name to be operated, and click Edit.
4. Check HTTPS under Protocol type, and expand the Advanced settings menu.

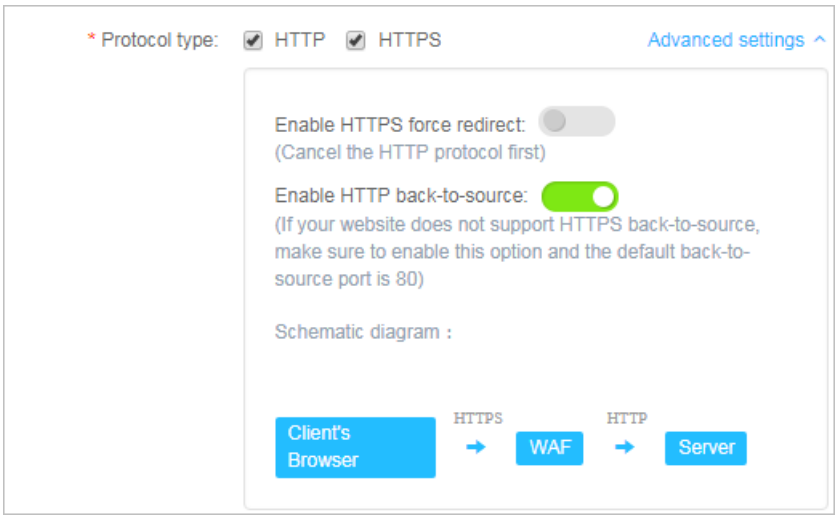


- Enable HTTP back-to-source

  You can enable an HTTP communication between Alibaba Cloud WAF and origin server by enabling HTTP back-to-source. By doing this, WAF returns the inspected traffic to the default port of 80 of your origin server.

  Note:
  Using HTTP back-to-source does not require any modification on origin server or any HTTPS configuration. However, you must make sure that you upload the

correct certificate and private key to Alibaba Cloud WAF. You can apply for a certificate for free in Alibaba Cloud SSL Certificate Service.



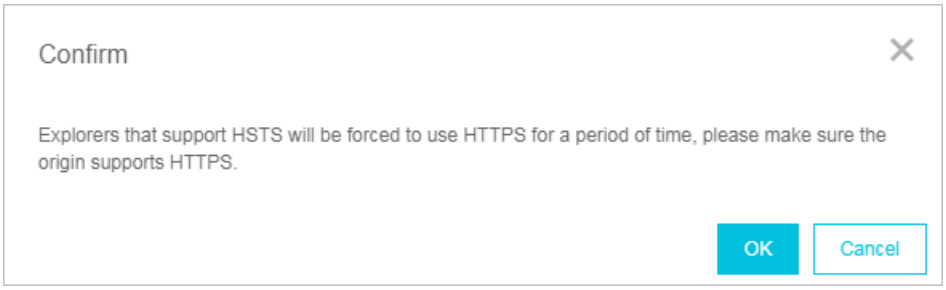
- Enable HTTPS force redirect

  If you want to force clients to use HTTPS to access your sites, you can enable HTTPS force redirect.

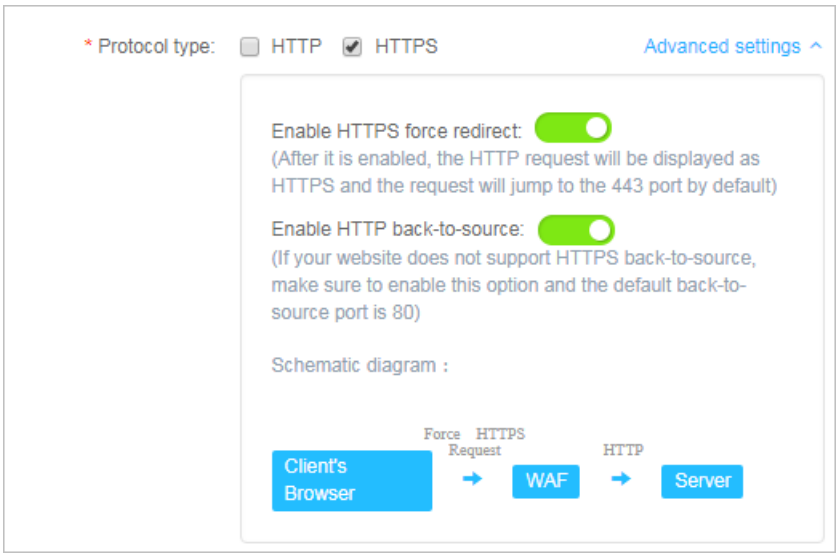
  Note:

You must cancel the HTTP protocol to enable HTTPS force redirect.

When HTTPS force redirect is enabled, some Web browsers that support HSTS (HTTP Strict Transport Security) will be forced to use HTTPS for a period of time. Therefore, you must make sure that the origin server supports HTTPS.



When HTTPS force redirect is enabled, all HTTP requests will be displayed as HTTPS and forwarded to port 443.



2.7 Supported non-standard ports

Alibaba Cloud WAF returns web traffic to the following ports of origin server by default: port 80 and 8080 for HTTP connection and port 443 and 8443 for HTTPS connection. You can specify other ports with the Business or Enterprise subscription plan. This topic explains the maximum number of ports you can specify and the custom ports you can use.

Maximum number of ports

For each Alibaba Cloud WAF subscription, the maximum number of different ports you can specify in all website configurations is as follows:

- Business plan: You can specify a maximum of 10 different ports, including port 80, 8080, 443, and 8443.
- Enterprise plan: You can specify a maximum of 50 different ports, including port 80, 8080, 443, and 8443.

Supported ports

> Note:
> Alibaba Cloud WAF only inspects web traffic that requests the supported ports. When a client requests an unsupported port (for example, 4444), the request will be discarded.

- For the Business or Enterprise subscription plan of Alibaba Cloud WAF, the following HTTP ports are supported:

  80, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8106, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9999, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702
- For the Business or Enterprise subscription plan of Alibaba Cloud WAF, the following HTTPS ports are supported:

  443, 4443, 5443, 6443, 7443, 8443, 9443, 8553, 8663, 9553, 9663, 18980

2.8 Mark WAF back-to-origin flow

When you add a website domain configuration in Web Application Firewall for protection, you can set the flow mark for the website domain. When the traffic of the website domain passes through WAF, WAF adds the specified flow mark to the requests. Thus, the origin server can easily collect corresponding information.

According to the HTTP header field name and the field value that you specify in the flow mark, when the traffic passes through WAF, WAF adds the fields and values to the HTTP Header of all requests. By marking the traffic, you can easily identify traffic that

are forwarded by WAF, and then configure precise origin server protection policies (Access Control), or analyze protection effects.

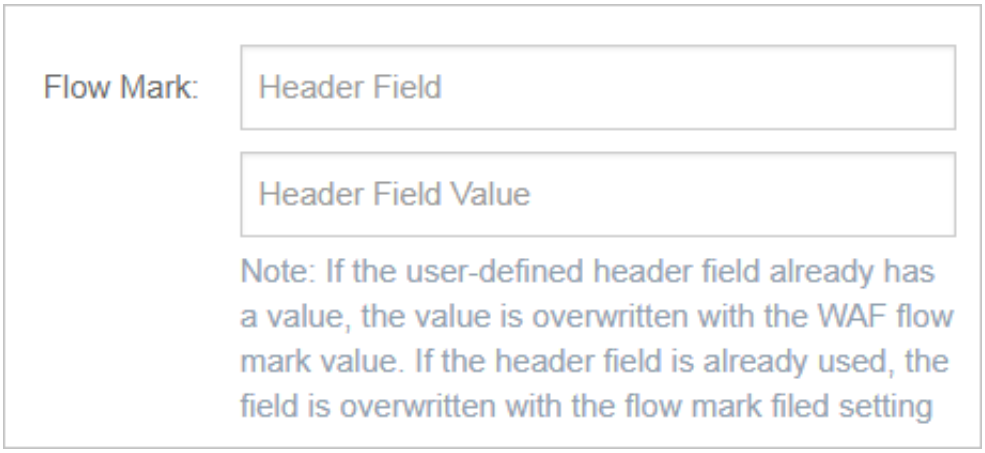
> Note:
> If the user-defined HTTP Header field that you specified as flow mark already exists in the request, WAF still overwrites the field value with the specified flow mark field value in the request.

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China, International.
3. Go to the Management > Website Configuration page, choose a domain configuration record, and click Edit.

   > Note:
   > You can also specify flow mark when adding a new website domain configuration record.
4. In the Flow Mark configuration item, enter the Header field name and the field value.

   > Note:
   > Do not specify a user-defined HTTP Header field that has already been used. Otherwise, the value of this field in the request is overwritten by the flow mark field value by WAF.

5. Click OK. After the configuration takes effect, WAF adds the specified HTTP header fields and values when forwarding requests to the website domain.

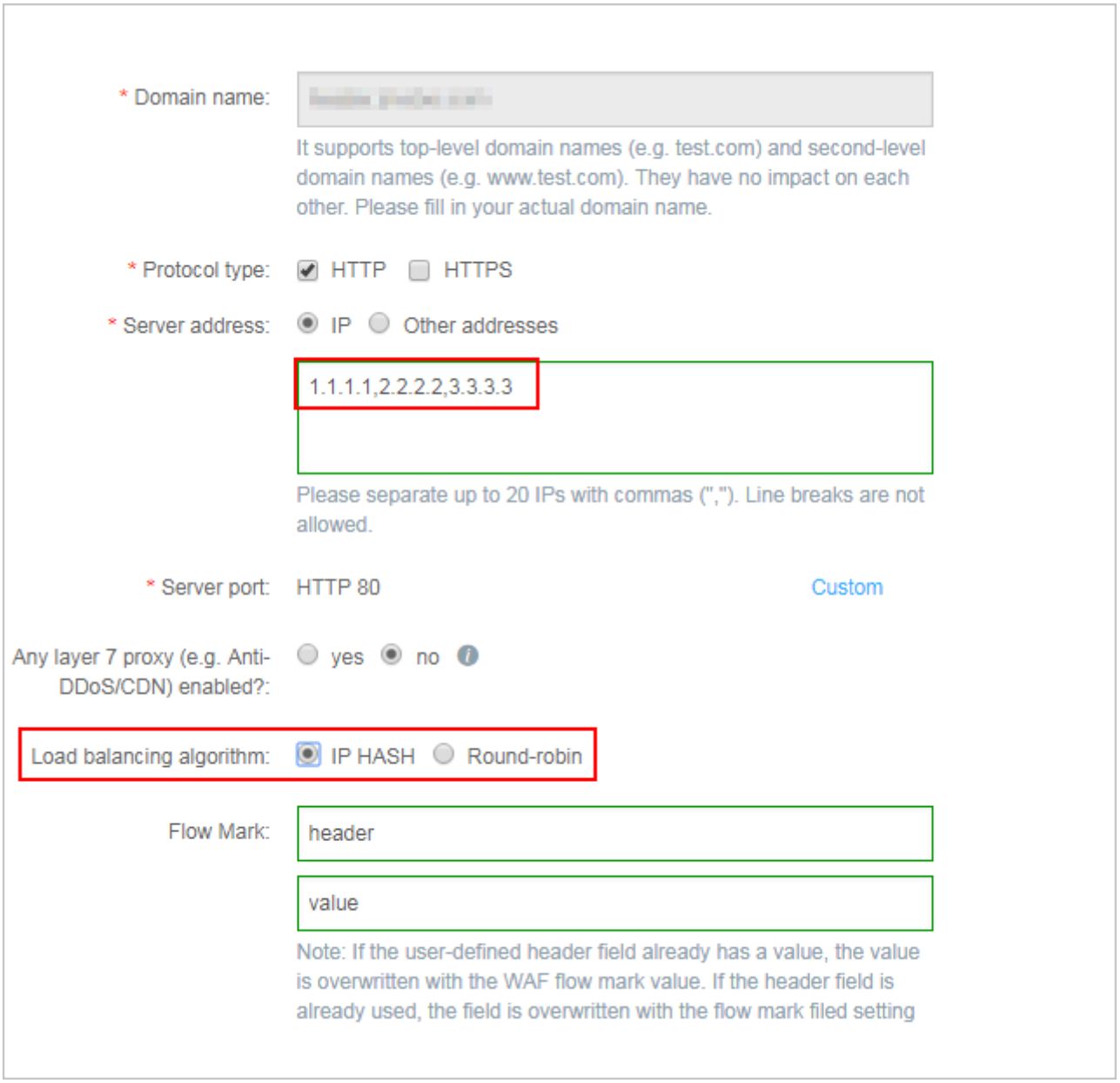
2.9 Load balance across multiple origin IPs

You can specify a maximum of 20 origin IP addresses in a website configuration.

When multiple origin IP addresses are specified, WAF performs load balance across them when returning the inspected web traffic. WAF also performs health check on all origin IPs. When one IP is inaccessible, WAF stops assigning requests to that IP until it can be accessed again.

Suppose you have three origin IPs: 1.1.1.1, 2.2.2.2, and 3.3.3.3. You can configure your website as follows.

 Note:
If you have other layer-7 proxies enabled together with WAF, such as DDoS protection or CDN, make sure that you select yes for Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled? in website configuration



When multiple origin IPs are specified, select a load balancing algorithm, such as IP HASH or Round-robin.

Note:

If you use IP hash, make sure that the origin IP addresses are discrete. Otherwise, load balancing may not work properly.

2.10 Deploy WAF and Anti-DDoS Pro together

Alibaba Cloud WAF and Anti-DDoS Pro and are fully compatible. You can use the following architecture to deploy WAF and Anti-DDoS Pro together: Anti-DDoS

Pro (entry layer, DDoS attack protection) > WAF (intermediate layer, web attack protection) > Origin.

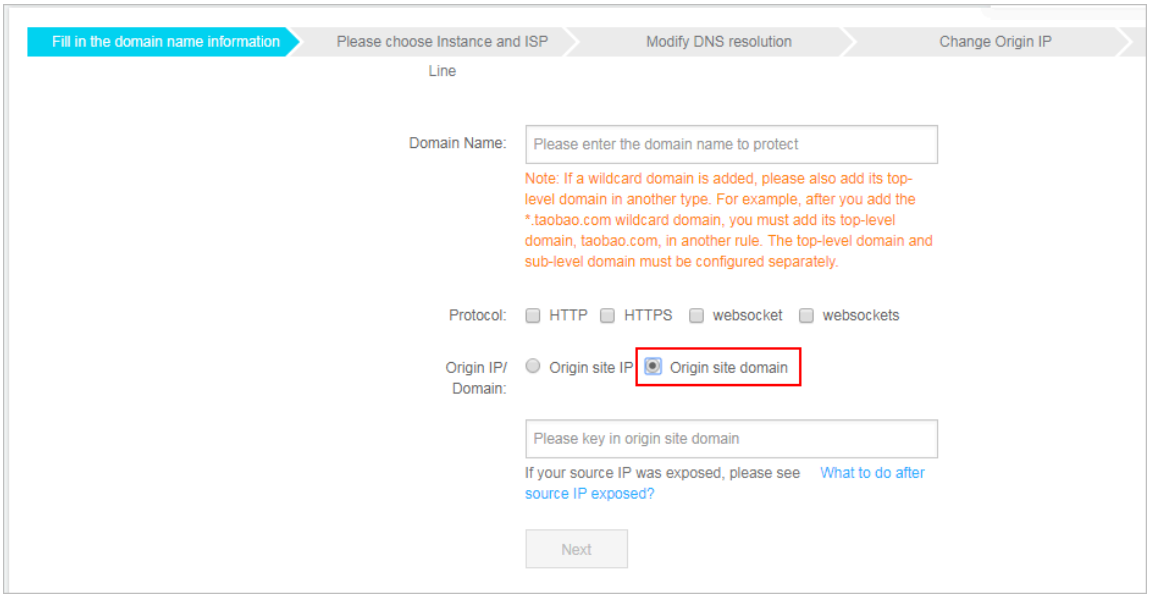
Procedure

1. Create a website configuration for your website in Alibaba Cloud WAF.
   - Server address: Check IP and enter the public IP address of the ECS instance/ Server Load Balancer instance or external server IP address.
   - Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?: Check yes.

   For more information, see *Website configuration*.
2. Create a web service access configuration for your website in Anti-DDoS Pro. The procedure is as follows:
   a. On the Access > Web Service page, click Add Domain.
   b. In the Fill in the domain name information task, do the following:
      - Domain name: Enter the domain name to be protected.
      - Protocol: Check the supported protocol.
      - Origin IP/Domain: Check Origin site domain and enter the WAF CNAME address.

        Note:

> For more information about how to view the WAF CNAME address, see *WAF deployment guide*.



c. Click Next.

d. Complete the Please choose Instance and ISP Line task.

3. Update the DNS settings of your domain name. Log on to the DNS host's system and add a CNAME record to redirect web traffic to the Anti-DDoS Pro CNAME address.

   For more information, see *Access Anti-DDoS Pro through a CNAME record*.

Result

All web requests to your website are redirected to Anti-DDoS Pro for cleanup and then redirected to WAF for inspection before they reach your origin server.

2.11 Deploy WAF and CDN together

You can deploy Alibaba Cloud WAF and CDN (Content Delivery Network) together to speed up your website and protect against web attacks at the same time. We recommend that you use the following architecture: CDN (entry layer, website speed up) > WAF (intermediate layer, web attacks protection) > Origin.

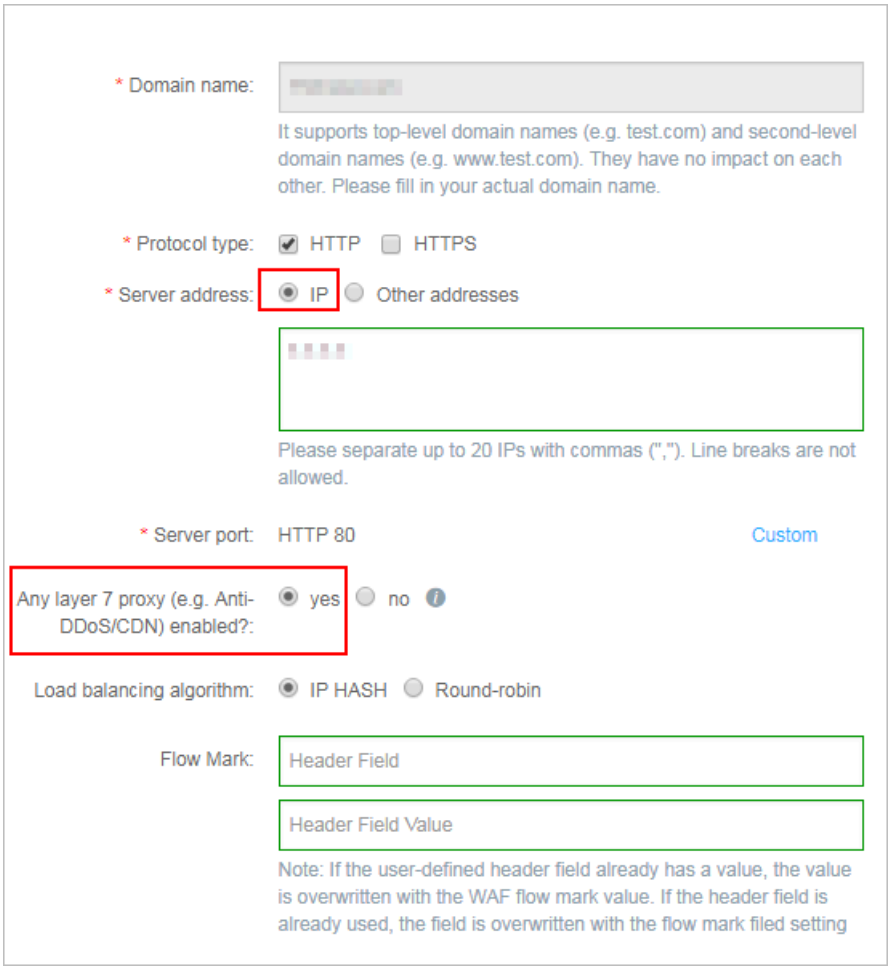
Procedure

Suppose you use Alibaba Cloud CDN. Follow these steps to deploy WAF and CDN together:

1. See *Get started with Alibaba Cloud CDN* to implement a CDN for your domain name.

2. Create a website configuration in Alibaba Cloud WAF.
   - Domain name: Enter the CDN-enabled domain name. Wildcard is supported.
   - Server address: Enter the public IP address of the ECS/Server Load Balancer instance, or the external server IP address of the origin server.
   - Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?: Check yes.

   For more information, see *Website configuration*.



3. When the website configuration is successfully created, WAF generates a dedicated CNAME address for it.

> **Note:**
> For more information about how to view the WAF CNAME address, see *WAF deployment guide*.

4. Modify the CDN configuration to change the origin site address to the WAF CNAME address.

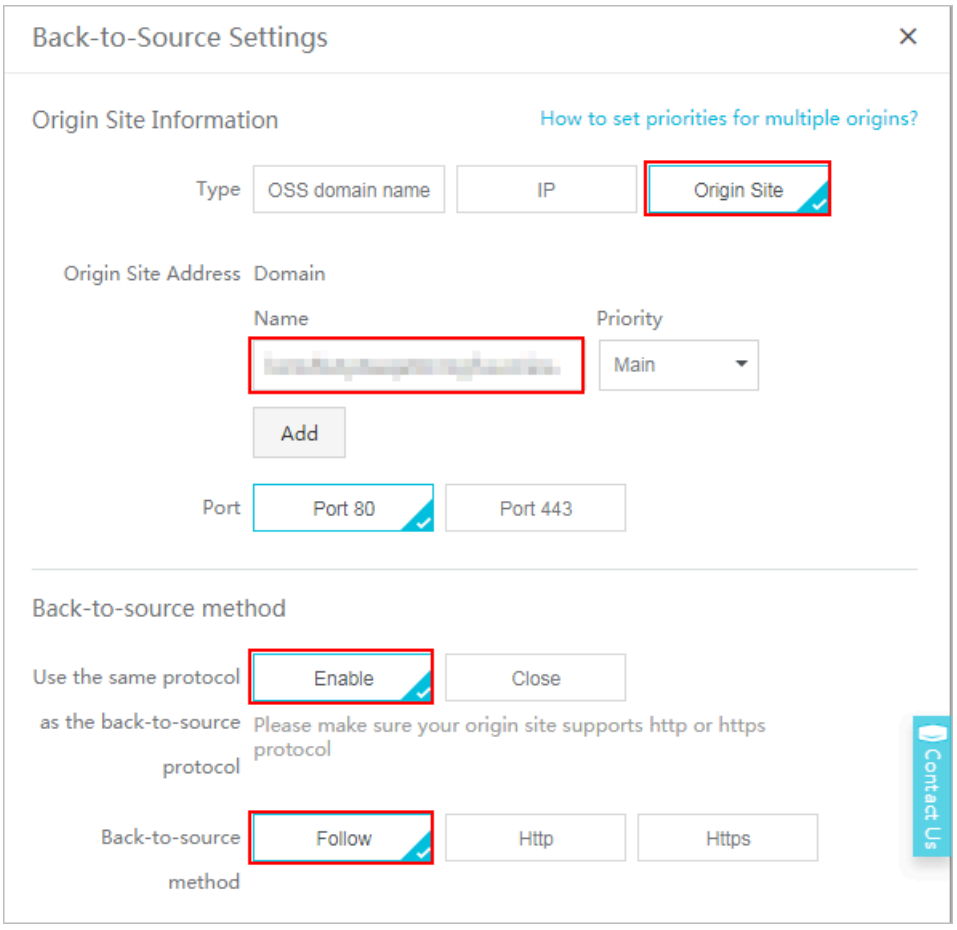
   a. Log on to the *Alibaba Cloud CDN console*.

   b. Go to the Domain Names page, select the domain to be configured, and click Configure.

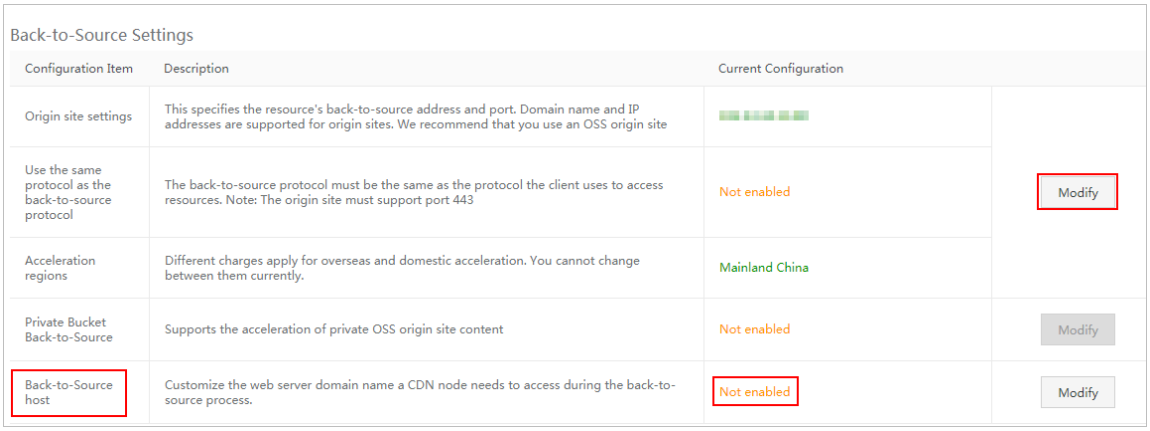
   c. Under Origin site settings, click Modify.

   d. Modify origin site information.

      - Type: Select Origin Site.
      - Origin site address IP: Enter the WAF CNAME address.
      - Use the same protocol as the back-to-source protocol: Select Enable.



   e. Under Back-to-Source Settings, make sure that Back-to-Source host is disabled.



After the operation is complete, the traffic goes through CDN, and the dynamic content continues to be checked and protected by WAF.

3 Protection configuration

3.1 Web application protection

Alibaba Cloud WAF protects your web resources against common Web application attacks, such as SQL injection and XSS cross-site attack. You can select a suitable inspection intensity, which includes loose, normal, and strict, to meet your actual needs.

Context

Once you have added your domain to the WAF protection list, you can enable Web application protection for it, and select a suitable protection policy at any time based on your actual needs. If you don't want to use the Web application protection function , you can disable it.

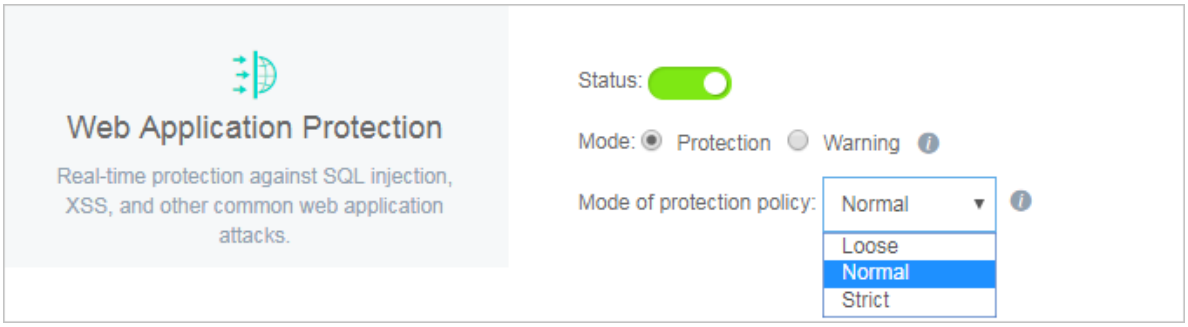
Make sure that you have added your domain to the WAF protection list before proceeding with the following operations. For more information, see *WAF deployment guide*.

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 Web Application Protection, and select the Mode.

Note:

If you don't want to use this function, you can disable it on this page.



- Protection: Blocks the request when an attack is detected.
- Warning: Alerts you when an attack is detected. You determine whether to block the request or not.

5. In the Mode of protection policy drop down box, select a protection policy:
   - By default, the Normal mode is selected.
   - Enable the Loose mode when you find many false positives or uncontrollable user inputs (for example, rich text editor and technology forum) with the Normal mode.
   - Enable the Strict mode when you require stricter protection against path traversal, SQL injection, and command running attacks.

3.2 Malicious IP Penalty

Malicious IP penalty helps you automatically block malicious IPs that attack your web assets repeatedly in a short period of time.

Function description

Traditional web application firewall products function in the IP-URL dimension. After determining whether a request is an attack, they only block this request once . However, malicious attackers may scan and attack your website repeatedly. These attackers observe and detect your website’ s vulnerabilities, study the protection policies, and plan attempts to bypass them.

To address this problem, Alibaba Cloud WAF provides the Malicious IP Penalty function. WAF detects and automatically blocks the malicious IP addresses, through which the website is attacked repeatedly.

WAF generates judging rules for malicious IP address through the database with a massive amount of malicious IP addresses. This database is backed with the machine

learning function of Alibaba Cloud platform that keeps studying and analyzing the attacks and attack frequencies of the malicious IP addresses. When an IP address starts continuous attacks, WAF blocks all access requests from this IP address.

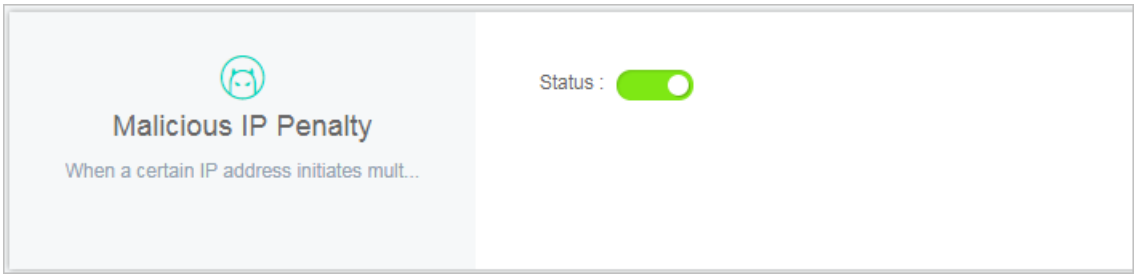
Procedure

Follow these steps to enable malicious IP penalty:

> 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 Malicious IP Penalty. The default protection rule is: when WAF detects two Web attacks by an IP in less than 1 minute, it blocks the IP's access request for 6 minutes.

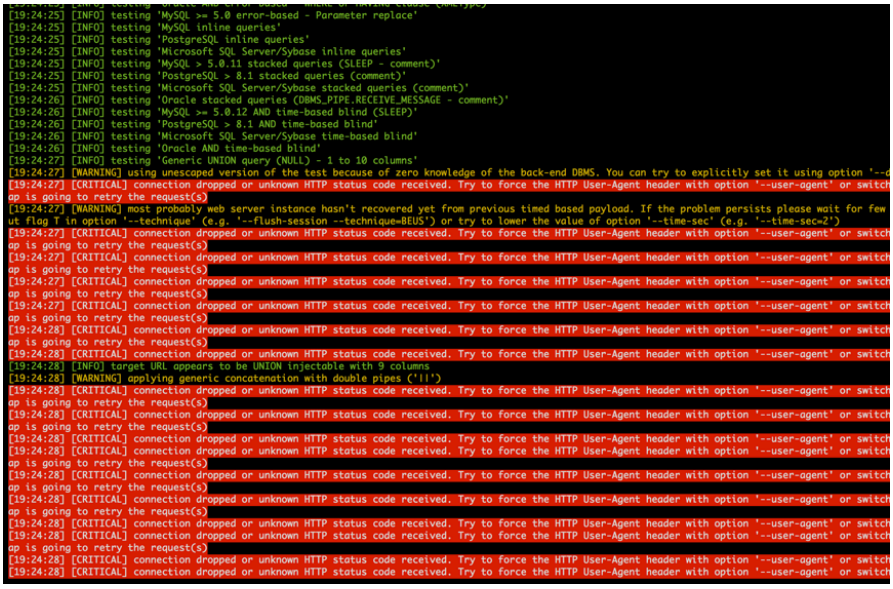
> Note:
> If you do not want to use malicious IP penalty, you can disable it on this page.



Test

Once the Malicious IP Penalty function is enabled, WAF scans the website to detect and automatically block the malicious attacks and access requests from them. This action can incur a higher cost to the hacker to start new attacks. The following is an actual effect test after malicious IP penalty is enabled.

With Malicious IP Penalty, WAF effectively blocks attacks from various automatic tools and scanners to safeguard your website.



3.3 New intelligent protection engine

New intelligent protection engine performs semantic analysis on requests. Using semantic detection, the engine can discover disguised or hidden malicious content in web requests and effectively intercept malicious attacks that use obfuscation, variants, and other alike methods.

Function description

New intelligent protection engine performs semantic analysis on requests and matches the semantic analysis results against its exception and attack set to discover disguised and hidden web attack behaviors.

> **Note:**
> New intelligent protection engine mainly protects against SQL injection and other web attack methods, rather than HTTP flood attacks. If you have high web attack protection requirements, we recommend that you enable new intelligent protection engine.

New intelligent protection engine has the following features:

- 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

Follow these steps to enable new intelligent protection engine:

> 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 New Intelligent Protection Engine.

> Note:
> If you do not want to use this function, you can disable it on this page.

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

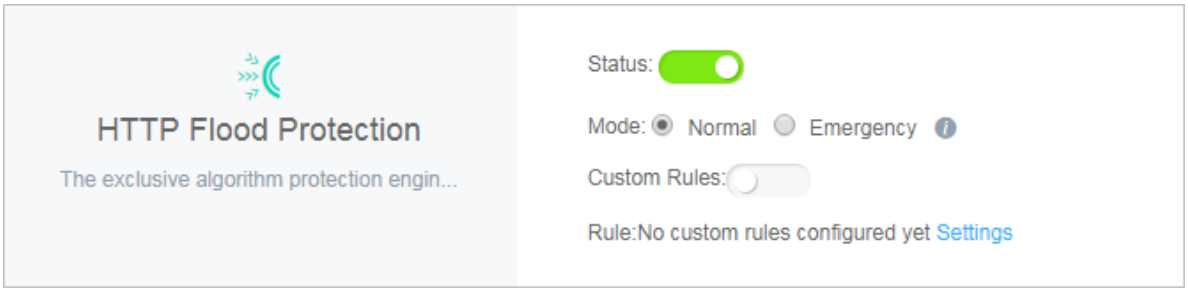
> **Note:**
> The Emergency mode is applicable to web pages, but not to API/Native Apps, because it may result in a large number of false positives. For API/Native Apps, you can use *Custom HTTP Flood Protection*.

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:



- 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 *Protec 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 ineffective, 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.

3.5 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

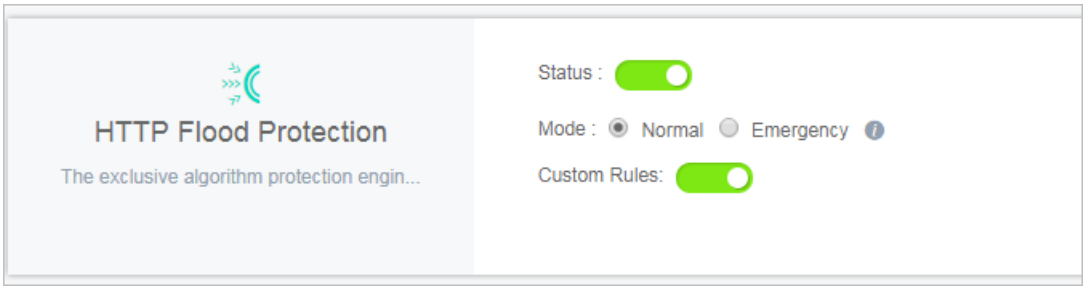
The frequency of certain URLs can be restricted from accessing your server by applying custom protection rules in the console. For example, you can define the following rule: when a single source IP address accesses `www.yourdomain.com/login.html` for more than 20 times within 10 seconds, then block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

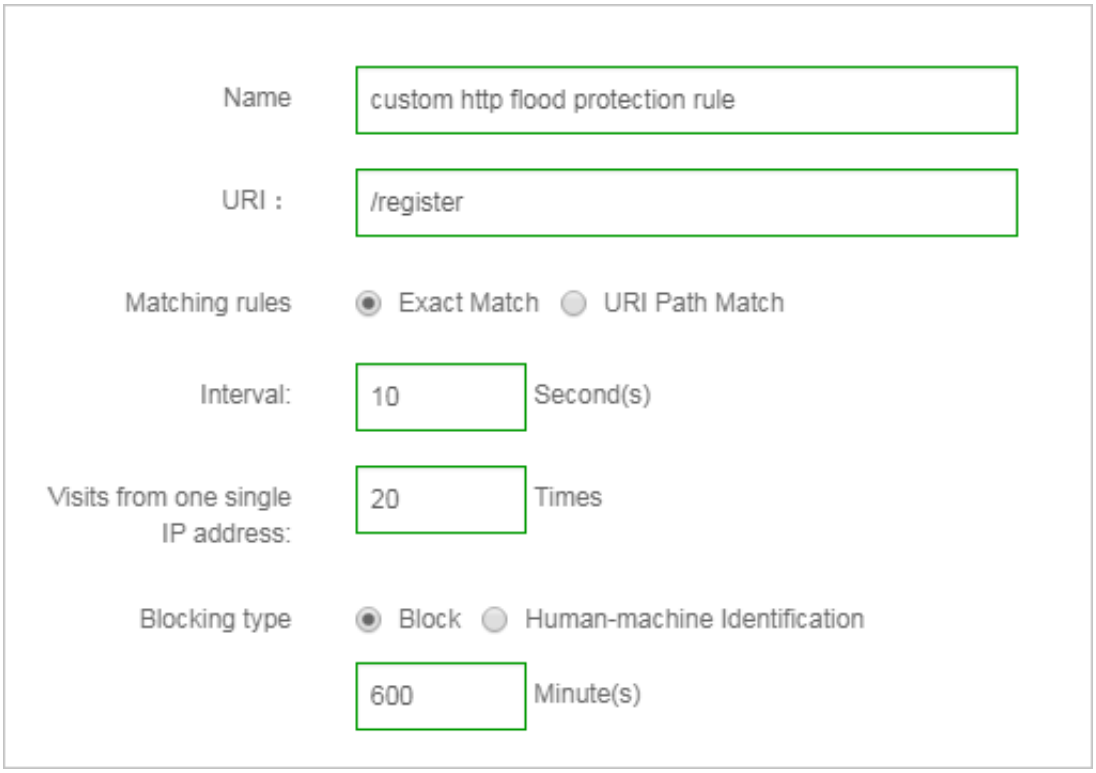
1. Log on to the *Alibaba Cloud WAF console*.
2. Go to the Management > Website Configuration page, and select the region of your WAF instance (Mainland China or International).
3. Select the domain to be configured, and click Policies.
4. Enable HTTP Flood Protection (Normal mode) and Custom Rules,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



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.



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.

3.6 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 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.	· 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.

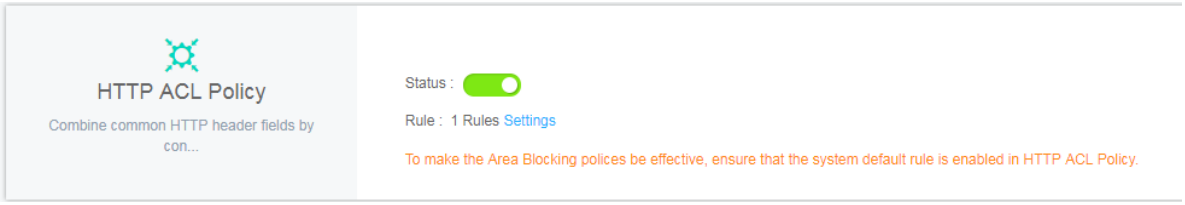
Procedure

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*.

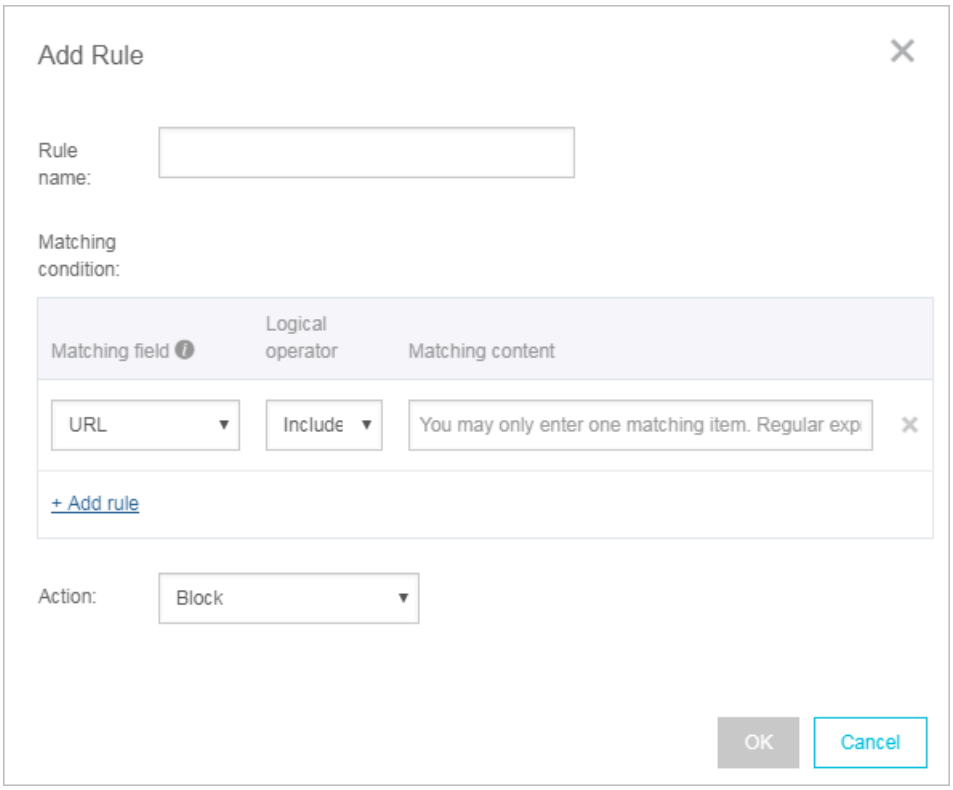
1. Log on to the *Alibaba Cloud WAF console*.
2. Go to the Management > Website Configuration page, and select the region of your WAF instance (Mainland China or International).
3. Select the domain to be configured, and click Policies.

4. Enable HTTP ACL Policy, and click Settings.



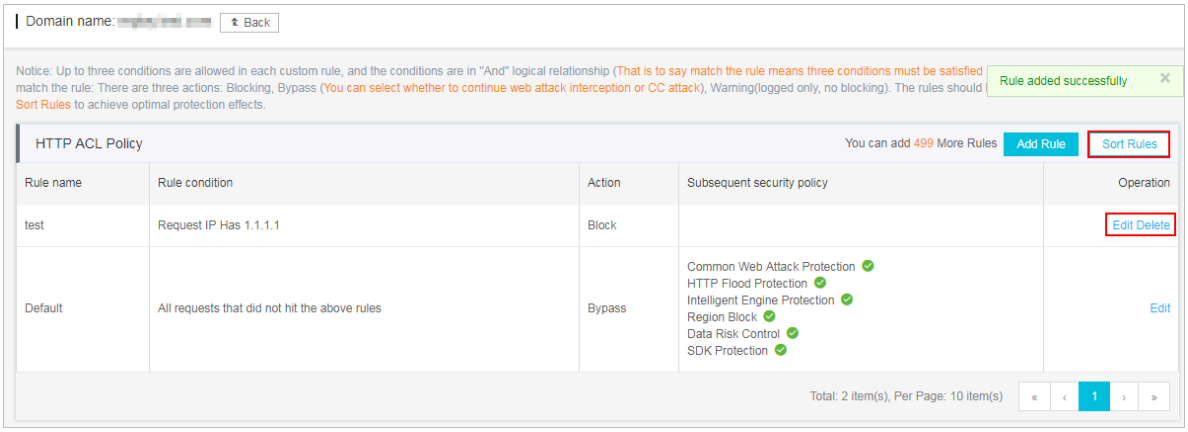
5. Click Add Rule, configure the expected rule, and click OK.

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



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.



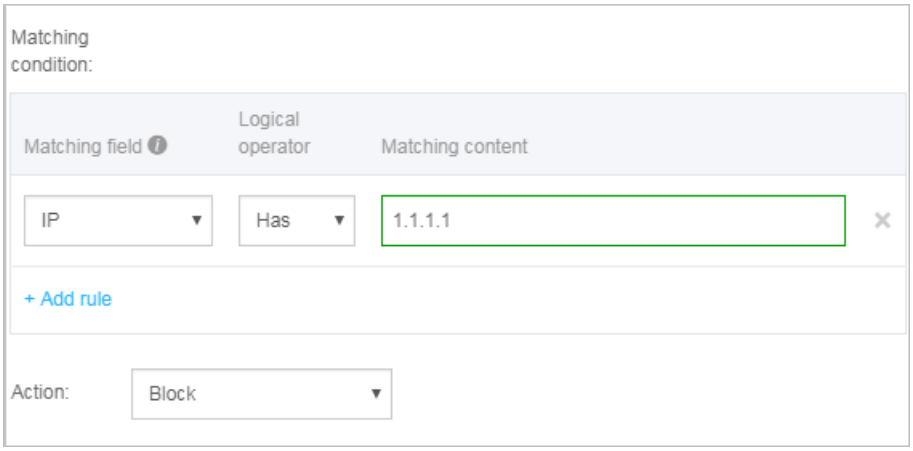
Configuration examples

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.

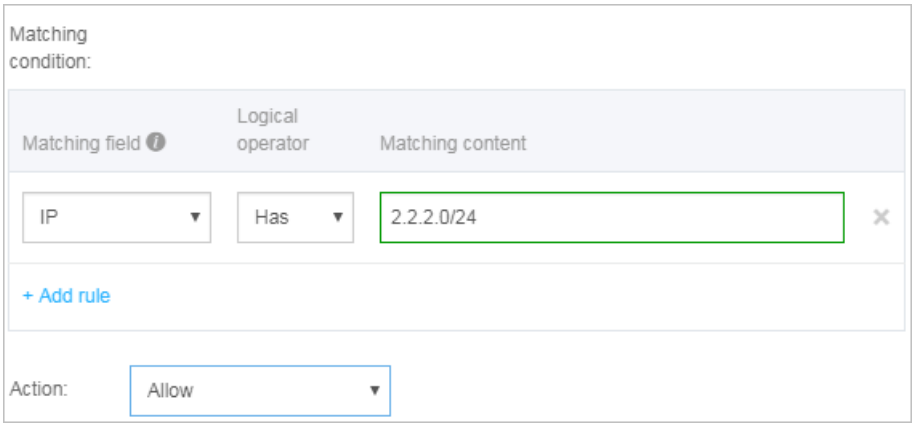
Some examples are as follows.

Configure IP blacklist and whitelist

Use the following configuration to block all access from 1.1.1.1.



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



Note:

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

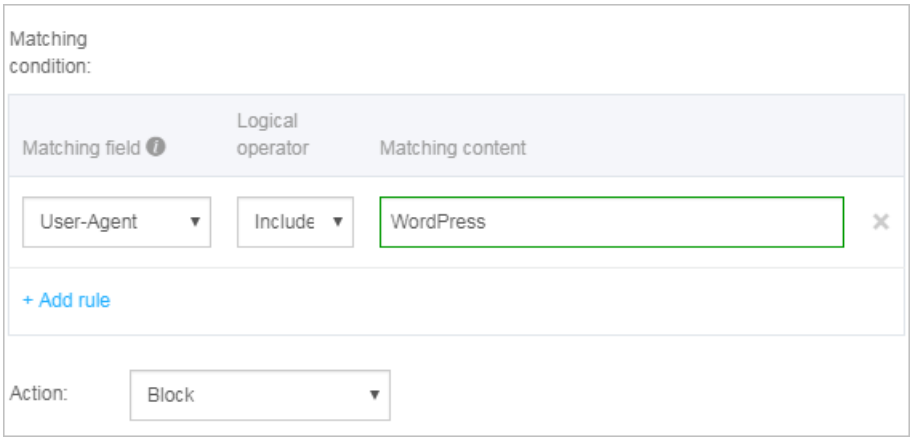
For more information, see *Set up IP whitelist and blcaklist*.

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

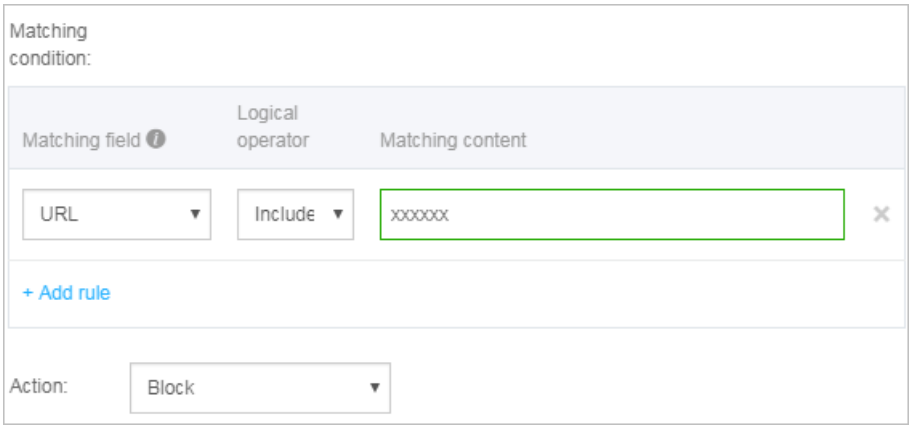
Use the following configuration to defend against this type of attack.



For more information, see *Prevent Wordpress pingback attacks*.

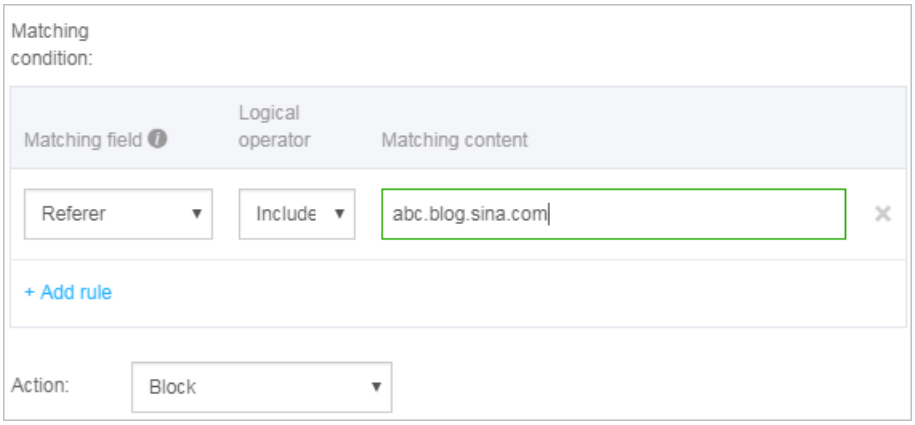
Block specific URLs

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



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.



3.7 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 Enterprise Edition or above. For more information about the upgrade, see *Renewal and upgrade*.

To enable and specify blocked regions, follow these steps:

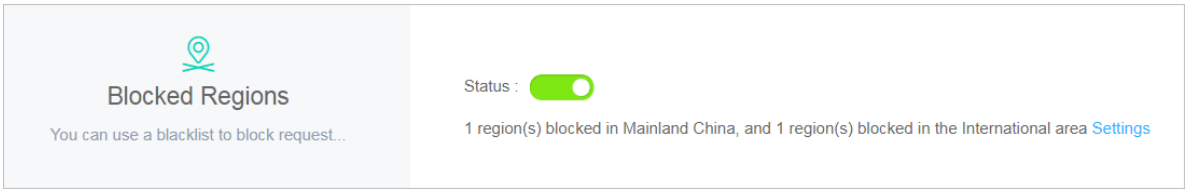
Note:

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.

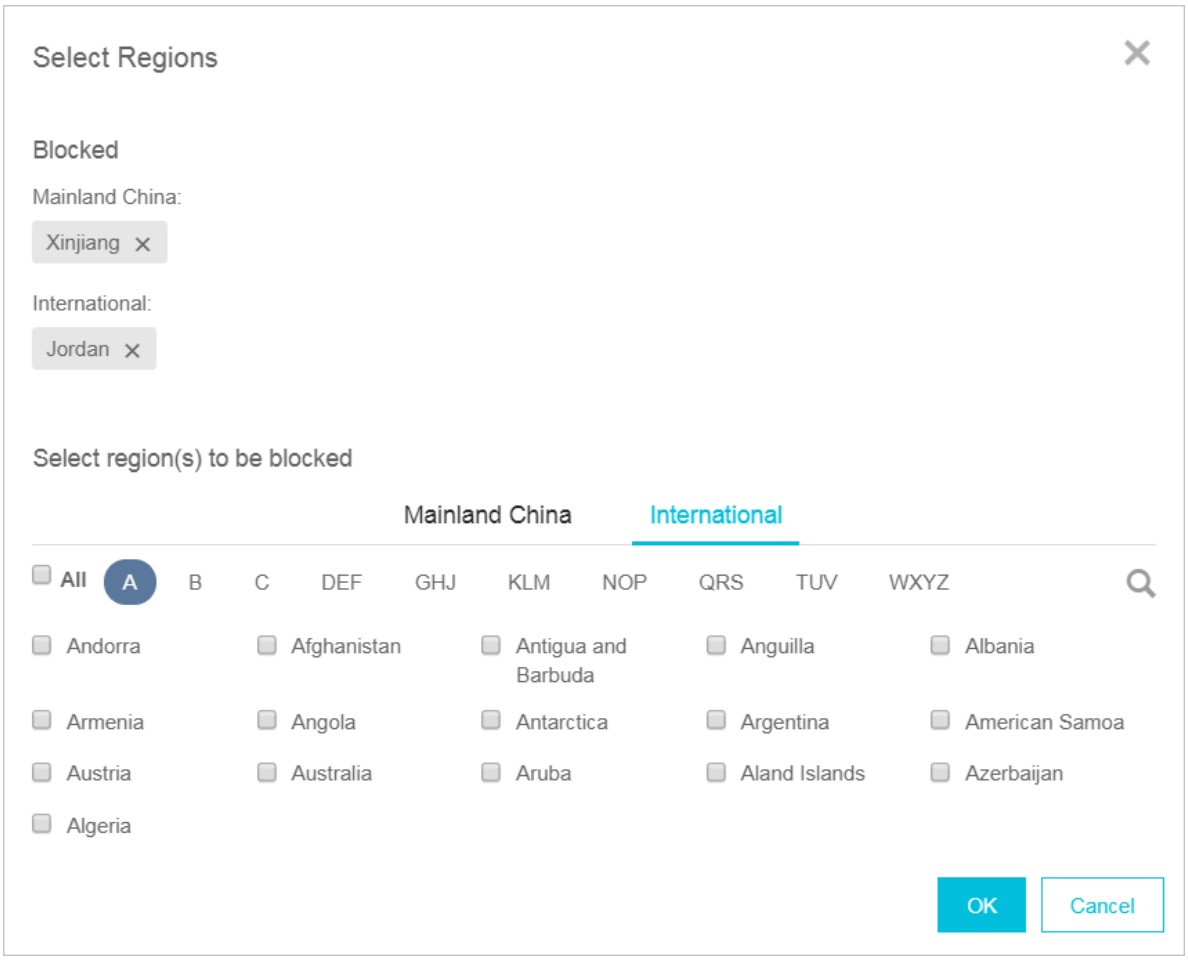
   Note:
   To make the Area Blocking polices be effective, ensure that the system default rule is enabled in HTTP ACL Policy.

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.



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*.

3.8 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.

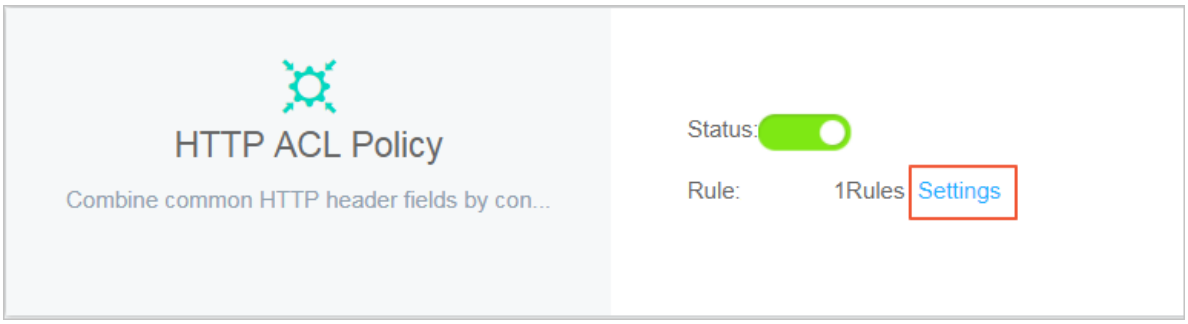
Procedure

Follow these steps to configure a whitelist or blacklist:

Note:

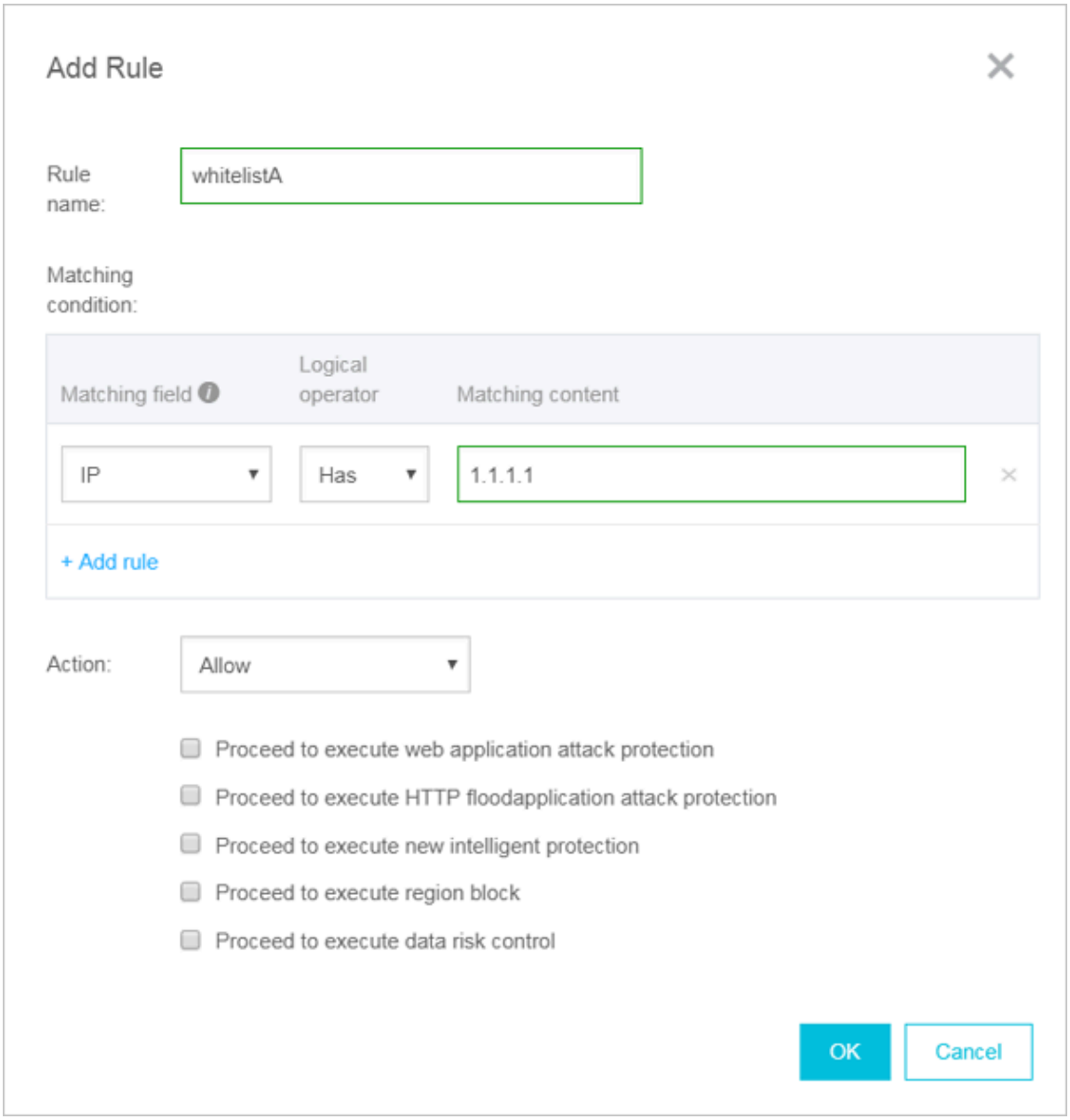
Make sure that you have added your domain to the WAF protection list before proceeding with the following operations. For more information, see *WAF deployment guide*.

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.**



5. Click Add Rule.

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



> **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.

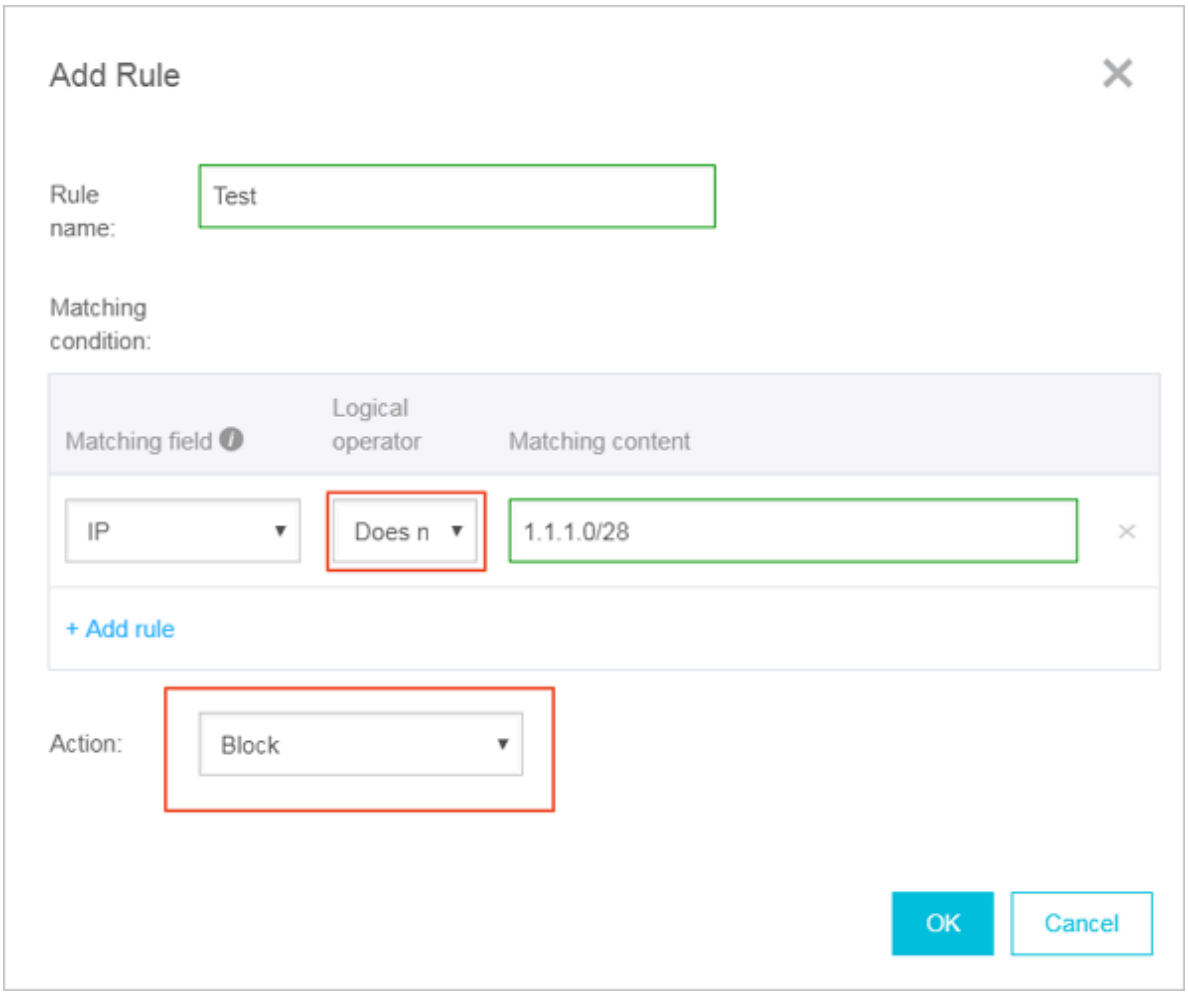
   - Similarly, you can also follow this procedure to set blacklist for a specific domain.

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.



- 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.

3.9 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.

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*.

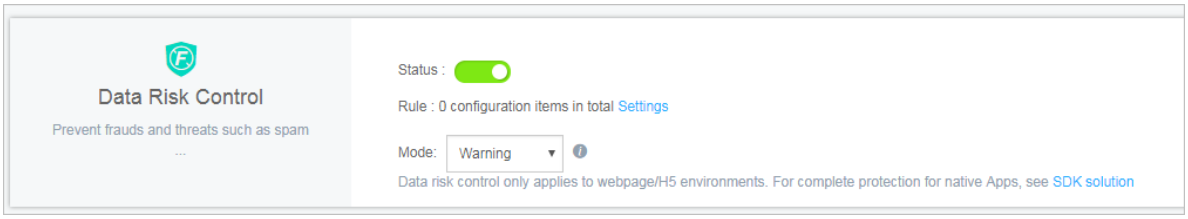
1. Log on to the *Alibaba Cloud WAF console*.

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.

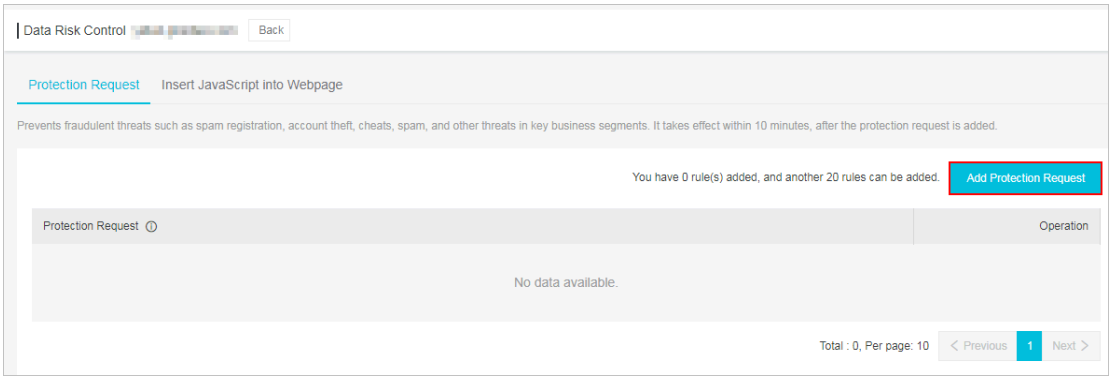
> Note:
> When enabled, Data risk control will inject JavaScript code into your webpage for detecting malicious behaviors, and disable all gzip compression settings. Even if your website uses a non-standard port, no additional configuration is required in data risk control. The JavaScript can be inserted 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.

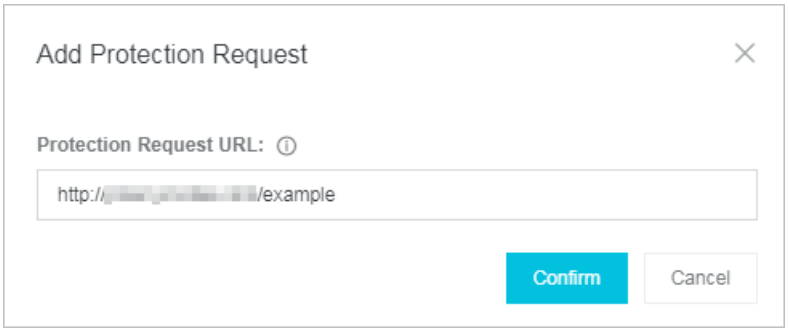
> Note:
> The warning mode is used by default. Data risk control does not block any request, but injects JavaScript code into webpages to analyze behaviors on the client.



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.



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



     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.

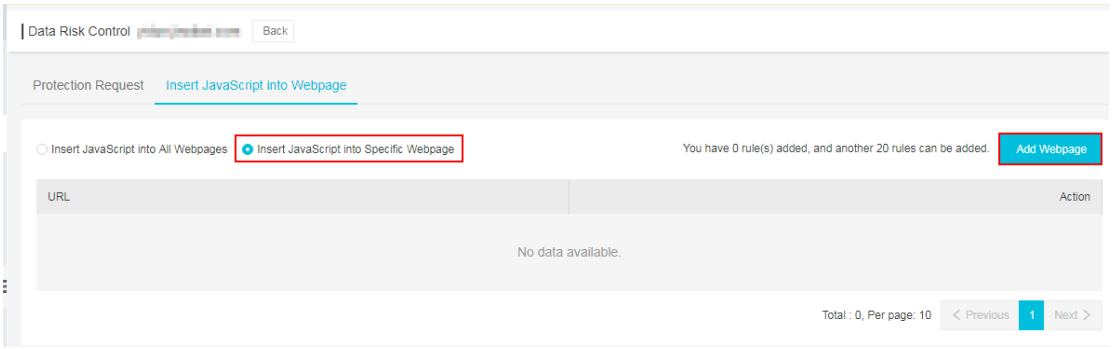
The successfully added protection request takes effect in about ten minutes.

- 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.

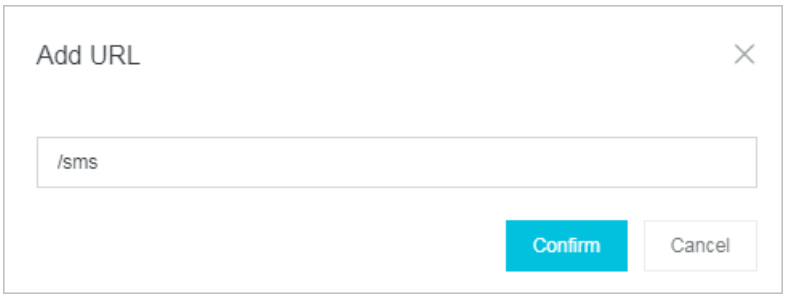
a. On the Insert JavaScript into Webpage tab page, click Insert JavaScript into Specific Webpage.



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.



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,

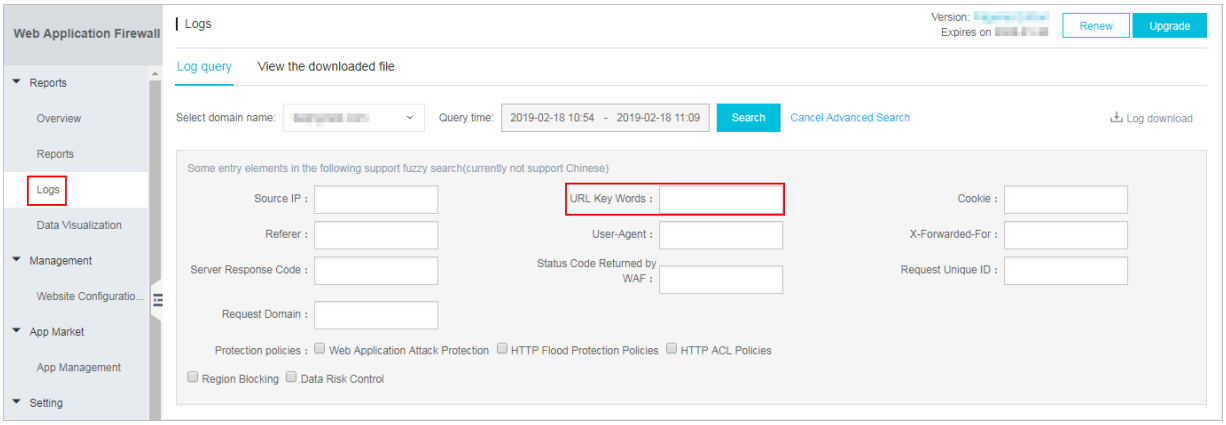
- The following figure shows the log that the user passed the validation test of data risk control.

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.

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.



3.10 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

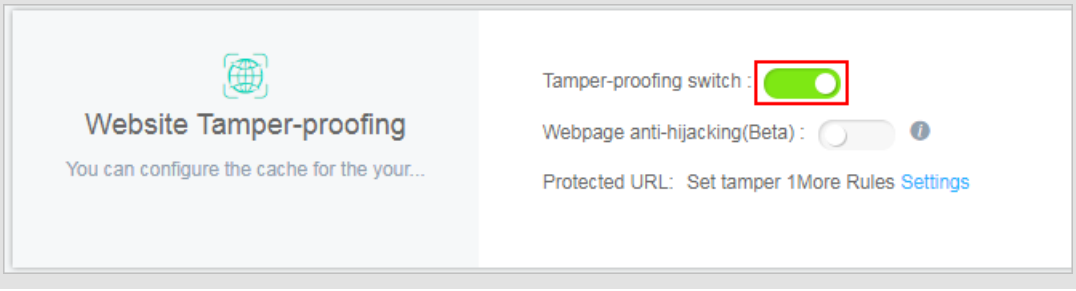
> **Note:**
> Make sure that you have implemented WAF for your website before performing this configuration. For more information, see *Implement Alibaba Cloud WAF*.

Procedure

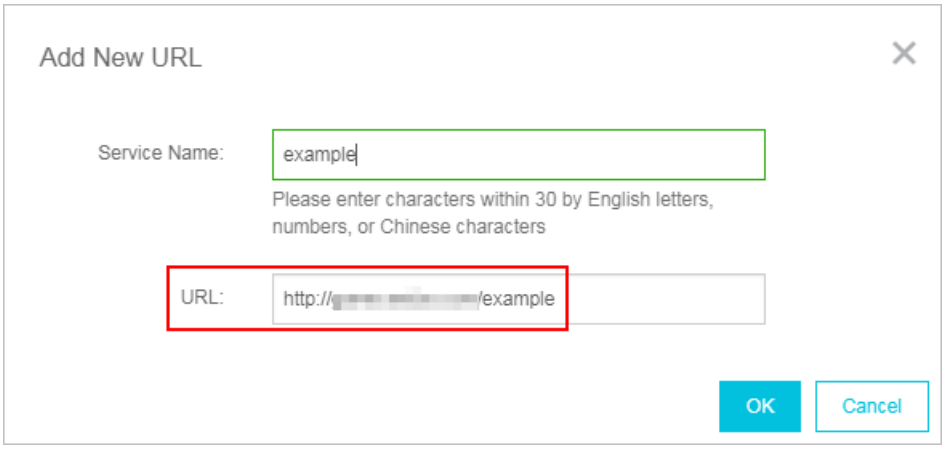
1. Log on to the *Alibaba Cloud WAF console*.

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.

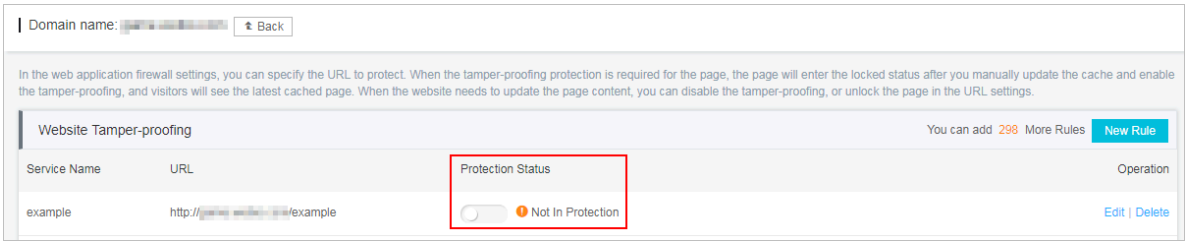


5. Click New Rule and complete the configuration in the Add New URL dialog box.

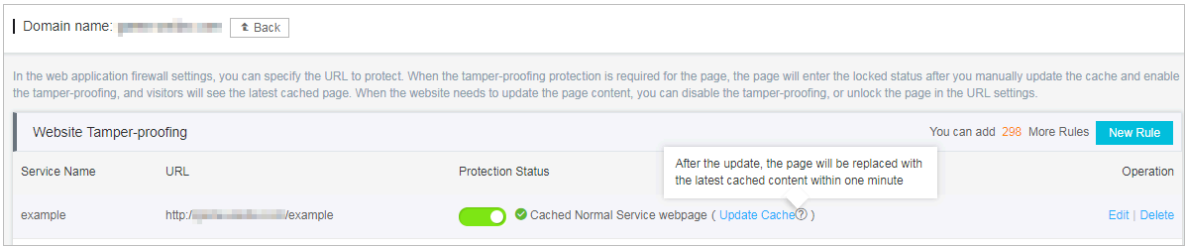


- Service Name: Name this rule.
- URL: Specify the exact path of the web page to be protected. Wildcard characters (such as `/*`) or parameters (such as `/abc? xxx=`) are not supported. WAF can protect all text, HTML, and pictures under this path against tampering.

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.



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.



3.11 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 informatio n. 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.

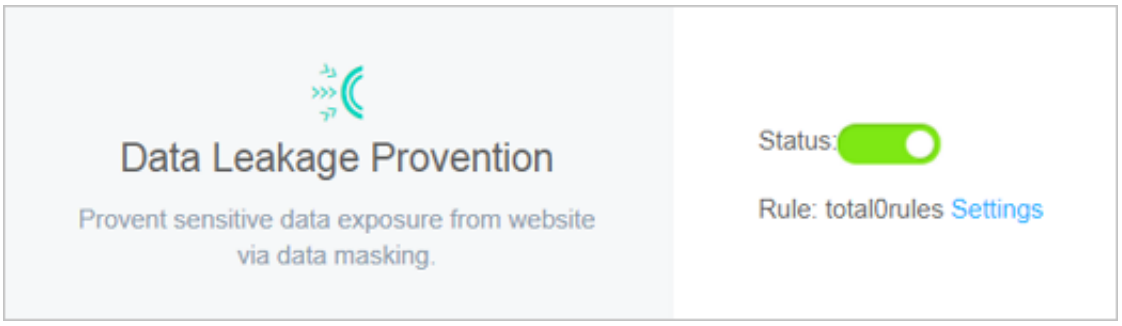
The data leakage prevention function supports Content-Types including `text/*`, `image/*`, and `application/*` and covers web terminals, app terminals, and API interfaces.

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.

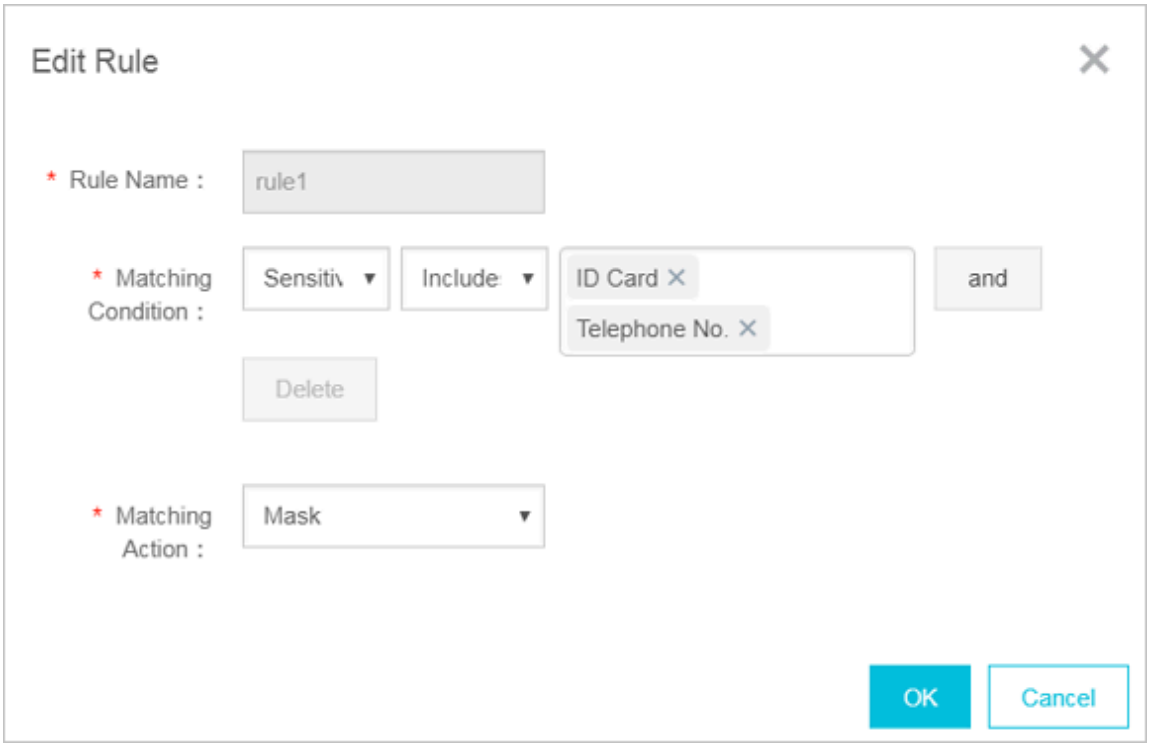


5. Click Add Rule to add a sensitive information protection rule.

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.

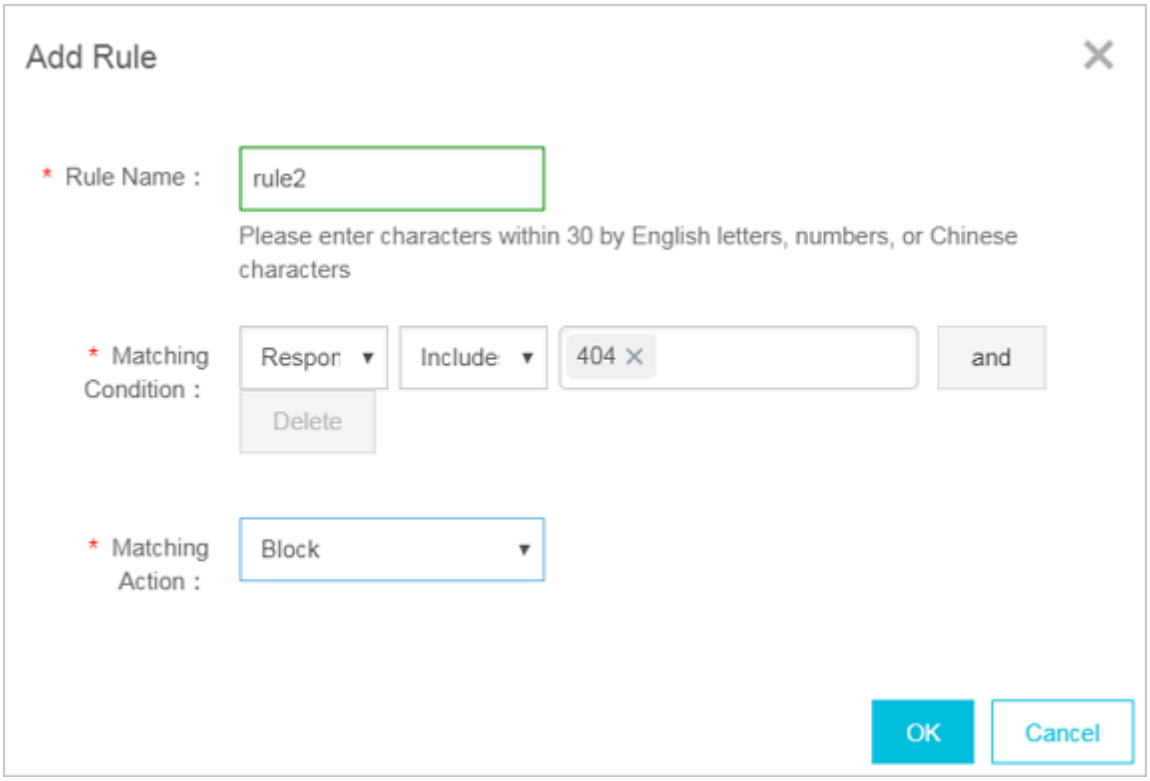


After setting this protection rule, mobile phone and ID card numbers displayed on all webpages in this website are automatically desensitized.

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.

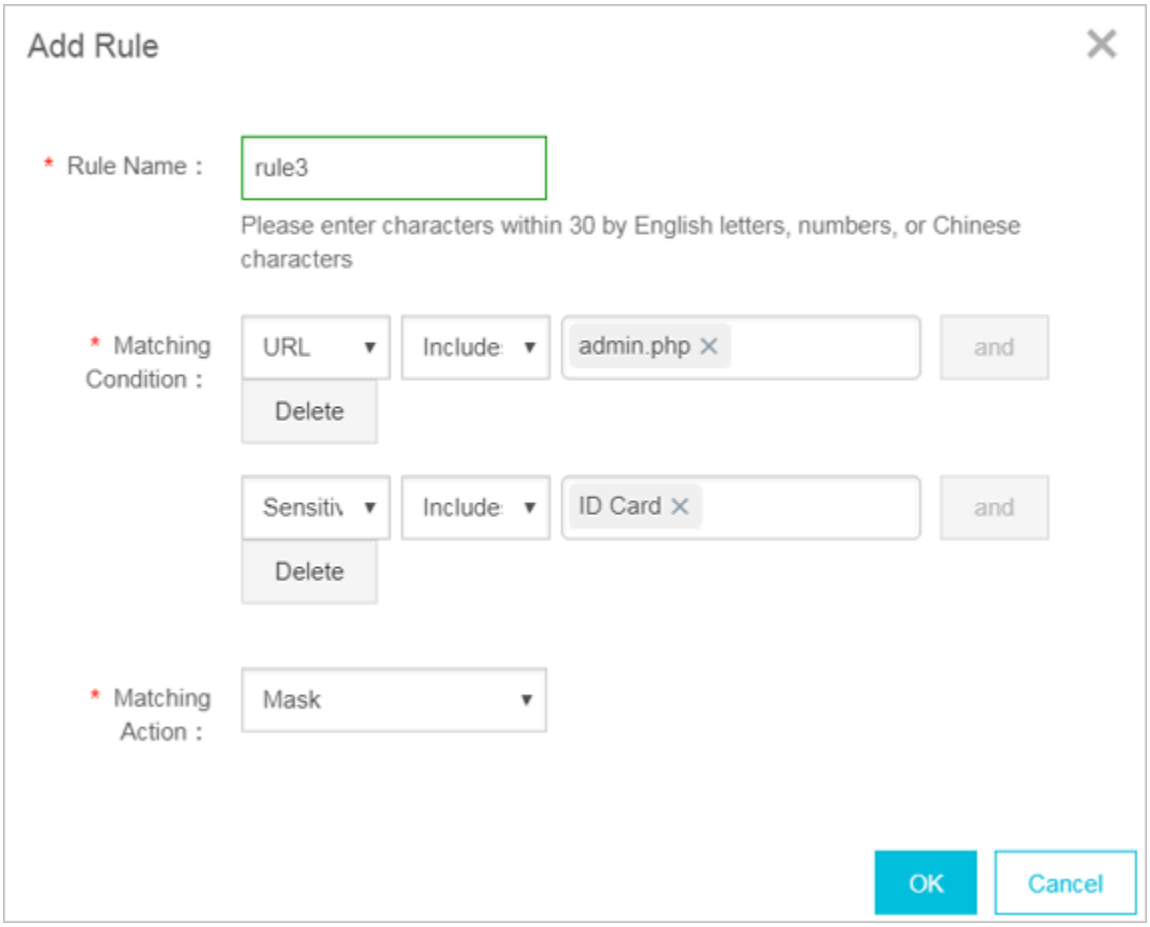
- Status code blocking: You can set rules to block or warn of specific HTTP request status codes to avoid leaking sensitive server information. For example, you can set the following protection rule to block HTTP 404 status codes.



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.



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.

4 Protection reports

4.1 Business and security overview

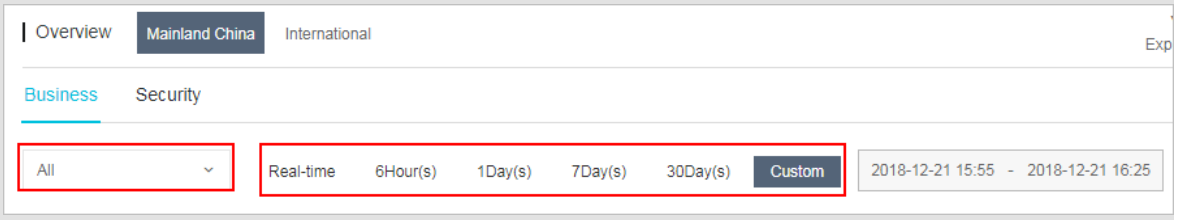
The Alibaba Cloud WAF Overview page gives you a glimpse of the business and security environment of a WAF-enabled site.

View business overview

Follow these steps to view the business overview page:

1. Log on to the *Alibaba Cloud WAF console*.
2. Go to the Reports > Overview page and select the region of your WAF instance (Mainland China or International).
3. On the Business tab page, select a domain name and time period to display the business summary of the specified domain name during the time period. The time period options include Real-time, 6 Hours, 1 Day, 7 Days, 30 Days, or Custom.

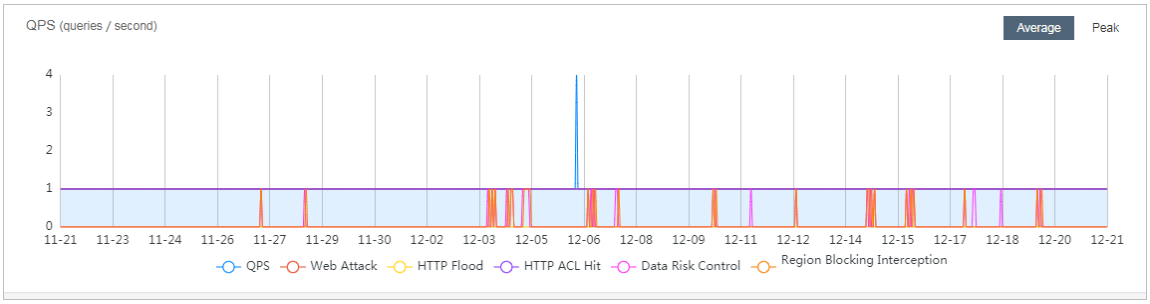
> **Note:**
> The business statistics for the last 30 days can be viewed. You can use Custom to specify a time period within the last 30 days to view the record.



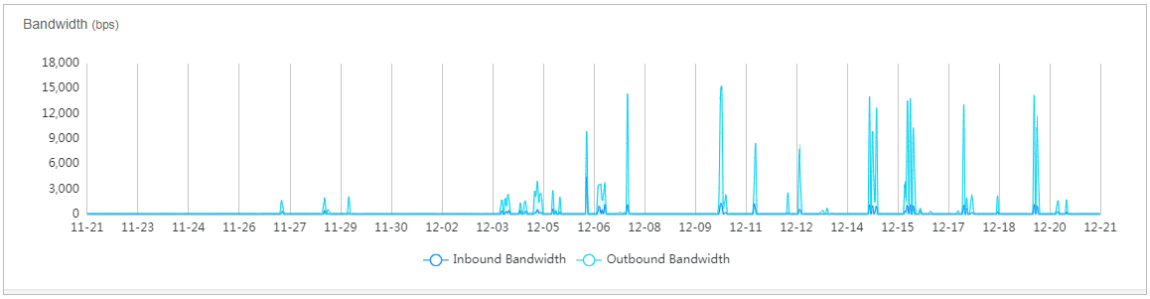
The business overview includes the following information:

- QPS: This graph displays all queries per second and the number of suspicious requests that hit the Web Attack, HTTP Flood, HTTP ACL, Data Risk Control, or Region Blocking Interception rules, in queries/second. The sampling interval is

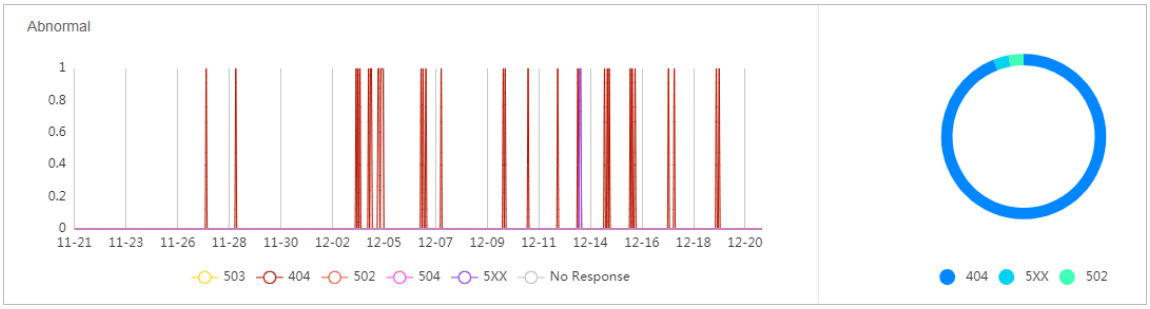
one minute. You can choose the data type (Average or Peak) to display or click the legend icon below the graph to clear or display the corresponding record.



- Bandwidth: This graph displays the inbound and outbound bandwidth, in bit/s. The sampling interval is one minute. You can click the legend icon below the graph to clear or display the corresponding record.

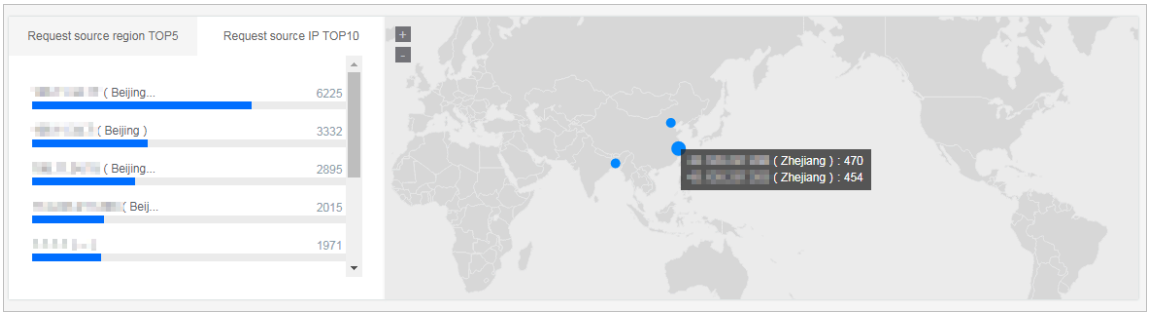


- Abnormal: This graph displays the number of HTTP error codes, such as 404, 502, 503, 504, 5XX, and No Response. The sampling interval is one minute. Next to the chart, a pie chart is provided showing the proportion of each error code. You can click the legend icon below the graph to clear or display the corresponding record.

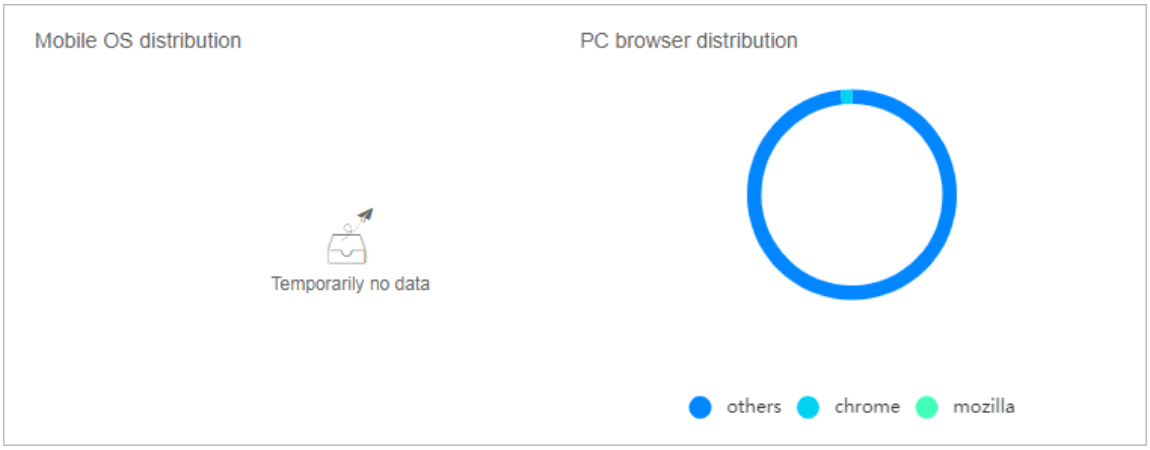


- Request source region TOP5 or Request source IP TOP10: This bar chart displays the top 5 regions that most requests originate from or the top 10 client IP addresses that send most requests. Next to the bar chart, a world map is

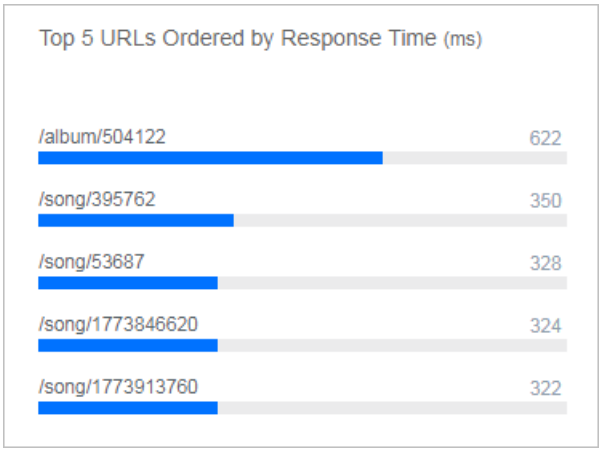
provided showing the corresponding IP location record. You can place the pointer over a blue dot to view details.



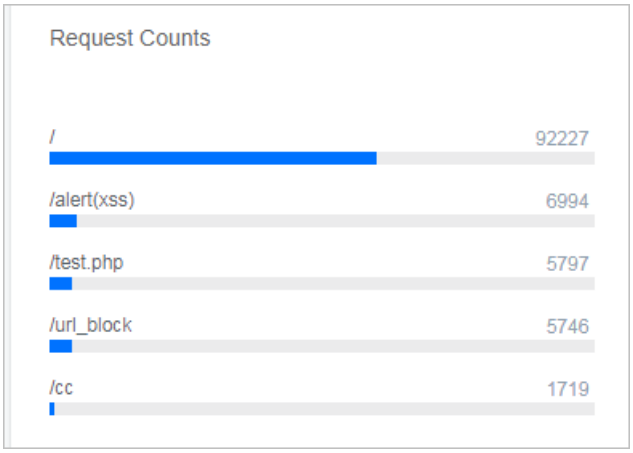
- Mobile OS distribution and PC browser distribution: These two pie charts display the system distribution of access requests from mobile or PC clients.



- Top 5 URLs Ordered by Response Time: This bar chart displays the top 5 URLs with the longest response time and their response time in ms.



- Request Counts: This bar chart displays the top 5 most frequently accessed paths and the corresponding request count.

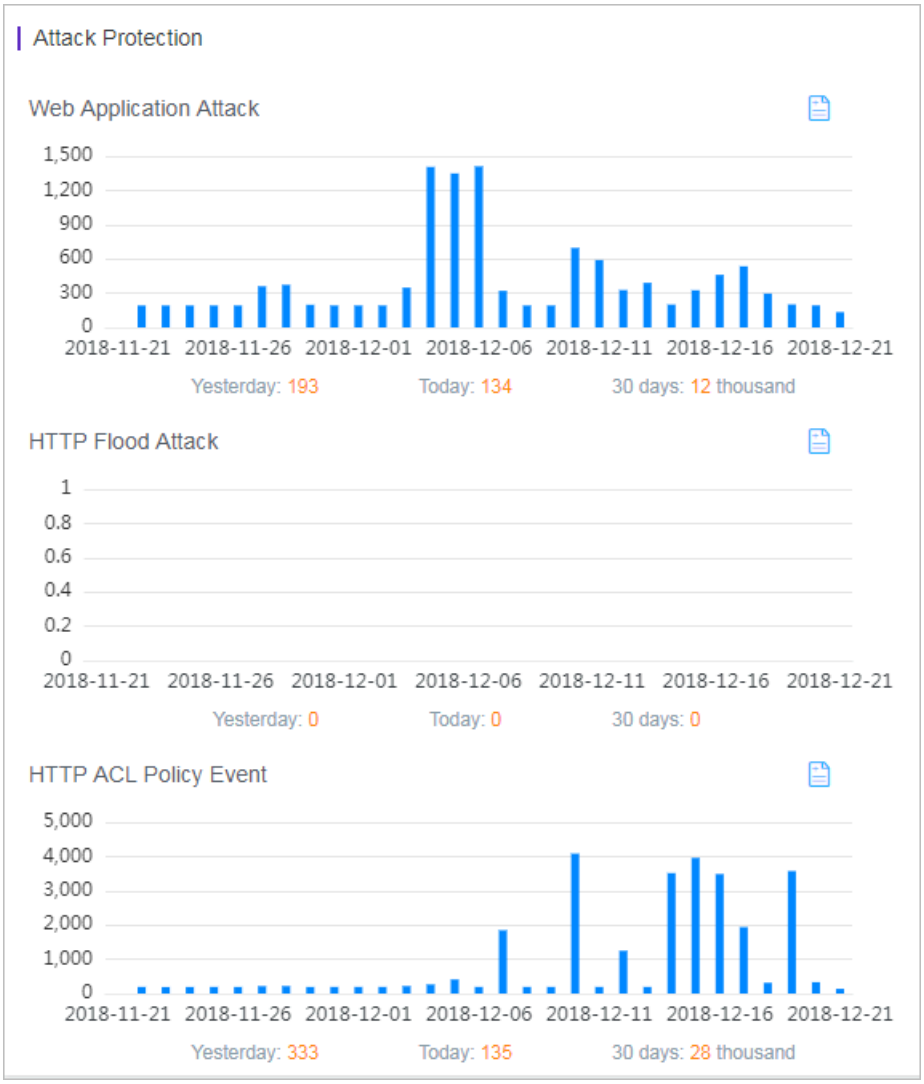


View security overview

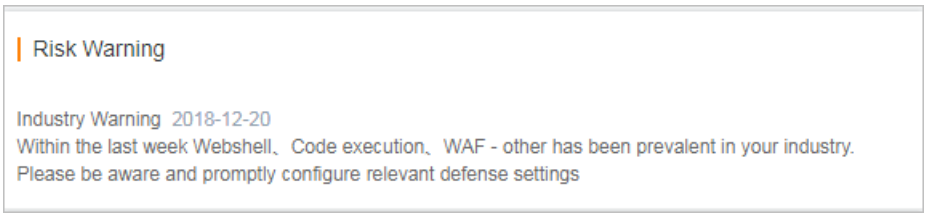
Follow these steps to view the security overview page:

1. Log on to the *Alibaba Cloud WAF console*.
2. Go to the Reports > Overview page and select the region of your WAF instance (Mainland China or International).
3. Go to the Security tab page to view the following security summary information:
   - Attack Protection: These bar charts show statistics for the Web Application Attack, HTTP Flood Attack, and HTTP ACL Policy Event over the last 30 days. You

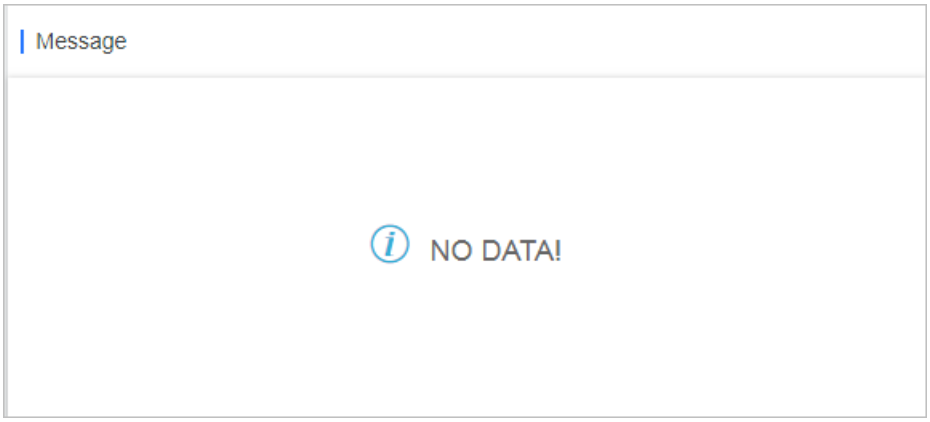
can place the pointer on a record to view details, or click the icon to go to the corresponding *Attack protection report*.



- Risk Warning: This area lists the new security risks that WAF finds on your site and the latest security risks in your industry. Protection suggestions are also provided. You can click View reports to go to the corresponding *Risk warning report*.



- Message: This area lists WAF protection rule updates for the latest vulnerabilities. You can click View to view the corresponding vulnerability announcement.



4.2 Attack protection report

This topic describes how to view the attack protection report.

Context

Alibaba Cloud WAF provides security reports for you to view and understand all protection actions of WAF. The 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.

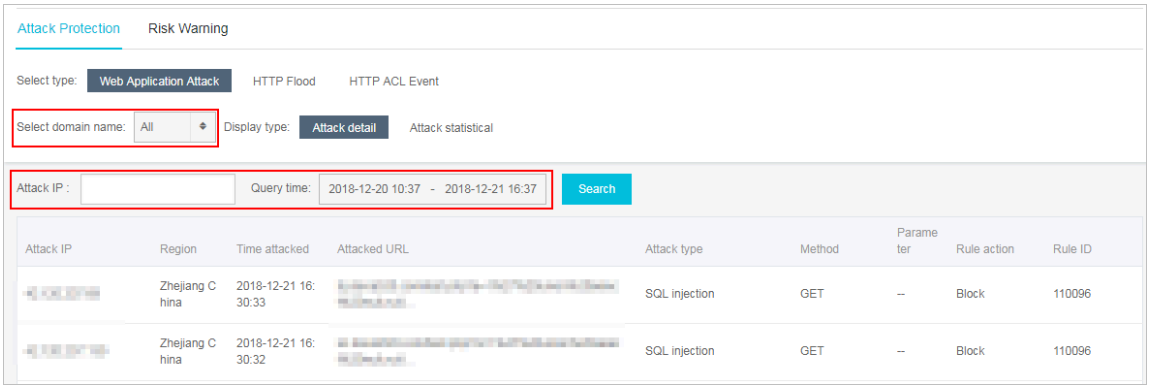
  For more information about how to use the risk warning report, see *Risk warning report*.

Procedure

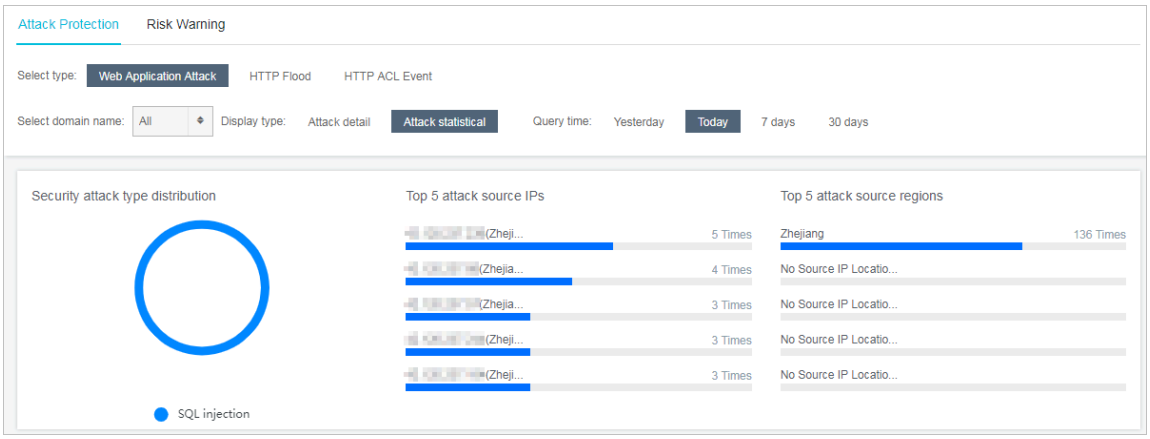
1. Log on to the *Alibaba Cloud WAF console*.
2. Go to the Reports > Reports page.
3. On the Attack Protection tab page, select the attack type to view the detailed records.
   - Web Application Attack: displays records of all Web attacks inspected by WAF. You can filter the records based on domain names, attack IP addresses, and attack time.

     Note:

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



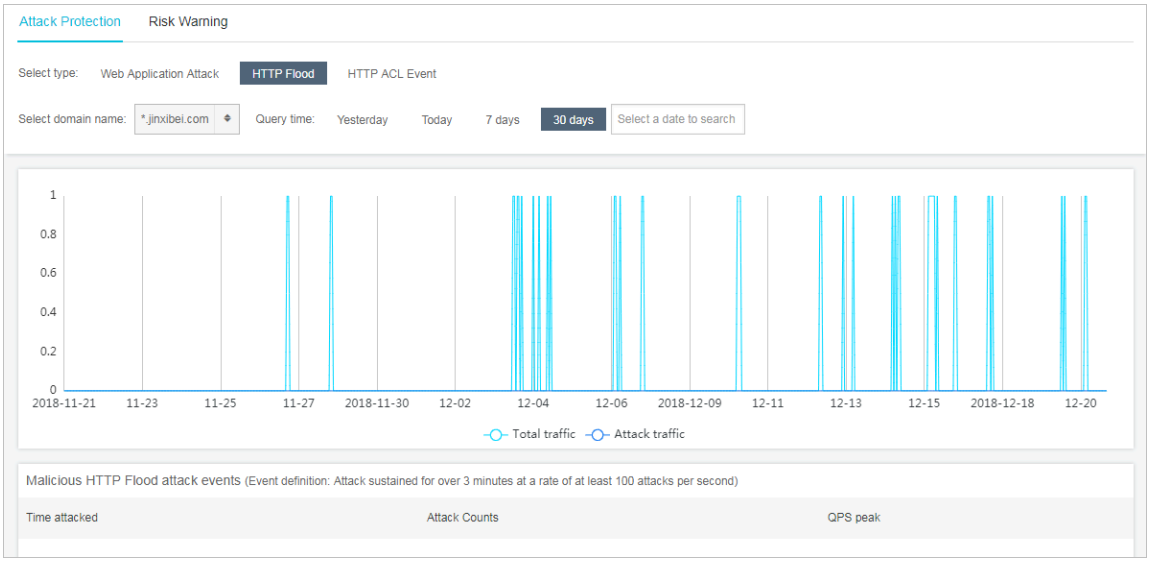
By default, the records are displayed in details. You can also view the attack statistics. Attack statistics displays the distribution of security attack types, top 5 attacker source IP addresses, and top 5 attacker source regions.



- 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*.

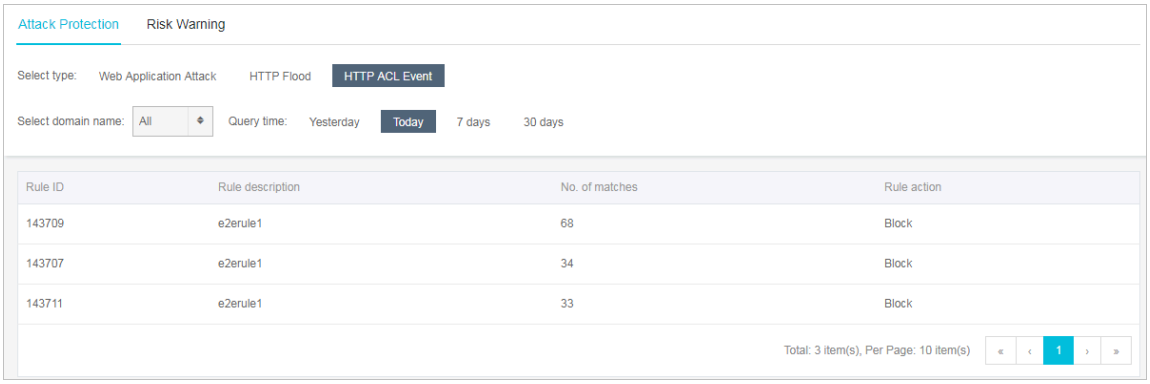


The real-time total QPS and attack QPS records are displayed at the top of the page, and all HTTP flood events are displayed at the bottom of the page. Alibaba Cloud WAF defines the HTTP flood attack as follows: attack duration > 3 minutes and attack frequency (per second) > 100.

- 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*.



4.3 Log search

When the Log search feature is enabled, Alibaba Cloud WAF helps you record all web requests to your website and enables you to search the stored logs for business analysis or security management.

Context

You must upgrade Alibaba Cloud WAF Pro to the Business or Enterprise plan to use this feature. For more information, see *Renewal and upgrade*.

> Note:
> The international WAF instance must be upgraded to the Enterprise edition to use this feature.

With the log search function, you can easily complete the following O&M tasks:

- Check the action (block or allow) WAF performs on a specific request.
- Check the type of rule that terminated a request: web attack protection rule, HTTP flood attack protection rule, or custom access control rule.
- Check the response time of a specific request to see if the origin server response timed out.
- Use a combination of field filtering conditions to search for specific requests. For example, source IP address, URL keyword, cookie, referer, user-agent, X-forwarded-for, server response status code, and more.

> Note:
> When you enable the Log search function, this constitutes your permission for Alibaba Cloud to record all of the web requests that are inspected by WAF (POST data is not recorded).

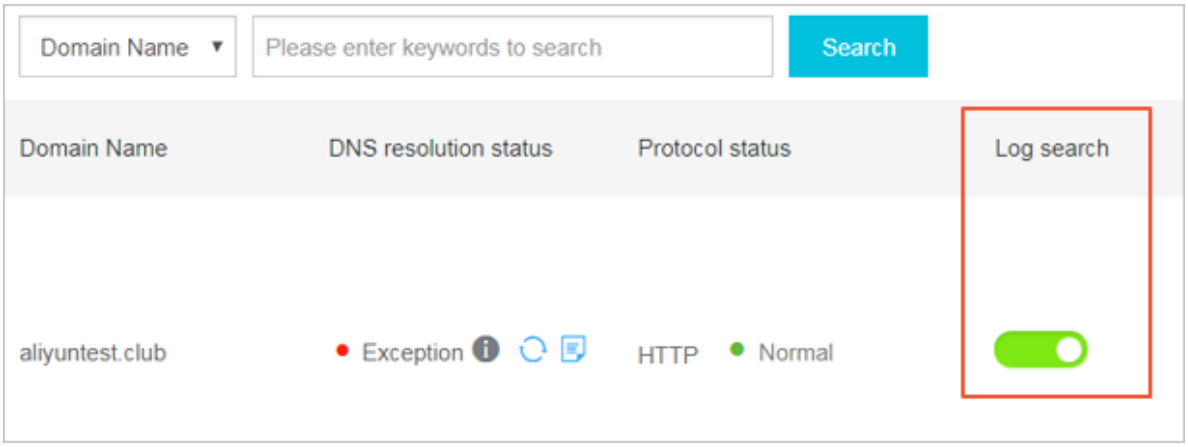
As a prerequisite, you must go to the Website Configuration page to enable the log search function for a specific domain name. Alibaba Cloud WAF starts recording request logs for the website only when the Log search switch is on. When Log search is enabled, you can go to the Logs page to search for logs of the domain name.

> Note:
> You can view the request log for up to 100 domain names.

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 name to be configured and enable Log search for it.

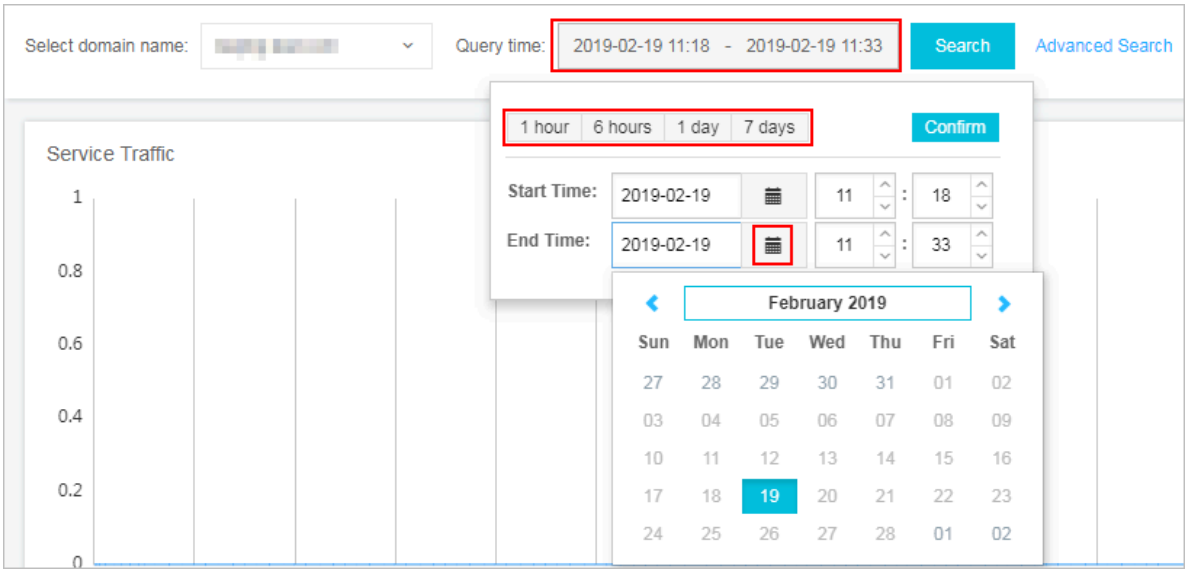
> Note:
> You can also disable Log search on this page. When Log search is disabled, the request log is no longer recorded. Even if you enable Log search again, you cannot query the request log for the time during which the function is disabled.



4. Go to the Reports > Logs page.
5. Select the domain name, Query time and click Search.

> Note:

Only the latest 30 days' logs can be accessed.



You can also click Advanced Search to define more detailed search conditions.

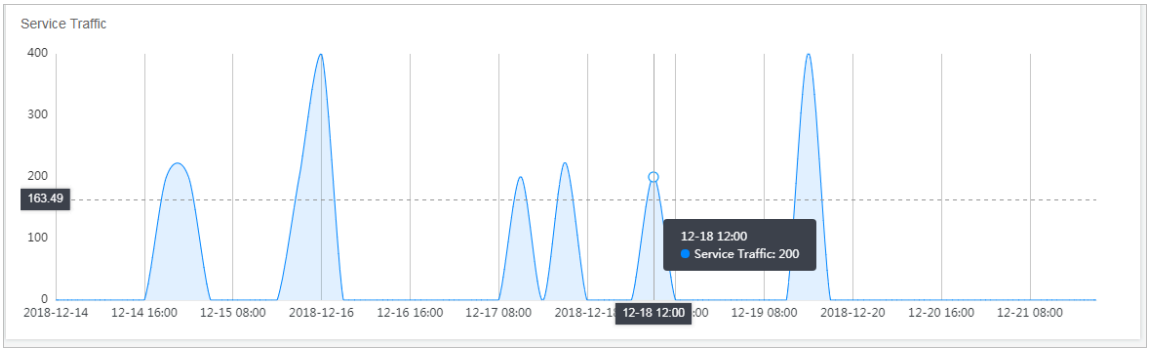
Table 4-1: Advanced search fields

Field	Description
Source IP	The source IP address.
URL Key Words	The requested URL. Note: This field supports the "/" symbol. For example, you can enter `/NTIS/casier`.
Cookie	The client-side cookie, which is included in the request header.
Referer	The referer field in the HTTP request header.
User-Agent	The user agent string in the request that identifies the client browser, operating system, and more.
X-Forwarded-For	The XFF field in the request header.

Field	Description
Server Response Code	The response status code that Alibaba Cloud WAF received from the origin server.  Note: A three-digit number is supported. You can also specify the -symbol to search for requests that have no response status information. For example, the request was blocked.
Status Code Returned by WAF	The response status code that Alibaba Cloud WAF returned to the client.  Note: A three-digit number is supported. You can also specify the -symbol to search for requests that have no response status information. For example, the request was blocked.
Request Unique ID	The request ID. If the request was blocked, you can find the request ID in the blocking page.
Request Domain	When a wildcard domain name is enabled with the log search function, you can use this field to search for a specific domain name.
Protection policies	You can use this option to specify the rule matching type, which includes Web Application Attack Protection, HTTP Flood Protection Policies, HTTP ACL Rules, Region Blocking, and Data Risk Control.

6. View the search result.

   · In the Service Traffic area, you can view access request volume trend charts for the search time range.



   · In the Request Logs list, you can view the access request records that match the search conditions. The following figure shows the log for an access request that was blocked against the HTTP flood attack protection rule.

   Descriptions of parameters in the Origin’s response info

   - Status: indicates the response status information that Alibaba Cloud WAF returns to the client.
   - Upstream_status: indicates the response status information that Alibaba Cloud WAF received from the origin server. If “-“ is returned, this indicates no response. For example, this request was blocked by Alibaba Cloud WAF or the origin server response timed out.
   - Upstream_ip: indicates the origin site IP address of this request. For example, when Alibaba Cloud WAF returns traffic back to an ECS instance, this parameter returns the IP address of the origin ECS instance.
   - Upstream_time: indicates the time the origin server took to respond to the WAF request. “-“ indicates the response timed out.

7. Click Log download in the upper-right corner of the Log query page to add a download task for the currently retrieved log. On the View the downloaded file page, you can download the log file to your local client.

   Note:

You can download up to 20 million lines of logs at a time. If you want to export more than 20 million lines of logs, we recommend that you perform multiple download tasks.

Description of request log fields

Field	Name	Description
Time	Time	The UTC time of the request.
Domain	Domain	The requested domain name.
Source_IP	Source IP	The source IP address.
IP_City	IP City	The city from which the request originated.
IP_Country	IP Country	The country from which the request originated.
Method	Method	The HTTP method of the request.
URL	Access request URL	The requested URL.
Https	Access Request Protocol	The protocol specified in the request.
Referer	Referer	The referer field in the HTTP header.
User-Agent	User Agent	The user agent string in the request that identifies the client browser, operating system, and more.
X-Forwarded-For	X-Forwarded-For	The x-forward-field in the request header that identifies the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer.
Cookie	Cookie	The cookie field in the request header that identifies the client cookie information.

Field	Name	Description
Attack_Type	Attack Type	The event triggered by the request. · 0: indicates that no attack was found. · 1: indicates that the Web application attack protection rule was triggered. · 2: indicates that the HTTP flood protection rule was triggered. · 3: indicates that the HTTP ACL policy rule was triggered. · 4: indicates that the Blocked region rule was triggered. · 5: indicates that the Data risk control rule was triggered.
Status	Response Status Code	The response status code that Alibaba Cloud WAF returned to the client.
Upstream_status	Status	The response status code that Alibaba Cloud WAF received from the origin site. "-" indicates that no response was received. For example, the request was blocked by WAF or the origin site timed out.
Upstream_IP	Upstream IP	The source IP address of the request. For example, when Alibaba Cloud WAF returns traffic to an ECS instance, this parameter indicates the IP address of the origin ECS instance.
Upstream_Time	Upstream Time	The time that the origin server took to respond to the request. "-" indicates that the response timed out.

5 Setting

5.1 View product information

The Product Information page of Alibaba Cloud WAF provides you with an intuitive view over your subscription details, the built-in protection rule updates, feature changes, and WAF’ s IP addresses.

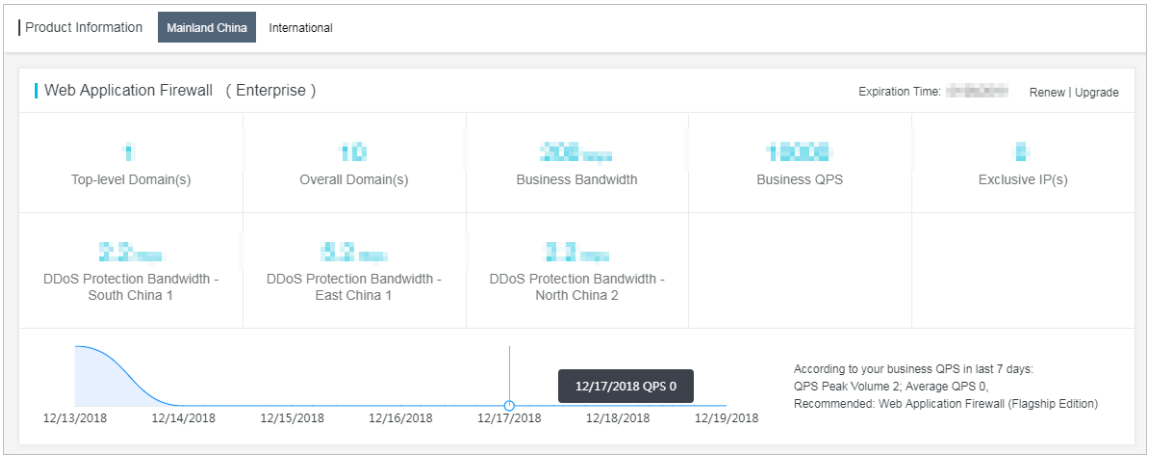
Procedure

1. **Log on to the *Alibaba Cloud WAF console*.**
2. **On the top of the page, select the region: Mainland China or International.**

3. Go to the Setting > Product Information page to view the following information.

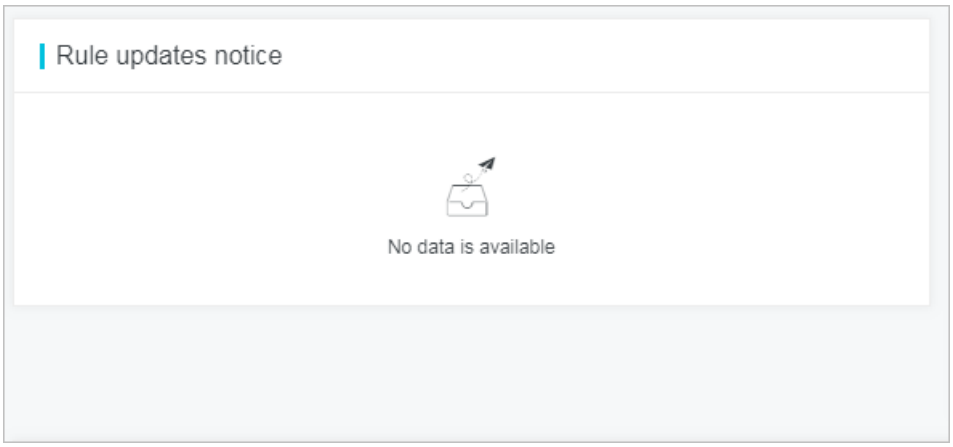
   · Subscription details

   - The current subscription plan and expiration time (Renew and Upgrade are supported)
   - The maximum number of Top-level Domain(s) can be configured
   - The maximum number of Overall Domains can be configured
   - The maximum Business Bandwidth of all accessed domains
   - The maximum Business QPS of all accessed domains
   - The number of Exclusive IP(s)
   - The extra DDoS Protection Bandwidth (by region)
   - The business QPS graph of the latest 7 days



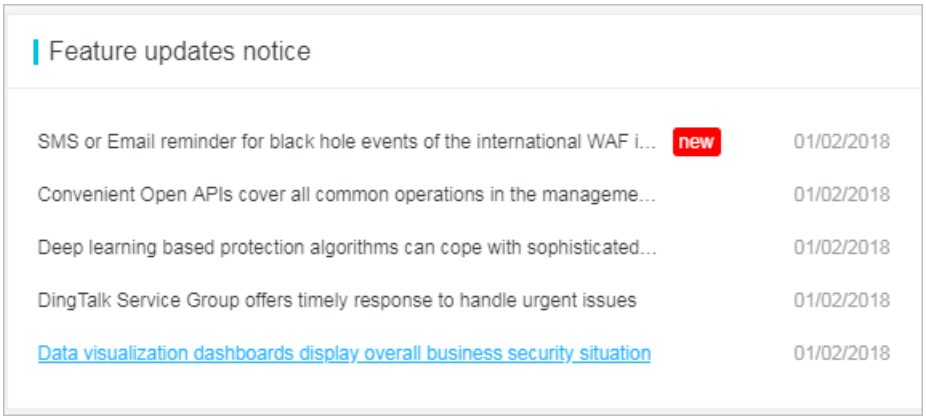
   · Rule Updates Notice

   Informs you about the latest updates of the built-in protection rules of Alibaba Cloud WAF. View details by clicking a title.



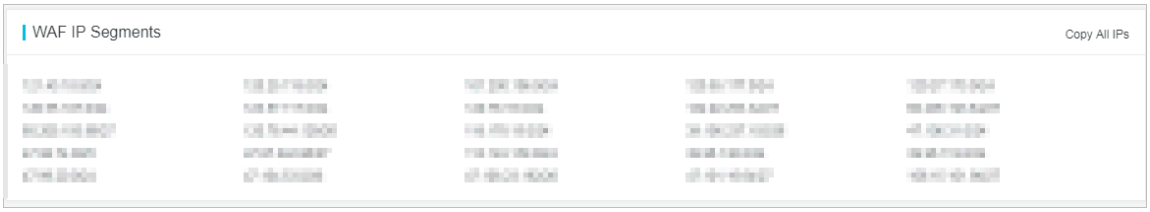
   · Feature Updates Notice

Informs you about the latest change in the Alibaba Cloud WAF feature.



- WAF IP Segments

  Lists all Alibaba Cloud WAF IP addresses. Click Copy All IPs to copy them to the clipboard.



5.2 Custom rule groups

A rule group is a combination of the built-in protection rules of Alibaba Cloud WAF that makes up an optional policy for a specific protection function. You can create and apply a custom rule group for a specific protection function of WAF to achieve dedicated protection effect.

> **Note:**
> Custom rule group is included in the Business or Enterprise subscription plan. Currently, this feature only applies to Web application protection. For more information about the default protection policy of Web application protection, see *Web application protection*.

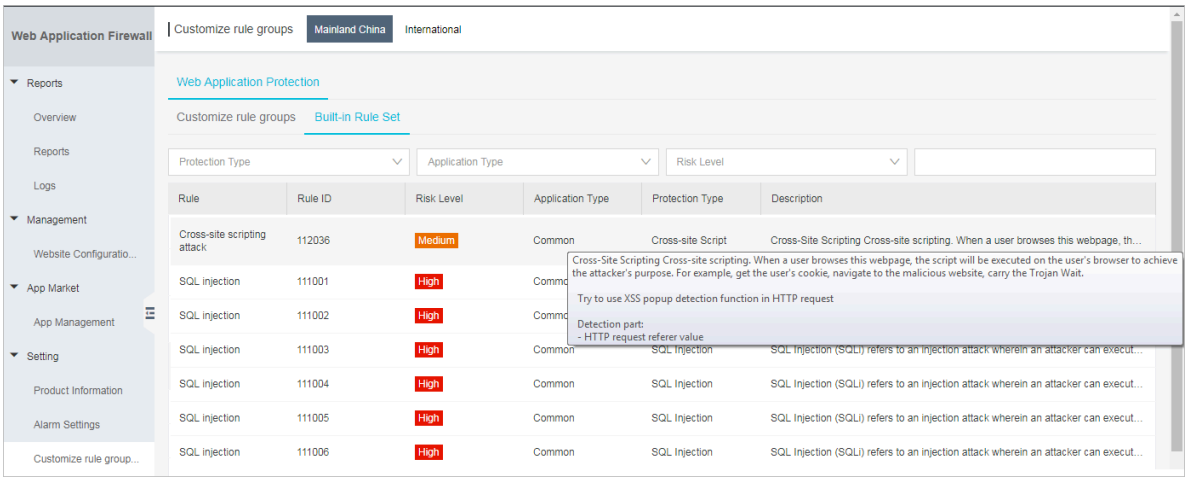
View the build-in protection rules

Before you create a custom rule group, we recommend that you get yourself familiar with the build-in protection rules of Alibaba Cloud WAF.

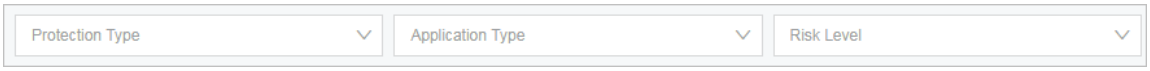
Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China or International.
3. On the Setting > Customize Rule Groups page, select the protection function to view. Currently, only Web Application Protection is supported.
4. Click the Built-in Rule Set page tab to view the protection rules of Web application protection. Each rule consists of the following information:
   - Rule: The name of this rule.
   - Rule ID: The unique identifier of this rule.
   - Risk Level: The risk level of the vulnerability that is defended against by this rule.
   - Application Type: The application that is protected by this rule. Options: Common, Wordpress, Discuz, Tomcat, phpMyAdmin, and more.
   - Protection Type: The type of the web attack that is defended against. Options: SQL Injection, Cross-site Script, Code Execution, CRLF, Local File Inclusion, Remote File Inclusion, Webshell, CSRF, and Others.
   - Description: The description of this rule, including web attack description, code to inspect, and on which selector to run the inspection.

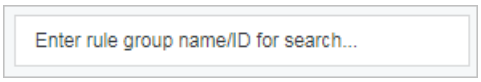
> **Note:**
> You can view the detailed description of a rule by placing the pointer on a description.



5. (Optional) Use filters and search to locate to a specific rule.
   - You can filter rules by protection type, application type, and risk level.

   - You can search for rules by rule name or ID.

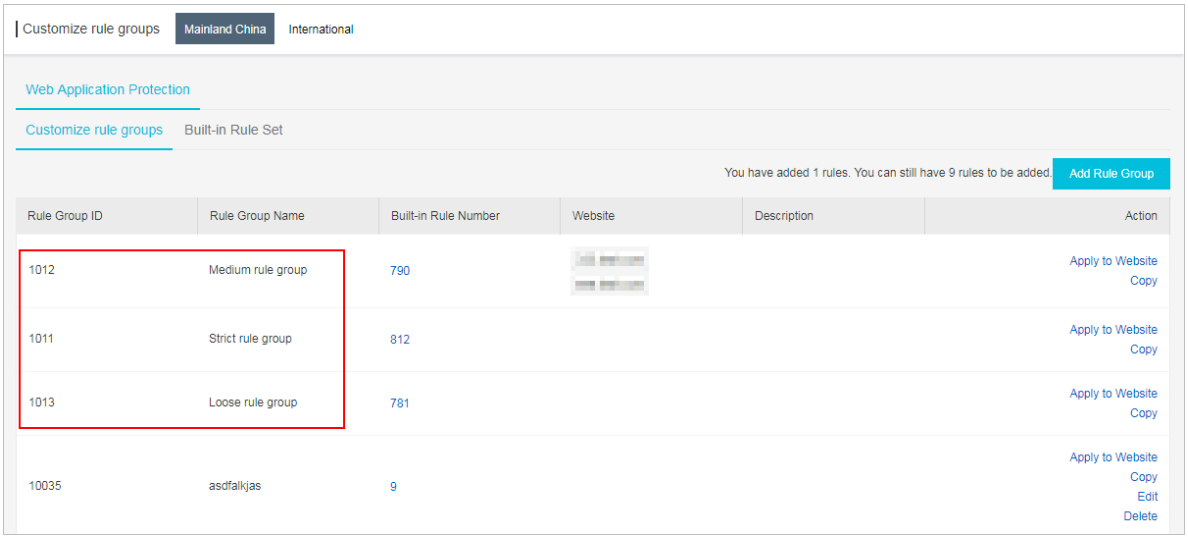
Add a custom rule group

You can create a custom rule group for a specific protection function (only Web Application Protection is supported now). When you are creating a custom rule group , you select built-in rules to add to the group to compose a dedicated protection policy .

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China or International.
3. On the Setting > Customize Rule Groups page, select the protection function to be operated. Currently, only Web Application Protection is supported.

   The Customize Rule Groups page displays all rule groups of Web Application Protection, among which the rule group IDs of 1011, 1012, and 1013 are the default rule groups.

4. Add a custom rule group by creating one or coping an existing one.

   Note:

You can add up to 10 custom rule groups for Web Application Protection.

- Create a custom rule group

  a. Click Add Rule Group.

  b. On the Add Rule Group page, complete the following configuration.

  - Rule Group Name: Required. Name this rule group. We recommend that you use a name with an indicative meaning, because this name will display in the drop down box for you to select a protection policy.
  - Description: Optional. Add a description for this rule group.
  - Rules: Select rules from the left-side area of all built-in rules to add to the right-side area of this rule group’ s rules.

    For more information about rules, see *Step 4 of View the built-in rules*. You can locate to a specific rule by using filters and search. For more information, see *Step 5 of View the built-in rules*.

  c. Click Confirm to add the rule group.

  The newly created rule group is assigned with a rule group ID.

- Copy an existing rule group

  a. Locate to the rule group to be copied and click Copy.

  b. On the Add Rule Group page, enter a new name in Rule Group Name, and confirm the inherited rules. (You cannot add or delete rules in this step.)

  c. Click Confirm to add the rule group.

  The newly copied rule group is assigned with a rule group ID. See *Edit a custom rule group* to add or delete rules in this rule group.

Apply a custom rule group to websites

When a rule group is added, you can enable it in the protection Policies of a specific website or enable it for bulk domains in the Customize Rule Groups page.

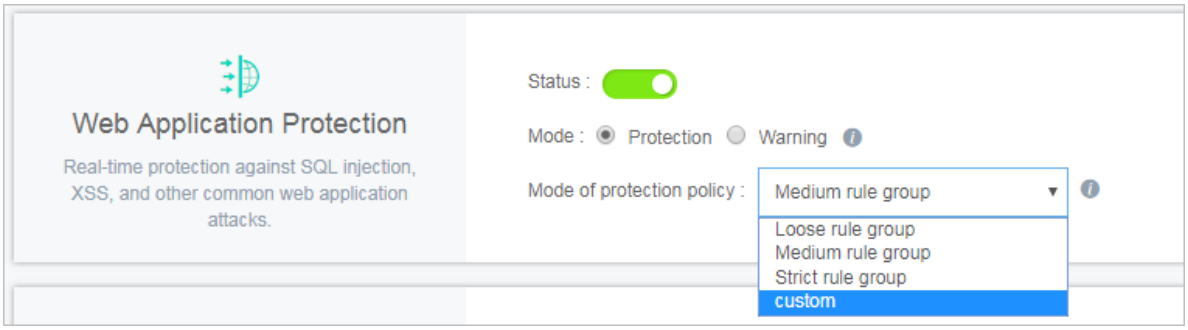
Procedure

Taking Web Application Protection as an example, you can follow these steps to enable or disable a custom rule group in website configuration.

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China or International.

3. On the Management > Website Configuration page, select the domain name to be configured and click Policies.
4. Under Web Application Protection, enable the protection.
5. Expand the Mode of protection policies drop down box, and select the newly added rule group by name. (In this example, select custom.)

   To disable a custom rule group, you select a default policy in the Mode of protecting policy drop down box. In this example, select Strict rule group, Medium rule group, or Loose rule group.



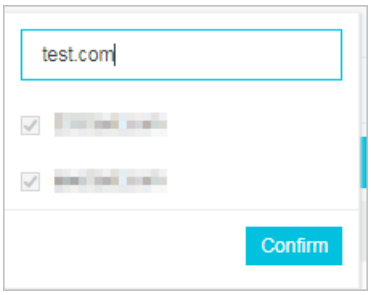
Taking Web Application Protection as an example, follow these steps to apply a custom rule group to bulk domains:

Note:
To disable a rule group, we recommend that you go to the protection Polices page of the specific domain.

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China or International.
3. On the Setting > Customize Rule Groups page, select the protection function to be operated. Currently, only Web Application Protection is supported.
4. On the Customize Rule Groups tab page, locate to the rule group to be operated, and click Apply to Website.

5. Check the website to apply the specified rule group and click Confirm.

   You can search for domains.



Edit a custom rule group

When a custom rule group is successfully added, you can edit it to manage the rules or change its name and description. The default rule group cannot be edited.

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China or International.
3. On the Setting > Customize Rule Groups page, select the protection function to be operated. Currently, only Web Application Protection is supported.
4. Locate to the rule group to be operated, and click Edit.
5. On the Edit Rule Group page, re-configure the rule group. For more information, see *Add a custom rule group*.
6. Click Confirm to update the rule group.

Delete a custom rule group

For an unnecessary custom rule group, you can delete it. Before deleting a rule group , you must make sure that the rule group has not been applied to any website. The default rule group cannot be deleted.

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China or International.
3. On the Setting > Customize Rule Groups page, select the protection function to be operated. Currently, only Web Application Protection is supported.
4. Locate to the rule group to be deleted, and click Delete.

5. In the Tips dialog box, click Confirm.

> Note:
> If the group has been applied to websites, you must disable it from the website configuration to continue the deletion. For more information, see *Apply a custom rule group to websites*.

5.3 Configure alarm settings

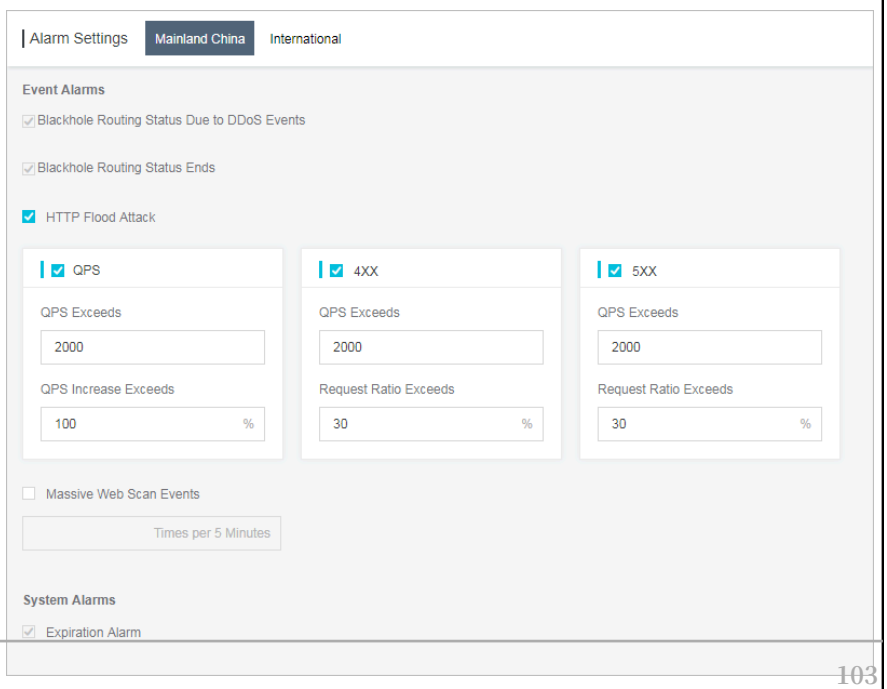
Context

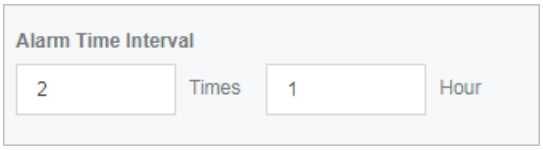
Alibaba Cloud WAF informs you about security events and system events through emails. You can configure the alarm triggering condition and alarm time interval.

Procedure

1. Log on to the *Alibaba Cloud WAF console*.
2. On the top of the page, select the region: Mainland China or International.

3. **On the Setting > Alarm Settings page, complete the following configuration.**

Configuration	Description
Triggered by	Specify which security or system event can trigger an alarm. Note: The default alarm cannot be disabled or configured. · Event Alarms - Blackhole Routing Status Due to DDoS Events (default) - Blackhole Routing Status Ends (default) - HTTP Flood Attack You must specify the conditions that trigger the alarm. ■ QPS exceeds a predefined maximum value (1 to 10,000,000) and increases by a predefined maximum rate (0% to 1,000%). ■ 4xx requests exceed a predefined maximum QPS (1 to 10,000,000) and occupy a predefined maximum proportion (0% to 1,000%). ■ 5xx requests exceed a predefined maximum QPS (1 to 10,000,000) and occupy a predefined maximum proportion (0% to 1,000%). - Massive Web Scan Events You must specify the maximum frequency per 5 minutes. · System Alarms: Expiration Alarm (default) 

Configuration	Description
Alarm Time Interval	Repeat alarms for xx (0 to 10) times per xx (0 to 24 hours). 

4. Click Save Settings.

5.4 Release WAF instance

Context

When the WAF instance expires, you can release it.

> Note:
> Before you release a WAF instance, make sure that all protected domain names are resolved to the origin sites instead of the WAF instance. Once the instance is released, all website configurations are cleared. If any request still reaches the WAF instance, it cannot be forwarded.

Procedure

1. Log on to the *Alibaba Cloud WAF console*, and select the region.
2. In the upper-right corner of the page, click Close WAF.

   > Note:
   > This button appears only when the WAF instance expires.

3. Confirm that all protected domain names are resolved to the origin sites, and click OK to release the WAF instance.

6 Real-time log query and analysis

6.1 Billing method

Web Application Firewall (WAF) Log Service is billed based on the log storage period and the log storage size of your choice.

WAF Log Service is activated on a subscription basis.

Note:
To activate WAF Log Service, you must buy a WAF subscription.

In the WAF purchase page, enable Activate Log Service and select the log storage period and the log storage size. Then, the price is automatically calculated based on the log store specification of your choice and the validity of the WAF instance.

Log storage specification

The detailed pricing for each log storage specification for WAF Log Service is shown in the following table.

Log storage period	Log storage size	Recommended scenarios	For International region instances		For Mainland China region instances	
			Monthly subscription	Yearly subscription	Monthly subscription	Yearly subscription
180 days	3 TB	Average daily QPS is up to 80.	USD 450	USD 5,400	USD 225	USD 2,700
	5 TB	Average daily QPS is up to 120.	USD 750	USD 9,000	USD 375	USD 4,500
	10 TB	Average daily QPS is up to 260.	USD 1,500	USD 18,000	USD 750	USD 9,000
	20 TB	Average daily QPS is up to 500.	USD 3,000	USD 36,000	USD 1,500	USD 18,000

Log storage period	Log storage size	Recommended scenarios	For International region instances		For Mainland China region instances	
			Monthly subscription	Yearly subscription	Monthly subscription	Yearly subscription
	50 TB	Average daily QPS is up to 1,200.	USD 7,500	USD 90,000	USD 3,000	USD 36,000
	100 TB	Average daily QPS is up to 2,600.	USD 15,000	USD 180,000	USD 7,500	USD 90,000
360 days	5 TB	Average daily QPS is up to 60.	USD 750	USD 9,000	USD 375	USD 4,500
	10 TB	Average daily QPS is up to 120.	USD 1,500	USD 18,000	USD 750	USD 9,000
	20 TB	Average daily QPS is up to 260.	USD 3,000	USD 36,000	USD 1,500	USD 18,000
	50 TB	Average daily QPS is up to 600.	USD 7,500	USD 90,000	USD 3,000	USD 36,000
	100 TB	Average daily QPS is up to 1,200.	USD 15,000	USD 180,000	USD 7,500	USD 90,000

Upgrade storage capacity

If you have no log storage left, a notification appears to remind you to expand the storage size. You can expand the log storage size at any time.

 Notice:

If log storage is full, WAF stops writing new log entries to the exclusive logstore in Log Service. A log entry stored in the logstore is deleted based on the specified period. If the WAF Log Service instance expires and you do not renew it within seven days, all log entries in the logstore are deleted.

Validity

The validity of the WAF Log Service instance is based on your WAF subscription.

- Buy: When you buy a WAF subscription and enable Log Service, the price of Log Service is calculated based on the validity of the subscription.
- Upgrade: When you enable Log Service by upgrading an existing WAF subscription, the price of Log Service is calculated based on the remaining validity of the existing WAF instance. The remaining validity is accurate to minutes.

Service expiration

If your WAF instance expires, WAF Log Service expires at the same time.

- When the service expires, WAF stops writing log entries to the exclusive logstore in Log Service.
- The log entries recorded by WAF Log Service are retained within seven days after the service expires. If you renew the service within seven days after the service expires, you can continue to use WAF Log Service. Otherwise, all stored WAF log entries are deleted.

6.2 Activate WAF Log Service

After purchasing a Web Application Firewall instance, you can activate the real-time log query and analysis service for your websites on the App Management page in the console.

Scope

With WAF Log Service, you can collect multiple log entries in real time from your websites that are protected by WAF. You can also perform real-time log query and analysis and display results in dashboards. WAF Log Service fully meets the business protection needs and operational requirements of your websites. You can select the log storage period and the log storage size as needed when enabling WAF Log Service.

 Note:
At the moment, WAF Log Service is only available to WAF subscription instances (Pro, Business, or Enterprise edition).

Benefits

The WAF real-time log query and analysis service has the following benefits:

- Simple configuration: You can easily configure the service to collect log entries that record visits to and attacks on your websites.
- Real-time analysis: Integrated with Log Service, the WAF console provides the real-time log analysis service and the out-of-the-box report center. You can know almost everything about visits to and attacks on your websites.
- Real-time alarms: Near real-time monitoring and alerts based on specific indicators are available to ensure timely responses to critical business exceptions.
- Collaboration: This service is used with real-time computing, cloud storage, visualization, and other data solutions to discover more data value.

Enable WAF Log Service

1. Log on to the *Web Application Firewall console*.
2. Choose App Market > App Management, and select the region where your WAF instance is located.
3. Click Upgrade in Real-time Log Query and Analysis Service.
4. On the page that is displayed, enable Log Service, select the log storage period and the log storage size, and then click Buy Now.

    Note:
   For more information about the billing of WAF Log Service, see *WAF Log Service Billing methods*.
5. Return to the WAF console and choose App Market > App Management, and then click Authorize in Real-time Log Query and Analysis Service.
6. Click Agree to authorize WAF to write log entries to your exclusive logstore.

   WAF Log Service is then enabled and authorized.
7. Return to the WAF console and choose App Market > App Management and then, click Configure in Real-time Log Query and Analysis Service.
8. On the Log Service page, select the domain name of your website that is protected by WAF, and turn on the Status switch on the right to enable WAF Log Service.

   Log Service collects all web log recorded by WAF in real time. These log entries can be queried and analyzed in real time.

6.3 Log collection

You can enable the Web Application Firewall (WAF) log collection feature for a specified domain in the WAF console.

Prerequisites

- Buy a WAF instance and protect the *domain using WAF*.
- Enable Log Service.

Context

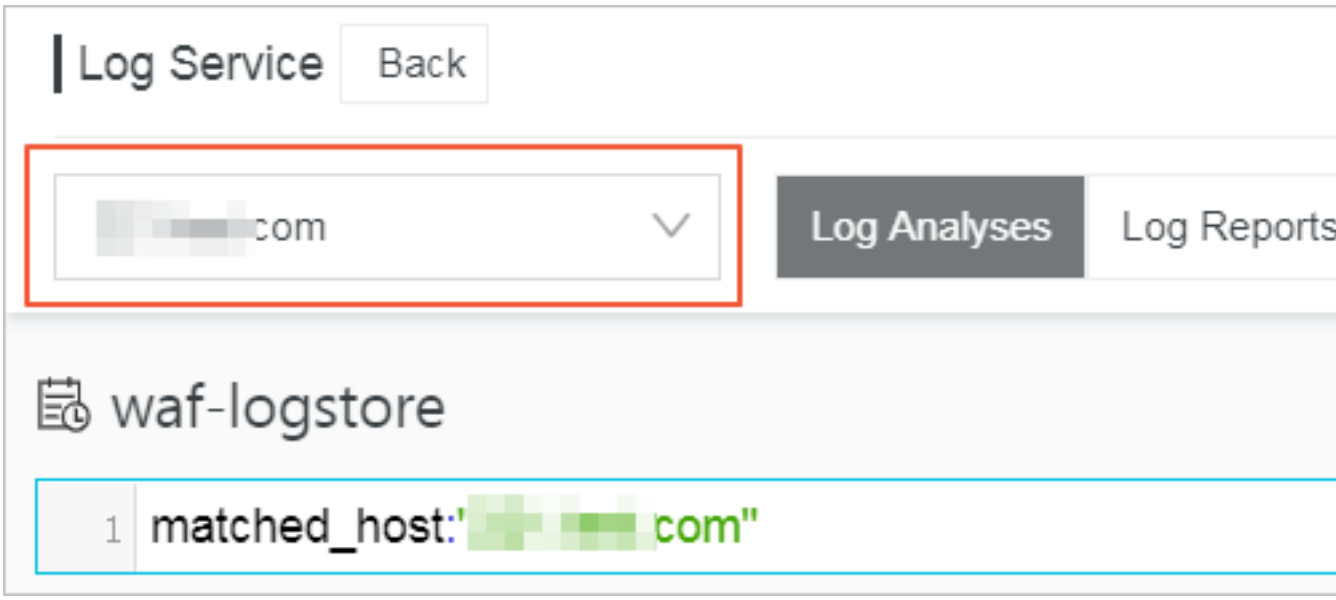
Log Service collects log entries that record visits to and attacks on websites that are protected by Alibaba Cloud WAF, and supports real-time log query and analysis. The query results are displayed in dashboards. You can timely perform analytical investigation on visits to and attacks on your websites and help security engineers to develop protection strategies.

Procedure

1. Log on to the *Web Application Firewall console*.
2. Choose App Market > App Management, and click Real-time Log Query and Analysis Service.

Note:
If you are configuring the WAF log collection feature for the first time, click Authorize and follow the instructions on the authorization page to authorize WAF to write all log entries to your exclusive logstore.

3. Select the domain and turn on the Status switch on the right to enable the log collection feature.



The WAF log collection feature has now been enabled for the domain. Log Service automatically creates an exclusive logstore for your account. WAF automatically writes log entries to the exclusive logstore. The following *Default configuration* table describes the default configuration of the exclusive logstore.

Table 6-1: Default configuration

Default configuration item	Description
Project	A project is created by default. The project name format is determined by the region of your WAF instance. · If the WAF instance is created in Mainland China, the project name is `waf-project-Your Alibaba Cloud account ID-cn-hangzhou`. · If the WAF instance is created in other regions, the project name is `waf-project-Your Alibaba Cloud account ID-ap-southeast-1`.
Logstore	A logstore `waf-logstore` is created by default. All log entries collected by the WAF log collection feature are saved in this logstore.

Default configuration item	Description
Region	· If the WAF instance is created in Mainland China , the project is saved in the Hangzhou region by default. · If the WAF instance is created in other regions, the project is saved in the Singapore region by default.
Shard	Two shards are created by default with the *Automatic shard splitting* feature enabled.
Dashboard	Three dashboards are created: · Access Center · Operation Center · Security Center For more information about dashboards, see *WAF Log Service—Log Reports*.

Limits and instructions

· Other data cannot be written to the exclusive logstore.

  Log entries generated by WAF are stored in the exclusive logstore. You cannot write other data to this logstore by using API, SDK or other methods.

  Note:
  The exclusive logstore has no special limits in query, statistics, alerts, streaming consumption and other functions.

· Basic configurations, such as the storage period of log entries, cannot be modified.

· The exclusive logstore is not billed.

  To use the exclusive logstore, you must enable Log Service for your account. The exclusive logstore is not billed.

  Note:
  When your Log Service is overdue, the WAF log collection feature is suspended until you pay the bills in a timely manner.

· Do not delete or modify the configurations of the project, logstore, index, and dashboards, which are created by Log Service by default. Log Service updates

the WAF log query and analysis service on an irregular basis. The index of the exclusive logstore and the default reports are also updated automatically.

- If you want to use the WAF log query and analysis service with a RAM user, you must grant the required Log Service permissions to the RAM user. For more information about how to grant permissions, see*Grant log query and analysis permissions to a RAM user*.

6.4 Log Analyses

The Real-time Log Query and Analysis Service page in the Web Application Firewall (WAF) console is integrated with the Log Analyses feature and the Log reports feature. After *enabling the WAF log collection feature* for a domain, you can perform real-time query and analysis, view or edit dashboards, and set up monitoring and alarms in the Real-time Log Query and Analysis Service page.

Procedure

1. Log on to the *Web Application Firewall console*, and choose App Market > App Management.
2. Click on the Real-time Log Query and Analysis Service area to open the Log Service page.
3. Select the domain and check that the Status switch on the right is turned on.
4. Click Log Analyses.

   The current page is integrated with the Querying and analyzing page. A query statement is automatically inserted. For example, `matched_host: "www.aliyun.com"` is used to query all log entries that is related to the domain in the statement.
5. Enter a query and analysis statement, select a log time range, and then click Search & Analysis.

More operations

The following operations are available in the Log Analyses page.

- Customize query and analysis

  Log Service provides rich query and analysis syntax for querying log entries in a variety of complex scenarios. For more information, see the *Custom query and analysis* in this topic.

- View the distribution of log entries by time period

  Under the query box, you can view the distribution of log entries that are filtered by time period and query statement. A histogram is used to indicate the distribution, where the horizontal axis indicates the time period, and the vertical axis indicates the number of log entries. The total number of the log entries in the query results is also displayed.

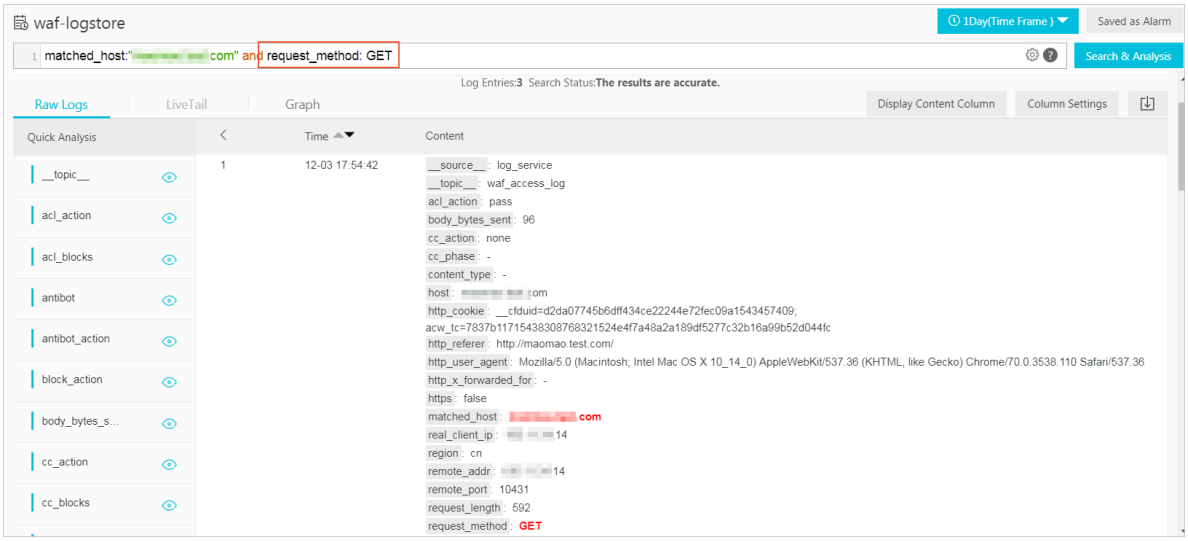
  > **Note:**
  > You can hold down the left mouse button and drag the histogram to select a shorter period. The `time picker` automatically updates the time period, and the query results are also updated based on the updated time period.

- View raw log entries

  In the Raw Logs tab, each log entry is detailed in a single page, which includes the time when the log entry is generated, the content, and the properties in the log entry. You can click Display Content Column to configure the display mode (Full Line or New Line) for long strings in the Content column. You can click Column Settings to display specific fields, or click the Download Log button to download the query results.

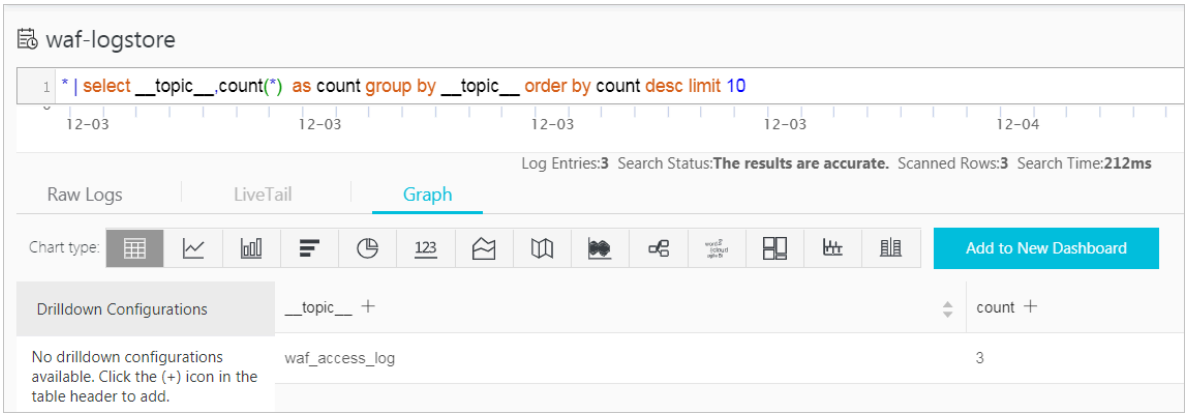
  Additionally, you can click a value or a property name to add a query criterion to the query box. For example, if you click the value `GET` in the `request_method: GET` filed, the query statement in the query box is updated to:

  ```
  <The original query statement> and request_method: GET
  ```



- View analysis graphs

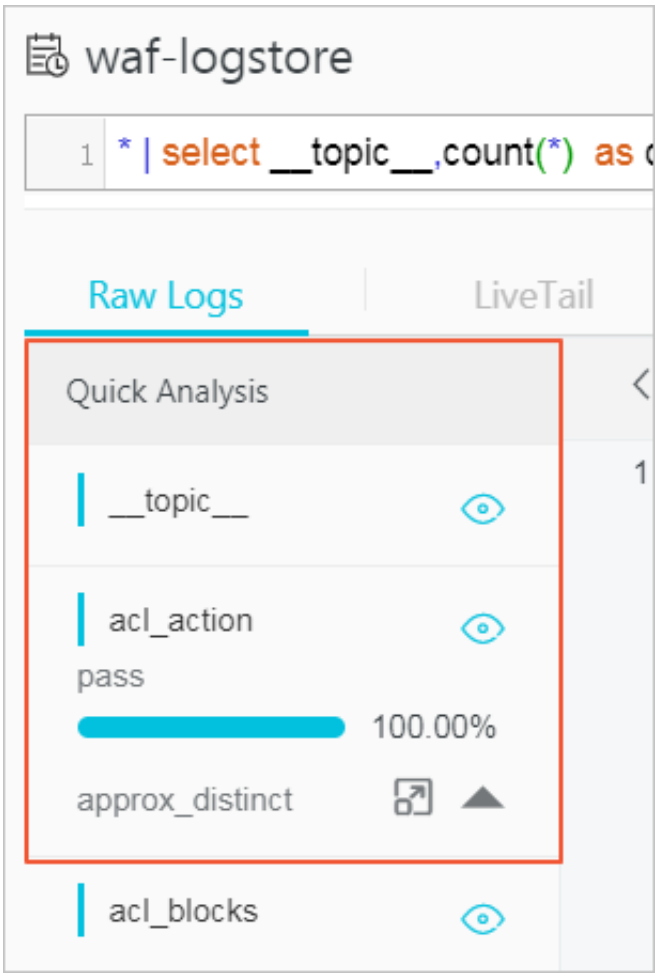
  Log Service enables you to display the analysis results in graphs. You can select the graph type as needed in the Graph tab. For more information, see *Analysis graph*.



- Perform quick analysis

  The Quick Analysis feature in the Raw Logs tab provides you with an one-click interactive experience, which gives you a quick access to the distribution of log entries by a single property within a specified time period. This feature can reduce

the time used for indexing key data. For more information, see *Quick analysis* in the following section.



Customize query and analysis

The log query statement consists of the query (Search) and the analysis (Analytics). These two parts are divided by a vertical bar (|):

```
$Search | $Analytics
```

Type	Description
Query (Search)	A keyword, a fuzzy string, a numerical value, a range, or other criteria can be used in the query criteria. A combined condition can also be used. If the statement is empty or only contains an asterisk (*), all log entries are displayed.
Analysis (Analytics)	Performs computing and statistics to the query results or all log entries.

 **Note:**

Both the query part and the analysis part are optional.

- **When the query part is empty, all log entries within the time period are displayed. Then, the query results are used for statistics.**
- **When the analysis part is empty, only the query results are returned without statistics.**

Query syntax

The query syntax of Log Service supports full-text index and field search. You can enable the New Line display mode, syntax highlighting, and other features in the query box.

- **Full text index**

  You can enter keywords without specifying properties to perform the query by using the full-text index. You can enter the keyword with double quotation marks

("") surrounded to query log entries that contain the keyword. You can also add a space or `and` to separate keywords.

Examples

- Multiple-keywords query

  The following statements can be used to query all log entries that contain `www.aliyun.com` and `error`.

  `www.aliyun.com error` or `www.aliyun.com and error`.

- Criteria query

  The following statement can be used to search for all log entries that contain `www.aliyun.com`, `error` or `404`.

  ```
  www.aliyun.com and (error or 404)
  ```

- Prefix query

  The following statement can be used to query all log entries that contain `www.aliyun.com` and start with `failed_`.

  ```
  www.aliyun.com and failed_*
  ```

  Note:
  An asterisk (*) can be added as a suffix, but it cannot be added as a prefix. For example, the statement cannot be `*_error`.

· Field search

  You can perform a more accurate query based on specified fields.

  The field search supports comparison queries for fields of numeric type. The format is `field name:value` or `field name>=value`. Moreover, you can perform combination queries using `and` or `or`, which can be used in combination with the full text index.

  Note:
  The log entries that record access, operation, and attack on the domain name in WAF Log Service can also be queried by fields. For more information about the

meaning, type, format, and other information of the fields, see *Fields in the WAF log entries*.

Examples

- Multiple-fields query

  The following statement can be used to query all log entries that record the HTTP flood attack on the `www.aliyun.com` domain and are intercepted by WAF .

  ```
  matched_host: www.aliyun.com and cc_blocks: 1
  ```

  If you want to query all log entries that record access from a specific client whose IP address is `1.2.3.4` to `www.aliyun.com`, and access is blocked by the 404 error, you can use the following statement.

  ```
  real_client_ip: 1.2.3.4 and matched_host: www.aliyun.com and
  status: 404
  ```

   Note:
  In this example, the `matched_host`, `cc_blocks`, `real_client_ip`, and `status` fields are the fields defined in the WAF log.

- Numeric fields query

  The following statement can be used to query all log entries where the response time exceeds five seconds.

  ```
  request_time_msec > 5000
  ```

  Range query is also supported. For example, you can query all log entries where the response time exceeds five seconds and is no more than 10 seconds.

  ```
  request_time_msec in (5000 10000]
  ```

   Note:

The following query statement has the same function.

```
request_time_msec > 5000 and request_time_msec <= 10000
```

- Field existence query

  You can perform a query based on the existence of a field.

  ■ The following statement can be used to search for all log entries where the `ua_browser` field exists.

  ```
  ua_browser: *
  ```

  ■ The following statement can be used to search for all log entries where the `ua_browser` field does not exist.

  ```
  not ua_browser: *
  ```

For more information about the query syntax that is supported by Log Service, see*Index and query*.

Syntax for analysis

You can use the SQL/92 syntax for log analysis and statistics.

For more information about the syntax and functions supported by Log Service, see*Syntax description*.

Note:

- The `from table name` part that follows the SQL standard syntax can be omitted from the analysis statement. In WAF Log Service, `from log` can be omitted.
- The first 100 results are returned by default, and you can modify the number of results that are returned by using the *LIMIT syntax*.

Examples of query and analysis

Time-based log query and analysis

Each WAF log entry has a `time` field, which is used to represent the time when the log entry is generated. The format of the value in this field is `<year>-<month>-<day>T<hour>:<minute>:<second>+<time zone>`. For example, `2018-05-31T20:11:58+08:00` is 20:11:58 `UTC+8` (Beijing Time), May 15, 2018.

In addition, each log entry has a built-in field `__time__`, which is also used to indicate the time when the log entry is generated. This field is used for calculation when

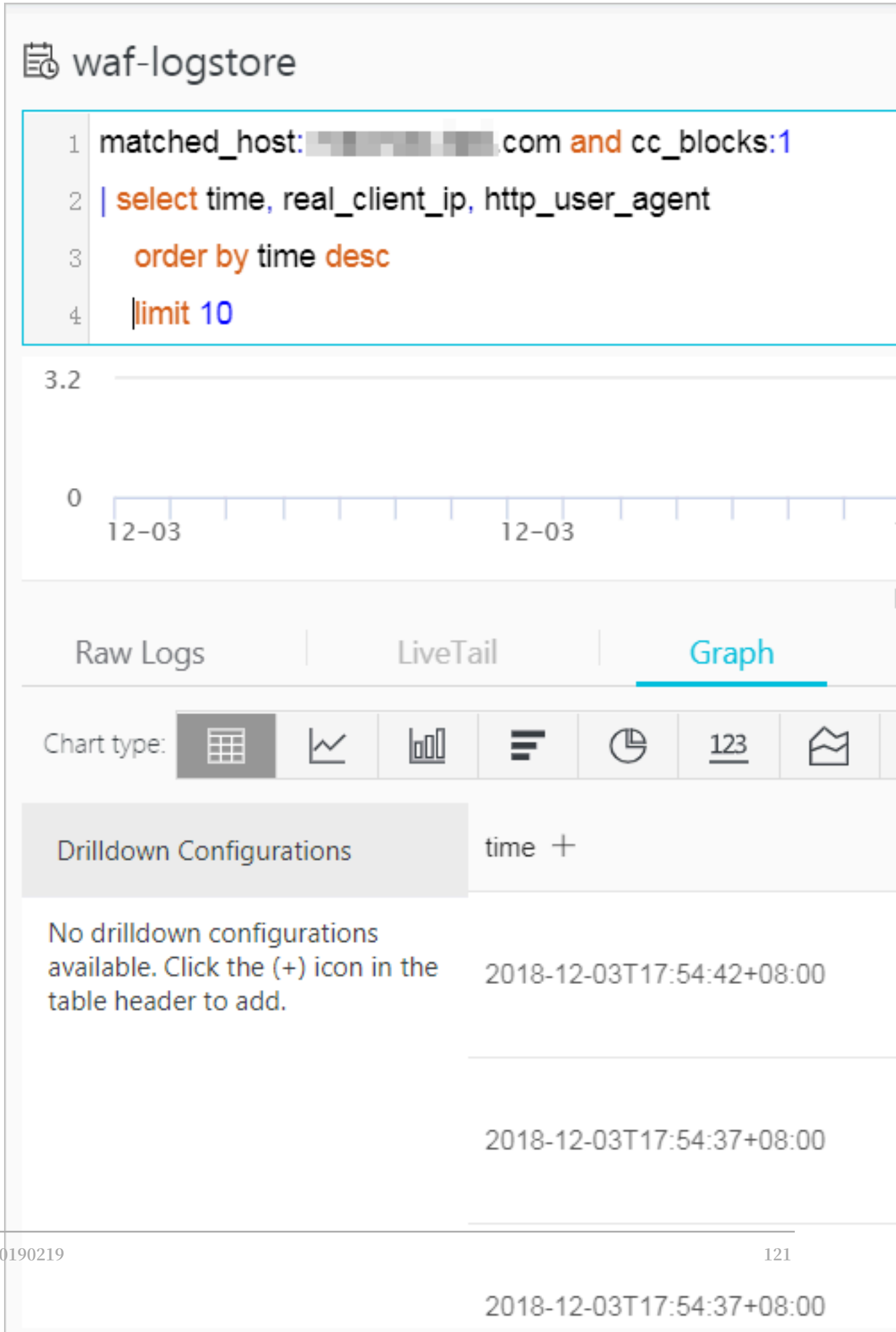
performing statistics. The format of this field is a *Unix timestamp*, and the value of this field indicates the number of seconds that have elapsed since 00:00:00 Coordinated Universal Time (UTC), January 1, 1970. Therefore, if you want to display a calculated result, you must convert the format first.

- Select and display the time

  You can query the log based on the `time` field. For example, you can search for the last 10 log entries that record the HTTP flood attacks on `www.aliyun.com` and are intercepted by WAF. Then, you can display the time field, the source IP field, and the client field.

  ```
  matched_host: www.aliyun.com and cc_blocks: 1
  | select time, real_client_ip, http_user_agent
      order by time desc
  ```

```
limit 10
```


waf-logstore
1 matched_host: com and cc_blocks:1
2 | select time, real_client_ip, http_user_agent
3 order by time desc
4 limit 10
3.2
0
12-03
12-03
Raw Logs
LiveTail
Graph
Chart type:
123
Drilldown Configurations
time +
No drilldown configurations available. Click the (+) icon in the table header to add.
2018-12-03T17:54:42+08:00
2018-12-03T17:54:37+08:00
2018-12-03T17:54:37+08:00

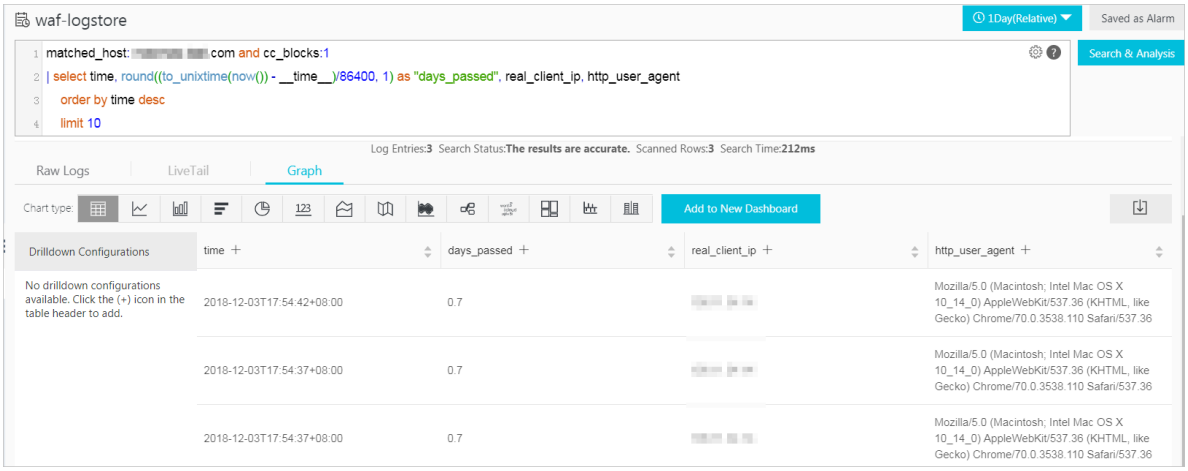
- Calculate using time.

  You can use the `__time__` field to calculate using time. For example, you can calculate the number of days that have elapsed since the domain suffered a HTTP flood attack.

```
matched_host: www.aliyun.com and cc_blocks: 1
round((to_unixtime(now()) - __time__)/86400, 1) as "days_passed",
real_client_ip, http_user_agent
      order by time desc
      limit 10
```

  Note:

  In this example, `round((to_unixtime(now()) - __time__)/86400, 1)` is used to calculate the number of days that have elapsed since the domain had a HTTP flood attack. First, use `now()` to get the current time, and convert the current time into a Unix timestamp using `to_unixtime`. Then, subtract the converted time with the value of the built-in field `__time__` to get the number of seconds that have elapsed. Finally, divide it by `86400` (the total number of seconds in a day) and apply the `round(data, 1)` function to keep one decimal place. The result is the number of days that have elapsed since each attack log entry is generated.



- Perform group statistics based on a specific time

  You can query the log based on the trend of HTTP flood attacks on the domain within a specified time period.

```
matched_host: www.aliyun.com and cc_blocks: 1
| select date_trunc('day', __time__) as dt, count(1) as PV
      group by dt
```

```
    order by dt
```

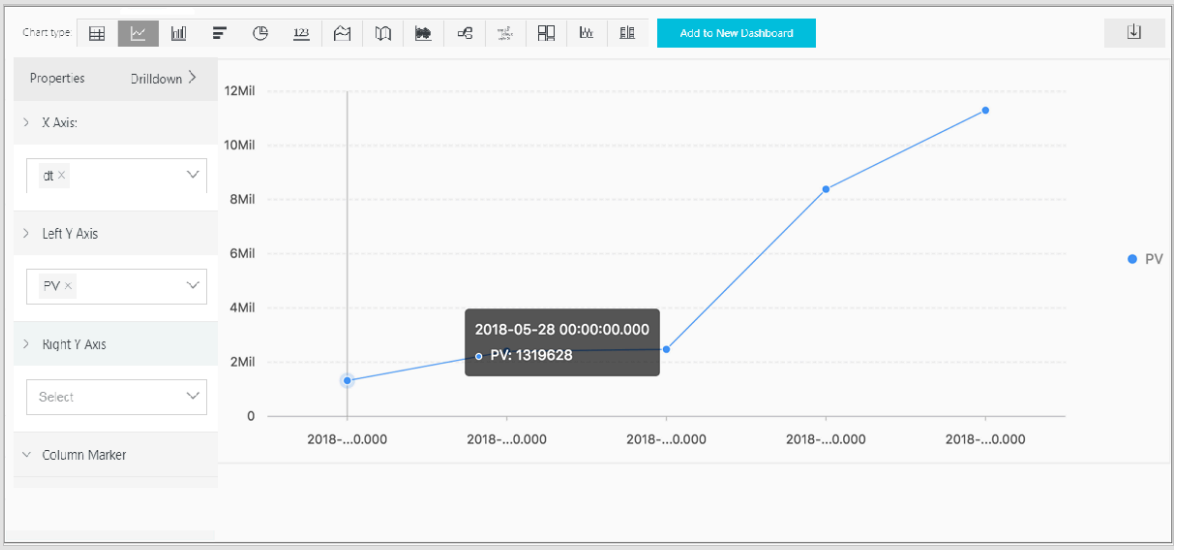
Note:

In this example, the built-in field `__time__` is used by the `date_trunc('day', ..)` function to align the time of the entries by day. Each log entry is assigned to a group based on the day when the log entry is generated. The total number of log entries in each group is counted using count(1). Then, these entries are ordered by the group. You can use other values for the first parameter of the `date_trunc` function to group the log entries based on other time units, such as `second`, `minute`, `hour`, `week`, `month`, and `year`. For more information about this function, see *Date and time functions*.

dt	PV
2018-12-03 00:00:00.000	3

Note:

You can also display the results with a line chart.



- Perform group statistics based on time.

  If you want to analyze the log based on time using more flexible groupings, complex calculations are required. For example, you can query the log based on the trend of HTTP flood attacks on the domain within every five minutes.

```
matched_host: www.aliyun.com and cc_blocks: 1
| select from_unixtime(__time__ - __time__% 300) as dt,
         count(1) as PV
      group by dt
```

```
order by dt
limit 1000
```

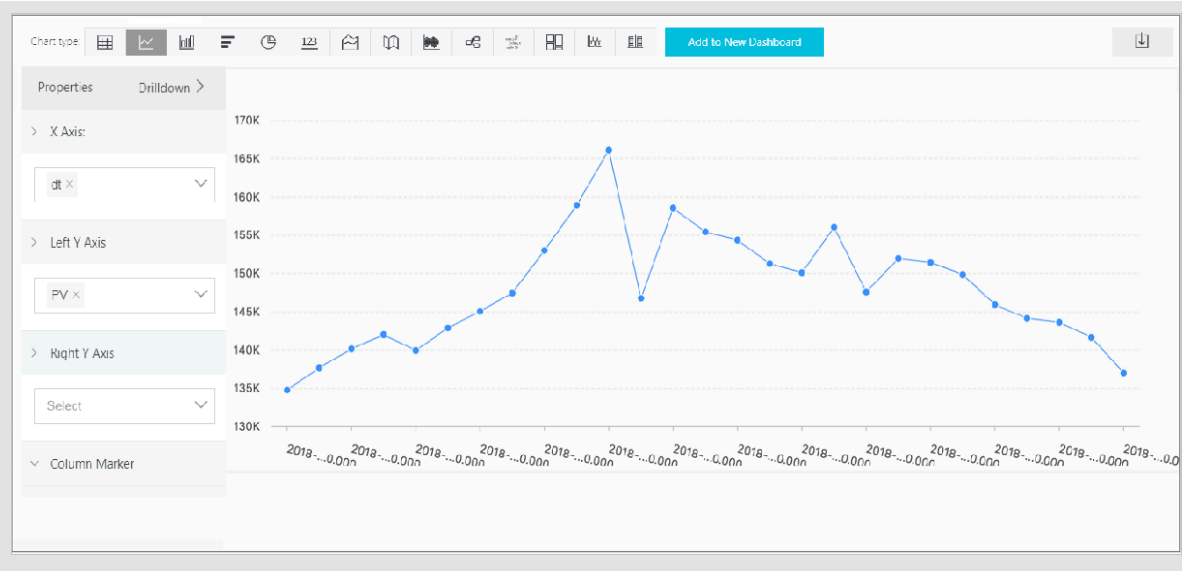
Note:

In this example, the built-in field is used for aligning the time by using the formula `__time__ - __time__% 300`, and the `from_unixtime` function converts the format of the result. Then, each entry is assigned to a group that indicates a time period of five minutes (300 seconds), and the total number of log entries in each group is counted using count(1). Finally, the query results are ordered by group and the first 1,000 results are returned, which include the log entries that are generated within 83 hours before the specified time period.

dt	PV
2018-05-31 21:30:00.000	134795
2018-05-31 21:35:00.000	137691
2018-05-31 21:40:00.000	140171
2018-05-31 21:45:00.000	142037
2018-05-31 21:50:00.000	139958
2018-05-31 21:55:00.000	142906
2018-05-31 22:00:00.000	145093
2018-05-31 22:05:00.000	147474

Note:

You can also display the results with a line graph.



The `date_parse` and `date_format` functions are used to convert the time format. For more information about the functions that can be used to parse the time field, see *Date and time functions*.

Client IP address-based log query and analysis

The WAF log contains the field `real_client_ip`, which reflects the real client IP address. In cases where the user accesses your website through a proxy server, or the IP address in the request header is wrong, you cannot get the real IP address of the user. However, the `remote_addr` field forms a direct connection to the client, which can be used to get the real IP address.

- Classify attackers by country

  You can query the log based on the distribution of HTTP flood attackers by country.

```
matched_host: www.aliyun.com and cc_blocks: 1
| SELECT ip_to_country(if(real_client_ip='-', remote_addr,
real_client_ip)) as country,
         count(1) as "number of attacks"
   group by country
```

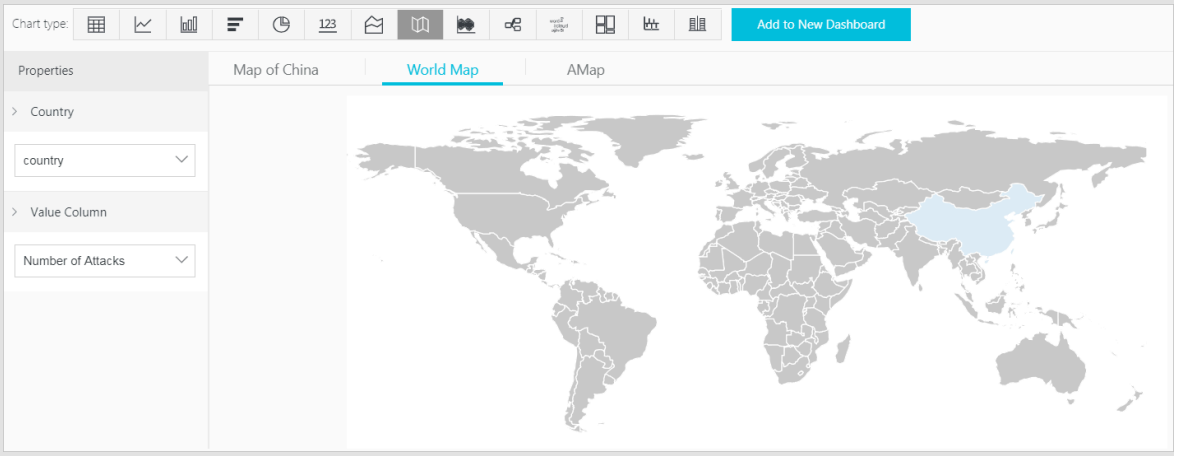
Note:

In this example, the function `if(condition, option1, option2)` returns the real client IP address. If `real_client_ip` is `-`, the function returns the value of

`remote_addr`. Otherwise, the function returns `real_client_ip`. Then, use the `ip_to_country` to get the country information from the IP address of the client.

Note:

You can also display the results with a world map.



- Distribution of visitors by province

  If you want to get the distribution of visitors by province, you can use the `ip_to_province` function to get the province information from the IP addresses.

```
matched_host: www.aliyun.com and cc_blocks: 1
| SELECT ip_to_province(if(real_client_ip='-', remote_addr,
real_client_ip)) as province,
         count (1) as "number of attacks"
   group by province
```

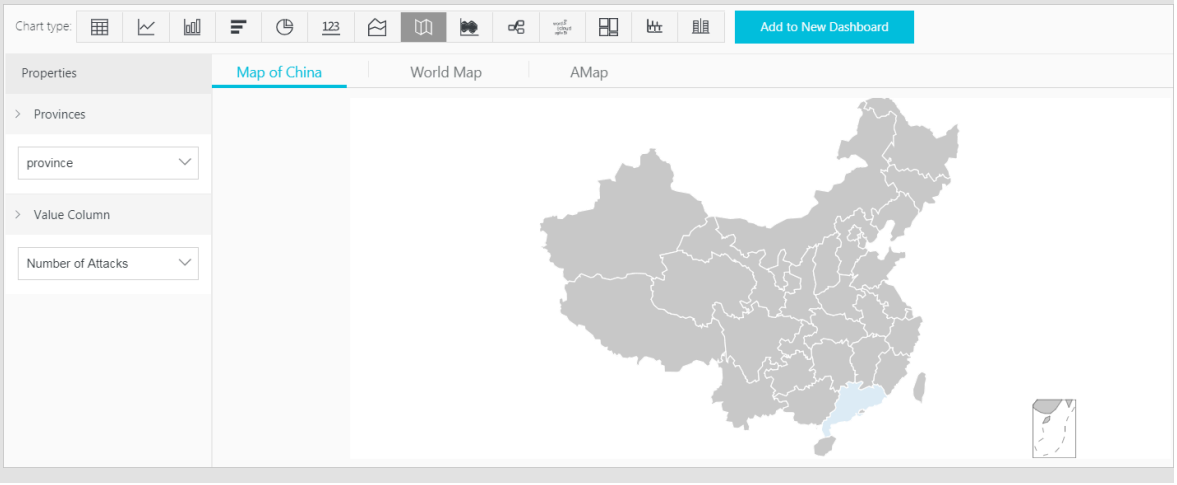
Note:

In this example, the `ip_to_province` function is used to get the country information from the real IP address of the client. If the IP address is not in the Mainland of China, the function returns the province or state of the IP address in the country field. However, if you choose to display the results with a map of China, IP addresses that are not in the Mainland of China are not displayed.

province	Number of Attacks
广东省	3

Note:

You can also display the results with a map of China.



- Heat map that indicates the distribution of attackers

  You can use the `ip_to_geo` function to get the geographic information (the latitude and the longitude) from the real IP addresses of the clients. This information can be used to generate a heat map to indicate the density of attacks.

```
matched_host: www.aliyun.com and cc_blocks: 1
| SELECT ip_to_geo(if(real_client_ip='-', remote_addr, real_clien
t_ip)) as geo,
         count (1) as "number of attacks"
   group by geo
   limit 10000
```

  Note:
  In this example, the `ip_to_geo` function is use to get the latitude and the longitude from the real IP addresses of the clients. The first 10,000 results are returned.

  Select Amap and click Show Heat Map.

The `ip_to_provider` function can be used to get the IP provider name, and the `ip_to_domain` function can be used to determine whether the IP is a public IP or a private IP. For more information about the functions that can be used to resolve IP addresses, see *IP functions*.

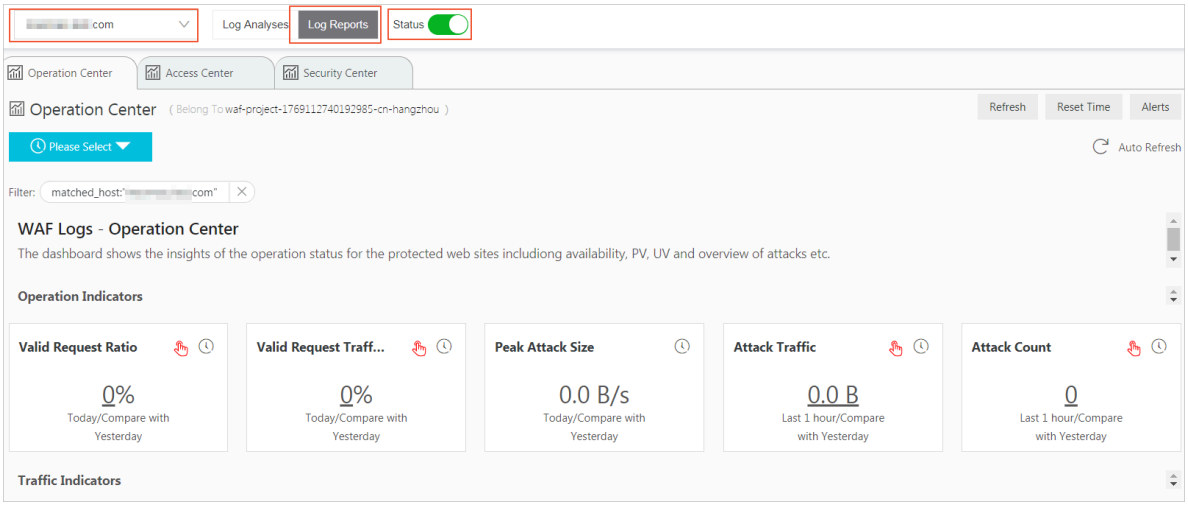
6.5 Log Reports

The Log Reports page is integrated with the Dashboard page of Log Service. On this page, you can view default dashboards. You can filter business and security data about your website by modifying the time range or adding filters.

View reports

1. Log on to the *Web Application Firewall console*, and choose App Market > App Management.
2. Click the Real-time Log Query and Analysis Service area to open the Log Service page.
3. [DO NOT TRANSLATE]
4. Select a domain and check that the Status switch on the right is turned on.
5. Click Log Reports.

   The page that appears is integrated with the Dashboard page of Log Service. A filter is automatically added to display all log entries that are recorded for the domain you selected. In this example, the filter is `matched_host: www.aliyun.com`.

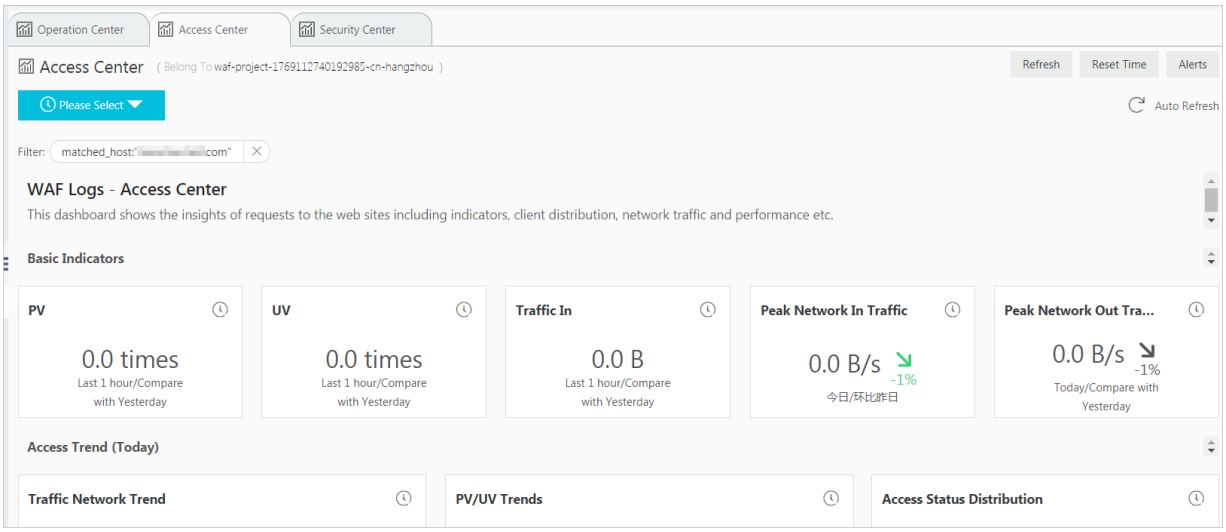


After you enable the WAF log collection feature, Log Service creates three dashboards by default: the Operation Center, Access Center, and Security Center.

Note:

For more information about the default dashboards, see *Default dashboards*.

Dashboard	Description
Operation Center	Displays operation details such as the proportion of valid requests and the statistics of attacks, traffic details such as the peak of both inbound and outbound throughput and the number of requests received, operation trends, attack overview, and other information.
Access Center	Displays basic access details such as the number of page views (PV) and the number of unique visitors (UV), the access trend, the distribution of visitors, and other information.
Security Center	Displays basic index information of attacks, attack types, attack trend, attacker distribution, and other information.



Note:

Dashboards displays various reports using the layout that is predefined in WAF Log Service. The following table describes the graph types supported for reports. For more information about the graph types supported by Log Service, see *Graph description*.

Type	Description
Number	Graphs of this type display important metrics, such as the valid request ratio and the peak of attacks.

Type	Description
Line chart and area chart	Graphs of these types display the trend of important metrics within a specified time period, such as the trend of inbound throughput and the trend of attack interceptions.
Map	Graphs of this type display the geographical distribution of visitors and attackers, for example, by country. Heat maps are also supported to illustrate the distribution of attackers.
Pie chart	Graphs of this type display a distribution, such as the distribution of attackers and the distribution of client types.
Table	Graphs of this type display a table that contains information, such as information of attackers.
Map	Graphs of this type display the geographical distribution of data.

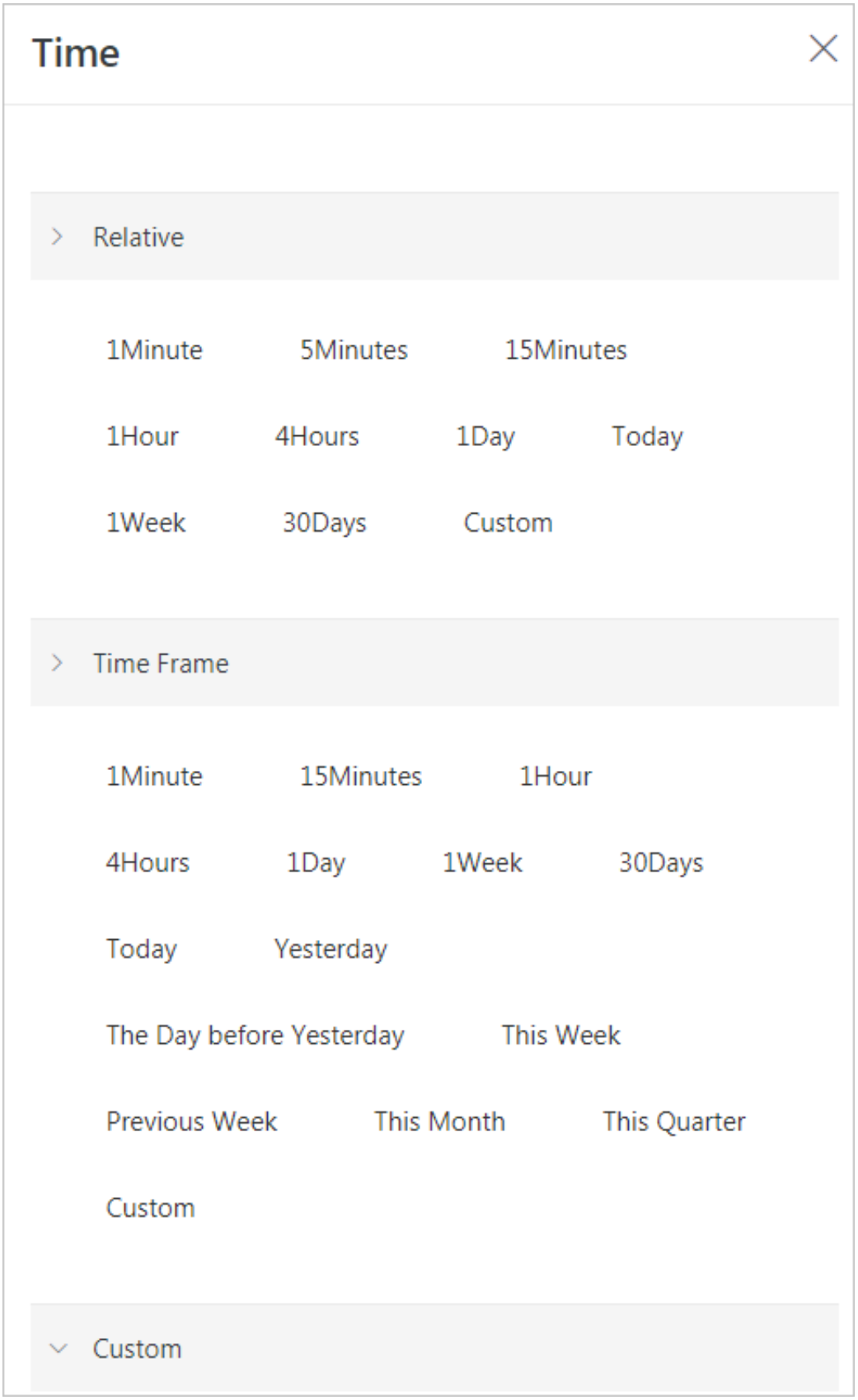
Time selector

The data in all graphs on the dashboard page are generated based on different time ranges. If you want to unify the time ranges, configure the time selector.

1. On the Log Reports page, click Please Select and
2. select a time range in the pane that appears. You can select a relative time, a time frame, or customize a time range.

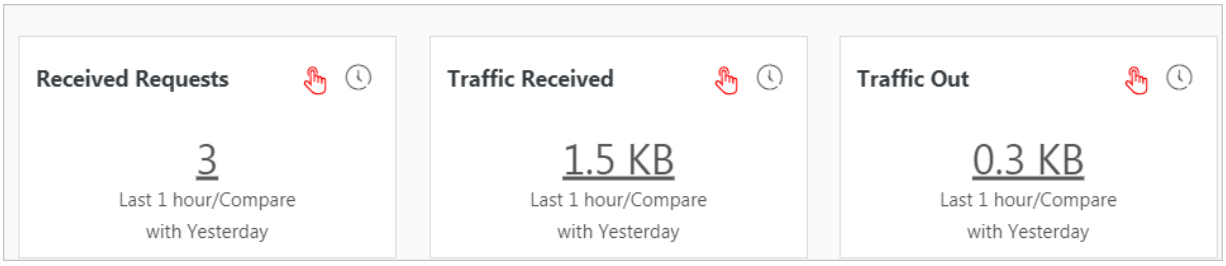
Note:

- After you set a time range, the time range is applied to all reports.
- If you set a time range, a temporary view is generated on the current page. When you view reports next time, the default time range is used.
- To change the time range for a single report in the dashboard, click  in the upper-right corner.


Time
Relative
1Minute
5Minutes
15Minutes
1Hour
4Hours
1Day
Today
1Week
30Days
Custom
Time Frame
1Minute
15Minutes
1Hour
4Hours
1Day
1Week
30Days
Today
Yesterday
The Day before Yesterday
This Week
Previous Week
This Month
This Quarter
Custom
Custom

Data drilldown

The drilldown operation is enabled for some graphs on the dashboard page, which provides you a quick access to the detailed data.



The drilldown operation is available for graphs marked with a  icon in the upper-right corner. You can click a number with an underline to view the detailed underlying data. For example, to quickly find the domains that are attacked and the number of attacks, click the number in the Attacked Hosts graph of the Security Center report.

 Note:
Alternatively, switch to the Raw Log tab to find the relevant log entries.

Description of values in default dashboards

- Operation Center: Displays operation details such as the proportion of valid requests and the statistics of attacks, traffic details such as the peak of both inbound and outbound throughput and the number of requests received, the operation trend, the attack overview, and other information.

Graph	Type	Default time range	Description	Example
Valid Request Ratio	Single value	Today (time frame)	Displays the percentage of valid requests in all requests. A valid request is a request that is neither an attack nor a request that is blocked by a 400 error.	95%

Graph	Type	Default time range	Description	Example
Valid Request Traffic Ratio	Single value	Today (time frame)	Displays the percentage of the traffic generated by valid requests in the traffic generated by all requests.	95%
Peak Attack Size	Single value	Today (time frame)	Displays the peak of attack traffic, which is measured in Bps.	100 B/s
Attack Traffic	Single value	1 hour (relative)	Displays the total attack traffic, which is measured in B.	30 B
Attack Count	Single value	1 hour (relative)	The total number of attacks.	100
Peak Network In	Single value	Today (time frame)	Displays the peak inbound throughput , which is measured in KB/s.	100 KB/s
Peak Network Out	Single value	Today (time frame)	Displays the peak outbound throughput, which is measured in KB/s.	100 KB/s
Received Requests	Single value	1 hour (relative)	Displays the total number of valid requests.	7,800
Received traffic	Single value	1 hour (relative)	Displays the total inbound traffic that is generated by valid requests, which is measured in MB.	1.4 MB
Traffic Out	Single value	1 hour (relative)	Displays the total outbound traffic that is generated by valid requests, which is measured in MB.	3.8 MB

Graph	Type	Default time range	Description	Example
Network Traffic In And Attack	Area chart	Today (time frame)	Displays the trends of throughput generated by valid requests and attacks, which is measured in Kbit/s.	-
Request And Interception	Line chart	Today (time frame)	Displays the trends of valid requests and requests that are intercepted, which is measure in Kbit/h.	-
Access Status Distribution	Flow chart	Today (time frame)	Displays the trends of requests with different status codes (404, 304, 200, and other status codes), which is measured in Kbit/h.	-
Attack Source (World)	World map	1 hour (relative)	Displays the distribution of attackers by country.	-
Attack Source (China)	Map of China	1 Hour (Relative)	Displays the distribution of attackers in China by province.	-
Attack Type	Pie chart	1 hour (relative)	Displays the distribution of attacks by attack type.	-
Attacked Hosts	Tree map	1 hour (relative)	Displays the domains that are attacked and the number of attacks.	-

- Access center: Displays basic access details such as the number of PV and the number of UV, the access trend, the distribution of visitors, and other information.

Graph	Type	Default time range	Description	Example
PV	Single value	1 hour (relative)	Displays the total number of PV.	100,000
UV	Single value	1 hour (relative)	Displays the total number of UV.	100
Traffic In	Single value	1 hour (relative)	Displays the total inbound traffic, which is measured in MB.	300 MB
Peak Network In Traffic	Single value	Today (time frame)	Displays the peak inbound throughput , which is measured in KB/s.	0.5 KB/s
Peak Network Out Traffic	Single value	Today (time frame)	Displays the peak outbound throughput, which is measured in KB/s.	1.3 KB/s
Traffic Network Trend	Area chart	Today (time frame)	Displays the trends of inbound and outbound throughput, which are measured in KB/ s.	-
PV/UV Trends	Line chart	Today (time frame)	Displays the trends of PV and UV, which is measured in Kbit/ h.	-
Access Status Distribution	Flow chart	Today (time frame)	Displays the trends of requests with different status codes (404, 304, 200 , and other status code), which is measured in Kbit/h.	-

Graph	Type	Default time range	Description	Example
Access Source	World map	1 hour (relative)	Displays the distribution of attackers by country.	-
Traffic In Source (World)	World map	1 hour (relative)	Displays the distribution (by country) of inbound traffic from requests.	-
Traffic In Source (China)	Map of China	1 hour (relative)	Displays the distribution (by province) of inbound traffic from requests in China.	-
Access Heatmap	Amap	1 hour (relative)	Displays the heat map that indicates the source distribution of requests by geographical position.	-
Network Provider Source	Pie chart	1 hour (relative)	Displays the source distribution of requests by Internet service provider that provides network for the source, such as China Telecom , China Unicom, China Mobile, and universities.	-
Referer	Table	1 hour (relative)	Displays the first 100 referer URLs which the hosts are most often redirected from, and displays the information of hosts and redirection frequency.	-

Graph	Type	Default time range	Description	Example
Mobile Client Distribution	Pie chart	1 hour (relative)	Displays the distribution of requests from mobile clients, by client type.	-
PC Client Distribution	Pie chart	1 hour (relative)	Displays the distribution of requests from PC clients, by client type .	-
Request Content Type Distribution	Pie chart	1 hour (relative)	Displays the distribution of request sources by content type, such as HTML, form, JSON, and streaming data.	-
Accessed Sites	Tree map	1 Hour (Relative)	Displays the addresses of 30 domains that are visited most.	-
Top Clients	Table	1 hour (relative)	Displays the information of 100 clients that visit your domains most. The information includes the client IP address , the region and city, network information , the request method , inbound traffic , the number of incorrect accesses , the number of attacks, and other information.	-

Graph	Type	Default time range	Description	Example
URL With Slowest Response	Table	1 hour (relative)	Displays the information of 100 URLs that have the longest response times. The information includes the website address, the URL, the average response time, the number of accesses, and other informatio n.	-

- Security Center: Displays basic details of attacks, attack types, the attack trend, the distribution of attackers, and other information.

Chart	Type	Default time range	Description	Example
Peak Attack Size	Single value	1 hour (relative)	Displays the peak of the throughput when your website is suffering attacks, which is measured in Bps.	100 B/s
Attacked Hosts	Single value	Today (time frame)	Displays the number of domains that are attacked.	3
Source Country Of Attack	Single value	Today (time frame)	Displays the number of countries that are attack sources.	2
Attack Traffic	Single value	1 hour (relative)	Displays the total amount of traffic that is generated by attacks, which is measured in B.	1 B
Attacker UV	Single value	1 hour (relative)	Displays the number of unique clients that are attack sources.	40

Chart	Type	Default time range	Description	Example
Attack type distribution	Flow chart	Today (time frame)	Displays the distribution of attacks by attack type.	-
Intercepted Attack	Single value	1 hour (relative)	Displays the number of attacks that are intercepted by WAF.	100
HTTP flood attack Interception	Single value	1 hour (relative)	Displays the number of HTTP flood attacks that are intercepted by WAF.	10
Web Attack Interception	Single value	1 hour (relative)	Displays the number of Web applicatio n attacks that are intercepted by WAF.	80
Access Control Event	Single value	1 hour (relative)	Displays the number of requests that are intercepted by the HTTP ACL policies of WAF.	10
HTTP flood attack (World)	World map	1 hour (relative)	Displays the distribution of HTTP flood attackers by country.	-
HTTP flood attack (China)	China map	1 hour (relative)	Displays the distribution of HTTP flood attackers by province in China.	-
Web Attack (World)	World map	1 Hour (Relative)	Displays the distribution of Web application attacks by country.	-
Web Attack (China)	Map of China	1 hour (relative)	Displays the distribution of Web application attacks by province in China .	-

Chart	Type	Default time range	Description	Example
Access Control Attack (World)	World Map	1 hour (relative)	Displays the distribution by country of requests that are intercepte d by the HTTP ACL policies of WAF.	-
Access Control Attack (China)	Map of China	1 Hour (Relative)	Displays the distribution by province in China of requests that are intercepted by the HTTP ACL policy of WAF.	-
Attacked Hosts	Tree map	1 hour (relative)	Displays the websites that are attacked most.	-
HTTP flood attack Strategy Distribution	Pie chart	1 hour (relative)	Displays the distribution of security policies being activated for HTTP flood attacks.	-
Web Attack Type Distribution	Pie chart	1 hour (relative)	Displays the distribution of Web attacks by attack type.	-
Top Attackers	Table	1 hour (relative)	Displays IP addresses, provinces , and network providers of the first 100 clients that launch the recent attacks, and displays the number of attacks and the amount of traffic generated by these attacks.	-

Chart	Type	Default time range	Description	Example
Attacker Referer	Table	1 Hour (Relative)	Displays the information in referers of attack requests, which includes referer URLs, referer hosts , and the number of attacks.	-

6.6 Fields in the log entry

WAF keeps detailed log entries for your domains, including access requests and attack logs. Each log entry contains dozens of fields. You can perform query and analysis based on specific fields.

Field	Description	Example
__topic__	The topic of the log entry. The value of this field is waf_access _log, which cannot be changed.	waf_access_log
acl_action	The action generated by the WAF HTTP ACL policy to the request, such as pass, drop, and captcha. Note: If the value is null or -, it indicates that the action is pass.	pass
acl_blocks	Indicates whether the request is blocked by the HTTP ACL policy. · If the value is 1, the request is blocked. · If the value is not 1, the request is passed.	1

Field	Description	Example
antibot	The type of the Anti-Bot Service protection strategy that applies, which includes: · ratelimit: Frequency control · sdk: APP protection · intelligence: Algorithmic model · acl: HTTP ACL policy · blacklist: Blacklist	ratelimit
antibot_action	The action performed by the Anti-Bot Service protection strategy, which includes: · challenge: Verifying using an embedded JavaScript script · drop: Blocking · report: Logging the access event · captcha: Verifying using a slider captcha	challenge
block_action	The type of the WAF protection that is activated, which includes: · tmd: Protection against HTTP flood attacks · waf: Protection against Web application attacks · acl: HTTP ACL policy · geo: Blocking regions · antifraud: Risk control for data · antibot: Blocking Web crawlers	tmd
body_bytes_sent	The size of the body in the access request, which is measured in Bytes.	2
cc_action	Protection strategies against HTTP flood attacks, such as none, challenge, pass, close, captcha, wait, login, and n.	close

Field	Description	Example
cc_blocks	Indicates whether the request is blocked by the CC protection. · If the value is 1, the request is blocked. · If the value is not 1, the request is passed.	1
cc_phase	The CC protection strategy that is activated, which can be seccookie, server_ip_blacklist, static_whitelist, server_header_blacklist, server_cookie_blacklist, server_args_blacklist, or qps_overmax.	server_ip_blacklist
content_type	The content type of the access request.	application/x-www-form-urlencoded
host	The source website.	api.aliyun.com
http_cookie	The client-side cookie, which is included in the request header.	k1=v1;k2=v2
http_referer	The URL information of the request source, which is included in the request header. - indicates no URL information.	http://xyz.com
http_user_agent	The User Agent field in the request header, which contains information such as the client browser and the operating system.	Dalvik/2.1.0 (Linux; U; Android 7.0; EDI-AL10 Build/HUAWEIEDISON-AL10)
http_x_forwarded_for	The X-Forwarded-For (XFF) information in the request header, which identifies the original IP address of the client that connects to the Web server using a HTTP proxy or load balancing.	-

Field	Description	Example
https	Indicates whether the request is an HTTPS request. · true: the request is an HTTPS request. · false: the request is an HTTP request.	true
matched_host	The matched domain name (extensive domain name) that is protected by WAF. If no domain has been matched, the value is -.	*.aliyun.com
querystring	The query string in the request.	title=tm_content%3Darticle&pid=123
real_client_ip	The real IP address of the client. If the system cannot get the real IP address, the value is -.	1.2.3.4
region	The information of the region where the WAF instance is located.	cn
remote_addr	The IP address of the client that sends the access request.	1.2.3.4
request_length	The size of the request, measured in Bytes.	123
request_method	The HTTP request method used in the access request.	GET
request_path	The relative path of the request. The query string is not included.	/news/search.php
request_time_msec	The request time, which is measured in microseconds.	44
request_traceid	The unique ID of the access request that is recorded by WAF.	7837b117154103869434370009ea1f0
server_protocol	The response protocol and the version number of the origin server.	HTTP/1.1
status	The status of the HTTP response to the client returned by WAF.	200

Field	Description	Example
time	The time when the access request occurs.	2018-05-02T16:03:59+08:00
ua_browser	The information of the browser that sends the request.	ie9
ua_browser_family	The family of the browser that the sent the request.	internet explorer
ua_browser_type	The type of the browser that the sent the request.	web_browser
ua_browser_version	The version of the browser that sends the request.	9.0
ua_device_type	The type of the client device that sends the request.	computer
ua_os	The operating system used by the client that sends the request.	windows_7
ua_os_family	The family of the operating system used by the client.	windows
upstream_addr	A list of origin addresses, separated by commas. The format of an address is `IP:Port`.	1.2.3.4:443
upstream_ip	The origin IP address that corresponds to the access request. For example, if the origin server is an ECS instance , the value of this field is the IP address of the ECS instance.	1.2.3.4
upstream_response_time	The time that the origin site takes to respond to the WAF request, which is measured in seconds. "-" indicates the timeout of the request.	0.044
upstream_status	The response status that WAF receives from the origin server. "-" indicates that no response is received. The reason can be the response timeout, or the request being blocked by WAF.	200
user_id	Alibaba Cloud account ID.	12345678

Field	Description	Example
waf_action	The action from the Web attack protection policy. · If the value is block, the attack is blocked. · If the value is bypass or other values, the attack is ignored.	block
web_attack_type	The Web attack type such as xss, code_exec, webshell, sqli, lfilei, rfilei, and other.	xss

6.7 Advanced settings

If you click Advanced Settings on the page of WAF log query and analysis service, you will be redirected to the Log Service console. Then you can set advanced features for Log Service. For example, you can set alarms and notifications, real-time log collection and consumption, shipping log data, or provide visual representations with other products.

Procedure

1. Log on to the *Web Application Firewall console*, choose App Market > App Management.
2. Click the Real-time Log Query and Analysis Service area to open the Log Service page.
3. Click Advanced Settings in the upper-right corner.
4. In the dialog box that appears, click Go to open the Log Service console.
5. In the Log Service console, you can set the following advanced features for log projects and logstores:
   - *Real-time log collection and consumption*
   - *Shipping log data to other Alibaba Cloud storage services in real time*
   - *Providing visual representations with other products*

6.8 Export log entries

The WAF log query and analysis service enables you to export log query results to a local file.

You can export the log entries on the current page to a CSV file, or export all log entries to a TXT file.

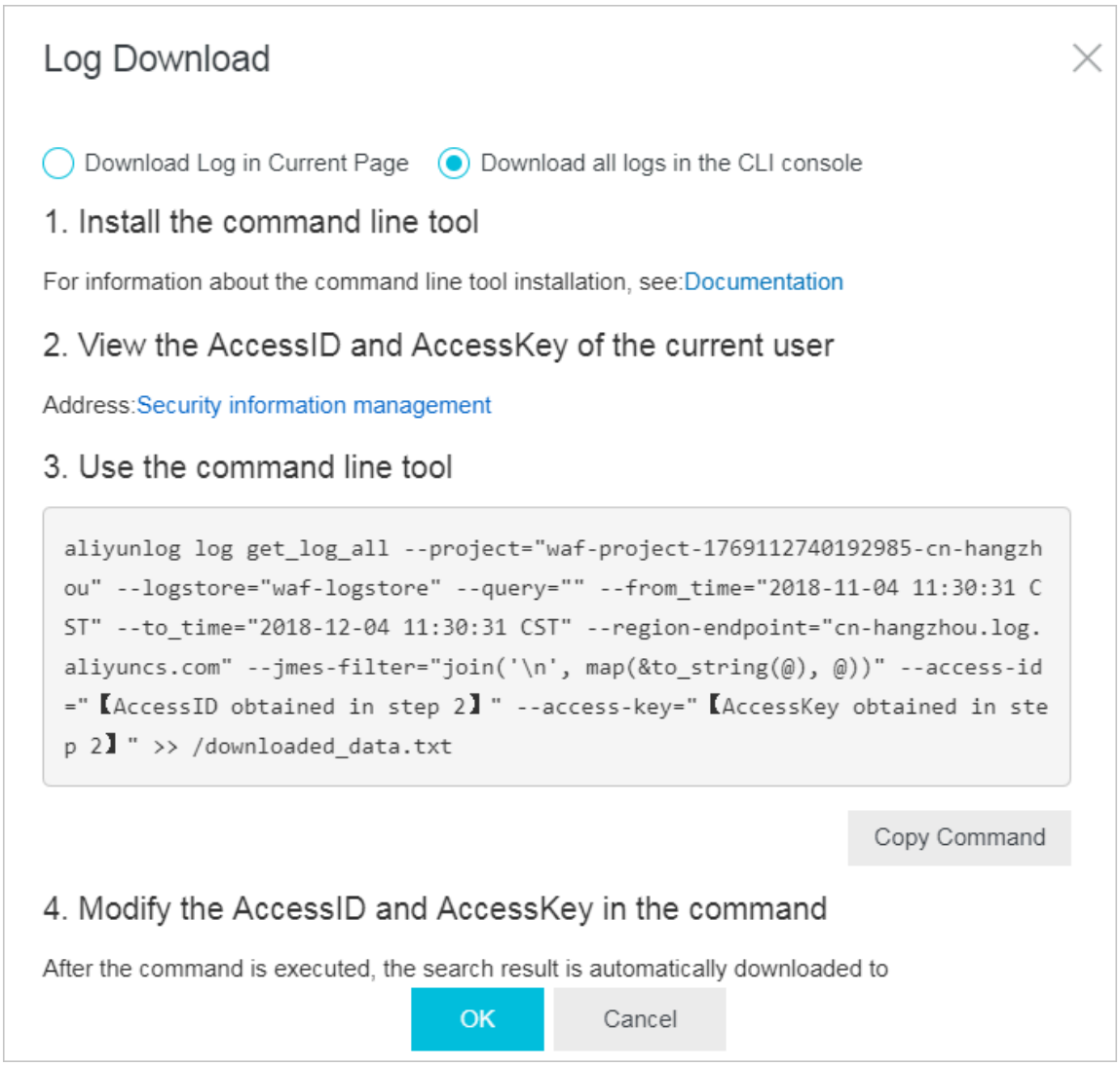
Procedure

1. Log on to the *Web Application Firewall console* and choose App Market > App Management.
2. Click the log query and analysis service area to open the Log Service page.
3. On the Raw Logs tab of the Log Service page, click the download button  on the right.

   > **Note:**
   > The download button does not appear if no result is found for a query.

4. In the Download Log dialog box that appears, select Download Log in Current Page or Download all logs in the CLI console.
   - Download Log in Current Page : Click OK to download the raw log entries on the current page to a CSV file.
   - Download all logs in the CLI console
     a. For more information about installing the command-line interface (CLI), see the *CLI guide*.
     b. Go to the *Security Management* page, and find the AccessKey ID and AccessKey Secret of the current user.
     c. Click Copy Command and paste the command into CLI, replace the `AccessID obtained in step 2` and `AccessKey obtained in step 2` with the

AccessKey ID and AccessKey Secret of the current user, and then run the command.



All raw log entries recorded by WAF are automatically downloaded and saved to the download_data.txt file in the directory where the command is run.

6.9 Grant log query and analysis permissions to a RAM user

If you want to use the WAF log query and analysis service with a RAM user, you must grant required permissions to the RAM user using the Alibaba Cloud account.

Context

The following permissions are required for enabling and using the WAF log query and analysis service.

Operation	Required account type and permissions
Enable Log Service (the service remains enabled after this operation)	Alibaba Cloud account
Authorize WAF to write log data to the exclusive logstore in Log Service in real-time (the authorization remains valid after this operation)	· Alibaba Cloud account · RAM user that has the `AliyunLogFullAccess` permission · RAM user that has specific permissions
Use the log query and analysis service	· Alibaba Cloud account · RAM user that has the `AliyunLogFullAccess` permission · RAM user that has specific permissions

Grant permissions to RAM users as required.

Scenario	Permission	Procedure
Grant permissions on all Log Service operations to a RAM user.	`AliyunLogFullAccess`	For more information, see *RAM users*.
Grant the log viewing permission to a RAM user after you enable the WAF log query and analysis service and complete the authorization on the Alibaba Cloud account.	`AliyunLogReadOnlyAccess`	For more information, see *RAM users*.
Grant the RAM user permissions on enabling and using the WAF log query and analysis service. This RAM user is not granted other administrative permissions on Log Service.	Custom authorization policy	For more information, see the following procedure.

Procedure

1. Log on to the *RAM console*.
2. On the Policies page, select the Custom Policy tab.

3. In the upper-right corner of the page, click Create Authorization Policy.
4. Click Create Authorization Policy. In the template, specify the Authorization Policy Name, and then enter the following in the Policy Content field.

 **Note:**

Replace `${Project}` and `${Logstore}` in the following policy content with the names of the exclusive project and logstore in WAF Log Service.

```
{
  "Version": "1",
  "Statement": [
   {
      "Action": "log:GetProject",
      "Resource": "acs:log:*:*:project/${Project}",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateProject",
      "Resource": "acs:log:*:*:project/*",
      "Effect": "Allow"
    },
 {
      "Action": "log:ListLogStores",
      "Resource": "acs:log:*:*:project/${Project}/logstore/*",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateLogStore",
      "Resource": "acs:log:*:*:project/${Project}/logstore/*",
      "Effect": "Allow"
    },
 {
      "Action": "log:GetIndex",
      "Resource": "acs:log:*:*:project/${Project}/logstore/${
Logstore}",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateIndex",
      "Resource": "acs:log:*:*:project/${Project}/logstore/${
Logstore}",
      "Effect": "Allow"
    },
    {
      "Action": "log:UpdateIndex",
      "Resource": "acs:log:*:*:project/${Project}/logstore/${
Logstore}",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateDashboard",
      "Resource": "acs:log:*:*:project/${Project}/dashboard/*",
      "Effect": "Allow"
    },
 {
      "Action": "log:UpdateDashboard",
      "Resource": "acs:log:*:*:project/${Project}/dashboard/*",
```

```
      "Effect": "Allow"
    },
 {
      "Action": "log:CreateSavedSearch",
      "Resource": "acs:log:*:*:project/${Project}/savedsearch/*",
      "Effect": "Allow"
    },
 {
      "Action": "log:UpdateSavedSearch",
      "Resource": "acs:log:*:*:project/${Project}/savedsearch/*",
      "Effect": "Allow"
    }
  ]
}
```

5. Click Create Authorization Policy.
6. Go to the Users page, find the RAM user, and then click Authorize.
7. Add the authorization policy that you created and click OK.
   This RAM user can enable and use the WAF log query and analysis service, and cannot use other features of Log Service.

6.10 Manage log storage

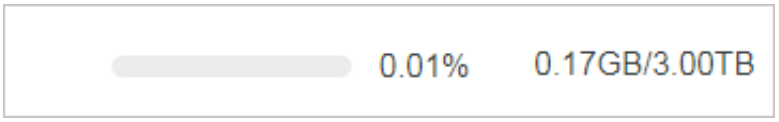
After WAF Log Service is activated, log storage is allocated for your WAF Log Service based on the specified log storage size. You can view the usage of the log storage on the Log Service page in the Web Application Firewall console.

View the usage of the log storage

You can view the usage of the log storage that is generated by the WAF log query and analysis service at any time.

> **Note:**
> It takes two hours for changes in the storage usage to be updated in the console. You need to upgrade the log storage when only a little log storage space is available.

1. Log on to the *Web Application Firewall console*.
2. Choose App Market > App Management, select the region where your WAF instance is located, and then click Real-time Log Query and Analysis Service.
3. At the top of the Log Service page, view the usage of log storage.



Upgrade log storage

To upgrade the log storage size, click Upgrade Storage at the top of the Log Service page.

 Note:
If log storage is full, new log data cannot be written to the exclusive logstore. We recommend that you upgrade log storage before log storage is full.

Clear log storage

You can delete all log entries in the log storage as needed. For example, you can delete the log entries generated during the test phase to make full use of the log storage by recording only log entries that is generated during the production phase.

Click Clear at the top of the Log Service page, and click Confirm to delete all log entries in the log storage.

 Notice:
Log entries that are deleted cannot be restored. Delete log entries with caution.

 Note:
You can clear the log storage for only a limited number of times.