Web Application Firewall

Getting Started

Issue	02
Date	2024-10-31

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

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.
   - **Buying a Cloud WAF Instance**

     NOTE

     - To use ELB-access cloud WAF, you need to to enable it for you first. ELB-access cloud WAF is available in some regions. For details, see .
     - 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.
   - **Buying a Dedicated WAF Instance**

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	● 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)**
Dedicated mode	● 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 heave-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	Purchase 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: Enable CC Attack Protection	Configure and enable CC attack protection rules to mitigate CC attacks against the protected website.

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 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. ● **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

WAF provides the cloud mode and dedicated mode instances. For details about the differences between the two modes, see **Edition Differences**.

1. Log in to Huawei Cloud management console.
2. On the management console page, choose **Security** > **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

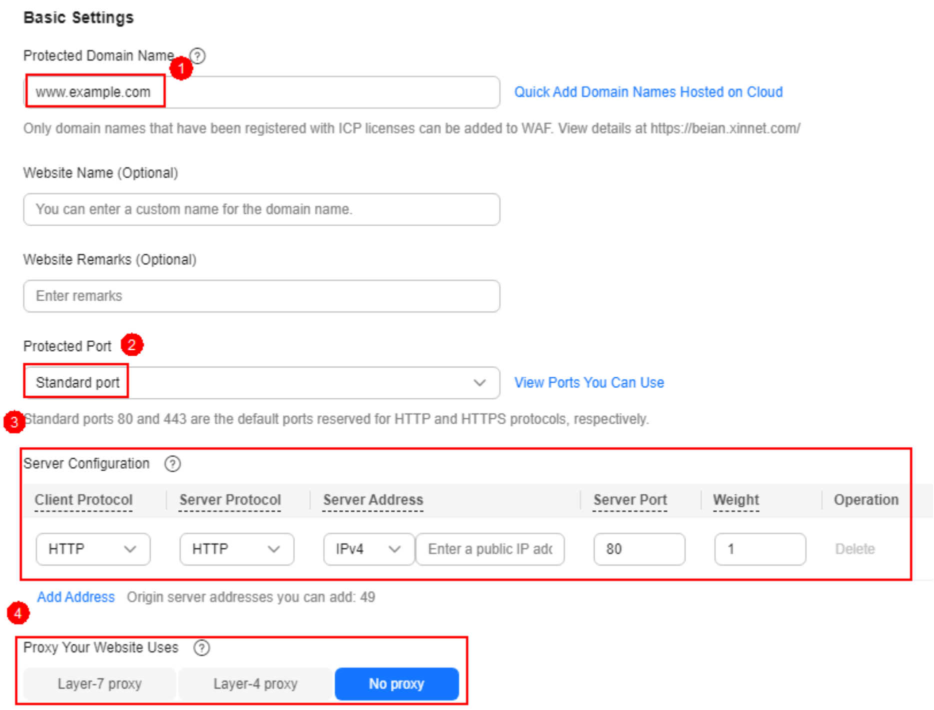
Parameter	Example Value	Description
WAF Mode	**Cloud Mode**	Cloud mode - CNAME access is supported. Web services deployed on Huawei Cloud, other clouds, or on-premises can be protected. The protected objects are domain names.
Billing Mode	**Yearly/ Monthly**	Yearly/Monthly is a prepaid billing mode, 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	**EU-Dublin**	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

www.example.com

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)

You can enter a custom name for the domain name.

Website Remarks (Optional)

Enter remarks

Protected Port

Standard port

View Ports You Can Use

Standard ports 80 and 443 are the default ports reserved for HTTP and HTTPS protocols, respectively.

Server Configuration

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

Add Address Origin server addresses you can add: 49

Proxy Your Website Uses

Layer-7 proxy | Layer-4 proxy | [✓ No proxy]

Table 2-3 Mandatory parameters

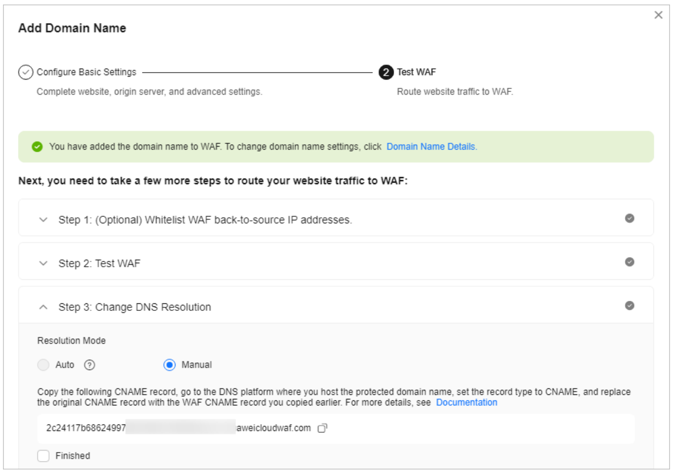
Parameter	Example Value	Description
Protected Domain Name	**www.example.com**	The domain name you want to add to WAF for protection.
Protected Port	**Standard port**	The port over which the website service traffic goes. To protect port 80 or 443, select **Standard port** from the drop-down list.

Parameter	Example Value	Description
Server Configuration	**Client Protocol**: **HTTP**. **Server Protocol**: **HTTP** **Server Address**: *IPv4 XXX.XXX.1.1* **Server Port**: **80**	Server address configuration. You need to configure the client protocol, server protocol, server address, and server port. ● **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. ● **Server Port**: service port over which the WAF instance forwards client requests to the origin server.

Parameter	Example Value	Description
Proxy Your Website Uses	**No proxy**	● **Layer-7 proxy**: Web proxy products for layer-7 request forwarding are used, products such as anti-DDoS, CDN, and other cloud acceleration services. ● **Layer-4 proxy**: Web proxy products for layer-4 forwarding are used, products such as anti-DDoS. ● **No proxy**: No proxy products are deployed in front of WAF. In our example, no proxies are used.

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

Figure 2-2 Basic settings completed



Add Domain Name

Configure Basic Settings — Complete website, origin server, and advanced settings.

2 Test WAF — Route website traffic to WAF.

You have added the domain name to WAF. To change domain name settings, click Domain Name Details.

Next, you need to take a few more steps to route your website traffic to WAF:

Step 1: (Optional) Whitelist WAF back-to-source IP addresses.

Step 2: Test WAF

Step 3: Change DNS Resolution

Resolution Mode

○ Auto ● Manual

Copy the following CNAME record, go to the DNS platform where you host the protected domain name, set the record type to CNAME, and replace the original CNAME record with the WAF CNAME record you copied earlier. For more details, see Documentation

2c24117b68624997[redacted]aweicloudwaf.com

□ Finished

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.

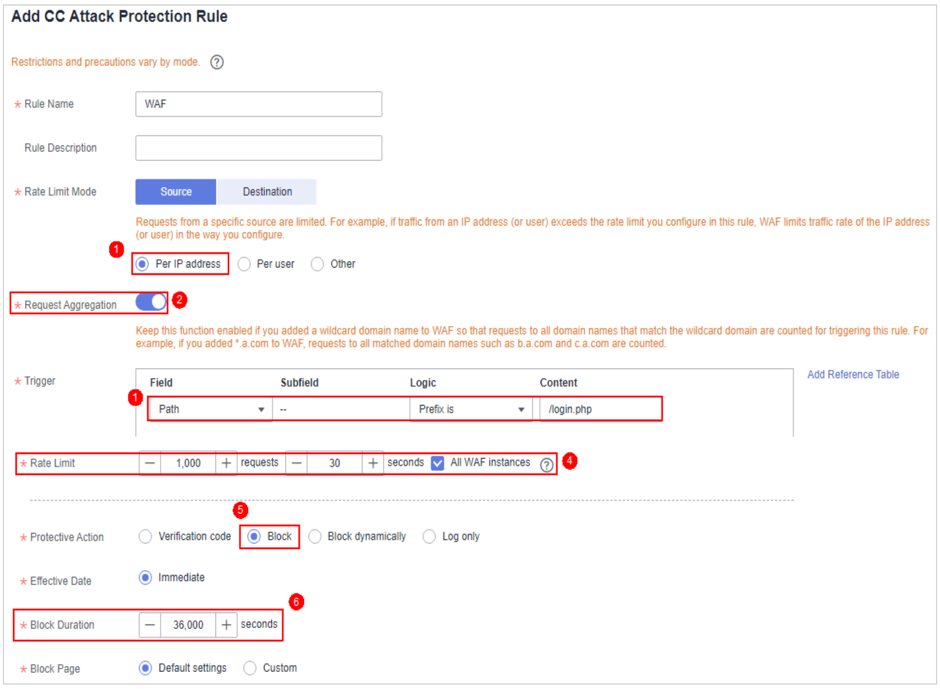
   ●: enabled

   ○: 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

Restrictions and precautions vary by mode.

* Rule Name: WAF

Rule Description:

* Rate Limit Mode: [✓ Source] Destination

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.

● Per IP address ○ Per user ○ Other

* Request Aggregation: enabled

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	Subfield	Logic	Content
Path	--	Prefix is	/login.php

Add Reference Table

* Rate Limit: 1,000 requests 30 seconds ☑ All WAF instances

* Protective Action: ○ Verification code ● Block ○ Block dynamically ○ Log only

* Effective Date: ● Immediate

* Block Duration: 36,000 seconds

* Block Page: ● Default settings ○ Custom

Table 2-4 Mandatory parameters

Parameter	Example Value	Description
Rate Limit Mode	**Source** > **Per IP address**	● **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. – **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). **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**. For example, if you do not want visitors to access www.test.com, set **Referer** to **http://www.test.com**. ● **Destination**: If this parameter is selected, the following rate limit types are available: – **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. <br/>· 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
		– **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	● **Field**: **Path** ● **Logic**: **Prefix is** ● **Content**: **/ login.php**	Click **Add** 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. ● Field ● **Subfield**: Configure this field only when **IPv4**, **IPv6**, **Cookie**, **Header**, or **Params** is selected for **Field**. **NOTICE** A subfield cannot exceed 2,048 bytes. ● **Logic**: Select the desired logical relationship from the drop-down list. ● **Content**: Enter or select the content that matches the condition.
Rate Limit	**1,000 requests** within **30 seconds**	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**.
Protective Action	**Block**	The action that WAF will take if the number of requests exceeds **Rate Limit** you configured. You can select: ● **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.
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 **Confirm**.

Related Information

- For more details, see **Configuring a CC Attack Protection 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. **Buy a dedicated WAF instance**.
  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 CNAME access mode.

- Website access mode: Cloud mode - CNAME access
- Protected object: domain names
- 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	Add the website you want to protect to WAF for traffic inspection and forwarding.
Step 4: 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. ● **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** > **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

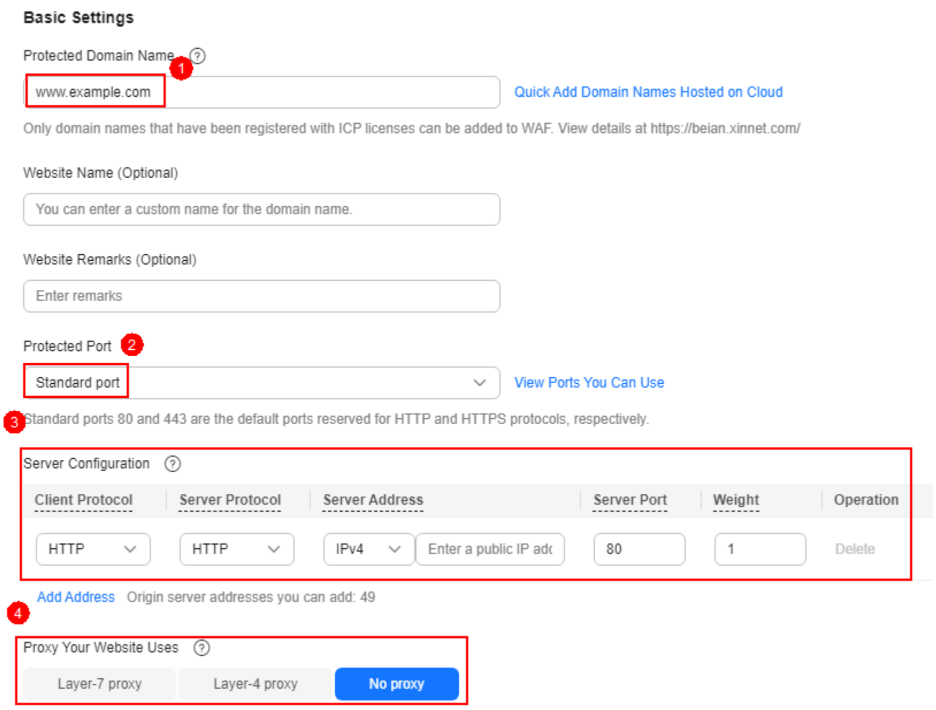
Parameter	Example Value	Description
WAF Mode	**Cloud Mode**	Cloud mode - CNAME access is supported. Web services deployed on Huawei Cloud, other clouds, or on-premises can be protected. The protected objects are domain names.
Billing Mode	**Yearly/Monthly**	Yearly/Monthly is a prepaid billing mode, where 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	**EU-Dublin**	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.

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 3-3** describes the parameters.

Figure 3-1 Add Domain Name



Basic Settings

Protected Domain Name ⓘ 1

www.example.com — 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)

You can enter a custom name for the domain name.

Website Remarks (Optional)

Enter remarks

Protected Port 2

Standard port — View Ports You Can Use

3 Standard ports 80 and 443 are the default ports reserved for HTTP and HTTPS protocols, respectively.

Server Configuration ⓘ

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

Add Address Origin server addresses you can add: 49

4 Proxy Your Website Uses ⓘ

Layer-7 proxy | Layer-4 proxy | ● No proxy

Table 3-3 Mandatory parameters

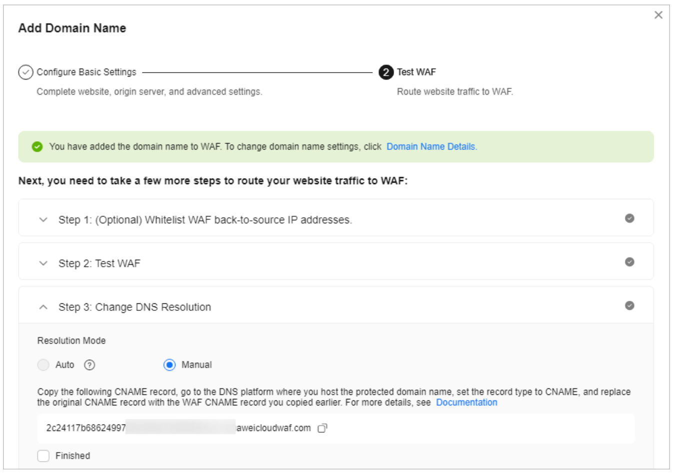
Parameter	Example Value	Description
Protected Domain Name	**www.example.com**	The domain name you want to add to WAF for protection.
Protected Port	**Standard port**	The port over which the website service traffic goes. To protect port 80 or 443, select **Standard port** from the drop-down list.

Parameter	Example Value	Description
Server Configuration	**Client Protocol**: **HTTP**. **Server Protocol**: **HTTP** **Server Address**: *IPv4 XXX.XXX.1.1* **Server Port**: **80**	Server address configuration. You need to configure the client protocol, server protocol, server address, and server port. ● **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. ● **Server Port**: service port over which the WAF instance forwards client requests to the origin server.

Parameter	Example Value	Description
Proxy Your Website Uses	**No proxy**	- **Layer-7 proxy**: Web proxy products for layer-7 request forwarding are used, products such as anti-DDoS, CDN, and other cloud acceleration services. - **Layer-4 proxy**: Web proxy products for layer-4 forwarding are used, products such as anti-DDoS. - **No proxy**: No proxy products are deployed in front of WAF. In our example, no proxies are used.

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

Figure 3-2 Basic settings completed



Add Domain Name

✓ Configure Basic Settings — Complete website, origin server, and advanced settings.

2 Test WAF — Route website traffic to WAF.

You have added the domain name to WAF. To change domain name settings, click Domain Name Details.

Next, you need to take a few more steps to route your website traffic to WAF:

Step 1: (Optional) Whitelist WAF back-to-source IP addresses.

Step 2: Test WAF

Step 3: Change DNS Resolution

Resolution Mode

○ Auto ● Manual

Copy the following CNAME record, go to the DNS platform where you host the protected domain name, set the record type to CNAME, and replace the original CNAME record with the WAF CNAME record you copied earlier. For more details, see Documentation

2c24117b68624997[redacted]aweicloudwaf.com

□ Finished

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 3-2.

   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 4: 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.

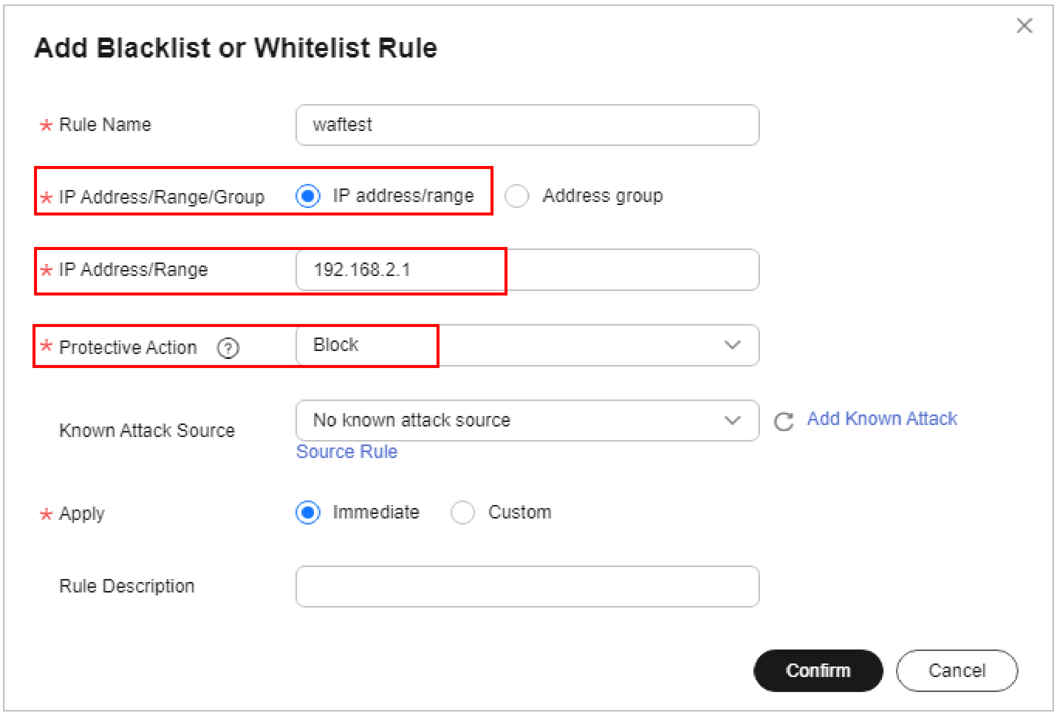
Step 3 Choose **Blacklist and Whitelist** and enable it.

- : enabled
- : disabled

Step 4 Above the blacklist and whitelist rule list, click **Add Rule** and configure a rule as shown in **Figure 3-3**.

- **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 3-3 Blocking a specified ip address



Add Blacklist or Whitelist Rule

* Rule Name: waftest

* IP Address/Range/Group: ● IP address/range ○ Address group

* IP Address/Range: 192.168.2.1

* Protective Action: Block

Known Attack Source: No known attack source

* Apply: ● Immediate ○ Custom

Rule Description:

Step 5 Click **Confirm**.

----End

Related Information

- For details, see **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**.
- **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. **Buy a dedicated WAF instance**.

  b. **Connect your website to WAF (Dedicated Mode)**.

  c. **Step 4: 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 Domain Name to WAF for Websites with no Proxy Used**	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 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 make websites respond more fast.
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.

Practice		Description
	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.
	Combining WAF and HSS to Get Improved Web Tamper Protection	With HSS and WAF in place, you can stop worrying about web page tampering.
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: ● Identify publicly accessible origin servers. ● Configure access control policy to protect origin servers.
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.