

Web Application Firewall

Getting Started

Issue 03
Date 2025-02-19



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

Contents

1 Before You Start.....	1
2 Blocking Heavy-Traffic CC Attacks Through CC Attack Protection Rules.....	4
3 Blocking Malicious Traffic Through IP Address Blacklist or Whitelist Rules.....	16
4 Common Tasks.....	21

1 Before You Start

Web Application Firewall (WAF) examines HTTP/HTTPS requests to identify and block malicious traffic, keeping your core service data secure and web server performance stable. This document describes how to quickly use WAF to protect your workloads.

Overview

A glance at WAF:

- [What is WAF?](#)
- [WAF Editions and Their Differences](#)
- [Features](#)
- [How Is WAF Billed?](#)
- [What Types of Protections Rule Can WAF Provide?](#)

Step 1: Buy a WAF Instance

1. [Log in to Huawei Cloud management console](#). On the console page, choose **Security & Compliance > Web Application Firewall**.
2. In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select a WAF mode.

WAF provides three access modes, CNAME and ELB access modes for cloud WAF and dedicated access mode for dedicated WAF. For their differences, see [Edition Differences](#).

Dedicated WAF instances are not available in some regions. For details, see [Notice on Web Application Firewall \(Dedicated Mode\) Discontinued](#).

- [Buying a Cloud WAF Instance](#)

NOTE

- To use ELB-access cloud WAF, you need to [submit a service ticket](#) to enable it for you first. ELB-access cloud WAF is available in some regions. For details, see [Functions](#).
- If you want to use the ELB access mode, make sure you are using standard, professional, or platinum cloud WAF. When you are using cloud WAF, the quotas for the domain name, QPS, and rule extension packages are shared between the ELB access and CNAME access modes.

Step 2: Connect a Website to WAF

After buying a WAF instance, you need to add it to WAF, or WAF cannot check HTTP or HTTPS requests.

Access Mode	Protection Scenario	Reference Document
Cloud Mode - CNAME Access	<ul style="list-style-type: none"> Service servers are deployed on any cloud or in on-premises data centers. Protected objects: domain names 	Connecting Your Website to WAF (Cloud Mode - CNAME Access)
Cloud Mode - Load Balancer Access	<ul style="list-style-type: none"> Service servers are deployed on Huawei Cloud. This mode is suitable for large enterprise websites having high security requirements on service stability. Protected objects: domain names and IP addresses 	Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)
Dedicated mode	<ul style="list-style-type: none"> Service servers are deployed on Huawei Cloud. This mode is suitable for large enterprise websites that have a large service scale and have customized security requirements. Protected objects: domain names and IP addresses 	Connecting Your Website to WAF (Dedicated Mode)

Step 3: Configure a Protection Policy

After your website is connected to WAF, WAF applies a protection policy to your website and enables **General Check** (with **Protective Action** set to **Log only** and **Protection Level** set to **Medium**) in **Basic Web Protection** and enables **Scanner check** (with **Protective Action** set to **Log only**) in **Anti-Crawler** protection.

- If you do not have special security requirements, you can retain the default settings and view WAF protection logs on the **Events** page at any time. For details, see [Viewing Protection Event Logs](#).
- If your website were under attacks, you can configure a custom protection policy based on attack details on the **Dashboard** and **Events** pages. For details, see [Adding Rules to One or More Policies](#).

Step 4: View Protection Logs

On the **Events** page, view the protection details of the configured protection policy and handle the source IP address.

- To quickly whitelist a source IP address, locate the row that contains the corresponding event, choose **Handle as False Alarm** in the **Operation** column, and configure a global protection whitelist rule.
- To block or allow a source IP address, add it to an IP address blacklist or whitelist.

For details, see [Handling False Alarms](#).

2 Blocking Heavy-Traffic CC Attacks Through CC Attack Protection Rules

A CC attack protection rule can limit access to your website based on the IP address or cookie of a visitor. If the number of access requests from a visitor exceeds the threshold you configure, you can require the visitor to enter a verification code to continue the access, or block the request and return a custom page of certain type to the visitor.

In heavy-traffic CC attacks, a single zombie server can send far more packets than a common user does. In this scenario, a rate limiting rule is the most effective method to fend off this type of CC attacks.

This topic provides an example for you to show how to configure an IP-based CC attack protection rule to limit access traffic.

- Website access mode: Cloud mode - CNAME access
- Protected object: domain names
- Billing mode: Yearly/Monthly
- Edition: Standard
- Protection rule: CC attack protection

Process

Procedure	Description
Preparations	Sign up for a HUAWEI ID, enable Huawei Cloud services, top up your account, and assign WAF permissions to the account.
Step 1: Buy WAF	Buy WAF and select the region and WAF mode.
Step 2: Add a Website to WAF	Add the website you want to protect to WAF for traffic inspection and forwarding.

Procedure	Description
Step 3: Configure a CC Attack Protection Rule	Configure and enable CC attack protection rules to mitigate CC attacks against the protected website.

Preparations

- Before purchasing WAF, create a Huawei account and subscribe to Huawei Cloud. For details, see [Registering a HUAWEI ID and Enabling HUAWEI CLOUD Services](#) and [Real-Name Authentication](#).
If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
- Make sure that your account has sufficient balance, or you may fail to pay to your WAF orders.
- Make sure your account has WAF permissions assigned. For details, see [Creating a User Group and Granting Permissions](#).

Table 2-1 System policies supported by WAF

Role/Policy Name	Description	Category	Dependencies
WAF Administrator	Administrator permissions for WAF	System-defined role	Dependent on the Tenant Guest and Server Administrator roles. <ul style="list-style-type: none"> Tenant Guest: A global role, which must be assigned in the global project. Server Administrator: A project-level role, which must be assigned in the same project.
WAF FullAccess	All permissions for WAF	System-defined policy	None.
WAF ReadOnlyAccess	Read-only permissions for WAF.	System-defined policy	

Step 1: Buy the Standard Edition Cloud WAF

- [Log in to Huawei Cloud management console.](#)
- On the management console page, choose **Security & Compliance > Web Application Firewall**.

3. In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, complete the purchase by referring to configurations in [Table 2-2](#).

Table 2-2 Purchase parameters

Parameter	Example Value	Description
WAF Mode	Cloud Mode	Cloud mode - CNAME access is supported. Web services deployed on Huawei Cloud, other clouds, or on-premises can be protected. The protected objects are domain names.
Billing Mode	Yearly/ Monthly	Yearly/Monthly is a prepaid billing mode, where you pay in advance for a subscription term and receive a discounted rate. This mode is ideal when the resource use duration is predictable.
Region	CN-Hong Kong	You can select the region nearest to your services WAF will protect.
Edition	Standard	This edition is suitable for small and medium-sized websites.

4. Confirm the product details and click **Buy Now** in the lower right corner of the page.
5. Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
6. On the payment page, select a payment method and pay for your order.

Step 2: Add a Website to WAF

1. In the navigation pane on the left, choose **Website Settings**.
2. In the upper left corner of the website list, click **Add Website**.
3. Select **Cloud - CNAME** and click **Configure Now**.
4. On the **Add Website** page, set the following parameters and retain the default values for other parameters. [Table 2-3](#) describes the parameters.

Figure 2-1 Add Domain Name

Basic Settings

Protected Domain Name ¹
 [Quick Add Domain Names Hosted on Cloud](#)
Only domain names that have been registered with ICP licenses can be added to WAF. View details at <https://beian.xinnet.com/>

Website Name (Optional)

Website Remarks (Optional)

Protected Port ²
 [View Ports You Can Use](#)
³ Standard ports 80 and 443 are the default ports reserved for HTTP and HTTPS protocols, respectively.

Server Configuration ⁴

Client Protocol	Server Protocol	Server Address	Server Port	Weight	Operation	
HTTP	HTTP	IPv4	Enter a public IP ad	80	1	Delete

[Add Address](#) Origin server addresses you can add: 59

Use Layer-7 Proxy ⁵
 Yes No

Table 2-3 Mandatory parameters

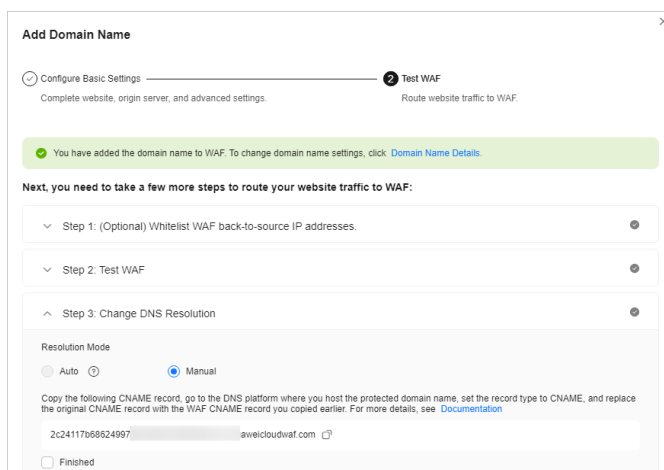
Parameter	Example Value	Description
Protected Domain Name	www.example.com	The domain name you want to add to WAF for protection.
Protected Port	Standard port	The port over which the website service traffic goes. To protect port 80 or 443, select Standard port from the drop-down list.

Parameter	Example Value	Description
Server Configuration	<p>Client Protocol: HTTP.</p> <p>Server Protocol: HTTP</p> <p>Server Address: <i>IPv4</i> <i>XXX.XXX.1.1</i></p> <p>Server Port: 80</p>	<p>Server address configuration. You need to configure the client protocol, server protocol, server weights, server address, and server port.</p> <ul style="list-style-type: none"> ● Client Protocol: protocol used by a client to access a server. The options are HTTP and HTTPS. ● Server Protocol: protocol used by WAF to forward client requests. The options are HTTP and HTTPS. ● Server Address: public IP address (generally corresponding to the A record of the domain name configured on the DNS) or domain name (generally corresponding to the CNAME record of the domain name configured on the DNS) of the web server that a client accesses. The following IP address formats are supported: <ul style="list-style-type: none"> – IPv4, for example, XX.XXX.1.1 – IPv6, for example, fe80:0000:0000:0000:0000:0000:0000:0000 ● Server Port: service port over which the WAF instance forwards client requests to the origin server. ● Weight: Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.

Parameter	Example Value	Description
Use Layer-7 Proxy	No	<ul style="list-style-type: none"> • Yes: Web proxy products for layer-7 request forwarding are used, products such as anti-DDoS, CDN, and other cloud acceleration services. • No: No layer-7 proxies are not used. <p>No is used in this example.</p>

5. Click **Next**. The basic information about the domain name is configured.


Figure 2-2 Basic settings completed



6. Complete steps **Whitelist WAF Back-to-Source IP Addresses** and **Test WAF** as prompted.
7. Complete DNS resolution.

Configure the CNAME record on the DNS platform hosting your domain name. For details, contact your DNS provider.

The following uses Huawei Cloud DNS as an example to show how to configure a CNAME record. The following configuration is for reference only.

- a. Copy the CNAME value provided by WAF in **Figure 2-2**.
- b. Click  in the upper left corner of the page and choose **Networking > Domain Name Service**.
- c. In the navigation pane on the left, choose **Public Zones**.
- d. In the **Operation** column of the target domain name, click **Manage Record Set**. The **Record Sets** tab page is displayed.
- e. In the row containing the desired record set, click **Modify** in the **Operation** column.
- f. In the displayed **Modify Record Set** dialog box, change the record value.

- **Name:** Domain name configured in WAF
 - **Type:** Select **CNAME-Map one domain to another**.
 - **Line:** **Default**
 - **TTL (s):** The recommended value is **5 min**. A larger TTL value will make it slower for synchronization and update of DNS records.
 - **Value:** Change it to the CNAME record copied in [7.a](#).
 - Keep other settings unchanged.
- g. Click **OK**.

Step 3: Configure a CC Attack Protection Rule

Configuration example: You can configure such a CC rule to mitigate CC attacks. If an IP address accessed any path under the current domain name more than 1000 times within 30 seconds, this rule will block requests from the IP address for 10 hours. This rule can be used as a preventive configuration for common small and medium-sized websites

1. In the navigation pane on the left, choose **Policies**.
2. Click the name of the target policy to go to the protection configuration page.
3. In the **CC Attack Protection** area, enable it.

 : enabled

 : disabled

4. In the upper left corner of the **CC Attack Protection** rule list, click **Add Rule**. In the dialog box displayed, configure the CC attack protection rule by referring to [Figure 2-3](#).

In this example, only some parameters are described. Retain the default values for other parameters. [Table 2-4](#) describes some parameters.

Figure 2-3 Add CC Attack Protection Rule

Add CC Attack Protection Rule

Rate Limit Type ¹

Per IP address Per user Other

Request Aggregation ²

Keep this function enabled if you added a wildcard domain name to WAF so that requests to all domain names that match the wildcard domain are counted for triggering this rule. For example, if you added *.a.com to WAF, requests to all matched domain names such as b.a.com and c.a.com are counted.

Trigger

Field ²	Subfield	Logic	Content	Operation
Path	-	Prefix is	/login.php	Delete

[+ Add Condition](#) You can add 29 more conditions.(The rule is only applied when all conditions are met.) [Add Reference Table](#)

Rate Limit ³

- 1000 + requests - 30 + seconds

All WAF instances ⁴

Take Protective Action ⁴

Protective Action ⁵

Block Block dynamically Verification code Log only JS Challenge

Block Duration ⁵

- 36000 + seconds

Block Page

Default settings Custom

Application Schedule ⁶

Table 2-4 Mandatory parameters

Parameter	Example Value	Description
Rate Limit Mode	Source > Per IP address	<ul style="list-style-type: none"> ● Source: Requests from a specific source are limited. For example, if traffic from an IP address (or user) exceeds the rate limit you configure in this rule, WAF limits traffic rate of the IP address (or user) in the way you configure. <ul style="list-style-type: none"> - Per IP address: A website visitor is identified by the IP address. - Per user: A website visitor is identified by the key value of Cookie or Header. - Other: A website visitor is identified by the Referer field (user-defined request source). <p>NOTE If you set Rate Limit Mode to Other, set Content of Referer to a complete URL containing the domain name. The Content field supports prefix match and exact match only, but cannot contain two or more consecutive slashes, for example, ///admin. If you enter ///admin, WAF will convert it to /admin.</p> <p>For example, if you do not want visitors to access www.test.com, set Referer to http://www.test.com.</p> <ul style="list-style-type: none"> ● Destination: If this parameter is selected, the following rate limit types are available: <ul style="list-style-type: none"> - By rule: If this rule is used by multiple domain names, requests for all these domain names are counted for this rule no matter what IP addresses these requests originate from. If you have added a wildcard domain name to WAF, requests for all domain names matched the wildcard domain name are counted for triggering this rule no matter what IP addresses these requests originate from. - By domain name: Requests for each domain name are counted separately. If the number exceeds the threshold you configure, the protective action is triggered no matter what IP addresses these requests originate from.

Parameter	Example Value	Description
		<ul style="list-style-type: none"> - By URL: Requests for each URL are counted separately. If the number exceeds the threshold you configure, the protective action is triggered no matter what IP addresses these requests originate from.
Trigger	<ul style="list-style-type: none"> • Field: Path • Logic: Prefix is • Content: /login.php 	<p>Click Add Conditions and add conditions. At least one condition is required, but up to 30 conditions are allowed. If you add more than one condition, the rule will only take effect when all conditions are met.</p> <ul style="list-style-type: none"> • Field • Subfield: Configure this field only when IPv4, IPv6, Cookie, Header, or Params is selected for Field. <p>NOTICE A subfield cannot exceed 2,048 bytes.</p> <ul style="list-style-type: none"> • Logic: Select the desired logical relationship from the drop-down list. • Content: Enter or select the content that matches the condition.
Rate Limit	<p>1,000 requests within 30 seconds</p> <p>All WAF instances</p>	<p>The number of requests allowed from a website visitor in the rate limit period. If the number of requests exceeds the rate limit, WAF takes the action you configure for Protective Action.</p> <p>All WAF instances: Requests to on one or more WAF instances will be counted together according to the rate limit mode you select. By default, requests to each WAF instance are counted. If you enable this, WAF will count requests to all your WAF instances for triggering this rule. To enable user-based rate limiting, Per user or Other (Referer must be configured) instead of Per IP address must be selected for Rate Limit Mode. This is because IP address-based rate limiting cannot limit the access rate of a specific user. However, in user-based rate limiting, requests may be forwarded to one or more WAF instances. Therefore, All WAF instances must be enabled for triggering the rule precisely.</p>

Parameter	Example Value	Description
Protective Action	Block	The action that WAF will take if the number of requests exceeds Rate Limit you configured. You can select: <ul style="list-style-type: none">• Verification code: WAF allows requests that trigger the rule as long as your website visitors complete the required verification.• Block: WAF blocks requests that trigger the rule.• Block dynamically: WAF blocks requests that trigger the rule based on Allowable Frequency, which you configure after the first rate limit period is over.• Log only: WAF only logs requests that trigger the rule.• JS Challenge: WAF returns a piece of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes the JavaScript code, WAF allows all requests from the client within a period of time (30 minutes by default). During this period, no verification is required. If the client fails to execute the code, WAF blocks the requests.
Block Duration	36,000 seconds	Period of time for which to block the item when you set Protective Action to Block .

5. Confirm the configuration and click **OK**.

Related Information

- For more details, see [Configuring a CC Attack Protection Rule](#).
- The **Cloud Mode - Load Balancer** access mode is recommended for large enterprise websites that are deployed on Huawei Cloud, have high service stability requirements, and are accessible over domain names or IP addresses. For details, see the following procedure:
 - a. [Buy a standard edition cloud WAF instance](#).

After the purchase is complete, [submit a service ticket](#) to enable WAF cloud mode load balancer access mode.
 - b. [Connect your website to WAF \(Cloud Mode - Load Balancer Access\)](#).
 - c. [Configure a CC attack protection rule to block heavy-traffic attacks](#).
- **Dedicated Mode** is recommended for large websites that are deployed on Huawei Cloud, have special security requirements, and are accessible over domain names or IP addresses. For details, see the following procedure:

- a. Dedicated WAF instances are not available in some regions. For details, see [Notice on Web Application Firewall \(Dedicated Mode\) Discontinued](#). If you have purchased a dedicated WAF instance, skip this step.
- b. [Connect your website to WAF \(dedicated mode\)](#).
- c. [Configure a CC attack protection rule to block heavy-traffic attacks](#).

3 Blocking Malicious Traffic Through IP Address Blacklist or Whitelist Rules

By default, WAF allows access from all IP addresses. If you find that your website is accessed from malicious IP addresses, you can add a WAF blacklist or whitelist rule to block malicious IP addresses.

The following example shows you how to configure an IP address whitelist or blacklist rule. In this example, we use the WAF cloud load balancer access mode.

- Website access mode: Cloud mode - Load balancer access
- Protected objects: domain names and IP addresses
- Billing mode: Yearly/Monthly
- Edition: Standard
- Protection rule: blacklist and whitelist settings

Process

Procedure	Description
Preparations	Sign up for a HUAWEI ID, enable Huawei Cloud services, top up your account, and assign WAF permissions to the account.
Step 1: Buy the Standard Edition Cloud WAF	Purchase WAF and select the region and WAF mode.
Step 2: Add a Website to WAF in Load Balancer Access Mode	Add the website you want to protect to WAF for traffic inspection.
Step 3: Configure an IP Address Blacklist or Whitelist Rule	Add blacklist and whitelist rules to block malicious IP addresses.

Preparations

1. Before purchasing WAF, create a Huawei account and subscribe to Huawei Cloud. For details, see [Registering a HUAWEI ID and Enabling HUAWEI CLOUD Services](#) and [Real-Name Authentication](#).
If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. Make sure that your account has sufficient balance, or you may fail to pay to your WAF orders.
3. Make sure your account has WAF permissions assigned. For details, see [Creating a User Group and Granting Permissions](#).

Table 3-1 System policies supported by WAF

Role/Policy Name	Description	Category	Dependencies
WAF Administrator	Administrator permissions for WAF	System-defined role	Dependent on the Tenant Guest and Server Administrator roles. <ul style="list-style-type: none">• Tenant Guest: A global role, which must be assigned in the global project.• Server Administrator: A project-level role, which must be assigned in the same project.
WAF FullAccess	All permissions for WAF	System-defined policy	None.
WAF ReadOnlyAccess	Read-only permissions for WAF.	System-defined policy	

Step 1: Buy the Standard Edition Cloud WAF

You can use the load balancer access mode only after you purchase the standard, professional, or platinum edition cloud WAF. The following describes how to buy the standard edition cloud WAF.

1. [Log in to Huawei Cloud management console](#).
2. On the management console page, choose **Security & Compliance > Web Application Firewall**.
3. In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, complete the purchase by referring to configurations below.

Table 3-2 Purchase parameters

Parameter	Example Value	Description
WAF Mode	Cloud Mode	After purchasing WAF, submit a service ticket to enable the cloud load balancer access mode. WAF then can protect your websites deployed on Huawei Cloud. In this mode, the protected objects can be website domain names or IP addresses.
Billing Mode	Yearly/Monthly	Yearly/Monthly is a prepaid billing mode, where you pay in advance for a subscription term and receive a discounted rate. This mode is ideal when the resource use duration is predictable.
Region	CN-Hong Kong	You can select the region nearest to your services WAF will protect.
Edition	Standard	This edition can protect small and medium-sized websites.

4. Confirm the product details and click **Buy Now** in the lower right corner of the page.
5. Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
6. On the payment page, select a payment method and pay for your order.

 **NOTE**

After the purchase is complete, [submit a service ticket](#) to enable WAF cloud load balancer access mode.

Step 2: Add a Website to WAF in Load Balancer Access Mode

Step 1 [Create a dedicated load balancer](#).

- **Specifications:** Select **Application load balancing (HTTP/HTTPS)**.
- Set other parameters based on your service requirements.

Step 2 Add a listener to the load balancer created in [Step 1](#). For details, see [Adding an HTTP Listener](#) or [Adding an HTTPS Listener](#).

Step 3 [Create a backend server group](#).

- **Load Balancer:** Select **Associate existing** and select the load balancer created in [Step 1](#) from the drop-down list.
- Set the backend server to the server address of the website you plan to add to WAF in [Step 8](#).

Step 4 Click in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

- Step 5** In the navigation pane on the left, choose **Website Settings**.
- Step 6** In the upper left corner of the website list, click **Add Website**.
- Step 7** Select **Cloud - Load balancer** and click **Configure Now**.
- Step 8** On the **Add Website** page, set the parameters by referring to **Figure 3-1**.
- **ELB (Load Balancer)**: Select an ELB load balancer. Make sure you have added the server address corresponding to the protected website to the ELB load balancer.
 - **ELB Listener**: Select **All listeners**.
 - **Protected Domain Name**: Enter the domain name or IP address you want to protect. We use **www.example.com** in this example.
 - **Policy**: **System-generated policy** is selected by default.

Figure 3-1 Domain name settings



The screenshot shows the 'Add Website' configuration page with the following settings:

- ELB (Load Balancer)**: A dropdown menu showing 'elb-c00474594' with a search icon to the right.
- ELB Listener**: Two buttons, 'All listeners' (highlighted in blue) and 'Specific listener' (greyed out).
- Website Name**: A text input field with the placeholder text 'Enter a custom name for the domain name.'
- Domain Name**: A text input field containing 'www.example.com'.
- Website Remarks**: An empty text input field.
- Policy**: A dropdown menu showing 'System-generated policy' with a help icon to the left.

Step 9 Click **OK**.

----End

Step 3: Configure an IP Address Blacklist or Whitelist Rule

- Step 1** In the navigation pane on the left, choose **Policies**.
- Step 2** Click the name of the target policy to go to the protection configuration page.
- Step 3** Choose **Blacklist and Whitelist** and enable it.
-  : enabled
 -  : disabled
- Step 4** Above the blacklist and whitelist rule list, click **Add Rule** and configure a rule as shown in **Figure 3-2**.
- **IP Address/Range/Group**: Select **IP address/range**. To block multiple IP addresses, select **Address group**.

- **IP Address/Range:** Configure the IP addresses or IP address ranges you want to block, for example, 192.168.2.1.
- **Protective Action:** Select **Block**.

Figure 3-2 Blocking a specified IP address

Add Blacklist or Whitelist Rule ✕

* Rule Name

* IP Address/Range/Group IP address/range Address group

* IP Address/Range

* Protective Action

Known Attack Source [Add Known Attack Source](#)
Source Rule

* Application Schedule Immediate Custom

Rule Description

OK Cancel

Step 5 Click **OK**.

----End

Related Information

- For details, see [Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses](#).
- The **Cloud Mode - CNAME Access** mode can be used for web services that are accessible through domain names, no matter where your web services are deployed, on Huawei Cloud, on other clouds, or even in on-premises data centers. For details, see the following procedure:
 - a. [Buy a standard edition cloud WAF instance](#).
 - b. [Connect your website to WAF \(Cloud Mode - CNAME Access\)](#).
 - c. [Step 3: Configure an IP Address Blacklist or Whitelist Rule](#).
- **Dedicated Mode** is recommended for large websites that are deployed on Huawei Cloud, have special security requirements, and are accessible over domain names or IP addresses. For details, see the following procedure:
 - a. Dedicated WAF instances are not available in some regions. For details, see [Notice on Web Application Firewall \(Dedicated Mode\) Discontinued](#). If you have purchased a dedicated WAF instance, skip this step.
 - b. [Connect your website to WAF \(dedicated mode\)](#).
 - c. [Step 3: Configure an IP Address Blacklist or Whitelist Rule](#).

4 Common Tasks

WAF provides a series of common practices for you. These practices can help you start WAF protection for your workloads quickly.

Table 4-1 Common practices

Practice	Description
Connecting a domain name to WAF	Connecting a Website Without a Proxy to WAF Using CNAME If your website is not added to WAF, DNS resolves your domain name to the IP address of the origin server. If your website is added to WAF, DNS resolves your domain name to the CNAME of WAF. In this way, the traffic passes through WAF. WAF inspects every traffic coming from the client and filters out malicious traffic. This section describes how to change DNS settings for WAF to take effect.
	Combining AAD and WAF to Get All-Round Protection The combination of AAD and WAF can protect domain names deployed on Huawei Cloud, other clouds, or on-premises from DDoS attacks and web attacks, ensuring service continuity and reliability. <ul style="list-style-type: none">• Mitigation of DDoS attacks: NTP flood, SYN flood, ACK flood, ICMP flood, and HTTP Get flood attacks.• Defense against web attacks: WAF identifies and blocks a wide range of suspicious attacks, such as SQL injections, XSS attacks, web shell upload, command or code injections, file inclusion, unauthorized sensitive file access, third-party vulnerability exploits, CC attacks, malicious crawlers, and CSRF.

Practice		Description
	Combining CDN and WAF to Get Improved Protection and Load Speed	The combination of CDN and WAF can protect websites on Huawei Cloud, other clouds, or on-premises and improve website response time.
	Combining WAF and Layer-7 Load Balancers to Protect Services over Any Ports	This topic walks you through how to combine dedicated WAF instances and layer-7 load balancers to protect your services over non-standard ports that cannot be protected with WAF alone. For ports that can be protected with WAF, see Ports Supported by WAF .
	Using WAF, ELB, and NAT Gateway to Protect Services Not Deployed on Our Cloud	By default, in cloud load balancer access mode, WAF can protect only workloads deployed on our cloud. If your origin servers are not deployed on our cloud, but you want to use WAF in this mode, you can use Network Address Translation (NAT) gateways to route traffic from Huawei Cloud to the public IP addresses of your origin server. Then, you can connect your website to WAF in cloud load balancer access mode to let WAF check your website traffic.
Policy configuration	Best Practices for Website Protection	This topic describes how Web Application Firewall (WAF) protects workloads in different scenarios. You can refer to configurations in this topic to make WAF work better for you.
	Using WAF to Defend Against CC Attacks	This section guides you through configuring IP address-based rate limiting and cookie-based protection rules against Challenge Collapsar (CC) attacks.
	Configuring Anti-Crawler Rules to Prevent Crawler Attacks	WAF provides three anti-crawler policies, bot detection by identifying User-Agent, website anti-crawler by checking browser validity, and CC attack protection by limiting the access frequency, to help mitigate crawler attacks against your websites.
	Verifying a Global Protection Whitelist Rule by Simulating Requests with Postman	After your website is connected to WAF, you can use an API test tool to send HTTP/HTTPS requests to the website and verify that WAF protection rules take effect. This topic uses Postman as an example to describe how to verify a global protection whitelist (formerly false alarm masking) rule.

Practice		Description
	Combining WAF and HSS to Get Improved Web Tamper Protection	With HSS and WAF in place, you can stop worrying about web page tampering.
LTS log analysis	Using LTS to Query and Analyze WAF Access Logs	If you enable LTS for WAF logging, Log Tank Service (LTS) will log attack and access logs for WAF. With LTS, users can perform real-time decision analysis, device O&M management, and service trend analysis in a timely and efficient manner.
	Using LTS to Analyze How WAF Blocks Spring Core RCE Vulnerability	This topic walks you through on how to enable the LTS quick analysis for WAF attack logs and use the Spring rule ID to quickly query and analyze the logs of the blocked Spring Core RCE vulnerabilities.
	Using LTS to Configure Block Alarms for WAF Rules	This topic walks you through how to enable LTS quick analysis for WAF attack logs and configure alarm rules to analyze WAF attack logs and generate alarms. In this way, you can gain insight into the protection status of your workloads in WAF in real time and make informed decisions.
Configuring TLS encryption	Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections	HTTPS is a network protocol constructed based on Transport Layer Security (TLS) and HTTP for encrypted transmission and identity authentication. When you add a domain name to WAF , set Client Protocol to HTTPS . Then, you can configure the minimum TLS version and cipher suite to harden website security.
Protecting origin servers	Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections	HTTPS is a network protocol constructed based on Transport Layer Security (TLS) and HTTP for encrypted transmission and identity authentication. If a client uses HTTPS to access WAF, that is, the client protocol is set to HTTPS, you can configure the minimum TLS version and cipher suite for the domain name to ensure website security.
	Configuring ECS and ELB Access Control Policies to Protect Origin Servers	This topic describes how to protect origin servers deployed on ECSs or added to ELB backend server groups. It helps you: <ul style="list-style-type: none"> • Identify publicly accessible origin servers. • Configure access control policy to protect origin servers.

Practice		Description
Obtaining real client IP addresses	Obtaining Real Client IP Addresses	This topic describes how to obtain the client IP address from WAF and how to configure different types of web application servers, including Tomcat, Apache, Nginx, IIS 6, and IIS 7, to obtain the client IP address.
Configuring Alarms on Cloud Eye for Abnormal WAF Metrics	Configuring Alarms for Abnormal WAF Metrics on Cloud Eye	This topic describes how to create alarms for abnormal WAF metrics on Cloud Eye. So, you can learn about the WAF protection status in a timely manner. If there is something wrong, you can take actions in time.