

Alibaba Cloud

Web应用防火墙
Website Access

Document Version: 20220704

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
 Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1. Tutorials	05
2. Website access with CNAME	07
2.1. Add a domain name	07
2.2. Verify domain name settings	24
2.3. Allow access from back-to-origin CIDR blocks of WAF	26
2.4. Change a DNS record	27
2.5. Specify ports	31
2.6. Configure custom TLS settings	32
2.7. Configure protection for an origin server	34
2.8. Retrieve actual IP addresses of clients	41
3. Connect cloud services to WAF	47
3.1. Use WAF with CDN	47
3.2. Add a website to both Anti-DDoS Pro or Anti-DDoS Premi...	49
4. View the allowed port range	53

1. Tutorials

Before you can use Web Application Firewall (WAF) to protect your web services, you must add your website to WAF. If you do not add your website to WAF, WAF does not protect your website.

Add your website to WAF

After you activate WAF, you can add your website to WAF in **CNAME record** mode.

After you add the domain name of your website in the WAF console, you must change the DNS record to redirect the requests that are destined for your website to WAF. Then, WAF filters the requests and forwards normal requests to the origin server of the domain name. You can manually add your website or configure WAF to automatically add your website.

In CNAME record mode, perform the following operations to add your website to WAF:

1. **Add a domain name**: This topic describes how to manually add a website to WAF or configure WAF to automatically add a website.

Note

- If your website uses HTTPS, you must upload a valid HTTPS certificate in the WAF console to make sure that WAF processes HTTPS requests as expected. For more information, see [Upload an HTTPS certificate](#).
- If the origin server uses a port other than HTTP port 80 and HTTPS port 443, you can specify the port and check whether the port is within the port range that is supported by WAF. For more information, see [View the allowed port range](#).

2. **Allow access from back-to-origin CIDR blocks of WAF**: WAF uses specified back-to-origin CIDR blocks to forward normal requests to the origin server. To allow inbound requests from the back-to-origin CIDR blocks, you must configure security software or access control policies on the origin server when you add a website to WAF.
3. **Verify domain name settings**: This topic describes how to set up a staging environment after a domain name is added to WAF and how to check whether the settings to forward requests are in effect. We recommend that you do not change the DNS record before the settings take effect. If you change the DNS record before the settings take effect, access failures may occur.
4. **Change a DNS record**: This topic describes how to manually change the DNS record to redirect the requests that are destined for your website to WAF.

After you add the website, WAF filters the requests that are destined for the website and forwards normal requests to the origin server. WAF provides multiple features to protect your website against different types of attacks. By default, only the **protection rules engine** and **HTTP flood protection** features are enabled. The protection rules engine feature protects your website against common web attacks, such as SQL injections, cross-site scripting (XSS) attacks, and webshell uploads. The HTTP flood protection feature protects your website against HTTP flood attacks. To use other features, you must manually enable the features and configure protection rules. For more information, see [Overview](#).

Best practices

- **Configure protection for an origin server**: If the origin server is deployed on an Elastic Compute Service (ECS) instance, you can configure security group policies for the ECS or Server Load Balancer (SLB) instance to allow inbound requests only from WAF to the origin server. This way, attackers

cannot bypass WAF to attack the origin server.

- **Retrieve actual IP addresses of clients:** After you configure WAF, all requests that are destined for your website are forwarded to WAF, and then WAF forwards the normal requests to the origin server. The origin server can use the X-Forwarded-For header to retrieve the originating IP addresses of these requests.

Add cloud services to WAF

- **Add a website to both Anti-DDoS Pro or Anti-DDoS Premium and WAF:** You can deploy Anti-DDoS Pro or Anti-DDoS Premium and WAF in sequence to protect your website against web application attacks and DDoS attacks.
- **Use WAF with CDN:** You can deploy Alibaba Cloud CDN and WAF in sequence to protect your website against web application attacks and accelerate access to your website.


2. Website access with CNAME

2.1. Add a domain name

This topic describes how to add a domain name to Web Application Firewall (WAF) in CNAME record mode after you purchase a WAF instance.

Prerequisites

-
- If you use a WAF instance in the Chinese mainland to protect your domain name, you must complete Internet Content Provider (ICP) filing for your domain name before you can add your domain name to the WAF instance. If you have not completed ICP filing for your domain name, an error is reported when you add your domain name to WAF. For more information about ICP filing, see [ICP filing application overview](#).


 **Notice** After you add your domain name to WAF, we recommend that you keep the ICP filing information up-to-date. To meet the requirements of laws and regulations, WAF removes the domain names whose ICP filing information is invalid on a regular basis.

Context

When you add your domain name to WAF in CNAME record mode, you must enter the domain name information and change the DNS record to resolve the domain name to the CNAME assigned by WAF. This way, the requests destined for your domain name are redirected to WAF. This mode is supported regardless of whether your origin server is deployed on the cloud. However, the origin server must be accessible over the Internet. The following sections describe how to add a domain name in CNAME record mode.

You can use one of the following methods to add a domain name:

- **Configure WAF to automatically add domain name configurations:** You need only to select the domain name that you want to add and the network protocol type on the **Add Domain Name** page. WAF automatically reads the information about the domain name within your Alibaba Cloud account. Then, WAF automatically adds the domain name configurations, such as the domain name, server address, and standard ports 80 and 443, and changes the DNS record of the domain name.

 **Notice** The account that you use to add domain names must have management permissions on Alibaba Cloud DNS resources. If the account does not have the permissions, WAF cannot automatically change the DNS record. If WAF does not automatically change the DNS record, you can manually change the DNS record of the domain name after the domain name is added.

- **Manually add domain name configurations:** If WAF cannot automatically add the configurations of a domain name, you can add the domain name configurations, such as the domain name, protocol type, server address, and server port. After you add the domain name configurations, you must change the DNS record of the domain name to redirect the requests that are destined for the domain name to WAF.

Configure WAF to automatically add domain name configurations

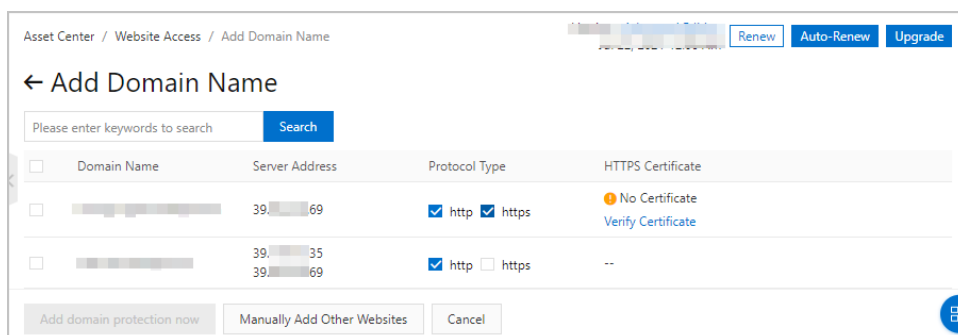
You can select an eligible domain name that you want to add to WAF from the list on the **Automatically Add** tab. Then, the domain name is automatically added.

Eligible domain names include only the valid domain names that are configured in Alibaba Cloud DNS.

Procedure

- 1.
- 2.
- 3.
4. On the **Domain Names** tab, click **Website Access**.
5. (Optional) On the **Add Domain Name** page, set **Access Mode** to **CNAME Record**.
If **CNAME Record** is automatically selected, skip this step.
6. On the **Automatically Add** tab, select the required domain name and protocol type from the **Domain Name** and **Protocol Type** columns. Then, click **Automatically Add**.

Note If the **Automatically Add** tab displays an empty list, no eligible domain names are found from your account. In this case, you must manually add a domain name. For more information, see [Complete the wizard](#).




If the domain name supports HTTPS, you must select **https**. If you select **https**, you must verify the HTTPS certificate of the domain name before the domain name can be added. To verify the HTTPS certificate, perform the following steps:

- i. Select the domain name and **https**. Then, click **Verify Certificate** in the **HTTPS Certificate** column.
- ii. In the **Verify Certificate** dialog box, specify **Upload Type** and upload the certificate that is associated with the domain name as prompted.
For more information, see [Upload an HTTPS certificate](#).
- iii. After you upload the certificate, click **Confirm**.
WAF automatically verifies the uploaded certificate.
 - If the certificate verification is successful, click **Automatically Add**.
 - If the certificate verification fails, resolve the failure based on the error message that is returned and perform the certificate verification again until the verification is successful.
Error message example: **The certificate and key do not match**.

For more information, see [How do I handle the mismatch between a certificate and its private key?](#).

WAF automatically adds the domain name configurations and changes the DNS record.

 **Note** If you want to add ports in addition to ports 80 and 443, modify the domain name information after the domain name is automatically added. For more information, see [What to do next](#).

Possible issues and solutions:

- Domain name was added, but you need to manually change the DNS record.

Possible causes: The account that you use to add the domain name does not have management permissions on Alibaba Cloud DNS resources, or the uploaded HTTPS certificate does not match your domain name.

 **Note** If your domain name supports HTTPS but the uploaded HTTPS certificate does not match the domain name, WAF cannot detect the certificate even if the certificate verification is successful. In this case, WAF does not automatically change the DNS record. You must upload a valid and correct certificate and then manually change the DNS record. For more information, see [Upload an HTTPS certificate](#).

Click **manually access the DNS**. In the **Manual Configuration** dialog box, change the DNS record. For more information, see [Change a DNS record](#).

- The maximum number of domain names has been reached.

Click **extra domain package** to purchase an extra domain package. Then, add the domain name again.

- No ICP filing records are found for the domain name.

If you use a WAF instance in the Chinese mainland to protect your domain name, you must complete Internet Content Provider (ICP) filing for your domain name before you can add your domain name to the WAF instance. If WAF does not find ICP filing records for your domain name, you must complete ICP filing for your domain name and try again. For more information, see [ICP filing application overview](#).

Manually add domain name configurations

To add a domain name to WAF in CNAME record mode, perform the following steps:

-
-
-
- On the **Domain Names** tab, click **Website Access**.
- (Optional) On the **Add Domain Name** page, set **Access Mode** to **CNAME Record**.
If **CNAME Record** is automatically selected, skip this step.
- Click the **Manually Add** tab and complete the wizard as prompted.
 - In the **Enter Site Information** step,
Configure the parameters and click **Next**. The following table describes the parameters.

1

Enter Your Website Information

2

Change DNS Settings

3

Add Completed

* Domain Name:

Enter the domain name of your website. For example: www.aliyun.com

You can enter top-level domains (such as .com) and second-level domains (such as www.aliyun.com). The domains will not conflict with each other.

* Protection Resource

☒ Shared Cluster

* Protocol Type:

☐ HTTP ☐ HTTPS

* Destination Server (IP Address): ⓘ

☒ IP ☐ Domain Name (Such as CNAME) ⓘ

Enter the public IP addresses of servers that you want to protect, such as 1.1.1.1 and 10.10.10.1. Press Enter each time you enter an IP address. You can enter a maximum of 20 IP addresses.

0

* Destination Server Port:

HTTP Port

Select HTTP first.

HTTPS Port

Select HTTPS first.

Load Balancing Algorithm:

☒ IP hash ☐ Round-robin ☐ Least time

This function is not yet supported by the current version. Please Upgrade

Does a layer 7 proxy (DDoS Protection/CDN, etc.) exist in front of WAF:

☐ Yes ☒ No

☐ Enable Traffic Mark ⓘ

Next

Cancel

> How to determine the protocol type?

> How to obtain the website IP address?

> Which ports can the Web Application Firewall protect? Click to view

Meet Expert

Join the WAF Technical Support DingTalk group

Need Service Configuration?


One-on-one consultation with security engineers to solve problems with Web Application Firewall during installation, configuration, etc.

Buy


Parameter	Description
-----------	-------------




10

> Document Version: 20220704




Parameter	Description
Domain Name	<p>Enter the domain name. The domain name must meet the following requirements:</p> <ul style="list-style-type: none"> The domain name can be an exact match domain name such as <code>www.aliyun.com</code>. The domain name can also be a wildcard domain name such as <code>*.aliyun.com</code>. If you enter a wildcard domain name, WAF automatically matches specific domain names for the wildcard domain name. For example, if you enter <code>*.aliyun.com</code>, WAF matches <code>www.aliyun.com</code> and <code>test.aliyun.com</code>. <div style="border: 1px solid #add8e6; padding: 10px; margin: 10px 0;"> <p> Notice If you enter a wildcard domain name, WAF does not match the parent domain name of the wildcard domain name. For example, if you enter <code>*.aliyun.com</code>, WAF does not match <code>aliyun.com</code>. If you want to use WAF to protect <code>aliyun.com</code>, you must separately add the domain name to WAF.</p> </div> <ul style="list-style-type: none"> If you enter a wildcard domain name and an exact match domain name, WAF uses the forwarding rules and protection policies of the exact match domain name. <code>.edu</code> domain names are not supported. If you want to add <code>.edu</code> domain names, you must submit a request for technical support.
Protection Resource	<p>Select the type of protection resource that you want to use. Valid values:</p> <ul style="list-style-type: none"> Shared Cluster: This is the default value. Exclusive cluster: This option is available only when you use a WAF instance of the Exclusive edition. You can customize an exclusive cluster to deliver service-specific protection. For more information, see Best practices for WAF exclusive clusters. Hybrid Cloud Cluster: If you use Hybrid Cloud WAF, you must select this option. For more information, see Add a website to Hybrid Cloud WAF.
	<p>Select a protocol type. Valid values:</p>



Protocol Type

Parameter	<div> <div>■ Enable Origin SNI.</div> <div>Description</div> </div>
	<p>Origin Server Name Indication (SNI) specifies the domain name to which an HTTPS connection must be established at the start of the TLS handshaking process when WAF forwards requests to the origin server. If the origin server hosts multiple domain names, you must enable this feature.</p> <p>After you select Enable Origin SNI, you can configure the SNI field. Valid values:</p> <ul style="list-style-type: none"> Use Domain Name in Host Header: indicates that the value of the SNI field in WAF back-to-origin requests is the same as the value of the Host header field. This is the default value. <p>For example, if the domain name you configured is <code>*.aliyundoc.com</code> and the client requests the <code>www.aliyundoc.com</code> domain name, the value of the SNI field in WAF back-to-origin requests is <code>www.aliyundoc.com</code>. The <code>www.aliyundoc.com</code> domain name is the value of the Host header field.</p> Custom: indicates that you can customize the SNI field in WAF back-to-origin requests. <p>If you want WAF to use an SNI field whose value is different from the value of the Host header field in back-to-origin requests, you must specify a custom value for the SNI field.</p> <p>■ HTTP 2 (You can select HTTP/2 only after you select HTTPS.)</p> <p>If your domain name supports HTTP/2, you must select HTTP2. The HTTP/2 port is the same as the HTTPS port. After you select HTTP2, you need only to set the HTTPS port.</p> <div>  Notice You can select HTTP2 only for WAF instances of the Enterprise or higher edition. </div> <p>For more information, see Is the origin server affected if you add HTTP/2 services to WAF?.</p>
	<p>Enter the address of the origin server. Valid values: IP and Domain Name (Such as CNAME). WAF filters and forwards requests to this address.</p>

Parameter	Description
Destination Server (IP Address)	<p>■ IP: Enter the public IP address of the origin server. The IP address must be accessible over the Internet.</p> <p>Press Enter each time you enter an IP address. You can enter up to 20 IP addresses.</p> <div>  Note If you enter multiple IP addresses, WAF automatically performs health checks and load balancing on these addresses. </div> <p>If your WAF instance resides outside the Chinese mainland, you can enter only IPv4 addresses. If your WAF instance resides in the Chinese mainland, you can enter IPv4 and IPv6 addresses or only IPv4 addresses. However, you cannot enter only IPv6 addresses. You can enter IPv4 or IPv6 addresses based on the following descriptions:</p> <ul style="list-style-type: none"> ■ If you configure both IPv4 and IPv6 addresses and select Use the Same Protocol, WAF forwards requests from IPv4 addresses to the origin server over IPv4, and requests from IPv6 addresses to the origin server over IPv6. If you do not select Use the Same Protocol, WAF randomly forwards requests to the origin server over IPv4 or IPv6. <div>  Notice If you want WAF to forward requests over IPv6, make sure that IPv6 is turned on for the domain name on the Website Access page. For more information, see Enable IPv6 traffic protection. </div> <ul style="list-style-type: none"> ■ If you enter only IPv4 addresses, WAF forwards all requests to the origin server over IPv4. <p>The following list describes how to enter an IP address:</p> <ul style="list-style-type: none"> ■ If the origin server is an Alibaba Cloud Elastic Compute Service (ECS) instance, enter the public IP address of the instance. ■ If the ECS instance is associated with a Server Load Balancer (SLB) instance, enter the public IP address of the SLB instance. ■ If the origin server is not deployed on Alibaba Cloud, we recommend that you ping the domain name to query the public IP address of the origin server. Then, enter the public IP address of the origin server. <ul style="list-style-type: none"> ■ Domain Name (Such as CNAME): Enter the domain name of the origin server. For example, enter the CNAME of an Object Storage Service (OSS) bucket. <p>If you select Domain Name (Such as CNAME), WAF forwards all requests to the origin server over IPv4.</p> <div>  Notice <ul style="list-style-type: none"> ■ The domain name of the origin server must be different from the domain name that you want to protect. ■ If you enter a domain name of an OSS bucket, you must map the domain name that you want to protect to the bucket in the OSS console. For more information, see Map custom domain names. </div>

Parameter	Description

Parameter	Description
Server Port	<p>Specify the port that you use to forward requests.</p> <p>WAF uses only the port that you specify to receive and forward requests. This way, the origin server is protected against security threats even if you enable ports that you do not specify.</p> <div> Notice Protocol Type and Destination Server Port must be configured to the protocol and port that the origin server uses to provide web services. WAF does not support port translation. For example, if the origin server provides web services by using HTTP and port 80, you must set Protocol Type to HTTP and Destination Server Port to 80.</div> <p>Default ports:</p> <ul style="list-style-type: none">■ HTTP 80: This port is used when HTTP is selected.■ HTTPS 443: This port is used when HTTPS is selected. <div> Note HTTP/2 uses the same port as HTTPS.</div> <p>Custom ports: Enter port numbers in the HTTP Port and HTTPS Port fields. Press Enter each time you enter a port number. Click View Allowed Port Range to query all supported ports.</p> <div><div><div>Destination Server Port:</div><div><div>HTTP Port</div><div>80 ×</div><div>1</div><div>View Allowed Port Range</div></div><div><div>HTTPS Port</div><div>443 ×</div><div>1</div><div>View Allowed Port Range</div></div></div></div> <div> Note<ul style="list-style-type: none">■ WAF Enterprise and Exclusive each support a maximum of 50 different server ports, which include ports 80, 8080, 443, and 8443. WAF Pro and Business each support a maximum of 10 ports, which include ports 80, 8080, 443, and 8443.■ For more information about the ports that are supported by shared clusters, see View the allowed port range.■ If you use a WAF instance of the Exclusive edition, you can select ports only from the Destination Server Port section on the Exclusive Settings page. For more information, see Create an exclusive cluster.</div>

Parameter	Description
Load Balancing Algorithm	<p>If you enter multiple addresses for origin servers, configure this parameter. Valid values:</p> <ul style="list-style-type: none">■ IP hash: Requests from a specific IP address are forwarded to the same origin server. This is the default value. <div><p> Note If you select IP hash but the IP addresses of origin servers are not scattered on different network segments, workloads may be unbalanced.</p></div> <ul style="list-style-type: none">■ Round-robin: All requests are distributed to origin servers in turn.■ Least time: WAF uses the intelligent DNS resolution feature and the upgraded least-time back-to-origin algorithm to minimize the latency when requests are forwarded to origin servers. <div><p> Note You can select Least time only when intelligent load balancing is enabled. For more information, see Intelligent load balancing.</p></div> <p>After the settings take effect, WAF distributes back-to-origin requests to multiple addresses of origin servers.</p>
	<p>Specify whether a Layer 7 proxy is deployed in front of WAF. The Layer 7 proxies include Anti-DDoS Pro, Anti-DDoS Premium, and Alibaba Cloud CDN. Valid values:</p> <ul style="list-style-type: none">■ No: No Layer 7 proxies are deployed in front of WAF, and WAF receives requests from clients. WAF uses the IP address that is used to establish connections with WAF as the actual IP address of a client. WAF obtains the actual IP address from the <code>REMOTE_ADDR</code> field.

■	Yes: A Layer 7 proxy is deployed in front of WAF, and WAF receives requests from the Layer 7 proxy, instead of clients. To make sure that
Description	WAF can obtain the actual IP address of a client for security analysis, you must configure Obtain Source IP Address .

By default, WAF uses the first IP address in the `X-Forwarded-For` field as the actual IP address of a client.

Does a layer 7 proxy (DDoS Protection/CDN, etc.) exist in front of WAF:

☒ Yes ☐ No

Obtain Source IP Address


☐ Use the First IP Address in X-Forwarded-For Field as Source IP Address

☒ [Recommended] Use the First IP Address in Specified Header Field as Source IP Address to Prevent X-Forwarded-For Forgery ⓘ

Header Field ⓘ

If you enter more than one request header, separate these headers with commas (,).

You can use other proxies that require the actual IP addresses of clients to be contained in a custom header field, such as X-Client-IP or X-Real-IP. In this case, you must select **Use the First IP Address in Specified Header Field as Source IP Address to Prevent X-Forwarded-For Forgery** and enter a custom header field in the **Header Field** field.

 **Note** We recommend that you use custom header fields to store the actual IP addresses of clients and configure the header fields in WAF. This way, attackers cannot forge X-Forwarded-For fields to bypass WAF protection rules. This improves the security of your business.

You can enter multiple header fields. You must enter a comma (,) each time you enter a header field. If you enter multiple header fields, WAF attempts to obtain the actual IP address of a client from the fields in sequence. WAF obtains the actual IP address of a client from the first header field until the IP address is obtained. If WAF fails to obtain the actual IP address of the client from all header fields, WAF uses the first IP address in the X-Forwarded-For field as the actual IP address of the client.

Specify whether to enable the WAF traffic marking feature.

This feature adds custom header fields to WAF back-to-origin requests. You can specify or modify the custom header fields to tag the requests that are forwarded by WAF or record the IP addresses of clients.

If you select **Enable Traffic Marking**, you must add custom header fields.

☒ Enable Traffic Mark ⓘ

Custom Header ▾

Header Name

Header Value

×




Client IP Address ▾

The name of the header field that

×

[+ Add Mark](#) Upper Limit: 5

You can add the following two types of header fields:

Parameter	Description
Enable Traffic Mark	<p>■ Custom Header: If you want to add a header field of this type, you must specify a header field name and header field value. WAF adds the header field to the back-to-origin requests. This helps the backend service identify whether requests pass through WAF, collect statistics, and analyze data.</p> <p>For example, you can specify the <code>ALIWAF-TAG: Yes</code> header field setting to tag the requests that pass through WAF. In this example, <code>ALIWAF-TAG</code> is the header field name, and <code>Yes</code> is the header field value.</p> <div>  Notice We recommend that you do not configure a standard HTTP header field, such as User-Agent. If you configure a standard HTTP header field, the value of the standard header field is overwritten by the value of the custom header field. </div> <p>■ Client IP Address: If you want to add a header field of this type, you must specify the name of the header field that records an IP address. This way, WAF adds the header field to the back-to-origin requests and adds the IP addresses of clients to the value of the header field. For more information about how WAF obtains the IP addresses of clients, see the description of the Does a layer 7 proxy (DDoS Protection/CDN, etc.) exist in front of WAF parameter.</p> <p>If the backend service needs to obtain the IP addresses of clients from a specified custom header field such as <code>example-client-ip</code> for analysis, you must add a header field of the Client IP Address type.</p> <div>  Notice We recommend that you do not configure a standard HTTP header field, such as User-Agent. If you configure a standard HTTP header field, the value of the standard header field is overwritten by the value of the custom header field. </div> <p>Click Add Mark to add a header field. You can add up to five header fields.</p>
Resource Group	<p>Select the resource group to which the domain name belongs from the resource group list.</p> <div>  Note You can use Resource Management to create resource groups and manage resources within your Alibaba Cloud account by department or project. For more information, see Create a resource group. </div>

ii. Change the DNS record.

Change the DNS record as prompted and click **Next**. After you change the DNS record, the domain name is mapped to WAF. For more information, see [Change a DNS record](#).

iii. Complete the settings.

Configure the back-to-origin CIDR blocks of WAF as prompted and click **Completed**. **Return to the website list**. Then, the **Website Access** page appears. For more information, see [Allow access from back-to-origin CIDR blocks of WAF](#).

Upload an HTTPS certificate

If you select **HTTPS** when you add a domain name, you must upload the valid and correct HTTPS certificate that is associated with the domain name in the WAF console. This way, WAF can protect HTTPS requests.

You can use one of the following methods to upload an HTTPS certificate:

- **Manually upload a certificate:**

You must prepare the following files before you upload a certificate. Before you upload a certificate, make sure that the certificate chain is valid.

- The certificate file in the CRT or PEM format
- The private key file in the KEY format

- **Select an existing certificate:** You can select the certificate that is associated with the domain name and is managed in the [SSL Certificates Service](#) console.

Procedure

- 1.
- 2.
- 3.
4. On the **Domain Names** tab, find the domain name that you want to manage and click the



icon in the **Origin Server** column.

Note The



icon appears in the **Origin Server** column only when you select **HTTPS** for the domain name that you add to WAF.

Domain Name	Access Mode	Origin Server
example.com	CNAME Record	47.11.24 Upload Certificate

5. In the **Upload Certificate** or **Update Certificate** dialog box, specify **Upload Type** to upload an HTTPS certificate.

Note If the certificate is uploaded, the **Update Certificate** dialog box appears. The **Update Certificate** and **Upload Certificate** dialog boxes have the same configuration items.

- **Manual Upload:** Specify **Certificate Name**, copy and paste the content of the certificate file to the **Certificate File** field, and then copy and paste the content of the private key file to the **Private Key File** field.

Upload Certificate

The website uses HTTPS. You need to import the certificate and private key to protect the website.

Upload Type

☒ Manual Upload ☐ Select Existing Certificate ☐ Purchase Certificate

The certificate is automatically hosted by SSL Certificates Service.

Domain Name
example.com

* Certificate Name

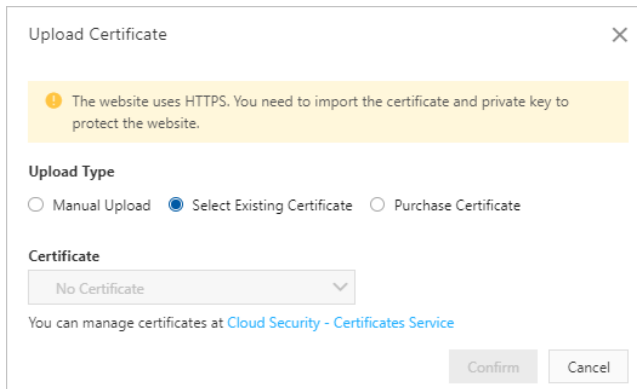
* Certificate File ⓘ

* Private Key File ⓘ

Confirm Cancel

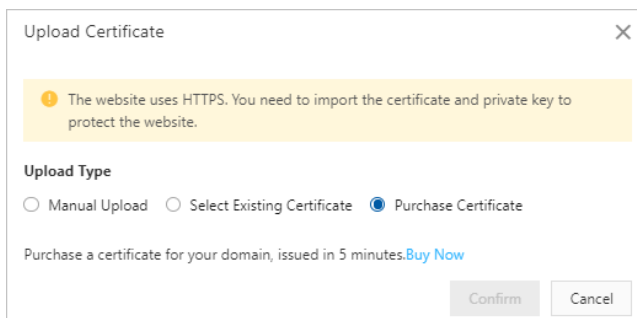
For more information about the **certificate file**, see the following descriptions:

- If the certificate file is in the PEM, CER, or CRT format, you can use a text editor to open the certificate file and copy the text content.
 - If the certificate file is in another format, such as PFX or P7B, you must convert the certificate file format to PEM. Then, you can use a text editor to open the certificate file and copy the text content. For information about how to convert the format of a certificate file, see [How do I convert an HTTPS certificate to the PEM format?](#)
 - Make sure that the certificate chain is valid. If the domain name is associated with multiple certificate files, you must combine the text content of the certificate files and then copy and paste the combined content to the **Certificate File** field.
- **Select Existing Certificate:** Select the certificate that you want to upload from the **Certificate** drop-down list.



The **Certificate** drop-down list is a collection of certificates that are issued in the SSL Certificates Service console. You can select the certificate that is associated with the domain name. You can click **Cloud Security - Certificates Service** to go to the SSL Certificates Service console to manage certificates.

- o **Purchase Certificate:** Click **Buy Now** to go to the configuration page of SSL Certificates Service to purchase a certificate for the domain name.



The certificate that you purchase is automatically uploaded to WAF.

Note You can purchase only a domain validated (DV) certificate on this page. If you want to purchase a different type of certificate, go to the buy page of SSL Certificates Service. For more information, see [选择购买方式Purchase an SSL certificate instance](#).

6. Click **OK**.

Subsequent configurations


After you add the domain name, the requests that are destined for the domain name are protected by WAF. You can modify domain name configurations to enhance protection.

Type	Description	References
Website protection configuration	WAF provides multiple features to protect your domain name against different types of attacks. By default, the Protection Rules Engine and HTTP Flood Protection features are enabled. The protection rules engine feature protects your domain name against common web attacks, such as SQL injections, XSS attacks, and webshell uploads. The HTTP flood protection feature protects your domain name against HTTP flood attacks. You must manually enable other features and configure protection rules.	Overview

Type	Description	References
Alert configuration	You can configure alert rules to enable WAF to send alert notifications when attacks and abnormal traffic are detected in access requests. This way, you can check the security status of your business in a timely manner.	Configure WAF alerting
Configuration of the Log Service for WAF feature	After you enable the Log Service for WAF feature, WAF can collect and store the log data of your domain name. You can query and analyze the log data. By default, the Log Service for WAF feature stores full logs for 180 days. This helps you meet the requirements of classified protection.	Overview of the Log Service for WAF feature

What to do next

You can go to the **Domain Names** tab of the **Website Access** page to view the added domain name and perform the following operations.

- Upload an HTTPS certificate: If your domain name supports HTTPS, make sure that the correct certificate and private key files are uploaded to WAF. This ensures that WAF protects HTTPS requests. To upload the HTTPS certificate and private key files for the domain name, you must click the  icon in the **Origin Server** column.

For more information, see [Upload SSL certificates](#).

- Enable IPv6 traffic protection: If you want to protect IPv6 traffic destined for your domain name, turn on **IPv6** for the domain name in the **Quick Action** column.


For more information, see [Enable IPv6 traffic protection](#).

- Enable Log Service for WAF: Turn on **Log Service** in the **Quick Access** column to enable the Log Service for WAF feature. This feature allows you to collect logs of your domain name. You can use the logs for query, analysis, dashboard data visualization, and alerting.

For more information, see [Step 2: Enable the log collection feature](#).




Notice Log Service for WAF is a value-added feature that is provided by WAF. You must enable this feature before you can use it. For more information, see [Enable Log Service for WAF](#).

- Configure protection resources: Click the  icon next to **Protection Resource** in the **Quick Access** column. Then, configure the protection resources for the domain name.

The following types of protection resources are supported:

- **Shared Cluster and Shared IP**: This is the default value.
 - **Shared Cluster and Exclusive IP**: For more information about exclusive IP addresses, see [Exclusive IP addresses](#).
 - **Shared Cluster and Load Balancing Among Multiple WAF Nodes**: For more information about global load balancing, see [Intelligent load balancing](#).
 - **Exclusive Cluster**: For more information about exclusive clusters, see [Create an exclusive cluster](#).
- View attack monitoring reports: Click **View Report** in the **Attack Monitoring** column to go to the **Security Report** page. On the page that appears, you can view a protection report of the domain name. For more information, see [View Security Reports](#).

- Configure protection policies: Click **Config** in the **Actions** column to go to the **Website Protection** page. On the page that appears, you can configure the **Web Security**, **Bot Management**, and **Access Control/Throttling** modules. For more information, see [Overview](#).
- Modify domain name configurations: Click **Edit** in the **Actions** column to modify domain name configurations, such as the protocol type, server address, and server port. The domain name cannot be changed.
- Delete a domain name: Click **Delete** in the **Actions** column to delete a domain name.

 **Warning** Before you can delete a domain name, you must change the DNS record to map the domain name to the IP address of the origin server. If you do not change the DNS record, the requests that are destined for the domain name cannot be forwarded after the domain name is deleted.

FAQ

For more information, see [FAQ about website access configuration](#) in [FAQ](#).

2.2. Verify domain name settings

After you add a domain name to Web Application Firewall (WAF), we recommend that you change the DNS record on your computer to verify domain name settings in WAF. Then, you can change the DNS record in the WAF console to redirect requests to WAF to protect your service. This topic provides an example on how to verify domain name settings on an on-premises computer. In the following example, a Windows machine is used.

Prerequisites

A domain name of your website is added to WAF in CNAME mode. For more information, see [Add domain names](#).

Context

You can modify the *hosts* file to reconfigure the DNS record on your computer. In this scenario, the DNS record takes effect only on your computer. To verify the domain name settings on your computer, you must resolve the domain name of your website to the IP address of your WAF instance on your computer. If you can access the domain name from your computer, the domain name settings configured in WAF are valid. The step on your computer prevents access exceptions caused by inappropriate domain name settings.

Procedure

In the following example, your computer runs a Windows operating system.

1. Open File Server Resource Manager on your computer.
2. Enter `C:\Windows\System32\drivers\etc\hosts` in the address bar and open the *hosts* file by using a text editor.
3. Append the following content to the *hosts* file:

```
<IP address of your WAF instance> <Protected domain name>
```

In the content, `<Protected domain name>` is the domain name that you add to WAF. `<IP address of your WAF instance>` is the IP address that is mapped to the domain name. Separate `<IP a`

address of your WAF instance> and <Protected domain name> with a space.

To obtain the IP address of your WAF instance, perform the following steps:

- i.
- ii.
- iii.
- iv. On the **Domain Names** tab, move the pointer over the domain name that you add and click the



icon to copy the **CNAME** of the domain name.

- v. Open Command Prompt in Windows.
- vi. Run the following command to obtain the IP address of your WAF instance:

```
ping <CNAME that you copy>
```

- vii. Record the IP address of your WAF instance in the output of the `ping` command.

Assume that you add the domain name `test.aliyundoc.com` to WAF and the IP address of your WAF instance is `47.XX.XX.213`. Append the following content to the `hosts` file:

```
47.XX.XX.213 test.aliyundoc.com
```

4. Save changes to the `hosts` file and run the `ping <Protected domain name>` command to verify that your changes are in effect.

If your changes are in effect, the IP address in the output of the `ping` command is the IP address of your WAF instance.


If the IP address of the origin server is displayed in the command output, refresh the local DNS cache. You can run the `.\ipconfig /flushdns` command to refresh the DNS cache. Then, run the `ping` command again until the changes take effect.

5. In the address bar of your browser, enter the protected domain name.
 - If the website can be accessed, the domain name settings in the WAF console are correct and valid. In this case, you can restore the `hosts` file. Then, you can change the DNS record in the WAF console to redirect requests to WAF for protection. For more information, see [Change a DNS record](#).
 - If the website cannot be accessed, the domain name settings may be inappropriate. We recommend that you check the domain name settings in the WAF console. After you fix errors in the domain name settings, verify the domain name settings on your computer again. For more information, see [Add a domain name](#).
6. (Optional) Simulate simple web attack commands to check whether WAF runs as expected.

For example, in the address bar of your browser, enter `<Protected domain name>/alert(xss)`, which is a web attack request. Then, check whether WAF blocks the request.

If the request is blocked, the following page appears.

7. After the verification is complete, delete the record that you add in Step 3 from the `hosts` file.

 **Notice** If you do not delete the record after the verification is complete, exceptions may occur when your computer sends requests to the protected domain name.

Contact technical support

If you cannot identify errors in domain name settings, contact technical support by using one of the following methods:

- Log on to the [WAF console](#). In the lower part of the left-side navigation pane, click **Meet Expert**. Then, use your DingTalk to scan the QR code to join the DingTalk group 21715946. This way, you can contact Alibaba Cloud security experts for assistance.
- Submit a .

2.3. Allow access from back-to-origin CIDR blocks of WAF

Web Application Firewall (WAF) uses specific back-to-origin classless inter-domain routing (CIDR) blocks to forward normal traffic back to an origin server. After you add a website to WAF, you must configure security software or access control policies for the origin server to allow inbound traffic from the back-to-origin CIDR blocks.

Context

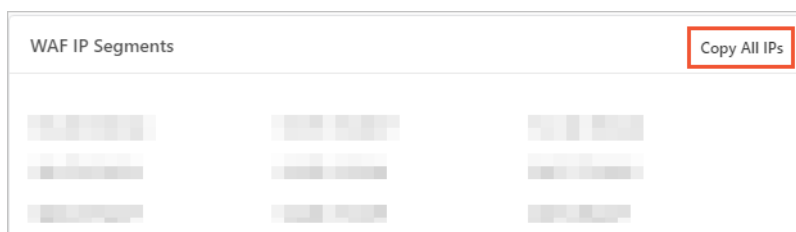
If you use security software such as FortiGate for your origin server, you must add the back-to-origin CIDR blocks of WAF to the IP address whitelist of the security software. This way, the security software does not block the normal traffic forwarded by WAF to the origin server.

For security purposes, we recommend that you configure access control policies for the origin server to allow inbound traffic only from the back-to-origin CIDR blocks of WAF. This way, attackers cannot bypass WAF to attack the origin server. For more information, see [Configure protection for an origin server](#).

Obtain the back-to-origin CIDR blocks of WAF

-
-
-
- In the lower part of the **Product Information** page, find the **WAF IP Segments** section and click **Copy All IPs**.

The **WAF IP Segments** section displays the latest back-to-origin CIDR blocks.



What to do next

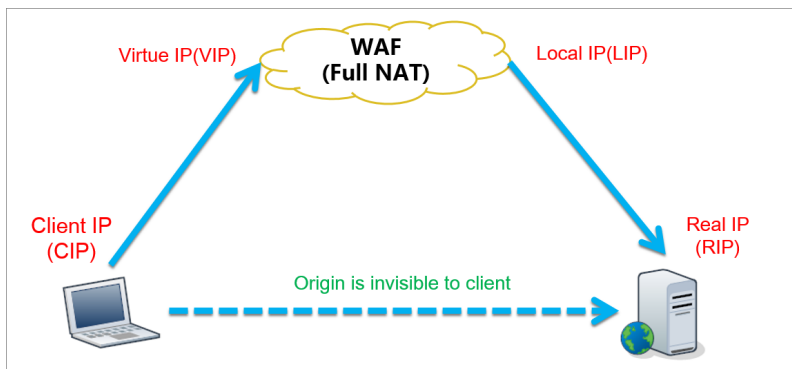
After you obtain the back-to-origin CIDR blocks of WAF, you must add them to the IP address whitelist of the security software on the origin server.

Warning If you do not add the back-to-origin CIDR blocks of WAF to the IP address whitelist of the origin server, normal requests forwarded by WAF may be blocked. This may cause service interruptions.

FAQ

- What is a back-to-origin CIDR block of WAF?

A back-to-origin CIDR block is a CIDR block used by WAF to forward requests that are sent from clients to the origin server. After a website is added to WAF, the origin server considers that all requests come from the back-to-origin CIDR blocks of WAF. The actual IP addresses of clients are added to the X-Forwarded-For (XFF) fields in the HTTP headers of requests.



- Why must I add the back-to-origin CIDR blocks of WAF to the IP address whitelist of the security software on the origin server?

After a website is added to WAF, the origin server receives most requests from the back-to-origin CIDR blocks of WAF, and requests are sent at a high rate. In this case, the firewall or security software on the origin server may consider these CIDR blocks as attack IP addresses and block them. If these IP addresses are blocked, WAF cannot receive responses from the origin server as expected. Make sure that the back-to-origin CIDR blocks of WAF are added to the IP address whitelist of the origin server after you add a website to WAF. Otherwise, the website may be inaccessible or become slow.

References

- [Does WAF automatically add its back-to-origin CIDR blocks to security groups?](#)
- [Do I need to allow access requests from all client IP addresses?](#)


2.4. Change a DNS record

After you add your website to WAF, you must use the CNAME or IP address of WAF to change the DNS record to redirect requests destined for your website to WAF. This topic describes how to change the DNS record.


Prerequisites

- The website configurations are manually added to WAF in CNAME mode. For more information, see [Manually add domain name configurations](#).
- You have the permissions to change the DNS record at your DNS service provider.

- (Optional)Requests from WAF back-to-origin CIDR blocks are allowed on the origin server. For more information, see [Allow access from back-to-origin CIDR blocks of WAF](#).

 **Notice** If you use security software such as FortiGate for your origin server, you must add the WAF back-to-origin CIDR blocks to the whitelist of the software. This prevents normal traffic from being blocked by access control policies.

- (Optional)The forwarding configurations for your website are correct and in effect. Before you change the DNS record, you must verify that the website forwarding configurations are correct. This prevents service interruptions caused by invalid configurations. For more information, see [Verify domain name settings](#).

 **Warning** If you change the DNS record before the forwarding configurations for your website take effect, service interruptions may occur.

Context

WAF redirects requests in one of the following methods:

- CNAME record: resolves the domain name to the CNAME assigned by WAF.

We recommend that you use the CNAME record method. If failures occur, such as node failures or failures in a data center, the CNAME record allows WAF to use another WAF IP address or directs requests to the origin server directly. This ensures service continuity and provides high availability and disaster recovery capabilities.

- A record: resolves the domain name to the WAF IP address.

We recommend that you use the A record method only when the CNAME record conflicts with the existing DNS settings. For example, the CNAME record conflicts with the MX record, and the MX record must be retained.


The following sections describe how to configure WAF for a website that does not use proxy services, such as CDN and Anti-DDoS Pro or Anti-DDoS Premium. If you want to deploy both WAF and other proxy services, see the following topics:

- [Deploy WAF and CDN together](#)
- [Add a website to both Anti-DDoS Pro or Anti-DDoS Premium and WAF](#)

Obtain the WAF CNAME and WAF IP address

You must obtain the WAF CNAME or WAF IP address of your domain name before you change the DNS record. If you have already obtained the WAF CNAME or IP address, skip the following steps.

- 1.
- 2.
- 3.
4. On the **Domain Names** tab of the Website Access page, move the pointer over the domain name and copy the WAF CNAME.
5. (Optional)Obtain the WAF IP address of the domain name.

 **Note** Perform this step only when you use the A record. If you use the CNAME record, skip this step.

- i. Open Command Prompt in Windows.
- ii. Run the following command to obtain the WAF IP address:

```
ping <WAF CNAME that you have copied>
```

- iii. Record the WAF IP address in the command output.


Use Alibaba Cloud DNS to change the DNS record

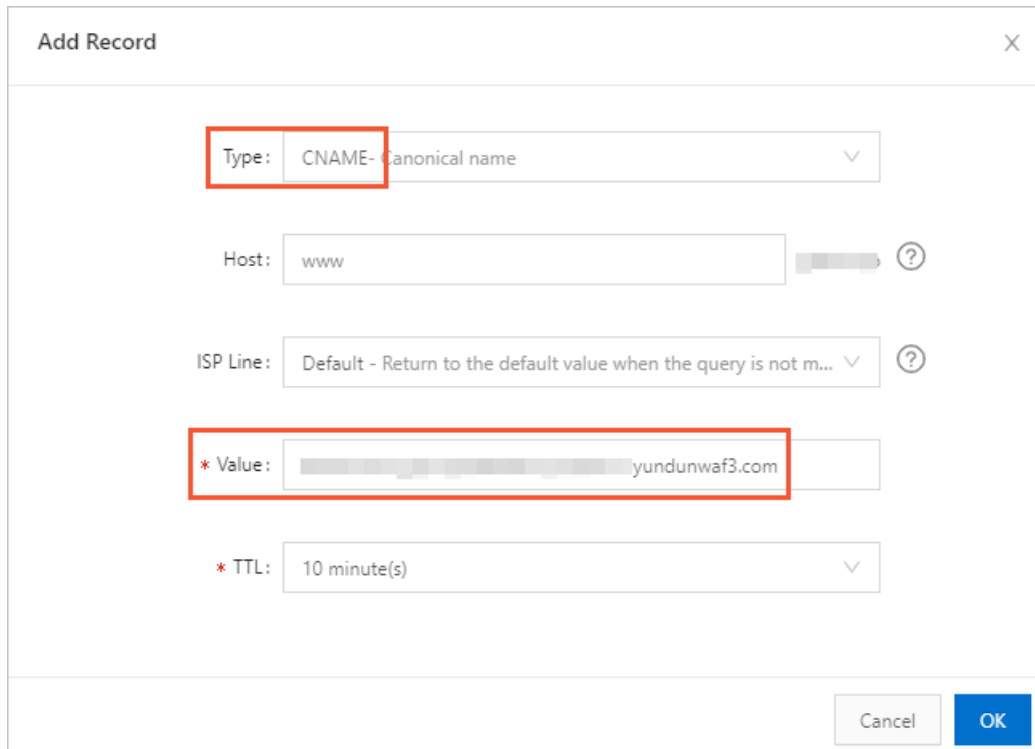
The following example demonstrates how to change the DNS record in Alibaba Cloud DNS. If your domain name is hosted on Alibaba Cloud DNS, perform the following steps to change the DNS record. If your domain name is not hosted on Alibaba Cloud DNS, refer to the following steps to change the DNS record at your DNS service provider.

1. Log on to the [Alibaba Cloud DNS console](#).
2. On the **Manage DNS** page, find the domain name and click **Configure** in the Actions column.
3. On the **DNS Settings** page, find the record in the **Host** column and click **Edit** in the Actions column.

In the following example, `aliyun.com` is used:


- o **www**: matches domain names that begin with `www`, such as `www.aliyun.com`.
 - o **@**: matches the root domain name, for example, `aliyun.com`.
 - o *****: matches all wildcard domain names, such as `blog.aliyun.com`, `www.aliyun.com`, and `aliyun.com`. The wildcard domain names include root domain names and subdomain names.
4. In the **Add Record** dialog box, select the CNAME record or the A record to change the DNS record.
 - o **CNAME record**: Set **Type** to **CNAME** and **Value** to the WAF CNAME and keep other settings unchanged.

 **Note** We recommend that you set the TTL to 10 minutes. The greater the TTL is, the longer it takes to synchronize and change the DNS record.




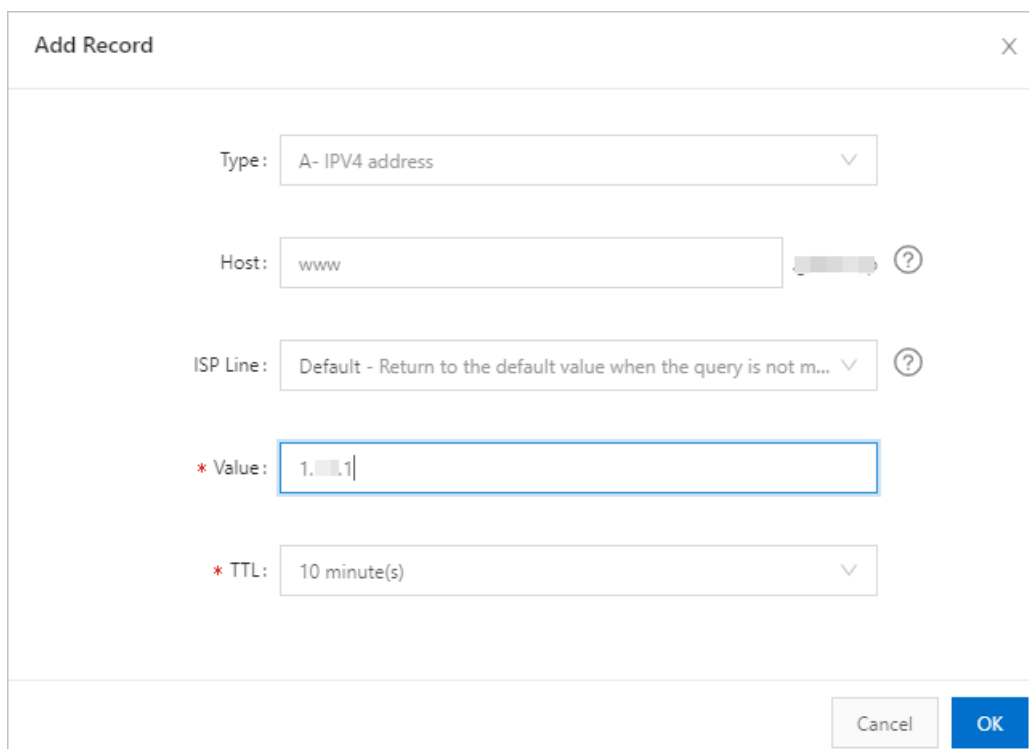
Note the following descriptions about conflicts:

- You can specify only one CNAME value for each record name. Set Value to the CNAME assigned by WAF.
- Different types of DNS records conflict with each other. For example, you cannot add a CNAME record and an A, MX, or TXT record with the same record name. If you cannot change the record type, delete all conflicting records and add a new CNAME record.


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

- If you must retain the MX record, we recommend that you use the A record method to resolve the domain name to the WAF IP address.
- **A record:** Set Type to A and Value to the WAF IP address and keep other settings unchanged.

 **Note** We recommend that you set the TTL to 10 minutes. The greater the TTL is, the longer it takes to synchronize and change the DNS record.



5. Click **OK** and wait for the new DNS record to take effect
6. Verify the DNS record. You can ping the domain name of your website or use a DNS detection tool to verify whether the DNS record takes effect.

 **Note** The DNS record does not take effect immediately. If the verification fails, verify the DNS record again after 10 minutes.

References

- Protect the origin server.

If the IP address of your origin server is exposed, attackers may bypass WAF and directly attack your origin server. To avoid such attacks, we recommend that you configure an ECS security group or SLB whitelist. For more information, see [Configure protection for an origin server](#).

- Retrieve actual IP addresses of clients.

After you add your website to WAF, WAF processes all requests destined for your website and forwards normal requests to the origin server. In this case, you must use the `X-Forwarded-For` header to retrieve the actual IP addresses of clients. For more information, see [Retrieve actual IP addresses of clients](#).

2.5. Specify ports

When you add a website to your Web Application Firewall (WAF) instance in CNAME record mode, you must specify the HTTP or HTTPS ports that the website uses. After you specify the ports and add the website, traffic destined for the website is redirected to WAF for detection and protection.

Context

WAF forwards the traffic only over the specified ports to the origin server. WAF does not forward the

traffic over a port that is not specified.

Scenarios


You must specify HTTP or HTTPS ports in the following scenarios:

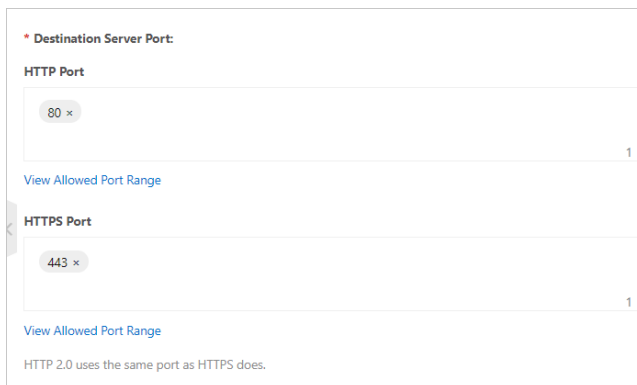
- A website is added to WAF in CNAME record mode.
- The HTTP or HTTPS ports that the website uses change.

Procedure

- 1.
- 2.
- 3.
4. In the **domain name list**, find the domain name for which you want to specify ports. Then, click **Edit** in the Actions column.
5. On the **Edit** page, find the **Destination Server Port** section and enter the required port numbers in the **HTTP Port** and **HTTPS Port** fields.

Press Enter each time you enter a port number.

 **Notice** The port numbers that you enter must be within the allowed port range. Otherwise, the settings cannot be saved. You can click **View Allowed Port Range** to check whether a port number is within the allowed port range.



* Destination Server Port:

HTTP Port

80 ×

1

[View Allowed Port Range](#)

HTTPS Port

443 ×

1

[View Allowed Port Range](#)

HTTP 2.0 uses the same port as HTTPS does.

6. Click **Confirm**.

References

If my website receives requests over an unconfigured port, is the origin server threatened?

Does WAF support custom ports?

What do I do if services on non-standard ports cannot be added to WAF of the Pro edition?


2.6. Configure custom TLS settings

If you add a website to Web Application Firewall (WAF) and the website uses HTTPS to transmit data, you can customize TLS version settings and cipher suites for the domain name of the website. This way, you can increase the security performance of the website in scenarios in which compliance with classified protection is required. You can also improve the TLS compatibility of the website in scenarios in which compatibility with earlier TLS versions of clients is required.

Background information

After an HTTPS website is added to WAF, WAF automatically specifies TLS settings for the website to ensure secure communication. If requests use TLS versions and cipher suites that are not within the specified ranges, WAF blocks the requests.

WAF allows you to customize TLS cipher suites. This helps prevent access failures caused by the mismatch between the cipher suites used by the website and the cipher suites automatically specified by WAF. You can modify TLS version settings and cipher suites for the website based on your business requirements.


 **Notice** If your website uses HTTP to transmit data, you do not need to configure TLS settings.

Prerequisites

- The website is added to WAF.
- The website uses HTTPS to transmit data, and the required HTTPS certificate is uploaded.

Configure TLS settings

- 1.
- 2.
3. On the page, find the domain name for which you want to configure TLS settings and click in the **Actions** column.

 **Note** You can configure TLS settings only for the domain names that use HTTPS to transmit data. If a domain name uses HTTP or a domain name uses HTTPS but has no HTTPS certificate uploaded, the button does not appear.

4. On the page, configure the TLS version settings and cipher suites.

Parameter	Description
	The domain name for which you want to configure TLS settings. This value is automatically filled. You do not need to enter the domain name.
	Select the TLS version used by the website. Valid values: <ul style="list-style-type: none">◦ : WAF supports TLS 1.0 and later for your website.◦ : WAF supports TLS 1.1 and later for your website. If an access request of the website uses TLS 1.0, the request fails.◦ : WAF supports TLS 1.2 and later for your website. If an access request of the website uses TLS 1.0 or 1.1, the request fails.
Enable support for TLS 1.3	Select Enable support for TLS 1.3.

Parameter	Description
	<p>Select the cipher suite template that you want to use. Valid values:</p> <ul style="list-style-type: none">◦ : The following cipher suites are supported:<ul style="list-style-type: none">▪ Strong cipher suites:<ul style="list-style-type: none">▪ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256▪ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384▪ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256▪ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384▪ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256▪ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384▪ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA▪ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA▪ Weak cipher suites:<ul style="list-style-type: none">▪ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA▪ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA▪ TLS_RSA_WITH_AES_128_GCM_SHA256▪ TLS_RSA_WITH_AES_256_GCM_SHA384▪ TLS_RSA_WITH_AES_128_CBC_SHA256▪ TLS_RSA_WITH_AES_256_CBC_SHA256▪ TLS_RSA_WITH_AES_128_CBC_SHA▪ TLS_RSA_WITH_AES_256_CBC_SHA▪ SSL_RSA_WITH_3DES_EDE_CBC_SHA◦

5. Click **Save**.

If requests use the TLS versions and cipher suites that are not within the specified ranges, WAF blocks the requests.

2.7. Configure protection for an origin server

After you add your website to Web Application Firewall (WAF) in CNAME record mode, you can configure access control policies for your origin server to allow inbound traffic only from back-to-origin CIDR blocks of WAF. This way, your website is protected from direct-to-origin attacks. This topic describes how to configure security group rules or whitelist policies for an origin server that is deployed on an Elastic Compute Service (ECS) instance or a Classic Load Balancer (CLB) instance. CLB is formerly known as Server Load Balancer (SLB).

Prerequisites

- The origin server is deployed on an ECS instance or a CLB instance. For more information about ECS and CLB instances, see [ECS instances](#) and [CLB instances](#).
- All domain names that are hosted on the ECS instance or CLB instance are added to WAF in **CNAME record** mode.

For more information, see [Add a domain name](#).

Precautions

After you add your website to WAF for protection, traffic is forwarded regardless of whether protection is configured for your origin server. If the IP address of your origin server is exposed, attackers can bypass WAF and launch direct-to-origin attacks. In this scenario, you must configure protection for your origin server. For more information about how to check whether the IP address of your origin server is exposed, see [How do I check whether the IP address of my origin server is exposed?](#).

If you configure access control policies on the origin server, security risks may occur. Before you configure protection for the origin server, take note of the following points:

- Make sure that all domain names that are hosted on the origin server are added to WAF. This way, attackers cannot use these domain names that are not added to WAF to attack the origin server. If a domain name that is not added to WAF is used to attack the origin server, services of the other domain names that are hosted on the origin server are not affected.
- If a WAF cluster fails, requests that are destined for your website are directed to the origin server in bypass mode. This ensures service continuity. In this case, if you have configured ECS security group rules or CLB whitelist policies for the origin server, the origin server cannot be accessed over the Internet.
- If back-to-origin CIDR blocks are added during a WAF cluster scale-out and you have configured ECS security group rules and CLB whitelist policies for the origin server, HTTP 5XX status codes may be frequently returned. We recommend that you take note of the notifications of changes in back-to-origin CIDR blocks in the and update the access control policies that involve back-to-origin CIDR blocks at the earliest opportunity.
- If you no longer need to use WAF, you must delete the access control policies that you added before you switch traffic back to the origin server. This way, traffic is sent to the origin server and service interruptions are prevented.

Obtain the WAF back-to-origin CIDR blocks

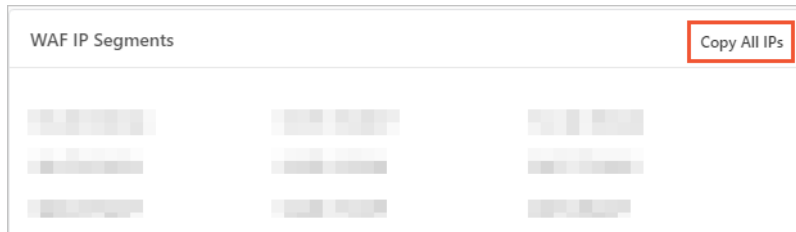


Notice The WAF back-to-origin CIDR blocks are updated on a regular basis. To avoid service interruptions, take note of update notifications and add the updated back-to-origin CIDR blocks to the security group rules and whitelist policies that are configured for your origin server at the earliest opportunity.

1.

- 2.
- 3.
4. In the lower part of the **Product Information** page, find the **WAF IP Segments** section and click **Copy All IPs**.

The **WAF IP Segments** section displays the latest back-to-origin CIDR blocks.



Configure ECS security group rules

If your origin server is deployed on an ECS instance, you must configure security group rules for the ECS instance after you obtain the WAF back-to-origin CIDR blocks. The security group rules allow inbound traffic only from the WAF back-to-origin CIDR blocks.

1. Log on to the [ECS console](#).
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select the resource group and the region to which the ECS instance belongs.
4. On the **Instances** page, find the ECS instance for which you want to configure security group rules and choose **More > Network and Security Group > Configure Security Group** in the **Actions** column.
5. Find the security group that you want to configure and click **Add Rules** in the **Actions** column.
6. Add a security group rule that has the highest priority to allow inbound traffic only from the WAF back-to-origin CIDR blocks.
 - i. On the **Inbound** tab of the **Access Rule** section, click **Add Rule**.

ii. Configure the following parameters and click **Save**.

Action

Priority

Protocol Type

Port Range

Authorization Object

Description

Actions

Allow

1

Custom TCP

Destination

Source


Allow WAF IP

Save


Preview

Delete

Parameter	Description
Action	Select Allow .
Priority	Enter 1 , which specifies the highest priority.
Protocol Type	Select Custom TCP .
Port Range	Select HTTP (80) and HTTPS (443) .
Authorization Object	Copy and paste the back-to-origin CIDR blocks of WAF to the Source field. You can press Ctrl+V to paste the back-to-origin CIDR blocks.
Description	The description of the security group rule. Example: Allow inbound traffic from the WAF back-to-origin CIDR blocks.

 **Notice** If your origin server uses IP addresses and ports other than the specified WAF back-to-origin CIDR blocks and HTTP or HTTPS ports to communicate with applications, you must add these IP addresses and ports to the security group rule.

After the security group rule is added, it takes the highest priority in the security group. This way, the ECS instance allows all inbound traffic from the WAF back-to-origin CIDR blocks.

 **Warning** Make sure that all WAF back-to-origin CIDR blocks are added to the security group rule. Otherwise, access exceptions may occur.

7. Add a security group rule that has the lowest priority to block all inbound traffic.

i. On the **Inbound** tab of the **Access Rule** section, click **Add Rule**.

ii. Configure the following parameters and click **Save**.

Action	Priority	Protocol Type	Port Range	Authorization Object	Description	Actions
Forbid	100	Custom TCP	Destination: HTTP (80) × HTTPS (443) ×	Source: 0.0.0.0/0 ×	Deny all	Save Preview Delete

Parameter	Description
Action	Select Forbid .
Priority	Enter 100 , which specifies the lowest priority.
Protocol Type	Select Custom TCP .
Port Range	Select HTTP (80) and HTTPS (443) .
Authorization Object	Enter 0.0.0.0/0 in the Source field. 0.0.0.0/0 specifies all CIDR blocks.
Description	The description of the security group rule. Example: Block all inbound traffic.

After the security group rules are added, the ECS instance blocks inbound traffic from all CIDR blocks except the CIDR blocks that are specified in Step 6. This way, all service traffic passes through WAF before the traffic reaches the ECS instance.

Configure CLB access control policies


If your origin server is deployed on a CLB instance, you must obtain the WAF back-to-origin CIDR blocks and configure an access control policy (whitelist) for the CLB instance. The whitelist policy allows inbound traffic only from the WAF back-to-origin CIDR blocks.

The following example describes how to configure a whitelist policy. In this example, a CLB instance is used. If you use an Application Load Balancer (ALB) instance, configure a whitelist policy based on the following steps and the description in [Enable access control for ALB instances](#).


1. Log on to the [SLB console](#).
2. In the left-side navigation pane, choose **CLB (FKA SLB) > Access Control**.
3. In the top navigation bar, select the resource group and the region to which the CLB instance belongs.
4. Create an access control list (ACL).
 - i. On the **Access Control** page, click **Create Access Control List**.

- ii. In the **Create Access Control List** panel, configure the following parameters and click **Create**.

The following configurations are used to create an ACL for WAF back-to-origin CIDR blocks.

Parameter	Description
Name	Enter the name of the ACL. Example: WAF back-to-origin CIDR blocks.
Add Multiple Addresses and Descriptions	<p>Copy and paste all the back-to-origin CIDR blocks of WAF.</p> <p>Enter one CIDR block in each line. Press Enter to start a new line.</p> <div> Note All the back-to-origin CIDR blocks that are copied are separated by commas (,). Before you paste the CIDR blocks, we recommend that you use a text editor that supports extension replacement to replace the commas (,) with line breaks (\n).</div>

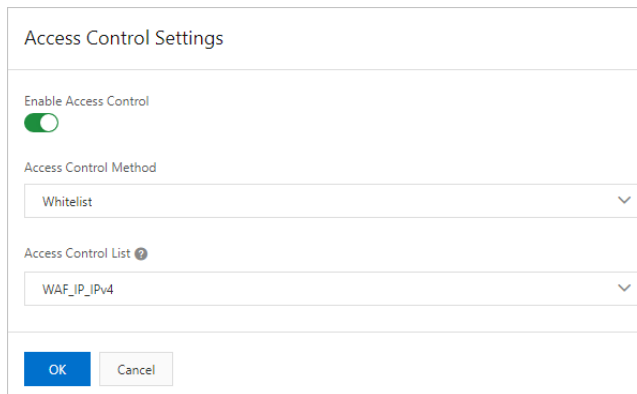
5. Configure the ACL for a listener.

- i. In the left-side navigation pane, choose **CLB (FKA SLB) > Instances**.
- ii. On the **Instances** page, find the instance that you want to manage and click the ID of the instance.
- iii. On the **Listeners** tab, find the listener that you want to configure, click the  icon in the **Actions** column, and then click **Set Access Control**.

Select the listener based on the type of service that is protected by WAF:

- If HTTP services are added to WAF, configure an HTTP listener.
- If HTTPS services are added to WAF, configure an HTTPS listener.
- If HTTP and HTTPS services are added to WAF, configure an HTTP listener and an HTTPS listener.

- iv. In the **Access Control Settings** panel, turn on **Enable Access Control** and configure the following parameters.



Parameter	Description
Access Control Mode	Select Whitelist to allow specified IP addresses to access the CLB instance.
Select ACL	Select the ACL that you created for the back-to-origin CIDR blocks of WAF.

After the preceding configurations are complete, the CLB instance allows inbound traffic from the back-to-origin CIDR blocks of WAF.

What to do next

After you configure an ECS security group rules and CLB whitelist policies, we recommend that you check whether the origin server can be connected over ports 80 and 8080. This way, you can check whether the protection configurations are in effect.

If the origin server cannot be connected over port 80 or 8080, but the service runs as expected, the protection configurations are in effect.

How do I check whether the IP address of my origin server is exposed?

Use Telnet to establish a connection from a host that is not deployed on Alibaba Cloud to your origin server by using the service port and the public IP address.

- If the connection is successful, the IP address of your origin server is exposed. In this case, attackers that obtain the public IP address can bypass WAF and launch attacks on your origin server.
- If the connection fails, the IP address of your origin server is not exposed.

Example: Check whether an origin server that is protected by WAF can be connected over ports 80 and 8080. If the origin server can be connected over ports 80 and 8080, the IP address of your origin server is exposed.

```
Last login: Tue Jul 31 13:48:10 on ttys000
$ telnet 4.0.0.0 80
Trying 4.0.0.0...
Connected to 4.0.0.0.
Escape character is '^['.
^ZConnection closed by foreign host.
```


2.8. Retrieve actual IP addresses of clients

If you deploy proxy servers, such as CDN, Anti-DDoS Premium, Anti-DDoS Pro, or WAF, on your website, the origin server can use the X-Forwarded-For header in back-to-origin requests to retrieve actual IP addresses of clients. This topic describes how to configure web application servers, such as NGINX, IIS 6, IIS 7, Apache, and Tomcat servers, and Kubernetes containers to retrieve the IP addresses of clients.


Background information

In most scenarios, access requests initiated from the browsers of clients (visitors) are not directly sent to the origin server of a website. Instead, the access requests may pass through intermediate proxy servers, such as CDN, Anti-DDoS Premium, Anti-DDoS Pro, or WAF. During the process, these access requests are forwarded through multiple proxies for security and acceleration. This increases the difficulty in retrieving the actual IP addresses of the clients that initiated the requests.

To address the issue, the X-Forwarded-For header is implemented to record the actual IP addresses of the clients. The transparent proxy adds the X-Forwarded-For header to the HTTP request header before forwarding the access requests to the next-hop server. The header is in the `X-Forwarded-For:Client IP address` format. If the access requests pass through multiple intermediate proxy servers, the X-Forwarded-For header records the actual IP addresses of the clients and IP addresses of intermediate proxy servers. The header records multiple IP addresses separated by a comma (,), such as `X-Forwarded-For:Client IP address, IP address of Proxy Server 1, IP address of Proxy Server 2, IP address of Proxy Server 3, ...`.

Therefore, common web application servers can use the X-Forwarded-For header to retrieve the actual IP addresses of the clients.

The following content demonstrates how to configure the X-Forwarded-For header on the NGINX, IIS 6, IIS 7, Apache, and Tomcat servers, as well as on the Kubernetes containers.


 **Notice** Before you start, make sure that you have backed up the existing environment, including ECS instance snapshots and configuration files of the web application servers.

Configure NGINX servers

The NGINX servers use an `http_realip_module` module to retrieve the actual IP addresses of the clients.

1. Install the `http_realip_module` module.

Run the `# nginx -V | grep http_realip_module` command on the NGINX server to check whether the module is installed. If the module is not installed, recompile NGINX and load the module.

 **Note** This module is not installed when NGINX is installed by using a quick installation package.

Install the `http_realip_module` module by using the following method:

```
wget http://nginx.org/download/nginx-1.12.2.tar.gz
tar zxvf nginx-1.12.2.tar.gz
cd nginx-1.12.2
./configure --user=www --group=www --prefix=/alidata/server/nginx --with-http_stub_status_module --without-http-cache --with-http_ssl_module --with-http_realip_module
make
make install
kill -USR2 `cat /alidata/server/nginx/logs/nginx.pid`
kill -QUIT `cat /alidata/server/nginx/logs/nginx.pid.oldbin`
```

2. Modify the configuration file of NGINX.

- i. Open the `default.conf` configuration file.
- ii. Add the following content to `location / {}` :

```
set_real_ip_from <ip_range1>;
set_real_ip_from <ip_range2>;
...
set_real_ip_from <ip_rangex>;
real_ip_header X-Forwarded-For;
```

where, `<ip_range1>` , `<ip_range2>` , and `<ip_rangex>` are the back-to-origin IP addresses of WAF. For more information about the back-to-origin CIDR blocks of WAF, see [Allow access from back-to-origin CIDR blocks of WAF](#).

Enter one back-to-origin IP address in each line. If the back-to-origin IP addresses of the proxy servers include 10.0.0.1, 10.0.0.2, and 10.0.0.3, use the format similar to:

```
set_real_ip_from 10.0.0.1;
set_real_ip_from 10.0.0.2;
set_real_ip_from 10.0.0.3;
real_ip_header X-Forwarded-For;
```

3. Modify the log format.

- i. Open the `nginx.conf` configuration file. `log_format` is typically located in the HTTP configuration.
- ii. In `log_format` , replace the `remote-address` field with the `x-forwarded-for` field.

The modified `log_format` is as follows:

```
log_format main '$http_x_forwarded_for - $remote_user [$time_local] "$request" '
'$status $body_bytes_sent "$http_referer" ' '"$http_user_agent" ';
```


4. Run the `nginx -s reload` command to restart NGINX.

The configurations take effect after the restart. The NGINX server records the actual IP addresses of the clients by using the X-Forwarded-For header.

Configure IIS 6 servers

You must install the `F5XForwardedFor.dll` plug-in to retrieve the actual IP addresses of the clients from the access log recorded by an IIS 6 server.

1. Depending on your server OS version, copy the `F5XForwardedFor.dll` file from the `x86\Release` or `x64\Release` directory to a custom directory, such as `C:\ISAPIFilters` .

 **Note** Make sure that the IIS process has read and write permissions on the custom directory.


If the plug-in is unavailable from the directory, click [F5XForwardedFor.dll](#) to download it.

2. Open Internet Information Services (IIS) Manager, find the website, right-click the website, and select **Properties**.
3. In the **Default Web Site Properties** dialog box that appears, click the **ISAPI Filters** tab and click **Add**.
4. In the **Add ISAPI Filter** dialog box, set the following parameters and click **OK**.
 - **Filter name:** Enter `F5XForwardedFor`.
 - **Executable:** Enter the complete path of `F5XForwardedFor.dll`, for example, `C:\ISAPIFilters\F5XForwardedFor.dll`.
5. Restart the IIS server for the configurations to take effect.

Configure IIS 7 servers

You can install the F5XForwardedFor module to retrieve the actual IP addresses of the clients from the access log recorded by an IIS 7 server.

1. Depending on your server OS version, copy the `F5XFFHttpModule.dll` and `F5XFFHttpModule.ini` files from the `x86\Release` or `x64\Release` directory to a custom directory, such as `C:\x_forwarded_for\x86` or `C:\x_forwarded_for\x64`.

 **Note** Make sure that the IIS process has read and write permissions on the custom directory.

If the files are unavailable from the directory, click [F5XForwardedFor](#) to download it.


2. In the **IIS Server** section, double-click **Module**.
3. Click **Configure Local Module**.
4. In the **Configure Local Module** dialog box, click **Register** to register the DLL file.
 - Register the `x_forwarded_for_x86` module in a 32-bit system.
 - **Name:** Enter `x_forwarded_for_x86`.
 - **Path:** Enter the full path of the `F5XFFHttpModule.dll` module, for example `C:\x_forwarded_for\x86\F5XFFHttpModule.dll`.
 - Register the `x_forwarded_for_x64` module in a 64-bit system.
 - **Name:** Enter `x_forwarded_for_x64`.
 - **Path:** Enter the full patch of the `F5XFFHttpModule.dll` module, for example `C:\x_forwarded_for\x64\F5XFFHttpModule.dll`.
5. In the **Configure Local Module** dialog box, select the newly registered `x_forwarded_for_x86` or `x_forwarded_for_x64` module and click **OK**.
6. In the **ISAPI and CGI Restrictions** section, add the registered DLL file and set **Restriction to** **Allow**.
7. Restart the IIS server and wait for the configurations to take effect.

Configure Apache servers

Configure Apache servers in Windows.

The installation packages of Apache 2.4 and later provide the `remoteip_module` module file (`mod_remoteip.so`). You can use this module to retrieve the actual IP addresses of clients.

1. Create a configuration file named `httpd-remoteip.conf` in the extra configuration folder of Apache (`conf/extra/`).

 **Note** You can load the related configurations by importing the `remoteip.conf` configuration file. This reduces the number of times that you modify the `httpd.conf` file and avoids service exceptions due to misoperations.

2. Add the following content to the `httpd-remoteip.conf` configuration file:

```
# Load the mod_remoteip.so module.
LoadModule remoteip_module modules/mod_remoteip.so
# Set the RemoteIPHeader header.
RemoteIPHeader X-Forwarded-For
# Set the back-to-origin IP addresses.
RemoteIPInternalProxy <ip_range1> <ip_range2> ..... <ip_rangeX>
```

where, `<ip_range1>` , `<ip_range2>` , and `<ip_rangeX>` are the back-to-origin IP addresses of WAF. For more information about the back-to-origin CIDR blocks of WAF, see [Allow access from back-to-origin CIDR blocks of WAF](#).

Separate multiple back-to-origin IP addresses with spaces. If the IP addresses of the proxy servers include 10.0.0.1, 10.0.0.2, and 10.0.0.3, use the format similar to:

```
RemoteIPInternalProxy 10.0.0.1 10.0.0.2 10.0.0.3
```

3. Add the following content to the `conf/httpd.conf` configuration file:

```
Include conf/extra/httpd-remoteip.conf
```

The preceding content inserts the `httpd-remoteip.conf` configuration file into `conf/httpd.conf`.

4. Modify the log format in the `httpd.conf` configuration file.

```
LogFormat "%a %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%a %l %u %t \"%r\" %>s %b" common
```

5. Restart Apache for the configurations to take effect.

Configure Apache servers in Linux.

Follow the preceding steps to add the `remoteip_module` module (`mod_remoteip.so`) and configure the log format to retrieve the actual IP addresses of clients. This module is included in Apache 2.4 and later.

If the version of Apache is earlier than 2.4, install `mod_rpaf` (third-party module) to retrieve the actual IP addresses of clients.

1. Install the `mod_rpaf` module.

```
wget https://github.com/gnif/mod_rpaf/archive/v0.6.0.tar.gz
tar zxvf mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/alidata/server/httpd/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

2. Append the following content to the `/alidata/server/httpd/conf/httpd.conf` configuration file of Apache:

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips <rpaf IP address>
RPAFheader X-Forwarded-For
```

where, `<rpaf IP address>` is the IP address of the `mod_rpaf` module. You can query the specific IP addresses in the Apache log. Do not use the IP addresses of the proxy servers. Typically, two IP addresses are included, as shown in the following example:

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips 10. ***. ***.65 10. ***. ***.131
RPAFheader X-Forwarded-For
```

3. Restart Apache for the configurations to take effect.

```
/alidata/server/httpd/bin/apachectl restart
```

For more information about the Apache modules, see [Apache help document](#).

Configure Tomcat servers

Take the following steps to allow the Tomcat servers to retrieve the actual IP addresses of clients by using the X-Forwarded-For header.

1. Open the `tomcat/conf/server.xml` configuration file.
2. Modify the `AccessLogValve` logging function as follows:

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%{X-FORWARDED-FOR}i %l %u %t %r %s %b %D %q %{User-Agent}i %T" resolveHosts="false"/>
```

Configure Kubernetes containers

If your ECS instance is deployed on Kubernetes, Kubernetes records the actual IP addresses of clients in the X-Original-Forwarded-For field and the back-to-origin IP addresses of WAF in the X-Forwarded-For field. To obtain the actual IP addresses of clients, you must modify the container configuration file to enable an Ingress controller to add them to the X-Forwarded-For field.

You can modify the container configuration file by performing the following steps:

1. Run the following command to modify the `kube-system/nginx-configuration` configuration file:

```
kubectl -n kube-system edit cm nginx-configuration
```

2. Add the following content to the configuration file:

```
compute-full-forwarded-for: "true"
forwarded-for-header: "X-Forwarded-For"
use-forwarded-headers: "true"
```

3. Save the configuration file.

The configurations take effect immediately after you save the configuration file. Then, the Ingress controller adds the actual IP addresses of clients to the X-Forwarded-For field.

4. Change the field you use to obtain the actual IP addresses of clients to the X-Original-Forwarded-For field.

3.Connect cloud services to WAF

3.1. Use WAF with CDN

Web Application Firewall (WAF) can be used in combination with a content delivery network (CDN), such as Alibaba Cloud CDN, to protect domain names against web attacks. The domain names have content acceleration enabled.

Context

You can deploy WAF and CDN in the following sequence: CDN, WAF, and origin servers. CDN is deployed at the ingress layer to accelerate the distribution of content. WAF is deployed at the intermediate layer to protect applications.

Use Alibaba Cloud CDN

1. Add the domain name that you want to accelerate to Alibaba Cloud CDN. For more information, see [CDN quick start](#).
2. Add the domain name to WAF.
 - **Domain Name:** Enter the domain name that you want to protect.
 - **Destination Server (IP Address):** Enter the public IP address of the SLB instance, the public IP address of the ECS instance, or the IP address of the server that is not deployed on Alibaba Cloud.
 - **Does a layer 7 proxy (DDoS Protection/CDN, etc.) exist in front of WAF:** Select Yes.

For more information, see [Add websites](#).

* Domain name:

It supports top-level domain names (e.g. test.com) and second-level domain names (e.g. www.test.com). They have no impact on each other. Please fill in your actual domain name.

* Protocol type: ☒ HTTP ☐ HTTPS

* Server address: ☒ IP ☐ Other addresses

Please separate up to 20 IPs with commas (","), Line breaks are not allowed.

* Server port: HTTP 80 [Custom](#)

Any layer 7 proxy (e.g. Anti-DDoS/CDN) enabled?: ☒ yes ☐ no [?](#)

Load balancing algorithm: ☒ IP HASH ☐ Round-robin

Flow Mark:

Note: If the user-defined header field already has a value, the value is overwritten with the WAF flow mark value. If the header field is already used, the field is overwritten with the flow mark filed setting

3. After the domain name is added to WAF, WAF generates a dedicated canonical name (CNAME) for the domain name.

[?](#) **Note** For more information about how to view the CNAME that is generated by WAF, see [Change a DNS record](#).

4. Change the DNS record of the origin server in the Alibaba Cloud CDN console to point to the CNAME.
- Log on to the [Alibaba Cloud CDN console](#).
 - Open the **Domain Names** page. On the page that appears, select the required domain name and click **Manage**.
 - In the **Origin Information** section, click **Modify**.

- iv. Modify the information of the origin server.
- **Origin Info**: Select **Site Domain**.
 - **Domain Name**: Enter the CNAME that is generated by WAF.
 - **Port**: Select **80**.

Modify Origin Information

Origin Info Type

OSS Domain IP Origin Domain

FC Domain

Domain Name

Priority Priorities for multiple origins

Enter a domain name Primary

Add

Port

Port 80 Port 443 Custom Port

Note: If a custom port is specified, then only HTTP is supported for forwarding network traffic back to origin. Before you specify a custom port, set the origin protocol to HTTP. [Configure origin protocol policy](#)

OK Cancel

- v. Go to the **Back-to-origin** page. On the **Configurations** tab, verify that **Origin Host** is disabled.

← Return to Domain

com Enabled

Basics

Back-to-origin Configurations Custom HTTP Origin Header

Origin Host

Origin Host Disabled

Customize the web server domain name that a CDN node needs to access during the back-to-origin process. [What is an origin host?](#)

Modify

After the configuration is complete, traffic passes through Alibaba Cloud CDN. The dynamic content remains detected and protected by WAF.

3.2. Add a website to both Anti-DDoS Pro or Anti-DDoS Premium and WAF


Anti-DDoS Pro or Anti-DDoS Premium and Web Application Firewall (WAF) can be used together to protect websites against both DDoS attacks and web application attacks. This topic describes how to add a website to both Anti-DDoS Pro or Anti-DDoS Premium and WAF.

Prerequisites

- An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see [Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance](#).
- A WAF instance is purchased. For more information, see [Purchase a WAF instance](#).

Context

To configure Anti-DDoS Pro or Anti-DDoS Premium and WAF for your website, you can deploy the following network architecture: Use Anti-DDoS Pro or Anti-DDoS Premium at the ingress to defend against DDoS attacks. Use WAF at the intermediate layer to defend against web application attacks. Configure an ECS instance, SLB instance, or on-premises server as the origin server.

 **Note** After you apply the preceding architecture, access requests are sent to multiple intermediate proxy servers before reaching the origin server. The origin server cannot directly obtain the actual source IP addresses of the requests. For more information about how to obtain the actual source IP addresses, see [Obtain the actual source IP addresses of requests](#).

Procedure

1. Add the domain name of your website to WAF. For more information, see [Add a domain name](#).

In the **Enter your website information** step, set **Destination Server (IP Address)** to **IP** and enter the public IP address of the origin server. The origin server can be an SLB instance, ECS instance, or on-premises server. Set **Does a layer 7 proxy (DDoS Protection/CDN, etc.) exist in front of WAF** to **Yes**.

Asset Center / Website Access / Add Domain Name

← Add Domain Name

1

2

Enter your website information

Change DNS Settings

*** Domain Name:**

Enter the domain name of your website. For example: www.aliyun.com

You can enter top-level domains (such as test.com) and second-level domains (such as www.test.com). The domains will not conflict with each other.

*** Protocol Type:**

☐ HTTP ☐ HTTPS

*** Destination Server (IP Address):**

☒ IP ☐ Destination Server (Domain Name)

Enter the public IP address of the destination server for protection, such as 1.1.1.1. The server can be in the Alibaba Cloud, any other cloud service providers, IDC rooms, etc.

Enter the IP addresses on a single line, up to , and separated by commas (,).

*** Destination Server Port:**

-- [Customize](#)

Load Balancing Algorithm:

☒ IP hash ☐ Round Robin ☐ Least time

This function is not yet supported by the current version. Please [Upgrade](#)

Does a layer 7 proxy (DDoS Protection/CDN, etc.) exist in front of WAF:

☒ Yes ☐ No

After you add the domain name to WAF, go to the **Website Access** page in the **WAF console** to obtain the **CNAME** address of WAF.

Domain Name	DNS Status	Protocol Status	Log Service
<div>Domain Name: <input type="text"/></div> <div>CName: <input type="text" value="yundunwaf5.com"/></div>			

2. Add your website service to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see [Add a website](#).

In the **Enter Site Information** step, set **Server IP** to **Origin Server Domain** and enter the **CNAME** address of WAF obtained in the previous step.

Anti-DDoS / Website Config / Add Domain

← Add Domain

1 Enter Site Information 2 Complete

* Function Plan Standard Enhanced

* Instance ☐ You can associate a domain with a maximum of eight Anti-DDoS instances. You have selected 0 instances.

* Domain Supports top-level domains, such as test.com, and secondary level domains, such as www.test.com.

* Protocol ☒ HTTP ☒ HTTPS ☐ Websocket ☐ Websockets

Enable HTTP/2 ☐ This feature is only available to domains that are associated with enhanced instances.

* Server IP ☐ Origin Server IP ☒ Origin Server Domain yundunwaf5.com

If the IP addresses of your origin server have been exposed, click here [to learn how to fix the issue.](#)

Server Port HTTP 80 HTTPS 443 Custom

Add Cancel

After you add the domain name to Anti-DDoS Pro or Anti-DDoS Premium, go to the **Website Config** page in the **Anti-DDoS Pro or Anti-DDoS Premium console** to obtain the **CNAME** address of Anti-DDoS Pro or Anti-DDoS Premium.

<input type="checkbox"/> Domain	Origin Server IP
<input type="checkbox"/> Domain: CNAME: 33emq2a8f2... Protection Package: Standard	yundunwaf5.com




- On the website of your DNS service provider, modify DNS records to point the domain name to the **CNAME** address of Anti-DDoS Pro or Anti-DDoS Premium. For more information, see [Change DNS records to protect website services](#).

After the preceding configuration is complete, traffic to access your website is first scrubbed by Anti-DDoS Pro or Anti-DDoS Premium and then forwarded to WAF to filter out web application attacks. Only normal traffic is forwarded to the origin server.

4. View the allowed port range

Web Application Firewall (WAF) protects services that use standard ports and specific non-standard ports. The standard ports include ports 80, 8080, 443, and 8443. You can customize server ports when you configure WAF. Then, WAF receives and redirects traffic at the server ports that you specify.

Limits on WAF-supported non-standard ports

Item	Description
WAF instances that support non-standard ports, in addition to ports 80, 8080, 443, and 8443	<p>The WAF instances are of the Business, Enterprise, or Exclusive edition.</p> <p>For more information, see Prerequisites.</p>
Allowed port range	<p>The following lists provide the ports that are supported by WAF. You can also query the allowed port range in the WAF console. For more information, see Procedure.</p> <div><p> Note A WAF instance of the Exclusive edition supports more non-standard ports, in addition to the following ports, and allows you to use HTTP ports, HTTPS ports, and HTTP/2 ports as back-to-origin ports. For more information, see Create an exclusive cluster.</p></div> <ul style="list-style-type: none">HTTP-compliant ports: 80, 81, 82, 83, 84, 86, 87, 88, 89, 97, 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, 7071, 7081, 7082, 7083, 7088, 7097, 7510, 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, 8686, 8800, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9021, 9023, 9027, 9037, 9080, 9081, 9082, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9999, 10000, 10001, 10080, 12601, 28080, 33702, and 48800 <div><p> Notice Only WAF instances that are deployed in mainland China support port 48800.</p></div> <ul style="list-style-type: none">HTTPS-compliant ports: 443, 4443, 5443, 6443, 7443, 8443, 8553, 8663, 9443, 9553, 9663, and 18980 <div><p> Notice Only WAF instances that are deployed in mainland China support port 18980.</p></div>

Item	Description
Number of ports that each WAF instance supports, including ports 80, 8080, 443, and 8443	<ul style="list-style-type: none">WAF instance of the Business edition: 30WAF instance of the Enterprise edition: 50WAF instance of the Exclusive edition: 50

Prerequisites

- Your website is added to WAF.

This topic provides an example on how to customize server ports for a website that is added to WAF. You can also customize server ports when you manually add a website. For more information, see [Manually add domain name configurations](#).

- To use non-standard ports, make sure that the WAF instance that you purchase meets the following specification requirements:
 - If the instance is billed on a subscription basis, the instance must be of the **Business** edition or higher. For more information, see [WAF deployment plans and editions](#).

Background information

WAF forwards traffic only on the specified ports of the origin server. WAF does not forward traffic on the ports that you have not specified.

Procedure

-
-
-
- On the **Domain Names** tab, find the domain name, and click **Edit** in the Actions column.
- In the **Destination Server Port** section of the **Edit** page, click **Customize**.
- Click the required protocol type (**HTTP** or **HTTPS**). Then, enter the ports that you want to add and click **Save**.

Note The ports that you entered must be within the allowed port range. Otherwise, the settings cannot be saved. You can click **View Allowed Port Range** to check whether the ports are within the allowed port range.

Allowed Port Range

HTTP

HTTPS

4

84

7004

7014

7024

8084

48800

OK

Cancel

7. Click **Confirm**.