

# Alibaba Cloud Web Application Firewall

## Quick Start

Issue: 20190807

## 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.	 <b>Danger:</b> 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.	 <b>Warning:</b> 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.	 <b>Notice:</b> 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.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
<code>Courier font</code>	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

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



# Contents

---

Legal disclaimer..... I

Generic conventions..... I

1 Quick start..... 1

2 Step 1: Automatically add a website configuration.....3

3 Step 2: Update the DNS settings.....7

4 Step 3: Configure WAF protection polices.....12

5 Step 4: View security reports..... 14



# 1 Quick start

This topic describes how to configure and use Web Application Firewall (WAF) after you activate WAF. To use WAF, you must complete the configuration procedure of WAF so that your website can be protected by WAF. You can view the security reports and statistics to learn about the security status of your website.




**Note:**

You can use the transparent proxy mode or the DNS proxy mode to configure WAF for your website. This topic describes how to use the DNS proxy mode to configure WAF. For more information about the transparent proxy mode, see [Use the transparent proxy mode to configure WAF](#).

**Procedure**

Operation	Description	Recommended method	Prerequisites
<a href="#">1. Add website configurations automatically</a>	Add the website configuration for the website that needs protection in the WAF console.	Add website configurations automatically.	<ul style="list-style-type: none"> <li>The domain name of the website is managed by Alibaba Cloud DNS, and you have created an A record on Alibaba Cloud DNS.</li> <li>(Mainland China regions) You have obtained an ICP license for the website.</li> <li>(HTTPS-based websites) You have obtained the HTTPS certificate and the private key file of the website, or the HTTPS certificate is managed by Alibaba Cloud SSL Certificates Service.</li> </ul>

Operation	Description	Recommended method	Prerequisites
<p><b>(Optional) 2. Change DNS records</b></p>	<p>Change the DNS record of the website to redirect requests that are sent to the website to WAF for monitoring.</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;">  <b>Note:</b>                      You must perform this operation when you are required to manually change the DNS record, or you need to manually add a website configuration.                 </div>	<p>Change the CNAME record to configure WAF.</p>	<ul style="list-style-type: none"> <li>• You have obtained the WAF CNAME address.</li> <li>• You have the permissions to change DNS records at your DNS service provider.</li> </ul>
<p><b>3. Specify WAF protection policies</b></p>	<p>Specify and adjust WAF protection policies in the WAF console.</p>	<p>Use the default protection settings.</p>	<p>You have configured WAF for your website and DNS resolution is working properly.</p>
<p><b>4. View security reports</b></p>	<p>View security reports of your website in the WAF console.</p>	<ul style="list-style-type: none"> <li>• View your business and security status on the Overview page.</li> <li>• View security details and risk warnings on the Reports page.</li> </ul>	<p>You have configured WAF for your website and DNS resolution is working properly.</p>

For more information, see [Overview](#).

## 2 Step 1: Automatically add a website configuration

---

After you activate Web Application Firewall (WAF), you need to add the website configuration of the website that needs protection in the WAF console. This topic describes how WAF automatically adds a website configuration when you use the DNS proxy mode to configure WAF.



### Note:

You can use the transparent proxy mode or the DNS proxy mode to configure WAF for your website. The following example demonstrates how to configure WAF by using the DNS proxy mode. For more information about the transparent proxy mode, see [Use the transparent proxy mode to configure WAF](#).

When you configure WAF by using the DNS proxy mode, WAF can automatically read the A records that you have created on [Alibaba Cloud DNS](#), the domain name of the website, and the origin server IP address to automatically add a website configuration. After the website configuration is added, WAF automatically updates the DNS record of the domain name. For more information, see [Step 2: Update the DNS settings](#).

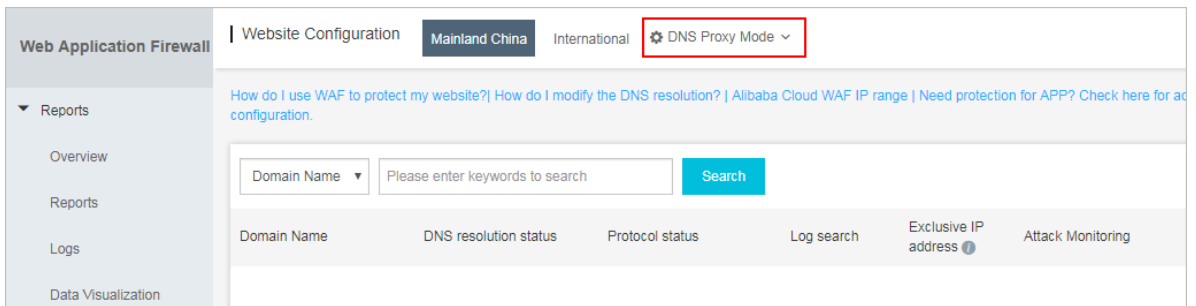
### Prerequisites

- The DNS records of the website are managed by Alibaba Cloud DNS, and at least one A record is valid.  
If you cannot host your domains on Alibaba Cloud DNS, you must manually add website configurations. For more information, see [Website configuration](#).
- (Mainland China regions) You have obtained an ICP license for the website.
- (HTTPS-based websites) You have obtained the HTTPS certificate and the private key file of the website, or the HTTPS certificate is managed by Alibaba Cloud SSL Certificates Service.

### Procedure

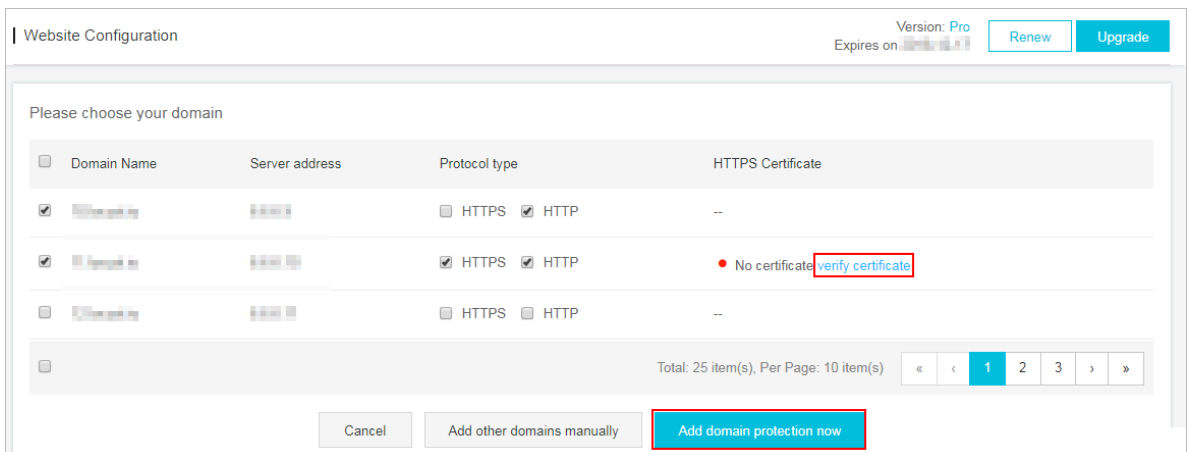
1. Log on to the [WAF console](#).
2. On the top of the page, select Mainland China or International.

3. Choose Management > Website Configuration and select DNS Proxy Mode.



4. Click Add Domain.

WAF automatically lists the domain names that have an A record configured on Alibaba Cloud DNS under the current Alibaba Cloud account. If you have not created an A record on Alibaba Cloud DNS, the Please choose your domain page will not appear. You can manually add the website configuration by following the procedure described in [Website configuration](#).



5. On the Please choose your domain page, choose the domain name and the protocol type for the website.

6. (Optional) If you choose HTTPS, you must verify the certificate before you add the website configuration.



Note:

Alternatively, do not select HTTPS. After you have added the website configuration, upload the HTTPS certificate by following the procedure described in [Update HTTPS certificates](#)

- a. Click Verify Certificate.
- b. In the Verify Certificate dialog box, upload the certificate and private key file.
  - If you have hosted your certificates on [Alibaba Cloud SSL Certificate Service](#), click Select Existing Certificate in the Verify Certificate dialog box, and select the certificate that is associated with the domain name.
  - Manually upload the certificate. Click Manual Upload, enter the certificate name, and copy the text content of the certificate and private key files to the Certificate File and Private Key File fields respectively.

For more information, see [Update HTTPS certificates](#).

verify certificate

The current domain name type is HTTPS. You must import a certificate and private key to implement normal website protection.

Domain name:

Certificate name :

Certificate file ⓘ :

Private key file ⓘ :

Verify Cancel

- 
- 
- c. Click Verify to verify the uploaded certificate.

## 7. Click Add domain protection now.

After you have added the website configuration, WAF automatically updates the CNAME record of the domain to redirect requests sent to your website to WAF for monitoring. This operation will take 10 to 15 minutes.



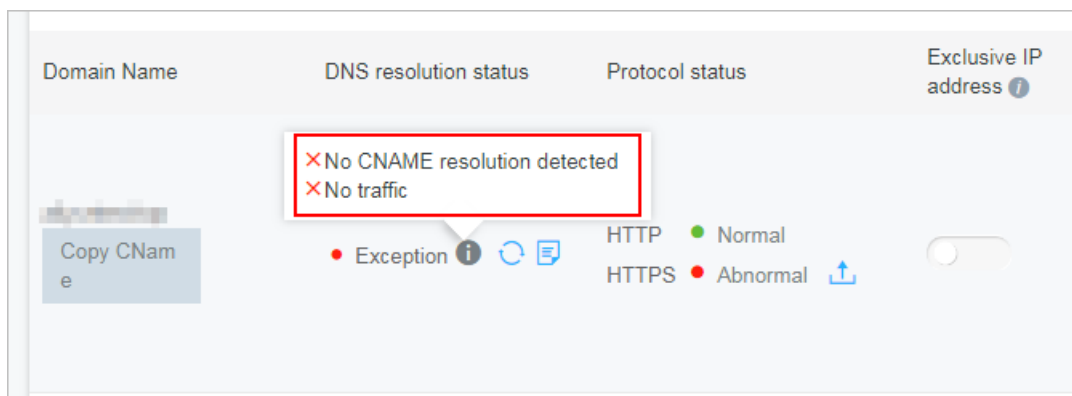
Note:

If you are required to add DNS records manually, follow the procedure described in [Step 2: Update the DNS settings](#) to complete the configuration.

## 8. You can choose Management > Website Configuration to view the domain name that you have added and the DNS status in the DNS resolution status column.

- Normal indicates that you have successfully configured WAF for your website. You can follow the procedure described in [Step 3: Configure WAF protection policies](#) to specify protection policies.
- Exception may be displayed after you have added the website configuration. Wait a few seconds and check the DNS status again, or check whether the DNS settings are configured correctly at your DNS service provider.

If the DNS settings are not configured correctly, see [Step 2: Update the DNS settings](#). For more information, see [DNS resolution status exception](#).



## 3 Step 2: Update the DNS settings

---

After you use the DNS proxy mode to configure Web Application Firewall (WAF) for your website and add the website configuration, WAF automatically generates a CNAME address for your website. You can use this CNAME address to update the CNAME value to redirect requests that are sent to your website to WAF for monitoring.

- If the DNS settings have been automatically updated in [Step 1: Automatically add a website configuration](#) and the DNS resolution status is Normal, skip this step and perform [Step 3: Configure WAF protection policies](#).
- If you are required to update DNS settings manually or the DNS resolution status is Exception in [Step 1: Automatically add a website configuration](#), perform the following steps to update the DNS settings.

The following example uses Alibaba Cloud DNS to describe how to change a CNAME record. If your domain name is managed by Alibaba Cloud DNS, perform the following steps to update the DNS settings. If your domain name is managed by other DNS service providers, perform the following steps to update the DNS settings in the system of your DNS service provider.

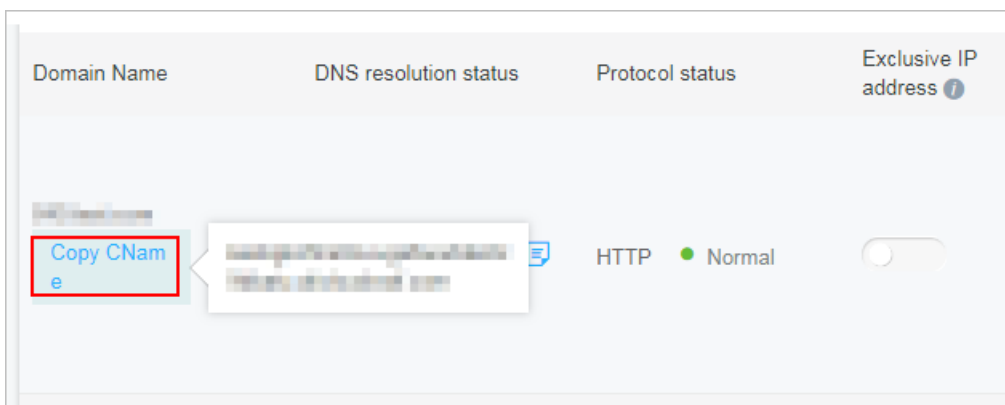


Note:


To enable WAF, you need to add a CNAME or A record to redirect requests. For more information about using A records, see [Configure DNS settings](#).

### Prerequisites

- You have obtained the WAF CNAME address.
  1. Log on to the [Alibaba Cloud WAF console](#).
  2. On the top of the page, select Mainland China or International.
  3. Choose Management > Website Configuration and select DNS Proxy Mode. Select the website configuration and hover over the domain name. A Copy CName button appears.



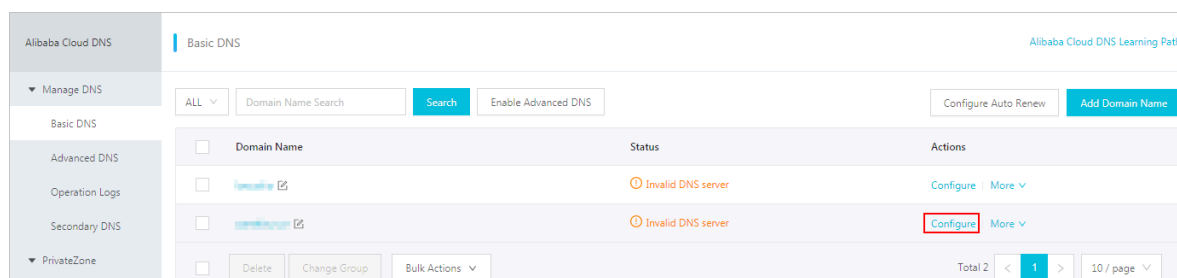
4. Click Copy CName to copy the WAF CNAME address.

 **Note:**  
If you want to use an A record to redirect requests to WAF, ping this CNAME address to obtain the corresponding WAF IP address. For more information, see [Set DNS settings](#). The IP address of the WAF instance that protects your website changes infrequently.

- You have the permissions to change the domain DNS settings in the system of your DNS service provider. This example uses a DNS record that is managed by Alibaba Cloud DNS, and WAF is activated under the same account.

### Procedure

1. Log on to the [Alibaba Cloud DNS console](#).
2. Select the domain name and click Configure.

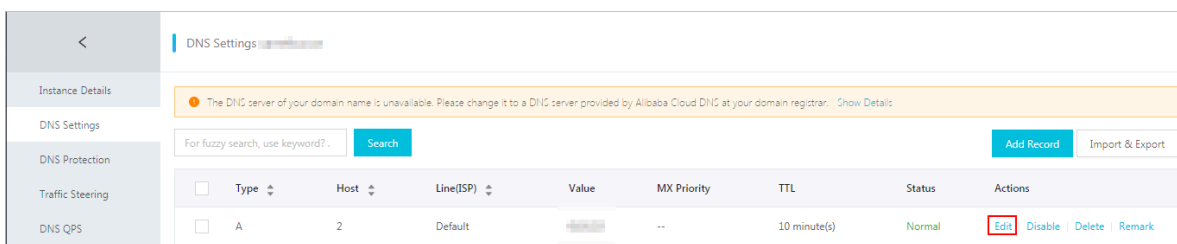




3. Select the specified host (hostname) and click Edit.

The following example uses `abc . com` :

- **www:** Used to select domain names that begin with www, such as `www . abc . com` .
- **@:** Matches the root domain `abc . com` .
- **\***: Matches all wildcard domains including root domains and subdomains, such as `blog . abc . com` , `www . abc . com` , and `abc . com` .



4. In the Edit Record dialog box, perform the following operations:

- **Type:** Select CNAME.
- **Value:** Paste the WAF CNAME address that you have copied in the preceding step.
- **Keep the remaining settings unchanged.** We recommend that you set the TTL to 10 minutes. A longer TTL indicates that the system takes a longer time to synchronize and update the DNS record.

Notes:

- You can only specify one CNAME record for each hostname. Change the value to the WAF CNAME address.
- Different record types conflict with each other. For example, a CNAME record, an A record, an MX record, and a TXT record cannot coexist with each other under the same hostname. If you cannot change the record type, delete all conflicting records, and then add a new CNAME record.

 **Note:**

You must delete conflicting records and add the new CNAME record in a short period of time. Otherwise, your domain becomes inaccessible.

- If you must keep the MX record, you can use an A record to redirect requests to WAF. For more information, see [Set DNS settings](#).

The screenshot shows a dialog box titled "Edit Record" with a close button (X) in the top right corner. The form contains the following fields:

- Type:** A dropdown menu with "CNAME- Canonical name" selected. This field is highlighted with a red box.
- Host:** A text input field containing "www".
- ISP Line:** A dropdown menu with "Default - Return to the default value when the query is not ..." selected.
- \* Value:** A text input field containing "aliyundunwaf.com". This field is highlighted with a red box.
- \* TTL:** A dropdown menu with "10 minute(s)" selected.

At the bottom right of the dialog, there are two buttons: "Cancel" and "OK".

5. Click OK and wait for the DNS record to take effect.
6. (Optional) Verify the DNS settings. Ping the domain or use [DNS Check](#) to check whether the DNS record takes effect.



Note:

It takes some time for the DNS record to take effect. If the verification fails, verify the DNS record again in 10 minutes.

7. Check the DNS resolution status.

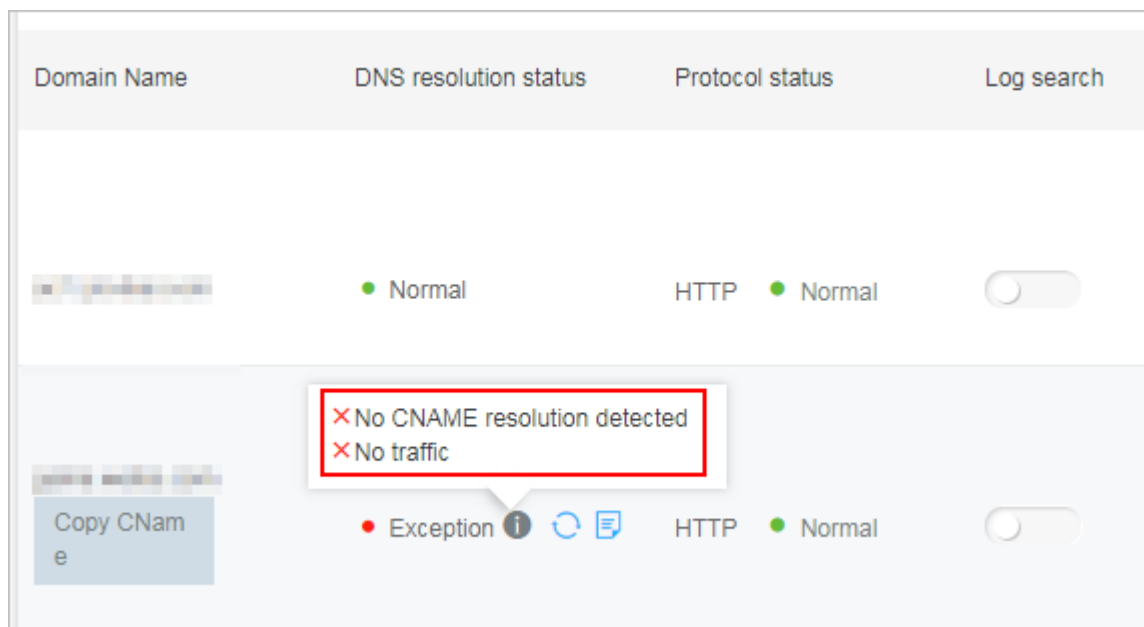
- a. Log on to the [WAF console](#).
- b. Choose Management > Website Configuration and select DNS Proxy Mode to view the DNS translation status.
  - Normal indicates that WAF has been successfully configured for your website. All requests that are sent to your website are redirected to WAF for monitoring.
  - Exception indicates that you have not correctly configured WAF for you website if the following error messages appear: No CNAME resolution detected, No traffic, and DNS check failed.

If you confirm that the DNS settings are correct, check the DNS translation status again in an hour, or troubleshoot the errors. For more information about troubleshooting, see [DNS resolution status exception](#).



Note:

The error message, as shown in the following figure, only indicates whether you have correctly configured WAF for your website. It does not indicate whether your website is accessible.



## 4 Step 3: Configure WAF protection polices

---

After the website is deployed with Alibaba Cloud WAF, WAF helps inspect the web traffic and block common web attacks (such as SQL injections and XSS scripting) and HTTP flood attacks, based on the default protection settings. You can enable more protection functions and configure their policies according to your actual business situation.

### 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 domain name to be configured and click Policies.
4. Enable/Disable different WAF protection functions and manage their protection rules.



#### Note:

Different subscription plans are offered with different functions. Not all of the following functions are included in your subscription. For more information, see [WAF subscription plans](#).

- **HTTP ACL Policy:** When enabled, it lets you create web access control rules to filter web requests based on conditions such as the IP addresses that requests originate from, the requested URL, and other common HTTP request header fields. For more information, see [HTTP ACL Policy](#).
- **Web Application Protection:** Enabled by default. It protects your website against common web attacks such as SQL injections and allows you to configure the strictness of the inspection and determine whether to block malicious requests. For more information, see [Web application protection](#).
- **HTTP Flood Protection:** Enabled by default. It protects your website against HTTP flood attacks and allows you to configure the strictness of the inspection. With the Business or Enterprise subscription, you can also create rate-based rules to limit the number of requests per specified time interval. The rate-based rule can count the requests received from a specific IP address per specified time interval. If the number of requests exceeds the limit, the rule triggers the

specified action. For more information, see [HTTP flood protection](#) and [Custom HTTP flood protection rules](#).

- **New Intelligent Protection Engine:** When enabled, it automatically performs semantic analysis on web requests to discover malicious attacks that exploit obfuscation or variations and are skillfully disguised or hidden. For more information, see [New intelligent protection engine](#).
- **Blocked Region:** When enabled, it lets you block requests originate from a specified geolocation, which currently can be a Chinese province or non-China region. For more information, see [Blocked region](#).
- **Data Risk Control:** When enabled, it redirects suspicious users to an additional security verification page for your key business interfaces such as registration, login, activities, and forums, to prevent machine frauds. It helps you protect against zombie accounts, hacked accounts, vote cheating, and spam messages. For more information, see [Data risk control](#).
- **Website tamper-proofing:** When enabled, it lets you lock the specified web pages to prevent the original content from being tampered with. When a locked web page is requested, the server returns the cached page you specify. For more information, see [Website tamper-proofing](#).
- **Data Leakage Prevention:** When enabled, it lets you create sensitive data filtering rules to cover up the ID card number, credit card number, telephone number, and the default sensitive word of your returned web content, and to block web pages with the specified request code. For more information, see [Data leakage prevention](#).

## 5 Step 4: View security reports

---

After the website is deployed with Alibaba Cloud WAF and WAF protection policies are configured, you can access the WAF security reports to gain an insight into the security situation of your web business or conduct business analysis.

### 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 Reports > Overview page, view the statistics of your Business and Security situations.

You can view the following Business statistics:

- Total QPS and the malicious QPS (triggering protection rules) of the latest 30 days
- Inbound and Outbound bandwidth of the latest 30 days
- Number of abnormal responses of the latest 30 days
- Top 5 cities and Top 10 IP addresses that requests originate from
- Mobile operating systems and PC browsers that requests originate from
- Top 5 URLs with the slowest response speed
- Top 5 URLs that are most frequently requested

You can view the following Security statistics:

- Frequencies of Web application attacks, HTTP flood attacks, and Web ACL events of the latest 30 days
- Risk warnings of newly exposed industry or business security events
- Messages of update of Alibaba Cloud WAF protection rule sets

For more information, see [Security overview](#).

4. On the Reports > Reports page, query the detailed Attack Protection records and Risk Warnings.

You can query the details of the following attack protection records:

- Web application attacks of the latest 30 days
- HTTP flood attacks of the latest 30 days
- Web ACL events of the latest 30 days

You can query the details of the following risk warnings:

- Known hacker attacks
- WordPress attacks
- Suspected attacks
- Robot scripts
- Web crawlers
- SMS interferes abuse

For more information, see [WAF security reports](#).