

# Web Application Firewall

## Best Practices

**Issue** 54  
**Date** 2025-01-17



**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.

---

# Contents

---

<b>1 WAF Best Practices You May Need</b>	<b>1</b>
<b>2 Website Access Configuration</b>	<b>3</b>
2.1 Connecting a Website Without a Proxy to WAF in CNAME Access Mode	3
2.2 Combining AAD and WAF to Get All-Round Protection	10
2.3 Combining CDN and WAF to Get Improved Protection and Load Speed	21
2.4 Combining WAF and Layer-7 Load Balancers to Protect Services over Any Ports	31
2.5 Using WAF, ELB, and NAT Gateway to Protect Services Not Deployed on Our Cloud	38
<b>3 Website Protection Configuration Suggestions</b>	<b>44</b>
<b>4 Mitigating Web Security Vulnerabilities</b>	<b>47</b>
4.1 Java Spring Framework Remote Code Execution Vulnerability	47
4.2 Apache Dubbo Deserialization Vulnerability	48
4.3 DoS Vulnerability in the Open-Source Component Fastjson	49
4.4 Remote Code Execution Vulnerability of Fastjson	49
4.5 Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability (CNVD-C-2019-48814)	50
<b>5 Defending Against Challenge Collapsar (CC) Attacks</b>	<b>52</b>
5.1 Overview	52
5.2 Configuring CC Attack Protection for Common Scenarios	53
5.3 Limiting Accesses Through IP Address-based Rate Limiting	56
5.4 Limiting Accesses Through Cookie Field Configuration	58
5.5 Restricting Malicious Requests in Promotions by Using Cookies and HWWAFSESID	60
<b>6 Using WAF to Block Crawler Attacks</b>	<b>64</b>
<b>7 Verifying a Global Protection Whitelist Rule by Simulating Requests with Postman</b>	<b>77</b>
<b>8 Combining WAF and HSS to Improve Web Page Tampering Protection</b>	<b>86</b>
<b>9 Configuring Header Field Forwarding to Disable Response Packet Compression</b>	<b>92</b>
<b>10 Configuring Origin Server Security</b>	<b>97</b>
10.1 Using WAF to Improve Connection Security	97
10.2 Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers	108

---

<b>11 Using LTS to Analyze WAF Logs.....</b>	<b>114</b>
11.1 Using LTS to Query and Analyze WAF Access Logs.....	114
11.2 Using LTS to Analyze How WAF Blocks Spring Core RCE Vulnerabilities.....	121
11.3 Using LTS to Configure Block Alarms for WAF Rules.....	127
<b>12 Obtaining the Real Client IP Addresses.....</b>	<b>138</b>
<b>13 Configuring Alarms on Cloud Eye for Abnormal WAF Metrics.....</b>	<b>146</b>
<b>14 Migrating Protection Policies for Your Website.....</b>	<b>150</b>

# 1 WAF Best Practices You May Need

This document introduces some common scenarios Web Application Firewall (WAF) can be applied to and describes applicable solution details and operation guidelines, helping you quickly get started with WAF.

## WAF Best Practices

**Table 1-1** WAF best practices

Category	Reference
Website access configuration	<a href="#">Connecting a Website Without a Proxy to WAF in CNAME Access Mode</a>
	<a href="#">Combining AAD and WAF to Get All-Round Protection</a>
	<a href="#">Combining CDN and WAF to Get Improved Protection and Load Speed</a>
	<a href="#">Combining WAF and Layer-7 Load Balancers to Protect Services over Any Ports</a>
	<a href="#">Using WAF, ELB, and NAT Gateway to Protect Services Not Deployed on Our Cloud</a>
Policy configuration	<a href="#">Website Protection Configuration Suggestions</a>
	<a href="#">Using WAF to Defending Against CC Attacks</a>
	<a href="#">Using WAF to Block Crawler Attacks</a>
	<a href="#">Verifying a Global Protection Whitelist Rule by Simulating Requests with Postman</a>
	<a href="#">Combining WAF and HSS to Improve Web Page Tampering Protection</a>
	<a href="#">Configuring Header Field Forwarding to Disable Response Packet Compression</a>

Category	Reference
	<a href="#">Migrating Protection Policies for Your Website</a>
Using WAF to patch web vulnerabilities	<a href="#">Java Spring Framework Remote Code Execution Vulnerability</a>
	<a href="#">Apache Dubbo Deserialization Vulnerability</a>
	<a href="#">DoS Vulnerability in the Open-Source Component Fastjson</a>
	<a href="#">Remote Code Execution Vulnerability in the Open-Source Component Fastjson</a>
	<a href="#">Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability (CNVD-C-2019-48814)</a>
LTS log analysis	<a href="#">Using LTS to Query and Analyze WAF Access Logs</a>
	<a href="#">Using LTS to Analyze How WAF Blocks Spring Core RCE Vulnerabilities</a>
	<a href="#">Using LTS to Configure Block Alarms for WAF Rules</a>
Origin server security configuration	<a href="#">Using WAF to Improve Connection Security</a>
	<a href="#">Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers</a>
Obtaining real client IP addresses	<a href="#">Obtaining Real Client IP Addresses</a>
Configuring Alarms on Cloud Eye for Abnormal WAF Metrics	<a href="#">Configuring Alarms on Cloud Eye for Abnormal WAF Metrics</a>
Security and governance	<a href="#">Building a WAF with ModSecurity</a>

# 2 Website Access Configuration

---

## 2.1 Connecting a Website Without a Proxy to WAF in CNAME Access Mode

### Application Scenarios

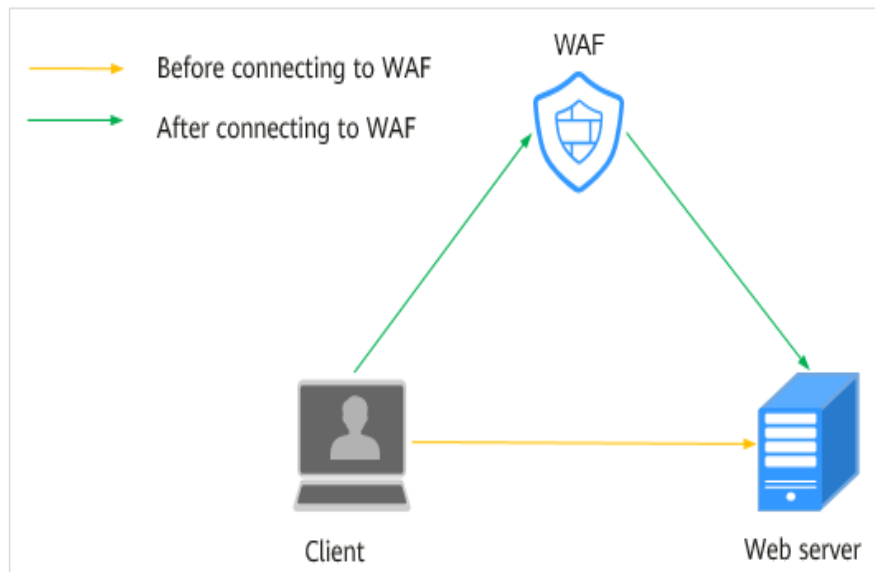
With the deepening of digital applications, web applications are widely used by most enterprises. Many web applications, such as enterprise websites, online shopping malls, and remote office systems, are publicly accessible. They are becoming major targets of hackers. According to historical data analysis, about 75% of information security attacks target web applications. In addition, web applications and components have more vulnerabilities than others. The critical Log4j vulnerability affected most web applications adversely.

This topic walks you through on how to add your website to WAF in cloud CNAME access mode when no proxies, such as anti-DDoS or CDN products, are used in front of WAF for your website.

### Architecture

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.

**Figure 2-1** No proxy used



## Advantages

After you enable cloud WAF for your website, the website traffic goes through WAF first. WAF examines HTTP/HTTPS requests to identify and block attacks such as SQL injections, cross-site scripting, web shells, command/code injections, file inclusion, sensitive file access, third-party application vulnerability exploits, CC attacks, malicious crawlers, and cross-site request forgery. Then, WAF forwards only legitimate traffic origin servers. In this way, WAF helps keep your website services secure and stable.

## Resource and Cost Planning

**Table 2-1** Resources and costs

Resource	Description	Monthly Fee
Web Application Firewall	Cloud - Standard edition <ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Number of domain names that can be protected: 10</li> <li>• QPS quota: 2,000 QPS</li> <li>• Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li> </ul>	For details about pricing rules, see <a href="#">Billing Description</a> .



## Step 1: Buy the Standard Edition Cloud WAF

- Step 1** [Log in to Huawei Cloud management console.](#)
- Step 2** On the management console page, choose **Security & Compliance > Web Application Firewall**.
- Step 3** In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select **Cloud Mode** for **WAF Mode**.
- **Region:** Select the region nearest to your services WAF will protect.
  - **Edition:** Select **Standard**.
  - **Expansion Package** and **Required Duration:** Set them based on site requirements.
- Step 4** Confirm the product details and click **Buy Now** in the lower right corner of the page.
- Step 5** Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
- Step 6** On the payment page, select a payment method and pay for your order.
- End

## Step 2: Add Website Information to WAF

- Step 1** In the navigation pane on the left, choose **Website Settings**.
- Step 2** In the upper left corner of the website list, click **Add Website**.
- Step 3** Select **Cloud - CNAME** and click **Configure Now**.
- Step 4** Configure website information as prompted.

**Figure 2-2** Configuring basic information

**Basic Settings**

Protected Domain Name ?  
 [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  
 [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 ▾ <input type="text" value="Enter a public IP ad"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	Delete

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

Use Layer-7 Proxy ?

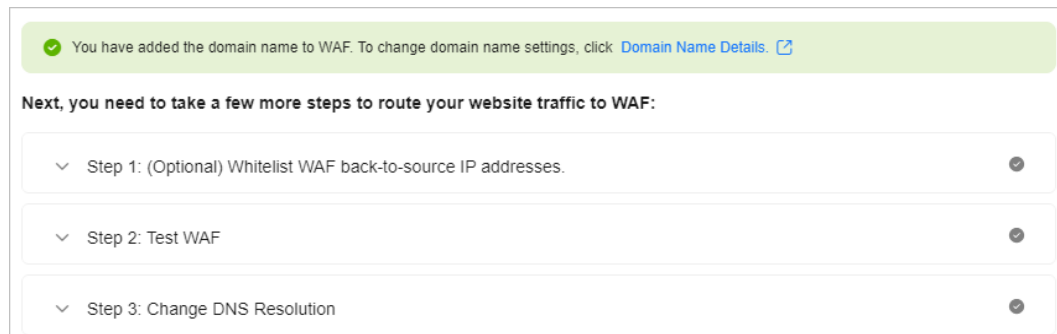
**Table 2-2** Key parameters

Parameter	Description	Example Value
Domain Name	Domain name you want to add to WAF. <ul style="list-style-type: none"> <li>The domain name has an ICP license.</li> <li>You can enter a single domain name (for example, top-level domain name <b>example.com</b> or level-2 domain name <b>www.example.com</b>) or a wildcard domain name (<b>*.example.com</b>).</li> </ul>	www.example.com
Protected Port	The port over which the website service traffic goes	Standard ports

Parameter	Description	Example Value
Server Configuration	<p>Web server address settings. You need to configure the client protocol, server protocol, server weights, server address, and server port.</p> <ul style="list-style-type: none"> <li>• <b>Client Protocol:</b> protocol used by a client to access a server. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>• <b>Server Protocol:</b> protocol used by WAF to forward client requests. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>• <b>Server Address:</b> public IP address (generally corresponding to the A record configured for the domain name on the DNS) or domain name (generally corresponding to the CNAME record configured for the domain name on the DNS) of the web server that a client accesses.</li> <li>• <b>Server Port:</b> service port over which the WAF instance forwards client requests to the origin server.</li> <li>• <b>Weight:</b> Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.</li> </ul>	<p><b>Client Protocol:</b> Select <b>HTTP</b>.</p> <p><b>Server Protocol:</b> <b>HTTP</b></p> <p><b>Server Address:</b> <i>IPv4 XXX.XXX.1.1</i></p> <p><b>Server Port:</b> <b>80</b></p>
Use Layer-7 Proxy	You need to configure whether you deploy other layer-7 proxies in front of WAF. Select <b>No</b> .	No

**Step 5** Click **Next**. Then, [whitelist WAF back-to-source IP addresses](#) and [test WAF](#) as prompted.

**Figure 2-3** Domain name added to WAF





----End

### Step 3: Complete CNAME Access

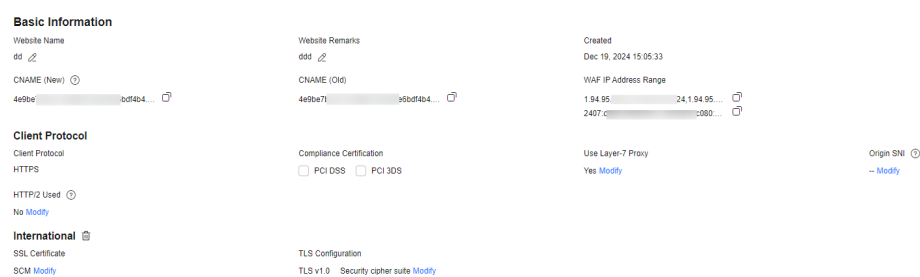
If the **Type** of the domain name host record added on DNS is **CNAME - Map one domain to another**, add the domain name to WAF by following the steps below.

The methods to change DNS records on different DNS platforms are similar. The following example is based on our Domain Name Service (DNS).

#### Step 1 Obtain the CNAME record.

1. Click  in the upper left corner of the management console and select a region or project.
2. Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
3. In the navigation pane, choose **Website Settings**.
4. In the **Domain Name** column, click the target domain name to go to the **Basic Information** page.

**Figure 2-4** Basic Information

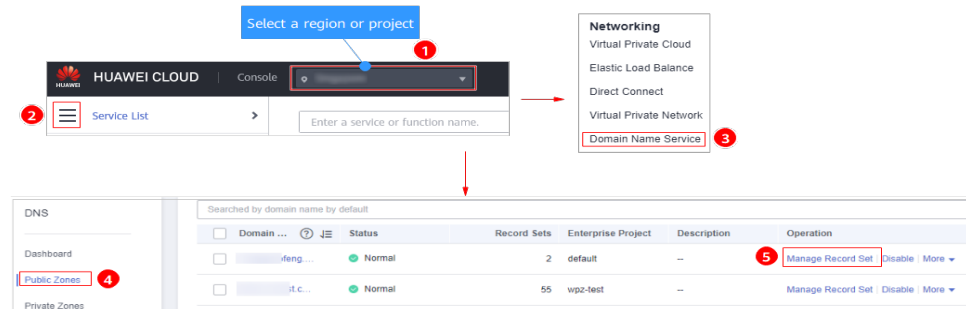


5. In the **CNAME** row, click  to copy the CNAME record.

#### Step 2 Change the DNS settings.

1. Access the DNS resolution page, as shown in [Figure 2-5](#).

Figure 2-5 DNS page



2. In the **Operation** column of the target domain name, click **Modify**. The **Modify Record Set** page is displayed.
3. In the displayed **Modify Record Set** dialog box, change the record.
  - **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 copied CNAME value from WAF.
  - Keep other settings unchanged.

**NOTE**

About modifying the resolution record:

- The CNAME record must be unique for the same host record. The existing CNAME record must be changed to the WAF CNAME record.
- Record sets of different types in the same zone may conflict with each other. For example, for the same host record, the CNAME record conflicts with another record, such as the A record, MX record, or TXT record. If the record type cannot be changed, you can delete the conflicting records and add a CNAME record. Deleting other records and adding a CNAME record should be completed in as short time as possible. If no CNAME record is added after the A record is deleted, domain resolution may fail.

For details about the restrictions on domain name resolution types, see [Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?](#)

Figure 2-6 Modifying a record set

**Modify Record Set** ✕

Name:

Type:

Alias:  Yes  No

Line:  ?

\* TTL (s):      ?

\* Value:  ?

Weight:

Other Settings:

4. Click **OK**.

**Step 3** (Optional) Ping the IP address of your domain name to check whether the new DNS settings take effect.

**NOTE**

It takes some time for the new DNS settings to take effect. If ping fails, wait for 5 minutes and ping again.

----End

## 2.2 Combining AAD and WAF to Get All-Round Protection

### Application Scenarios

With the deepening of digital applications, web applications are widely used by most enterprises. Many web applications, such as enterprise websites, online shopping malls, and remote office systems, are publicly accessible. They are becoming major targets of hackers. According to historical data analysis, about 75% of information security attacks target web applications. In addition, web applications and components have more vulnerabilities than others. The critical Log4j vulnerability affected most web applications adversely.

If your website has been protected with AAD already, you can use WAF as well to give better protection to the website.

#### NOTE

For details about how to connect your website to AAD, see [Configuring a Protected Domain Name \(Website Services\)](#).

## Architecture

- **Advanced Anti-DDoS** works as a proxy and uses AAD IP address to forward requests to origin servers. All public network traffic is diverted to the AAD IP address so that the origin server is hidden from the public. This protects origin servers from DDoS attacks.

Objects supported by AAD: domain names of web applications on Huawei Cloud, other cloud platforms, or on-premises data centers

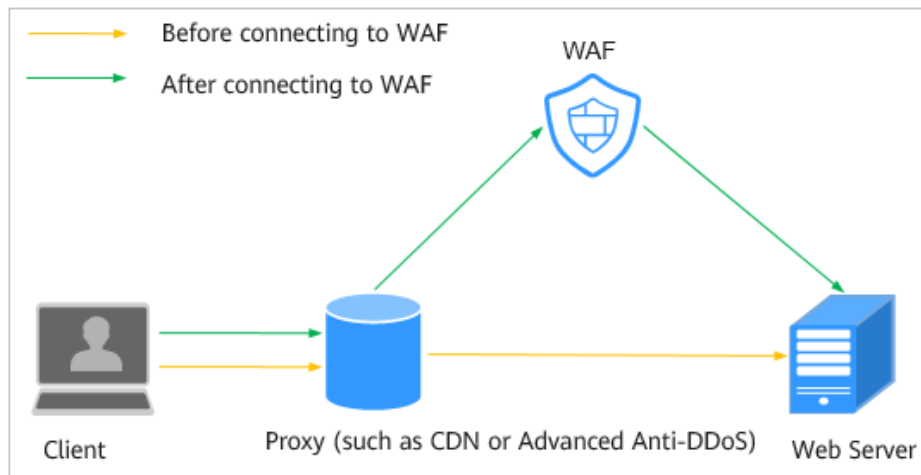
- Web Application Firewall (WAF) keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block the following attacks: Structured Query Language (SQL) injections, cross-site scripting (XSS), web shells, command and code injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

When adding a website to WAF, you can select **Cloud Mode - CNAME**, **Cloud Mode - Load balancer**, or **Dedicated Mode**. Before you start, get familiar with their differences:

- **Cloud Mode - CNAME**: protects your web applications that have domain name and are deployed on any clouds or in on-premises data centers.
- **Cloud Mode - Load balancer**: protects your web applications that are deployed on Huawei Cloud and accessible over domain names or IP addresses (public or private IP addresses).
- **Dedicated Mode**: protects your web applications that are deployed on Huawei Cloud and accessible over domain names or IP addresses (public or private IP addresses).

You can deploy both AAD and WAF to protect your websites hosted on Huawei Cloud, other clouds, or in on-promises data centers. The combination of AAD and WAF can protect your website against DDoS attacks (such as NTP flood, SYN flood, ACK flood, ICMP flood, and HTTP Get flood attacks), web application attacks (such as SQL injection, cross-site scripting, web shells, command/code injection, file inclusion, sensitive file access, third-party application vulnerability attacks, CC attacks, malicious crawler scanning, and cross-site request forgery). [Figure 2-7](#) shows the configuration.

**Figure 2-7** WAF configuration when a proxy is used



If you configure AAD and WAF for your website, website traffic goes to AAD first. AAD scrubs incoming traffic and forwards clean traffic to WAF. WAF blocks attacks and forwards only the normal traffic to the origin server. In this way, two layers of protection are implemented on your website.



The configurations are as follows:

- **Cloud - CNAME**  
Point the website domain name to AAD and change the AAD retrieval IP address to the WAF CNAME record. To prevent others from configuring your domain names on WAF in advance (this will cause interference on your domain name protection), add the subdomain name and TXT record on your DNS management platform.
- **Cloud - Load balancer**  
Resolve the domain name to AAD, modify the AAD retrieval IP address to the EIP bound to the load balancer selected in [Add a Website to WAF \(ELB Mode\)](#).
- **Dedicated mode**  
Point your website domain name to AAD and change the AAD retrieval IP address to the EIP bound to the load balancer configured for your dedicated WAF instance.

## Advantages

You can deploy both AAD and WAF to protect your website against DDoS attacks (such as NTP flood, SYN flood, ACK flood, ICMP flood, and HTTP Get flood attacks), web application attacks (such as SQL injection, cross-site scripting, web shells, command/code injection, file inclusion, sensitive file access, third-party application vulnerability attacks, CC attacks, malicious crawler scanning, and cross-site request forgery).



## Resource and Cost Planning

**Table 2-3** Resources and costs

Resource	Description	Monthly Fee
DDoS protection	<ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Basic protection bandwidth: 10 Gbit/s</li> <li>• Elastic protection bandwidth: 10 Gbit/s</li> <li>• Service bandwidth: 100 Mbit/s</li> <li>• Domain name protection quota: 50</li> </ul>	For details about billing rules, see <a href="#">Billing Description</a> .
Web Application Firewall	Cloud - Standard edition <ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Number of domain names that can be protected: 10</li> <li>• QPS quota: 2,000 QPS</li> <li>• Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li> </ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

### Constraints

- Joint protection with AAD and WAF is only for domain names.
- If your website uses proxies such as anti-DDoS, Content Delivery Network (CDN), and cloud acceleration services, select **Per user** for **Rate Limit Mode** and enable **All WAF instances** for your CC attack protection rules.

### Step 1: Buy the Standard Edition Cloud WAF

The following describes how to buy the standard edition cloud WAF.

- Step 1** [Log in to Huawei Cloud management console](#).
- Step 2** On the management console page, choose **Security & Compliance > Web Application Firewall**.
- Step 3** In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select **Cloud Mode** for **WAF Mode**.
  - **Region:** Select the region nearest to your services WAF will protect.
  - **Edition:** Select **Standard**.

- **Expansion Package and Required Duration:** Set them based on site requirements.

**Step 4** Confirm the product details and click **Buy Now** in the lower right corner of the page.

**Step 5** Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.

**Step 6** On the payment page, select a payment method and pay for your order.

----End

## Step 2: Add Website Information to WAF

The following example shows how to add a website information to WAF in cloud CNAME access mode.

- For details about the cloud load balancer access mode, see [Connecting a Website to WAF \(Cloud Mode - ELB Access\)](#).
- For details about the dedicated mode, see [Connecting a Website to WAF \(Dedicated Mode\)](#).

**Step 1** In the navigation pane on the left, choose **Website Settings**.

**Step 2** In the upper left corner of the website list, click **Add Website**.

**Step 3** Select **Cloud - CNAME** and click **Configure Now**.

**Step 4** Configure website information as prompted.

**Figure 2-8** Configuring basic information

**Basic Settings**

Protected Domain Name ?

[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

[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
<input type="text" value="HTTP"/>	<input type="text" value="HTTP"/>	<input type="text" value="IPv4"/> <input type="text" value="Enter a public IP ad"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	<a href="#">Delete</a>

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

Use Layer-7 Proxy ?

Yes  No

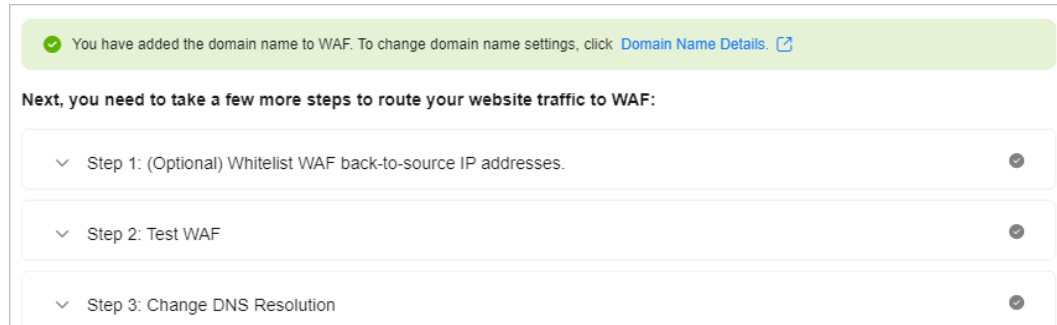
**Table 2-4** Key parameters

Parameter	Description	Example Value
Domain Name	Domain name you want to add to WAF for protection. <ul style="list-style-type: none"> <li>• The domain name has an ICP license.</li> <li>• You can enter a single domain name (for example, top-level domain name <b>example.com</b> or level-2 domain name <b>www.example.com</b>) or a wildcard domain name (<b>*.example.com</b>).</li> </ul>	www.example.com
Protected Port	The port over which the website traffic goes	Standard ports

Parameter	Description	Example Value
Server Configuration	<p>Web server address settings. You need to configure the client protocol, server protocol, server weights, server address, and server port.</p> <ul style="list-style-type: none"> <li>● <b>Client Protocol:</b> protocol used by a client to access a server. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Protocol:</b> protocol used by WAF to forward client requests. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Address:</b> 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.</li> <li>● <b>Server Port:</b> service port over which the WAF instance forwards client requests to the origin server.</li> <li>● <b>Weight:</b> Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.</li> </ul>	<p><b>Client Protocol:</b> Select <b>HTTP</b>.</p> <p><b>Server Protocol:</b> <b>HTTP</b></p> <p><b>Server Address:</b> <i>IPv4 XXX.XXX.1.1</i></p> <p><b>Server Port:</b> <b>80</b></p>
Use Layer-7 Proxy	<p>You need to configure whether you deploy other layer-7 proxies in front of WAF. Select <b>Yes</b>.</p> <p><b>NOTE</b> If you deploy AAD before WAF for your website, to let WAF obtain the real IP address of the client, you need to set <b>IP Tag</b> to <b>\$remote_addr</b> in the <b>Traffic Identifier</b> area on the basic information page for the protected domain name. For details, see <a href="#">Configuring a Traffic Identifier for a Known Attack Source</a>.</p>	Yes

- Step 5** Click **Next**. Then, **whitelist WAF back-to-source IP addresses** and **test WAF** as prompted.

**Figure 2-9** Domain name added to WAF



----End





### Step 3: Resolve the Domain Name

On the Advanced Anti-DDoS page, add the CNAME record of WAF to let the traffic pass through WAF.


### Cloud CNAME Mode Configuration

The methods to configure the DNS server are similar. The following uses Huawei Cloud AAD as an example.

**Step 1** Obtain settings of **CNAME**, **Subdomain Name**, and **TXT Record**.

1. Log in to the management console.
2. Click  in the upper left corner of the management console and select a region or project.
3. Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
4. In the **Protected Website** column, click the domain name you want to go to the **Basic Information** page.
5. Check that **Use Layer-7 Proxy** is set to **Yes**.
6. Click  in the **CNAME** row to copy CNAME records. On the top of the page, click  next to **Inaccessible**. In the dialog box displayed, copy the subdomain name and TXT record.

**Step 2** Change the back-to-source IP address of the AAD instance.

1. Click  at the top of the page and choose **Security & Compliance > DDoS Mitigation**. In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access** to go to the domain name configuration page.
2. In the **Operation** column of the target domain name, click **Edit**. On the displayed page, set **Origin Server IP Address/Domain Name** to the copied WAF CNAME record.

3. Click **OK**.

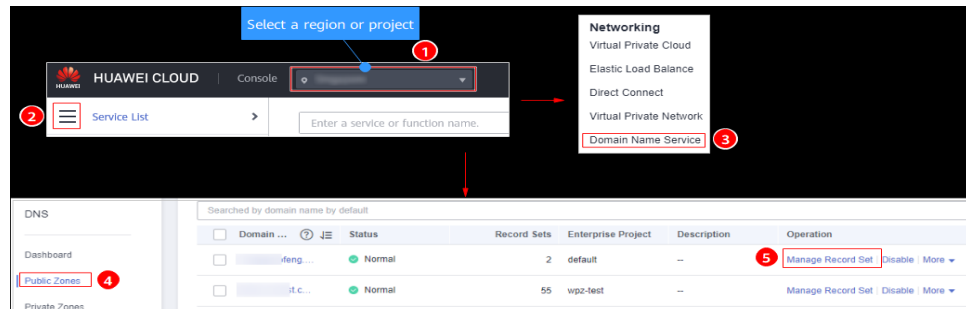
**Step 3** (Optional) Add a WAF subdomain name and TXT record at your DNS provider.

**NOTE**

To prevent others from configuring your domain names on WAF in advance (this will cause interference on your domain name protection), this step is recommended.

1. Access the DNS resolution page.

**Figure 2-10** DNS page



2. In the upper right corner of the page, click **Add Record Set**. The **Add Record Set** page is displayed.
  - **Name:** TXT record copied in [Step 1.6](#).
  - **Type:** Select **TXT – Specify text records**.
  - **Alias:** Select **No**.
  - **Line:** Select **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:** Add quotation marks to the TXT record copied in [Step 1.6](#) and paste them in the text box, for example, **TXT record**.
  - Keep other settings unchanged.

**Figure 2-11** Adding a record set

**Add Record Set**

[Add Record Sets for Email Domain](#)

Type  
TXT – Specify text records

Name  
37c795804124dd4a0dd88defff8941f .example1.com

Line ?  
Default

TTL (s) ?  
300

Value ?  
"37c795804124dd4a0dd88defff8941f"

3. Click **OK**.

**Step 4** (Optional) Ping the IP address of your domain name to check whether the new DNS settings take effect.

**NOTE**


It takes some time for the new DNS settings to take effect. If ping fails, wait for 5 minutes and ping again.


----End

## How to Configure in Dedicated/Load Balancer Access Modes

Perform the following steps to complete configurations on Huawei Cloud AAD:

**Step 1** [Log in to the management console](#).

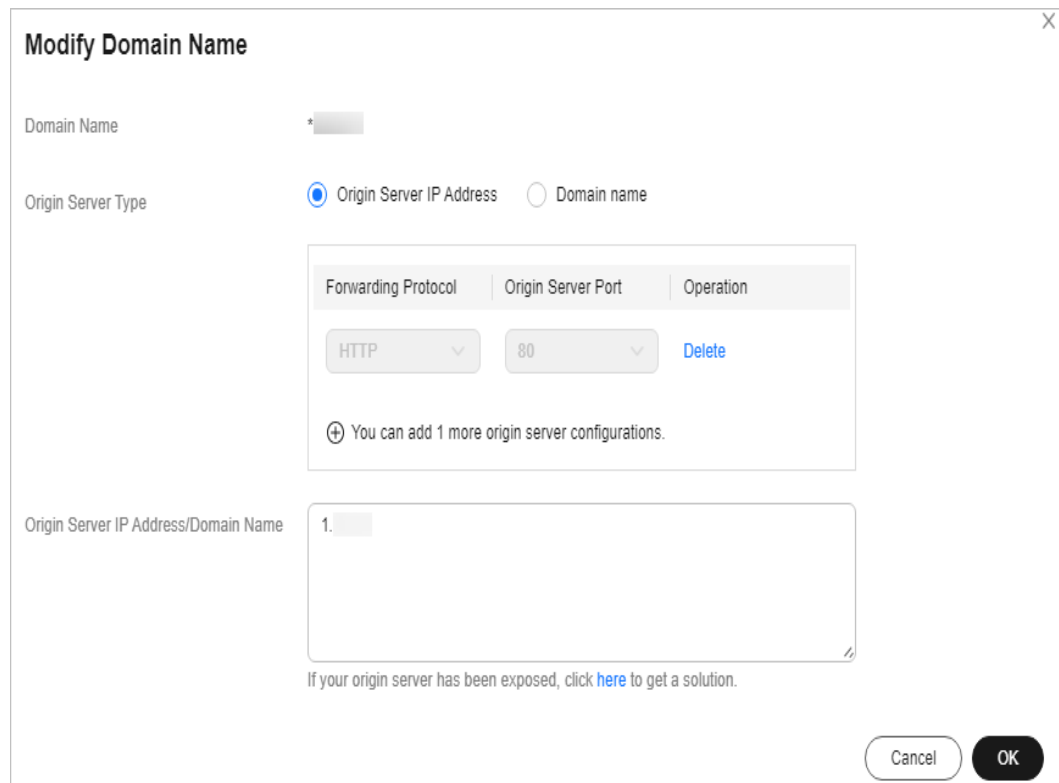
**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click  in the upper left corner of the page and choose **Security & Compliance > DDoS Mitigation**.

**Step 4** In the navigation pane on the left, choose **Advanced Anti-DDoS > Domain Name Access** to go to the **Domain Name Access** page.

- Step 5** In the row containing the domain name you want, click **Modify** in the **Operation** column.
- Step 6** In the **Modify Domain Name** dialog box, change the origin server IP address. **Figure 2-12** shows an example.

**Figure 2-12** Changing the origin server IP address



#### NOTICE

- If you use a dedicated WAF instance, in the **Origin Server IP Address/Domain Name** text box, **enter the EIP you bind to the load balancer**.
- If you use a cloud WAF instance and select ELB load balancer access for your services, enter the EIP bound to the load balancer selected in **Add a Website to WAF (ELB Mode)** in the **Origin Server IP Address/Domain Name** text box.

**Step 7** Click **OK**.


----End

## Verification

If **Access Status** is **Accessible**, the traffic destined for your website domain name or IP address is routed to WAF.



**NOTICE**

- WAF automatically checks the access status of protected websites every hour. If WAF detects that a protected website has received 20 access requests within 5 minutes, it considers that the website has been successfully connected to WAF.
- By default, WAF checks only the access status of domain names added or updated over the last two weeks. If a domain name was added to WAF two weeks ago and has not been modified in the last two weeks, you can click  in the **Access Status** column to refresh its status.

If a domain name fails to be connected to WAF, its access status is **Inaccessible**. To fix this issue, see [Why Is the Access Status of a Domain Name or IP Address Inaccessible?](#)

## 2.3 Combining CDN and WAF to Get Improved Protection and Load Speed

### Application Scenarios

With the deepening of digital applications, web applications are widely used by most enterprises. Many web applications, such as enterprise websites, online shopping malls, and remote office systems, are publicly accessible. They are becoming major targets of hackers. According to historical data analysis, about 75% of information security attacks target web applications. In addition, web applications and components have more vulnerabilities than others. The critical Log4j vulnerability affected most web applications adversely.

If your website has used CDN already, you can use WAF as well to give extra protection to the website.

** NOTE**

For details about how to use CDN for a website, see [Enabling CDN](#).

If you have configured a domain name for **website acceleration** in CDN, you can use EdgeSec to add the domain name to WAF to implement security functions such as network acceleration, web attack defense, anti-DDoS, and CC attack defense. For details, see [Adding a Website to WAF](#).

### Architecture

- When a user accesses a website that uses Huawei Cloud CDN, the local DNS server will redirect all domain requests to CDN using CNAME records. **CDN** uses a group of predefined policies (such as the content type, geographical location, and network load status) to respond visitors with the nearest CDN IP address so that visitors can obtain requested website content as quickly as possible.  
Objects supported by CDN: domain names of web applications on Huawei Cloud, other cloud platforms, or on-premises data centers
- Web Application Firewall (WAF) keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block the following

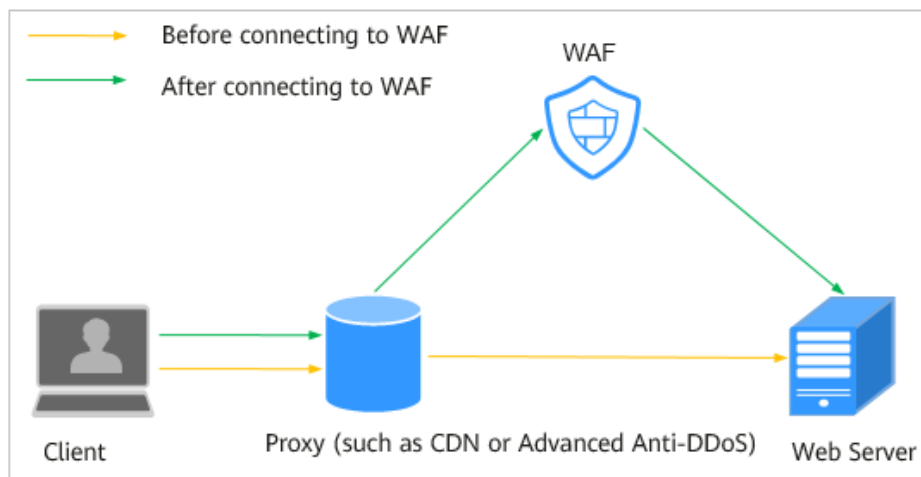
attacks: Structured Query Language (SQL) injections, cross-site scripting (XSS), web shells, command and code injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

When adding a website to WAF, you can select **Cloud Mode - CNAME**, **Cloud Mode - Load balancer**, or **Dedicated Mode**. Before you start, get familiar with their differences:

- **Cloud Mode - CNAME:** protects your web applications that have domain name and are deployed on any clouds or in on-premises data centers.
- **Cloud Mode - Load balancer:** protects your web applications that are deployed on Huawei Cloud and accessible over domain names or IP addresses (public or private IP addresses).
- **Dedicated Mode:** protects your web applications that are deployed on Huawei Cloud and accessible over domain names or IP addresses (public or private IP addresses).

The combination of CDN and WAF can protect websites on Huawei Cloud, other clouds, or on-premises and improve website response time. **Figure 2-13** shows the configuration diagram.

**Figure 2-13** WAF configuration when a proxy is used



After you deploy CDN and WAF for your website, traffic is accelerated by CDN and then forwarded to WAF. WAF checks received traffic and forwards only the normal traffic to the origin server. The combination protects the website against attacks while improving the website response speed and availability.

Point your website domain name to CDN and then change the CDN back-to-source address to the WAF CNAME record. After that, you can also add a WAF subdomain name and TXT record on your DNS management platform in case others have connected the website domain name to WAF before you configure CDN.



The configurations are as follows:

- Cloud - CNAME  
Point your website domain name to CDN and then change the CDN back-to-source address to the WAF CNAME record. After that, you can also add a WAF subdomain name and TXT record on your DNS management platform in case others have connected the website domain name to WAF before you configure CDN.
- Cloud - Load balancer  
Point your website domain name to CDN and change the CDN back-to-source IP address to the EIP bound to the load balancer configured for your load-balancing WAF instance.
- Dedicated mode  
Point your website domain name to CDN and change the CDN back-to-source IP address to the EIP bound to the load balancer configured for your dedicated WAF instance.

## Advantages

With both CDN and WAF deployed, your website will be accelerated with CDN while being protected with WAF. This combination will shorten website content access delay, speed up website response, and improve website availability. You can stop worrying about low network bandwidth, large user access traffic, and uneven distribution of branches. Besides that, this combination will protect your website from web application attacks, such as SQL injections, cross-site scripting (XSS), web shells, command/code injections, file inclusion, sensitive file access, third-party application vulnerability exploits, CC attacks, malicious crawlers, and cross-site request forgery.

## Resource and Cost Planning

**Table 2-5** Resources and costs

Resource	Description	Monthly Fee
CDN	<ul style="list-style-type: none"> <li>● <b>Billing Mode:</b> Select <b>Pay-per-use</b>.</li> <li>● Resource packages can be used.</li> </ul>	For details about billing rules, see <a href="#">Billing Description</a> .

Resource	Description	Monthly Fee
Web Application Firewall	Cloud - Standard edition <ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Number of domain names that can be protected: 10</li> <li>• QPS quota: 2,000 QPS</li> <li>• Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li> </ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

## Constraints

If you select cloud mode CNAME access for protection and your website uses proxies such as anti-DDoS, Content Delivery Network (CDN), and cloud acceleration services before WAF, select **Per user** for **Rate Limit Mode** and enable **All WAF instances** for your CC attack protection rules.

## Step 1: Buy the Standard Edition Cloud WAF

The following describes how to buy the standard edition cloud WAF.

- Step 1** [Log in to Huawei Cloud management console](#).
- Step 2** On the management console page, choose **Security & Compliance > Web Application Firewall**.
- Step 3** In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select **Cloud Mode** for **WAF Mode**.
  - **Region:** Select the region nearest to your services WAF will protect.
  - **Edition:** Select **Standard**.
  - **Expansion Package** and **Required Duration:** Set them based on site requirements.
- Step 4** Confirm the product details and click **Buy Now** in the lower right corner of the page.
- Step 5** Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
- Step 6** On the payment page, select a payment method and pay for your order.

----End

## Step 2: Add Website Information to WAF

The following example shows how to add a website information to WAF in cloud CNAME access mode.

- For details about the cloud load balancer access mode, see [Connecting a Website to WAF \(Cloud Mode - ELB Access\)](#).
- For details about the dedicated mode, see [Connecting a Website to WAF \(Dedicated Mode\)](#).

**Step 1** In the navigation pane on the left, choose **Website Settings**.

**Step 2** In the upper left corner of the website list, click **Add Website**.

**Step 3** Select **Cloud - CNAME** and click **Configure Now**.

**Step 4** Configure website information as prompted.

**Figure 2-14** Configuring basic information

**Basic Settings**

Protected Domain Name [?](#)  
 [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  
 [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
<input type="text" value="HTTP"/>	<input type="text" value="HTTP"/>	<input type="text" value="IPv4"/> <input type="text" value="Enter a public IP ad"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	Delete

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

Use Layer-7 Proxy [?](#)  
 Yes  No

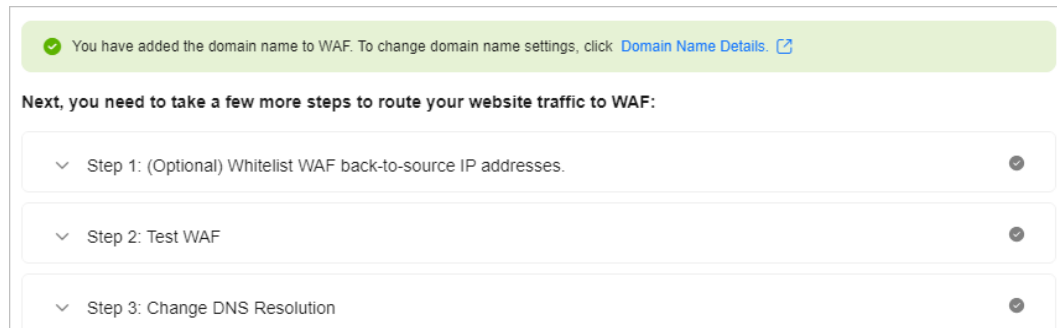
**Table 2-6** Key parameters

Parameter	Description	Example Value
Domain Name	Domain name you want to add to WAF for protection. <ul style="list-style-type: none"> <li>• The domain name has an ICP license.</li> <li>• You can enter a single domain name (for example, top-level domain name <b>example.com</b> or level-2 domain name <b>www.example.com</b>) or a wildcard domain name (<b>*.example.com</b>).</li> </ul>	www.example.com
Protected Port	The port over which the website traffic goes	Standard ports

Parameter	Description	Example Value
Server Configuration	<p>Web server address settings. You need to configure the client protocol, server protocol, server weights, server address, and server port.</p> <ul style="list-style-type: none"> <li>● <b>Client Protocol:</b> protocol used by a client to access a server. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Protocol:</b> protocol used by WAF to forward client requests. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Address:</b> 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.</li> <li>● <b>Server Port:</b> service port over which the WAF instance forwards client requests to the origin server.</li> <li>● <b>Weight:</b> Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.</li> </ul>	<p><b>Client Protocol:</b> Select <b>HTTP</b>.</p> <p><b>Server Protocol:</b> <b>HTTP</b></p> <p><b>Server Address:</b> <i>IPv4 XXX.XXX.1.1</i></p> <p><b>Server Port:</b> <b>80</b></p>
Use Layer-7 Proxy	<p>You need to configure whether you deploy other layer-7 proxies in front of WAF. Select <b>Yes</b>.</p> <p><b>NOTE</b> If you deploy AAD before WAF for your website, to let WAF obtain the real IP address of the client, you need to set <b>IP Tag</b> to <b>\$remote_addr</b> in the <b>Traffic Identifier</b> area on the basic information page for the protected domain name. For details, see <a href="#">Configuring a Traffic Identifier for a Known Attack Source</a>.</p>	Yes

- Step 5** Click **Next**. Then, **whitelist WAF back-to-source IP addresses** and **test WAF** as prompted.

**Figure 2-15** Domain name added to WAF



----End





### Step 3: Resolve the Domain Name

On the CDN page, add the CNAME record of WAF to let the traffic pass through WAF.

### How to Configure in Cloud Mode

The following uses Huawei Cloud CDN as an example to describe how to configure domain name resolution. If you use Huawei Cloud CDN, perform the following steps directly. If you use non-Huawei Cloud CDN, configure domain name resolution on non-Huawei Cloud CDN based on the instructions in the following steps.

**Step 1** Obtain settings of **CNAME**, **Subdomain Name**, and **TXT Record**.

1. Log in to the management console.
2. Click  in the upper left corner of the management console and select a region or project.
3. Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
4. In the navigation pane on the left, choose **Website Settings**.
5. In the row containing the desired domain name, click the domain name to go to the **Basic Information** page.
6. On the basic information page for the domain name, click  in the **CNAME** row and copy the CNAME records. On the top of the page, click  next to **Inaccessible**. In the dialog box displayed, copy the subdomain name and TXT record.

**Step 2** **Change the origin server domain name of the primary origin server of CDN to the CNAME of WAF.**

**Step 3** (Optional) Add a WAF subdomain name and TXT record at your DNS provider.

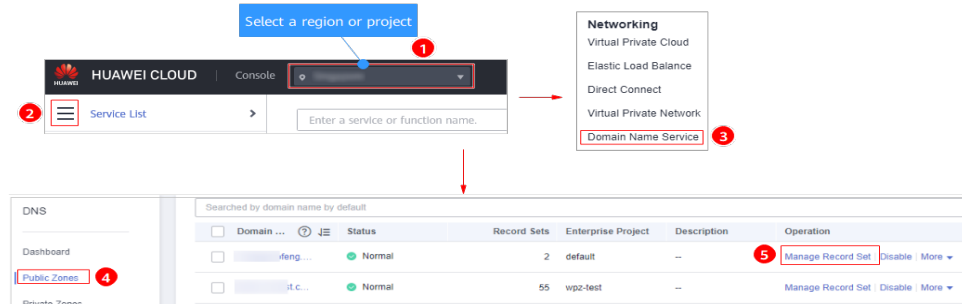


 NOTE

To prevent others from configuring your domain names on WAF in advance (this will cause interference on your domain name protection), this step is recommended.

1. Access the DNS resolution page, as shown in [Figure 2-16](#).

**Figure 2-16** DNS page



2. In the upper right corner of the page, click **Add Record Set**. The **Add Record Set** page is displayed. [Figure 2-17](#) shows an example.
  - **Name:** TXT record copied in [Step 1.6](#).
  - **Type:** Select **TXT – Specify text records**.
  - **Alias:** Select **No**.
  - **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:** Add quotation marks to the TXT record copied in [Step 1.6](#) and paste them in the text box, for example, **TXT record**.
  - Keep other settings unchanged.


**Figure 2-17** Adding a record set


**Add Record Set**


[Add Record Sets for Email Domain](#)

Type

Name  
 .example.com

Line 

TTL (s) 

Value 

3. Click **OK**.

**Step 4** (Optional) Ping the IP address of your domain name to check whether the new DNS settings take effect.

 **NOTE**


It takes some time for the new DNS settings to take effect. If ping fails, wait for 5 minutes and ping again.


----End

## Configuration of Dedicated/ELB WAF

Perform the following steps to complete configurations on Huawei Cloud CDN:

**Step 1** [Log in to the management console](#).

**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click  in the upper left corner of the page and choose **Content Delivery & Edge Computing > Content Delivery Network**.

**Step 4** In the navigation pane on the left, choose **Domains**.

**Step 5** In the domain list, click the target domain name or click **Configure** in the **Operation** column.

**Step 6** Click the **Basic Settings** tab. In the **Origin Server Settings** area, click **Edit**.

- If you use a dedicated WAF instance, in the **Server Address** text box, **enter the EIP you bind to the load balancer**.
- If you use a cloud WAF instance and select the load balancer access mode, in the **Address** text box, enter the EIP bound to the ELB load balancer selected in **Add a Website to WAF (ELB Mode)**.

**Step 7** Click **Save**.


----End

## Verification

If **Access Status** is **Accessible**, the traffic destined for your website domain name or IP address is routed to WAF.

---

### NOTICE

- WAF automatically checks the access status of protected websites every hour. If WAF detects that a protected website has received 20 access requests within 5 minutes, it considers that the website has been successfully connected to WAF.
- By default, WAF checks only the access status of domain names added or updated over the last two weeks. If a domain name was added to WAF two weeks ago and has not been modified in the last two weeks, you can click  in the **Access Status** column to refresh its status.

---

If a domain name fails to be connected to WAF, its access status is **Inaccessible**. To fix this issue, see [Why Is the Access Status of a Domain Name or IP Address Inaccessible?](#)

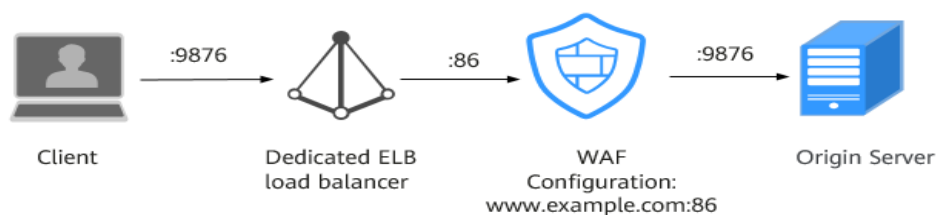
## 2.4 Combining WAF and Layer-7 Load Balancers to Protect Services over Any Ports

### Application Scenarios

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 supported by WAF, see [Ports Supported by WAF](#).

### Architecture

The following procedure describes how WAF and ELB together protect **www.example.com:9876**. Port 9876 is a non-standard port WAF alone cannot protect.



## Advantages

This solution makes it possible for WAF to protect your services over any ports.

## Resource and Cost Planning

**Table 2-7** Resources and costs

Resource	Description	Monthly Fee
Elastic Load Balance (ELB)	<ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Instance type: Dedicated</li> <li>• Specifications: application type (HTTP/HTTPS); small II</li> <li>• <b>Billed By: Bandwidth</b></li> <li>• <b>Bandwidth: 10 Mbit/s</b></li> </ul>	For details about billing rules, see <a href="#">Billing Description</a> .

Resource	Description	Monthly Fee
Web Application Firewall	<p>Dedicated mode:</p> <ul style="list-style-type: none"> <li>● <b>Billing Mode:</b> Select <b>Pay-per-use</b>.</li> <li>● Number of domain names that can be protected: 2,000</li> <li>● Specifications: WI-500. Referenced performance: <ul style="list-style-type: none"> <li>- HTTP services: 5,000 QPS (recommended)</li> <li>- HTTPS services: 4,000 QPS (recommended)</li> <li>- WebSocket service - Maximum concurrent connections: 5,000</li> <li>- Maximum WAF-to-server persistent connections: 60,000</li> </ul> </li> <li>● Specifications: WI-100. Referenced performance: <ul style="list-style-type: none"> <li>- HTTP services: 1,000 QPS (recommended)</li> <li>- HTTPS services: 800 QPS (recommended)</li> <li>- WebSocket service - Maximum concurrent connections: 1,000</li> <li>- Maximum WAF-to-server persistent connections: 60,000</li> </ul> </li> </ul>	-

### Prerequisites

- You have purchased a dedicated layer-7 load balancer. For details about load balancer types, see [Differences Between Dedicated and Shared Load Balancers](#).

 **NOTE**

Dedicated WAF instances issued before April 2023 cannot be used with dedicated network load balancers. If you use a dedicated network (TCP/UDP) load balancer, make sure your dedicated WAF instance has been upgraded to the latest version (version later than 202304). You can check the version you are using in the **Version** column of the target dedicated WAF instance on the **Dedicated Engine** page.

- Related ports have been enabled in the security group to which the dedicated WAF instance belongs.

You can configure your security group as follows:

- Inbound rules

Add an inbound rule to allow incoming network traffic to pass through over a specified port based on your service requirements. For example, if you want to allow access from port 80, add a rule that allows **TCP** and port **80**.

- Outbound rules

Retain the default settings. All outgoing network traffic is allowed by default.

For more details, see [Adding a Security Group Rule](#).

## Procedure

**Step 1** [Log in to Huawei Cloud management console](#).

**Step 2** On the management console page, choose **Security & Compliance > Web Application Firewall**.

**Step 3** In the navigation pane on the left, choose **Website Settings**.

**Step 4** Click **Add Website**.

**Step 5** Select **Dedicated Mode** and click **Configure Now**.

**Step 6** Connect www.example.com to WAF by referring to [Adding a Website to WAF \(Dedicated Mode\)](#). Select any non-standard port as the protected port, for example, port 86, set **Server Port** to **9876**, and set **Use Layer-7 Proxy** to **Yes**.

**Figure 2-18** Adding a domain name to WAF

**Basic Settings**

Protected Domain Name ?  
 [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  
 [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 <input type="text" value="Enter a public IP ad"/>	9876	1	Delete

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

Use Layer-7 Proxy ?

**Step 7** Add listeners and backend server groups to the load balancer.

1. Click  in the upper left corner of the page and choose **Elastic Load Balance** under **Networking** to go to the **Load Balancers** page.
2. Click the name of the load balancer in the **Name** column to go to the **Basic Information** page.
3. Click the **Listeners** tab and then click **Add Listener**. On the displayed page, configure the listener. In the **Frontend Port** text box, enter the port you want to protect. In this case, enter **9876**.

**Figure 2-19** Configuring a listener

Advanced Settings				
Access Policy	All IP addresses	Transfer Load Balancer EIP	Disabled	
Transfer Listener Port	Disabled	Transfer Port Number in the	Disabled	
Number		Request		
Rewrite X-Forwarded-Host	Enabled	Idle Timeout (s)	60	
Request Timeout (s)	60	Response Timeout (s)	60	

4. Click **Next: Configure Request Routing Policy**.

**Figure 2-20** Configuring a backend server group


**NOTICE**

- If you select **Weighted round robin** for **Load Balancing Algorithm**, disable **Sticky Session**. If you enable **Sticky Session**, the same requests will be forwarded to the same dedicated WAF instance. If this instance becomes faulty, an error will occur when the requests come to it next time.
- For details about ELB traffic distribution policies, see [Load Balancing Algorithms](#).

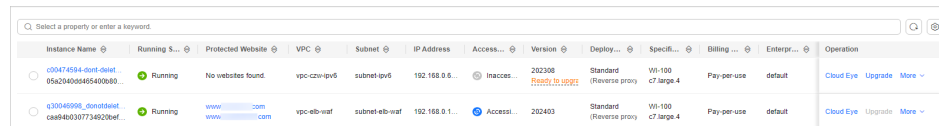
5. Click **Next: Add Backend Server** and click **Next: Confirm**.



**Step 8** Add the WAF instance to the load balancer.

1. Click  in the upper left corner, select a region, and choose **Security & Compliance > Web Application Firewall** to go to the **Dashboard** page.
2. In the navigation pane on the left, choose **Instance Management > Dedicated Engine** to go to the dedicated WAF instance page.

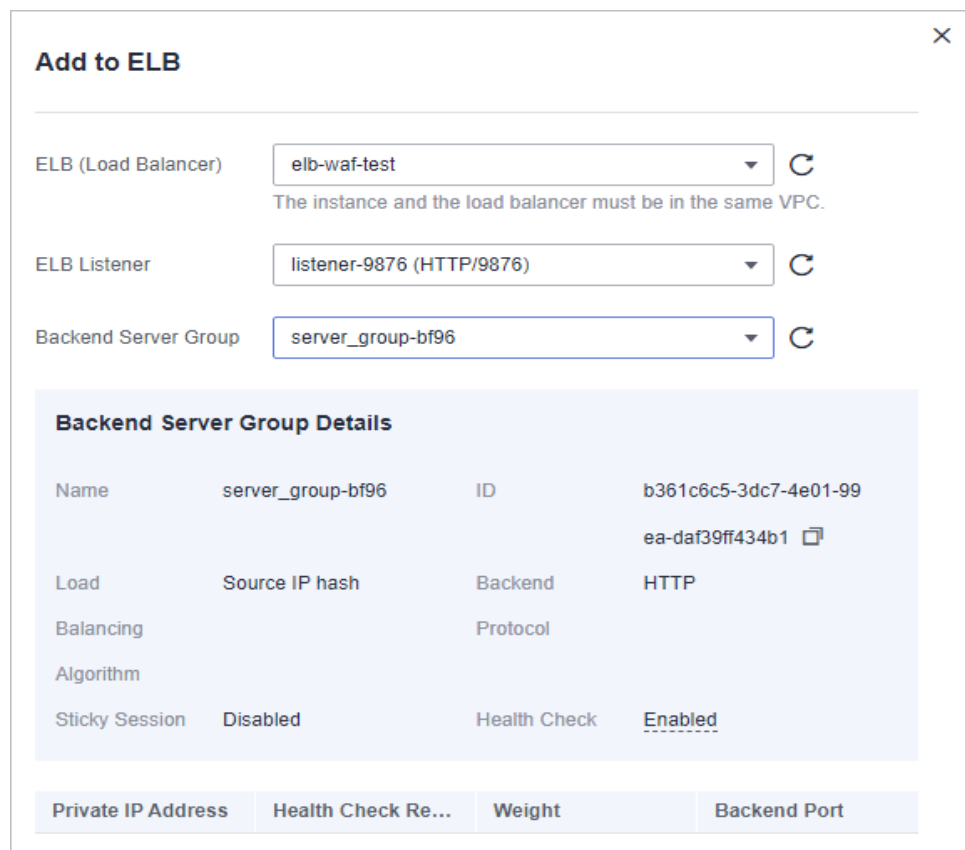
**Figure 2-21** Dedicated engine list




Instance Name	Running Status	Protected Website	VPC	Subnet	IP Address	Access...	Version	Deploy...	Specifi...	Billing...	Enterpr...	Operation
c0a74594-d0af-d6e1-05a23405a45400880...	Running	No websites found.	vpc-cw-vp6	subnet-ipv6	192.168.0.6...	Inaccess...	202208	Standard (Reverse proxy)	W1-100 c7.large.4	Pay-per-use	default	Cloud Eye Upgrade More
c1004698-d0ad8eaf-ca8460307734920bef...	Running	www.***.com www.***.com	vpc-eb-waf	subnet-eb-waf	192.168.0.1...	Access...	202403	Standard (Reverse proxy)	W1-100 c7.large.4	Pay-per-use	default	Cloud Eye Upgrade More

3. Locate the row containing the WAF instance. In the **Operation** column, click **More > Add to ELB**.
4. In the **Add to ELB** dialog box, specify **ELB (Load Balancer)**, **ELB Listener**, and **Backend Server Group** based on [Step 7](#).


**Figure 2-22** Add to ELB




**Add to ELB**


ELB (Load Balancer)  

The instance and the load balancer must be in the same VPC.

ELB Listener  

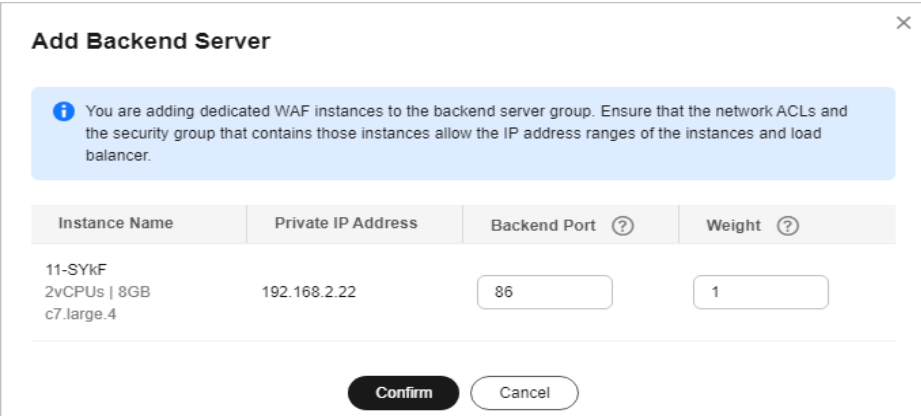
Backend Server Group  

**Backend Server Group Details**

Name	server_group-bf96	ID	b361c6c5-3dc7-4e01-99ea-daf39ff434b1 
Load	Source IP hash	Backend	HTTP
Balancing Algorithm		Protocol	
Sticky Session	Disabled	Health Check	<u>Enabled</u>

Private IP Address	Health Check Re...	Weight	Backend Port
--------------------	--------------------	--------	--------------

5. Click **Confirm**. Then, configure service port for the WAF instance. In this example, configure **Backend Port** to **86**, which is the one we configured in [Step 6](#).

**Figure 2-23** Configuring Backend Port

**Add Backend Server**

**i** You are adding dedicated WAF instances to the backend server group. Ensure that the network ACLs and the security group that contains those instances allow the IP address ranges of the instances and load balancer.

Instance Name	Private IP Address	Backend Port ?	Weight ?
11-SYkF 2vCPUs   8GB c7.large.4	192.168.2.22	86	1

**Confirm** **Cancel**

6. Click **Confirm**.

**Step 9** [Bind an EIP to a Load Balancer.](#)

**Step 10** [Whitelist IP addresses of your dedicated WAF instances.](#)

----End

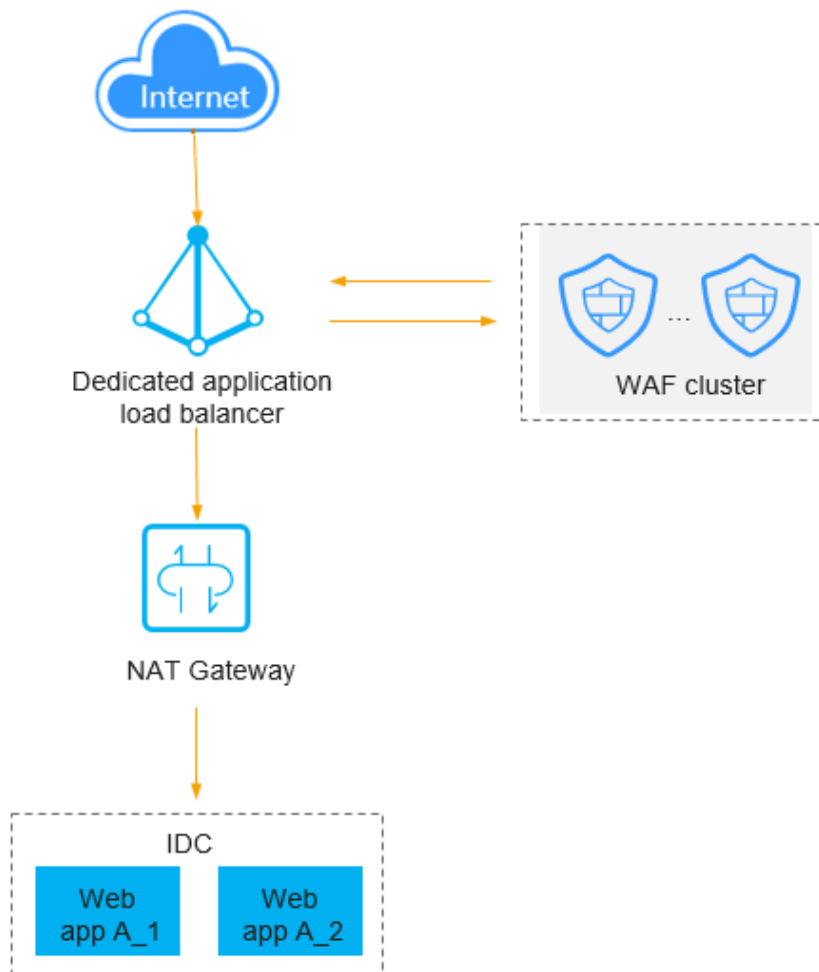
## 2.5 Using WAF, ELB, and NAT Gateway to Protect Services Not Deployed on Our Cloud

### Application Scenarios

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.

## Architecture

Figure 2-24 Architecture




## Resource and Cost Planning


**Table 2-8** Resources and costs

Resource	Description	Monthly Fee
Elastic Load Balance (ELB)	<ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Instance type: Dedicated</li> <li>• Specifications: Application load balancing (HTTP/HTTPS); Medium II</li> <li>• <b>Billed By: Bandwidth</b></li> <li>• <b>Bandwidth: 10 Mbit/s</b></li> </ul>	For details about billing rules, see <a href="#">Billing Description</a> .
NAT Gateway	<ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Specifications: Medium</li> </ul>	For details about billing rules, see <a href="#">Billing</a> .
Web Application Firewall (WAF)	Cloud - Standard edition <ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Number of domain names that can be protected: 10</li> <li>• QPS quota: 2,000 QPS</li> <li>• Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li> </ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

### Step 1: Create a Dedicated Load Balancer


**Step 1** Log in to the management console.

**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click  in the upper left corner of the page and choose **Networking > Elastic Load Balance**.

**Step 4** On the **Elastic Load Balance** page, click **Buy Elastic Load Balancer**.

1. Select the basic configuration for the load balancer as prompted.
  - **Type:** Select **Dedicated load balancer**.
  - **Specifications:** Select **Application load balancing (HTTP/HTTPS)**.
  - Other parameters: Set them based on your service requirements.

2. Configure the network as prompted.
  - **IP as a Backend:** Toggle it on ().
  - **Frontend Subnet:** Select the subnet for your load balancer to use the IP addresses in this subnet to receive requests.
  - **Backend Subnet:** Select the subnet for your load balancer to use IP addresses in this subnet to establish connections with backend servers. You need to select a backend subnet that is different from the frontend subnet.

 **NOTE**

If the frontend subnet is the same as the backend one, NAT Gateway will get confused.

- Other parameters: Set them based on your service requirements.

For details about how to create a dedicated load balancer, see [Creating a Dedicated Load Balancer](#).

**Step 5** Click **Next**.

**Step 6** Confirm the configuration details and complete the creation as prompted.

----End

## Step 2: Configure a Listener for the Load Balancer You Create

**Step 1** Click the name of the target load balancer in the **Name/ID** column.

**Step 2** Click the **Listeners** tab, click **Add Listener**, and configure the listener name, frontend protocol, and port.

**Step 3** Click **Next: Configure Request Routing Policy**.

**Step 4** Click **Next: Add Backend Server**. Then, click the **IP as Backend Servers** tab.

**Step 5** Click **Add IP as Backend Server**. In the displayed dialog box, configure **IP Address** and **Backend Port**.

- **IP Address:** Enter the IP address of your origin server.
- **Backend Port:** Enter the port number.


**Step 6** Click **OK**.

**Step 7** Click **Next: Confirm**, confirm the information, and click **Submit**.

----End

## Step 3: Configure a NAT Gateway

**Step 1** Buy a public NAT gateway.

1. Click  in the upper left corner of the page and choose **Networking > NAT Gateway**.
2. Click **Buy Public NAT Gateway** in the upper right corner.
  - **Subnet:** Select the one you configured as the [backend subnet in 2](#).

- Other parameters: Set them to meet your service requirements.
- 3. Click **Next** and confirm the public NAT gateway specifications on the displayed page.
- 4. Confirm the details and click **Submit**.  
It takes 1 to 6 minutes to create a public NAT gateway.

**Step 2** Add an SNAT rule.

1. On the displayed page, click the name of the public NAT gateway on which you need to add an SNAT rule.
2. On the **SNAT Rules** tab, click **Add SNAT Rule**.  
**Subnet:** Select the one you configured as the [backend subnet in 2](#).
3. Click **OK**.

----End

## Step 4: Add Website Domain Names to WAF in Cloud Load Balancer Access Mode

**Step 1** Buy the standard edition cloud WAF.

1. On the management 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 **Cloud Mode** for **WAF Mode**.
  - **Region:** Select the region nearest to your services WAF will protect.
  - **Edition:** Select **Standard**.
  - **Expansion Package** and **Required Duration:** Set them based on site requirements.
3. Confirm the product details and click **Buy Now** in the lower right corner of the page.
4. Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
5. On the payment page, select a payment method and pay for your order.

**Step 2** Add the domain name to WAF in cloud load balancer access mode.

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 - Load balancer** and click **Configure Now**.
4. On the **Add Domain Name** pane, configure related information.
  - **ELB (Load Balancer):** Select the load balancer created in [Step 1: Create a Dedicated Load Balancer](#).
  - **ELB Listener:** Select the one added in [Step 2: Configure a Listener for the Load Balancer You Create](#).
  - **Domain Name:** Enter the domain name you want to protect. This domain name has been pointed to the EIP of [the dedicated load balancer created earlier](#).

5. Click **Confirm**.

----End

## Verification

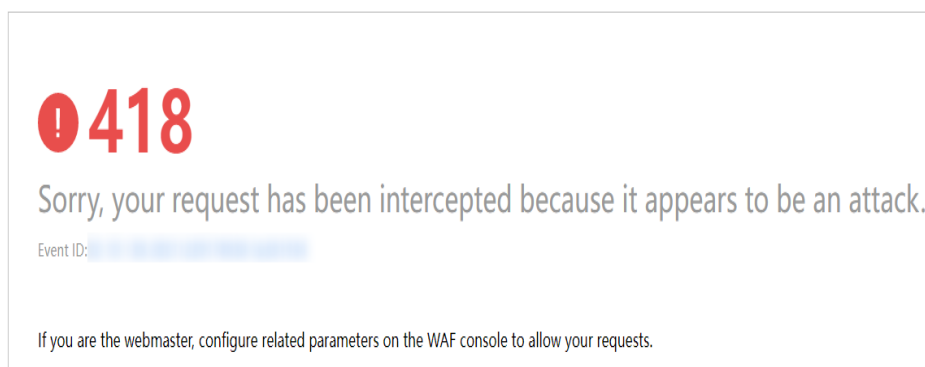
If **General Check** is enabled and **Mode** is set to **Block** for your domain name **www.example.com**, take the following steps to verify the protection effect:

- Step 1** Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.
- If the website is inaccessible, connect the website domain name to WAF by referring to [Step 1: Create a Dedicated Load Balancer](#) to [Step 4: Add Website Domain Names to WAF in Cloud Load Balancer Access Mode](#).
  - If the website is accessible, go to [Step 2](#).

- Step 2** Clear the browser cache and enter **http://www.example.com?id=1%27%20or%201=1** in the address box of the browser to simulate an SQL injection attack.

WAF blocks the access request. [Figure 2-25](#) shows an example block page.

**Figure 2-25** Block page



- Step 3** Return to the WAF console. In the navigation pane, choose **Events**. On the displayed page, view the event log.

----End

# 3 Website Protection Configuration Suggestions

---

If you are a first-time user, you may not know how to configure website protection policies after adding a website to WAF. This topic describes how Web Application Firewall (WAF) works and helps you get familiar with the protection rules in WAF in many scenarios.

## Prerequisites

- [The website has been connected to WAF.](#)
- The WAF edition you purchased supports the corresponding protection functions. For details about function differences between WAF editions, see [Edition Differences](#).

## Overview

This document provides suggestions on website protection settings from the perspectives of different roles or service requirements. You can select a scenario that best meets your actual requirements to learn about related protection settings.

- [I'm a novice. I know little about security and have no special requirements.](#)
- [I am a professional in security O&M, and I need comprehensive website protection operations.](#)
- [My services have strict requirements on security. Every attack must be killed even at the expense of more false positives.](#)
- [My business is often harassed by crawlers or faces data leakage and tampering risks.](#)

### **I'm a novice. I know little about security and have no special requirements.**

You may have purchased WAF to meet security and compliance requirements or to improve the security for your organization to a higher level. In this case, you can use the default basic protection settings of WAF. The default protection capability provided by WAF is sufficient to defend websites against most basic web threats.



You can watch out for **Dashboard** and **Events** pages on the WAF console to learn about your services and their security status. For more details, see:

- [Dashboard](#)
- [Viewing Protection Events](#)

## I am a professional in security O&M, and I need comprehensive website protection operations.

The following protection settings are recommended to you:

- **Basic Web Protection:** Defends against common web attacks, such as SQL injection, XSS, remote overflow attacks, file inclusion, Bash vulnerability exploits, remote command execution, directory traversal, sensitive file access, and command/code injection. It can also identify escape attacks in depth, check all fields in a request header, check Shiro encryption, and detect web shells.  
Operation: On the **Policies** page, click a policy name. On the displayed page, select **Basic Web Protection**, select **Block** or **Log only**, and enable all check items. For details, see [Configuring Basic Web Protection Rules](#).
- **Custom protection policies:** You can create custom protection rules and add them to a policy to give your website comprehensive and tailored protection.  
Operation: On the **Policies** page, perform related configurations. For details, see [How to Configure WAF Protection](#).

## My services have strict requirements on security. Every attack must be killed even at the expense of more false positives.

To meet your requirements, the following protection configurations are recommended:

- **Basic Web Protection (block mode):** Defends against common web attacks, such as SQL injection, XSS, remote overflow attacks, file inclusion, Bash vulnerability exploits, remote command execution, directory traversal, sensitive file access, and command/code injection. It can also identify escape attacks in depth, check all fields in a request header, check Shiro encryption, and detect web shells.  
Operation: On the **Policies** page, click a policy name. On the displayed page, select **Basic Web Protection**, select **Block**, and enable all check items. For details, see [Configuring Basic Web Protection Rules](#).
- **CC attack protection (block mode):** Helps precisely identify and block CC attacks by limiting the access rate of a single visitor based on its IP address, cookie, or referer.  
Operation: On the **Policies** page, click a policy name. On the displayed page, click the **CC Attack Protection** area, add a rule, and set the **Protective Action** to **Block**. For more details, see [Configuring a CC Attack Protection Rule](#).
- **Precise Protection:** You can create custom protection rules by combining HTTP headers, cookies, URLs, request parameters, and client IP addresses to give your website more precise protection.

Operation: On the **Policies** page, click a policy name. On the displayed page, click the **Precise Protection** area, add a rule, and set the **Protective Action** to **Block**. For details, see [Configuring a Precise Protection Rule](#).

- **Blacklist and Whitelist (block mode)**: You can block IP addresses and IP address ranges irrelevant to your services with ease.

Operation: On the **Policies** page, click a policy name. On the displayed page, click the **Blacklist and Whitelist** area, add a rule, and set the **Protective Action** to **Block**. For more details, see [Configuring an IP Blacklist or Whitelist Rule](#).

- **Geolocation Access Control (block mode)**: You can configure geolocation access control rules to block or allow requests from a specific location. If there are too many malicious requests from a specific region, this type of rule helps block every single request from the region. A geolocation access control rule allows you to allow or block requests from IP addresses from specified countries or regions.

Operation: On the **Policies** page, click a policy name. On the displayed page, click the **Geolocation Access Control** area, add a rule, and set the **Protective Action** to **Block**. For more details, see [Configuring a Geolocation Access Control Rule](#).

## My business is often harassed by crawlers or faces data leakage and tampering risks.

To meet your requirements, the following protection configurations are recommended:

- **Web Tamper Protection**: WAF caches the pages you want to protect and returns cached pages to visitors so that your website visitors will view right pages all the time even if a web page was tampered with.

Operation: On the **Policies** page, click the policy name. On the displayed page, click the **Web Tamper Protection** area, add a rule, and complete related settings. For details, see [Configuring a Web Tamper Protection Rule](#).

- **Information Leakage Prevention**: Helps mask sensitive information, such as ID numbers, phone numbers, and email addresses, on web pages when those pages are returned to visitors.

Operation: On the **Policies** page, click the policy name. On the displayed page, click the **Information Leakage Prevention** area, add a rule, and complete related settings. For details, see [Configuring an Information Leakage Prevention Rule](#).

- **Anti-Crawler Protection**

- **Feature Library**: You can allow access requests from legitimate crawlers (such as Googlebot and Baiduspider) but block crawler attacks from most scripts and automation programs.

- **JavaScript**: If you enable this protection, WAF checks JavaScript. You can also add custom rules to prevent JavaScript crawlers.

Operation: On the **Policies** page, click the policy name. On the displayed page, click the **Anti-Crawler** area, add a rule, and complete related settings. For details, see [Configuring Anti-Crawler Rules](#).

# 4 Mitigating Web Security Vulnerabilities

## 4.1 Java Spring Framework Remote Code Execution Vulnerability

Spring Framework is a lightweight open-source application framework for developing enterprise Java applications. A remote code execution (RCE) vulnerability was disclosed in the Spring framework and classified as critical. This vulnerability can be exploited to attack Java applications running on JDK 9 or later versions.

### Vulnerability Name

Zero-Day RCE Vulnerability in the Spring Framework

### Affected Versions

- JDK 9 or later
- Applications developed using the Spring Framework or derived framework

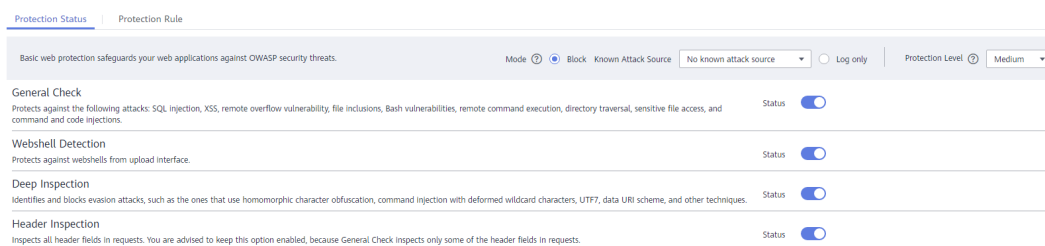
### Mitigation

**Step 1** [Buy a WAF instance](#) .

**Step 2** Add the website domain name to WAF and connect it to WAF. For details, see [Adding a Domain Name to WAF](#).

**Step 3** In the **Basic Web Protection** configuration area, set **Mode** to **Block** and complete the configuration. For details, see [Configuring Basic Web Protection Rules](#).

**Figure 4-1** Basic Web Protection



**NOTICE**

There are two types of malicious payload in this vulnerability. Whether to enable **Header Inspection** depends on the type of payloads in your services.

- Type 1: Malicious payloads are included in submitted parameters. In this situation, **Header Inspection** can be disabled.
- Type 2: Malicious payloads are included in a custom header field. In this situation, **Header Inspection** must be enabled to block attacks.

Type 2 malicious payloads depend on Type 1 malicious payloads so whether to enable **Header Inspection** is determined by your service requirements.

----End

## 4.2 Apache Dubbo Deserialization Vulnerability

On February 10, 2020, Apache Dubbo officially released the CVE-2019-17564 vulnerability notice, and the vulnerability severity is medium. Unsafe deserialization occurs within a Dubbo application which has HTTP remoting enabled. An attacker may submit a POST request with a Java object in it to completely compromise a Provider instance of Apache Dubbo, if this instance enables HTTP. Now, Huawei Cloud WAF provides protection against this vulnerability.

### Affected Versions

This vulnerability affects Apache Dubbo 2.7.0 to 2.7.4, 2.6.0 to 2.6.7, and all 2.5.x versions.

### Mitigation Version

[Apache Dubbo 2.7.5](#)

### Solutions

Upgrade Apache Dubbo to version 2.7.5.

If a quick upgrade is not possible or you want to defend against more vulnerabilities, use Huawei Cloud WAF. The procedure is as follows:

**Step 1** [Buy WAF](#).

**Step 2** Add the website domain name to WAF and connect it to WAF. For details, see [Adding a Domain Name](#).

**Step 3** In the **Basic Web Protection** configuration area, set **Mode** to **Block**. For details, see [Configuring Basic Web Protection Rules](#).

----End

## 4.3 DoS Vulnerability in the Open-Source Component Fastjson

On September 3, 2019, the Huawei Cloud security team detected a DoS vulnerability in multiple versions of the widely used open-source component Fastjson. An attacker can exploit this vulnerability to construct malicious requests and send them to the server that uses Fastjson. As a result, the memory and CPU of the server are used up, and the server breaks down, causing service breakdown. Huawei Cloud WAF provides protection against this vulnerability.

### Affected Versions

Versions earlier than Fastjson 1.2.60

### Mitigation Version

Fastjson 1.2.60

### Official Solution

Upgrade the open-source component Fastjson to 1.2.60.

### Mitigation

WAF can detect and defend against this vulnerability. The procedure is as follows:

- Step 1** [Buy WAF](#).
- Step 2** Add the website domain name to WAF and connect it to WAF. For details, see [Adding a Domain Name](#).
- Step 3** In the **Basic Web Protection** configuration area, set **Mode** to **Block**. For details, see [Enabling Basic Web Protection](#).

----End

## 4.4 Remote Code Execution Vulnerability of Fastjson

On July 12, 2019, the Huawei Cloud Emergency Response Center detected that the open-source component Fastjson had a remote code execution vulnerability. This vulnerability is an extension of the deserialization vulnerability of Fastjson 1.2.24 detected in 2017 and can be directly used to obtain server permissions, causing serious damage.

### Affected Versions

Versions earlier than Fastjson 1.2.51

### Mitigation Version

Fastjson 1.2.51 or later

## Official Solution

Upgrade Fastjson to 1.2.51 or the latest 1.2.58 version.

## Mitigation

The built-in protection rules of Huawei Cloud WAF can defend against this vulnerability. The procedure is as follows:

**Step 1** [Buy WAF](#).

**Step 2** Add the website domain name to WAF and connect it to WAF. For details, see [Adding a Domain Name](#).

**Step 3** In the **Basic Web Protection** configuration area, set **Mode** to **Block**. For details, see [Enabling Basic Web Protection](#).

----End

## 4.5 Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability (CNVD-C-2019-48814)

On April 17, 2019, Huawei Cloud Emergency Response Center found that China's National Vulnerability Database (CNVD) released a security notice on Oracle WebLogic wls9-async component. It revealed that the Oracle WebLogic wls9-async component had a deserialization vulnerability. Unauthorized remote attackers can use this vulnerability to implement remote code execution and gain server permissions.

### Vulnerability ID

CNVD-C-2019-48814

### Vulnerability Name

Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability

### Vulnerability Description

The WebLogic wls9-async component has a defect. The website built on the WebLogic Server has security risks. Attackers can construct HTTP requests to obtain the permission of the target server and execute arbitrary code remotely without authorization.

### Affected Products

- Oracle WebLogic Server 10.X
- Oracle WebLogic Server 12.1.3

## Official Solution

The patch for fixing this vulnerability has not been released.

## Mitigation

Configure precise protection rules to restrict access from the URLs whose prefixes are `/_async/` or `/wls-wsat/` by referring to [Figure 4-2](#) and [Figure 4-3](#) and block remote code execution requests initiated by exploiting this vulnerability. For details, see [Configuring a Precise Protection Rule](#).

**Figure 4-2** async configuration

The screenshot shows the 'Add Precise Protection Rule' configuration window. The rule name is 'waftest'. The condition list contains one entry: Path (Field), -- (Subfield), Prefix is (Logic), and /\_async/ (Content). The protective action is set to 'Block'.

Field	Subfield	Logic	Content
Path	--	Prefix is	/_async/

**Figure 4-3** wls-wsat configuration

The screenshot shows the 'Add Precise Protection Rule' configuration window. The rule name is 'waftest'. The condition list contains one entry: Path (Field), -- (Subfield), Prefix is (Logic), and /wls-wsat/ (Content). The protective action is set to 'Block'.

Field	Subfield	Logic	Content
Path	--	Prefix is	/wls-wsat/

# 5 Defending Against Challenge Collapsar (CC) Attacks

---

## 5.1 Overview

### Application Scenarios

If you find that your website becomes slow and its network bandwidth usage jumps high, the website may suffer from CC attacks. In this case, check whether the number of access logs or network connections increases sharply. If yes, your website is suffering from CC attacks. Then you can configure a protection rule to protect your website from CC attacks.

#### NOTE

- WAF protects application-layer traffic against DoS attacks, such as HTTP GET attacks.
- WAF does not protect your website at or below layer 4 against DDoS traffic, such as ACK Flood and UDP flood attacks. Anti-DDoS and Advanced Anti-DDoS (AAD) are recommended to defend against such attacks.

This section guides you through configuring IP address-based rate limiting and cookie-based protection rules to defend against Challenge Collapsar (CC) attacks.

### Solution Selection

- Solution 1: [Configuring CC Attack Protection for Common Scenarios](#)  
You can have a quick glance to learn how to set WAF protection in the similar scenarios to protect your services.
- Solution 2: [Limiting Traffic Through IP Address-based Rate Limiting](#)  
If no proxy is used between WAF and web visitors, limiting traffic by source IP address is an effective way to detect attacks. IP address-based rate limiting rules are recommended.
- Solution 3: [Limiting Traffic Based on the Cookie Field](#)  
In some cases, WAF cannot obtain the source IP addresses of visitors due to website settings. For example, websites use proxies, but the **X-Forwarded-For**



field is not inserted into the request header. In these cases, cookie-based rate limiting rules are recommended.

- Solution 4: [Limiting Malicious Requests in Promotions by Using Cookies and HWWAFSESID](#)

This solution works well in limiting malicious requests originated from different IP addresses and terminals but the same account and malicious requests originated from different accounts but the same PC.

## Advantages

This practice provides a solution to help quickly defend against CC attacks in multiple scenarios.

## Resource and Cost Planning

Table 5-1 Resources and costs

Resource	Description	Monthly Fee
Web Application Firewall	Cloud - Standard edition <ul style="list-style-type: none"><li>• Billing mode: Yearly/ Monthly</li><li>• Number of domain names that can be protected: 10</li><li>• QPS quota: 2,000 QPS</li><li>• Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li></ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

## 5.2 Configuring CC Attack Protection for Common Scenarios

This topic introduces how CC attack protection rules are used in certain scenarios.

### Overview

You can have a quick glance to learn how to set WAF protection in the similar scenarios to protect your services.

- [Heavy-traffic CC attacks](#)
- [The request features are malformed or improper.](#)

### Heavy-traffic CC attacks

In large-scale 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 against this type of CC attacks. We recommend IP address-based rate limiting CC attack protection rules. For details, see [Limiting Accesses Through IP Address-based Rate Limiting](#).

**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

To get improved and refined protection, you need to adjust rate limit settings and specify an appropriate protective action based on your service requirements. For example, if you need to prevent the login interface from being affected by crazy credential stuffing attacks, use the **prefix is** logical operator and set the matching content to the specific login path, such as **/login.php**.

**Add CC Attack Protection Rule**

Restrictions and precautions vary by mode. ?

\* Rule Name:

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.

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

4

\* Rate Limit:  requests  seconds  All WAF instances

5

\* Protective Action:  Verification code  Block  Block dynamically  Log only

\* Effective Date:  Immediate

\* Block Duration:  seconds

6

\* Block Page:  Default settings  Custom

**NOTE**

- **Request Aggregation:** Keep this function enabled so that requests to all domain names that match a protected 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.
- **All WAF instances:** This parameter is supported only in cloud mode. 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.

**The request features are malformed or improper.**

Many CC attack requests are constructed by attackers. After analyzing logs, it is found that these requests have many malformed packet features that do not match normal requests. The following protection rules are recommended to defend against requests having common malformed packets:

The following protection configurations are implemented through precise protection rules. For details, see [Configuring a Precise Protection Rule](#).

- Abnormal or malformed User-Agent: Invalid User-Agent (for example, Mozilla///), improper User-Agent (for example, www.example.com), and User Agent containing automation tool features. If a request matches the features, it will be blocked.

**Configuration example:** Blocking requests with User Agent containing Mozilla///.

The screenshot shows a configuration window for a protection rule. It has a title bar with a red asterisk and the text "Condition List". Below the title bar is a table with four columns: "Field", "Subfield", "Logic", and "Content". The "Field" column contains a dropdown menu with "User Agent" selected. The "Subfield" column contains "--". The "Logic" column contains a dropdown menu with "Include" selected. The "Content" column contains a text input field with "Mozilla///". Below the table is a blue plus icon and the text "Add You can add 29 more conditions. (The protective action is executed only when all the conditions are met.)". At the bottom left, there is a red asterisk and the text "Protective Action", followed by a dropdown menu with "Block" selected.

- Improper User-Agent: For example, for HTML5 pages promoted by WeChat, normal users should initiate access through WeChat. It obviously does not make sense if the request User-Agent comes from a Windows desktop browser (for example, MSIE 6.0). If a request matches the features, it will be blocked.

**Configuration example:** Blocking requests with User Agent containing MSIE 6.0.

The screenshot shows a configuration window for a protection rule. It has a title bar with a red asterisk and the text "Condition List". Below the title bar is a table with four columns: "Field", "Subfield", "Logic", and "Content". The "Field" column contains a dropdown menu with "User Agent" selected. The "Subfield" column contains "--". The "Logic" column contains a dropdown menu with "Include" selected. The "Content" column contains a text input field with "MSIE 6.0". Below the table is a blue plus icon and the text "Add You can add 29 more conditions. (The protective action is executed only when all the conditions are met.)". At the bottom left, there is a red asterisk and the text "Protective Action", followed by a dropdown menu with "Block" selected.

- Abnormal Referrer: For example, if a request does not contain a Referrer or the Referrer is fixed and comes from an unauthorized website, the request can be blocked (except when the website home page is accessed or the page is accessed for the first time). For URLs that can be accessed only through an internal address, you can analyze the behavior by checking the Referrer field and determine whether to block the URLs.

**Configuration example:** Blocking requests having no Referrer

The screenshot shows a configuration window for a protection rule. It has a title bar with a red asterisk and the text "Condition List". Below the title bar is a table with four columns: "Field", "Subfield", "Logic", and "Content". The "Field" column contains a dropdown menu with "Header" selected. The "Subfield" column contains a text input field with "Referer". The "Logic" column contains a dropdown menu with "Does not have" selected. The "Content" column contains an empty text input field. Below the table is a blue plus icon and the text "Add You can add 29 more conditions. (The protective action is executed only when all the conditions are met.)". At the bottom left, there is a red asterisk and the text "Protective Action", followed by a dropdown menu with "Block" selected.

- Abnormal Cookie: A normal request usually carries cookies that belong to the service set of the website (except when the user accesses the page for the first time). In most cases, CC attack packets do not carry any cookie. So you can block access requests having no cookies.

**Configuration example:** Blocking requests having no cookies

The screenshot shows a configuration window for a condition list. The 'Condition List' section contains one rule with the following settings: Field: Cookie, Subfield: (empty), Logic: Does not have, Content: (empty). Below the list is a '+ Add' button and a note: 'You can add 29 more conditions. (The protective action is executed only when all the conditions are met.)'. The 'Protective Action' section is set to 'Block'.

- Lack of some HTTP headers. For example, a common user will have the authentication header required by some services carried in the request, but attack packets do not.

**Configuration example:** Blocking requests with no authorization headers included.

The screenshot shows a configuration window for a condition list. The 'Condition List' section contains one rule with the following settings: Field: Header, Subfield: authorization, Logic: Does not have, Content: (empty). Below the list is a '+ Add' button and a note: 'You can add 29 more conditions. (The protective action is executed only when all the conditions are met.)'. The 'Protective Action' section is set to 'Block'.

- Incorrect request method: For example, if an interface designed for only POST requests is attacked by a large number of GET requests, you can directly block GET requests.

**Configuration example:** Blocking GET requests

The screenshot shows a configuration window for a condition list. The 'Condition List' section contains one rule with the following settings: Field: Method, Subfield: --, Logic: Equal to, Content: GET. Below the list is a '+ Add' button and a note: 'You can add 29 more conditions. (The protective action is executed only when all the conditions are met.)'. The 'Protective Action' section is set to 'Block'.

## 5.3 Limiting Accesses Through IP Address-based Rate Limiting

If no proxy is used between WAF and web visitors, limiting source IP addresses is an effective way to detect attacks. IP address-based rate limiting rules are recommended.

## Use Cases

Attackers use several hosts to continuously send HTTP POST requests to website **www.example.com**. Those malicious requests will use up website resources, such as the website connections and bandwidth. As a result, the website fails to respond to normal requests and its competitiveness decreases sharply.

## Protective Measures


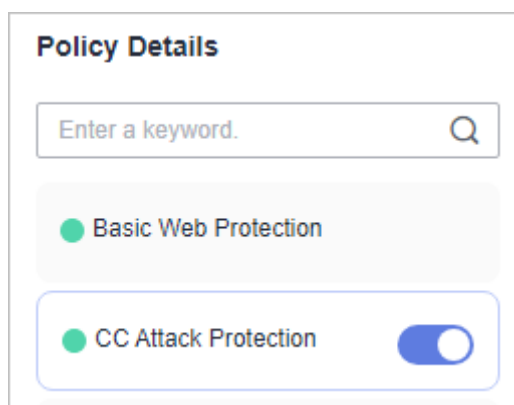
1. Based on the access statistics, check whether a large number of requests were sent from a specific IP address. If yes, it is likely that the website was hit by CC attacks.
2. Log in to the management console and route website traffic to WAF. For details about how to connect a domain name to WAF, see [Adding a Domain Name](#).
3. In the **Policy** column of the row containing the target domain name, click the number of enabled protection rules. On the displayed **Policies** page, keep the **Status** toggle on (  ) for **CC Attack Protection**.

Figure 5-1 CC Attack Protection configuration area



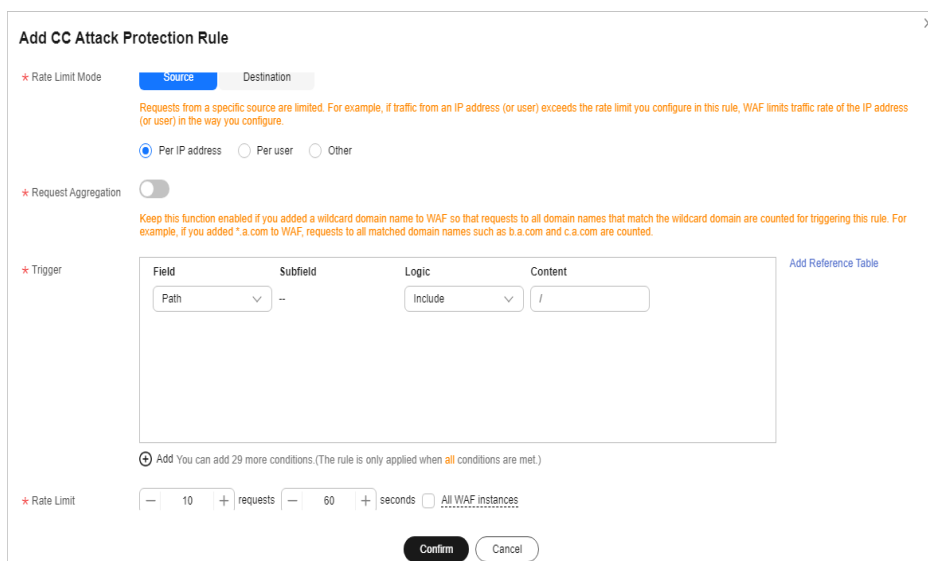
4. Then, add a CC attack protection rule to limit the rate of request traffic destined for the domain name. Set **Rate Limit Mode** to **Per IP address**, **Rate Limit** based on your service features, and **Protective Action** to **Verification code** to prevent blocking legitimate users.
  - **Rate Limit Mode:** Select **Source** and then **Per IP address** to distinguish a single web visitor based on IP addresses.
  - **Rate Limit:** Number of requests allowed from a web visitor in the rate limiting period. The visitor's access request is denied if the limit is reached.
  - **Protective Action:** To prevent legitimate requests from being blocked, select **Verification code**.

**Verification code:** A verification code is required if your website visitor's requests reaches **Rate Limit** you configured. WAF allows requests that trigger the rule as long as the website visitors complete the required verification.

If the number of access requests exceeds the configured rate limit, the visitors are required to enter a verification code to continue the access.

- Set other parameters based on site requirements.

Figure 5-2 Per IP address



5. In the navigation pane on the left, choose **Events**. You can view details about attack events.

Figure 5-3 Querying CC attack event logs

Time	Source IP Address	Domain Name	URL	Malicious Load	Event Type	Protective Action	Operation
2020/03/28 09:40:57 GMT+08:00	193.218.100.10	www.club.com	/	10	Challenge Collapsar	Block	Details Handle False Alarm

## 5.4 Limiting Accesses Through Cookie Field Configuration


In some cases, it may be difficult for WAF to obtain real IP addresses of website visitors. For example, if a website uses proxies that do not use the **X-Forwarded-For** HTTP header field, WAF is unable to obtain the real access IP addresses. In this situation, the cookie field should be configured to identify visitors and **All WAF instances** should be enabled for precise user-based rate limiting.

### Use Cases

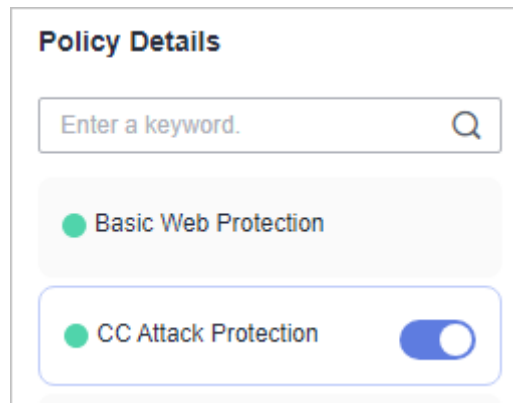
Attackers may control several hosts and disguise as normal visitors to continuously send HTTP POST requests to website **www.example.com** through the same IP address or many different IP addresses. As a result, the website may respond slowly or even fails to respond to normal requests as the attackers exhausted website resources like connections and bandwidth.

### Protective Measures

1. Based on the access statistics, check whether a large number of requests are sent from a specific IP address. If yes, it is likely that the website was hit by CC attacks.

2. Log in to the management console and route website traffic to WAF. For details about how to connect a domain name to WAF, see [Adding a Domain Name](#).
3. In the **Policy** column of the row containing the target domain name, click the number of enabled protection rules. On the displayed **Policies** page, keep the **Status** toggle on (  ) for **CC Attack Protection**.

**Figure 5-4** CC Attack Protection configuration area



4. Add a CC attack protection rule, as shown in [Figure 5-5](#).
  - **Rate Limit Mode:** Select **Source** and then **Per user** to distinguish a single web visitor based on cookies.
  - **User Identifier:** To identify visitors more effectively, use **sessionid** or **token**.
  - **Rate Limit:** Number of requests allowed from a web visitor in the rate limiting period. The visitor's access request is denied if the limit is reached.
  - **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. If you select **Per user** for **Rate Limit Mode**, requests may be forwarded to one or more WAF instances. So, All WAF instances must be enabled for triggering the rule precisely.
  - **Protective Action:** Select **Block**. Then specify **Block Duration**. Once an attack is blocked, the attacker will be blocked until the block duration expires. These settings are recommended if your applications have high security requirements.
    - **Verification code:** A verification code is required if your website visitor's requests reaches **Rate Limit** you configured. WAF allows requests that trigger the rule as long as the website visitors complete the required verification.
    - **Block:** Requests are blocked if the number of requests exceeds the configured rate limit.
    - **Log only:** Requests are logged only but not blocked if the number of requests exceeds the configured rate limit.

- **Block Page:** Select **Default settings** or **Custom**.

**Figure 5-5** Add CC Attack Protection Rule

The screenshot shows the 'Add CC Attack Protection Rule' configuration window. It has a title bar with a close button. The main content area is divided into several sections:

- Rate Limit Mode:** Two tabs, 'Source' (selected) and 'Destination'. Below them is a note: '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.' There are three radio buttons: 'Per IP address', 'Per user' (selected), and 'Other'.
- User Identifier:** A dropdown menu set to 'Cookie' and a text input field containing 'userid'. A note below says: 'If this field is not in a request, BENSESSCC\_TAG will be used for counting by default. If this field exists but is empty, the request will be counted.'
- Request Aggregation:** A toggle switch that is currently turned off. A note below says: '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:** A table with columns 'Field', 'Subfield', 'Logic', and 'Content'. The first row has 'Path' in the 'Field' column, '--' in the 'Subfield' column, 'Include' in the 'Logic' column, and '/' in the 'Content' column. There is an 'Add Reference Table' link to the right of the table.

5. In the navigation pane on the left, choose **Events**. You can view details about attack events.

## 5.5 Restricting Malicious Requests in Promotions by Using Cookies and HWWAFSESID

This topic describes how to configure cookies and HWWAFSESID fields in CC attack protection rules to restrict malicious requests in promotions.

### Application Scenarios

- **Scenario 1:** To steal extra bonus (such as goods in promotions or downloads), a malicious actor may use the same account to send requests to a website by changing IP addresses or terminals.

Protective measures: [Using Cookies \(or User IDs\) to Configure a Path-based CC Attack Protection Rule](#)

- **Scenario 2:** To steal extra bonus (such as goods in promotions or downloads), a malicious actor may use multiple accounts to send requests to a website through the same PC by frequently changing its IP address.

Protective measures: [Using HWWAFSESID to Configure a CC Attack Protection Rule](#)

### Using Cookies (or User IDs) to Configure a Path-based CC Attack Protection Rule

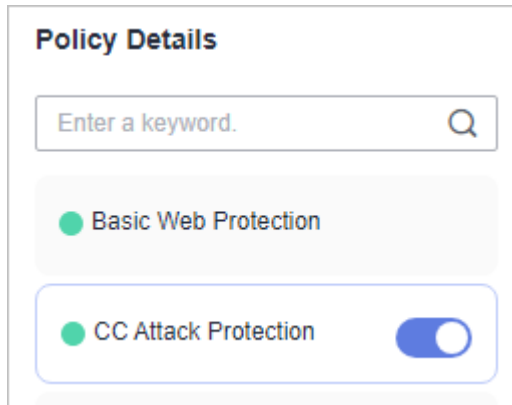
**Step 1** Log in to the management console and connect your website to WAF.

- Cloud WAF: [Adding a Domain Name to WAF \(Cloud Mode - CNAME Access\)](#)
- Dedicated WAF instances: [Adding a Website to WAF \(Dedicated Mode\)](#)



- Step 2** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.
- Step 3** In the **CC Attack Protection** configuration area, toggle **CC Attack Protection** on if needed.

**Figure 5-6** CC Attack Protection configuration area



- Step 4** In the upper left corner of the **CC Attack Protection** page, click **Add Rule**.
- Step 5** Configure a CC attack protection rule using a cookie or user ID to limit traffic to the path. **Figure 5-7** shows an example.
- **Rate Limit Mode:** Select **Source** and then **Per user**.
  - **User Identifier:** Select **Cookie** and enter the User ID as the key value.
  - **Trigger:** Set **Field** to **Path**, and set **Logic** and **Content** based on site requirements.
  - **Other parameters:** Set them to meet your service requirements.

**Figure 5-7** Configuring service cookies




- Step 6** Click **Confirm**.
- End

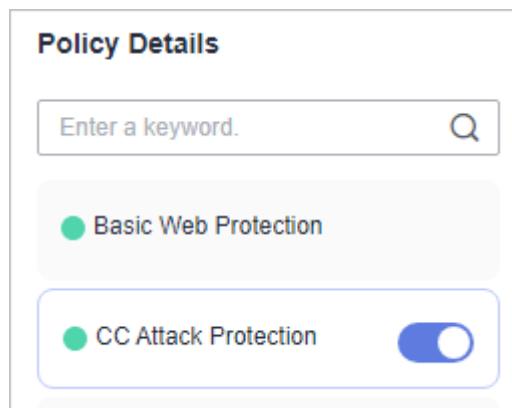
## Using HWWAFSESID to Configure a CC Attack Protection Rule

HWWAFSESID: session ID. WAF inserts HWWAFSESID (session ID) into the cookie of a customer request. WAF uses this field to count client requests. If the number

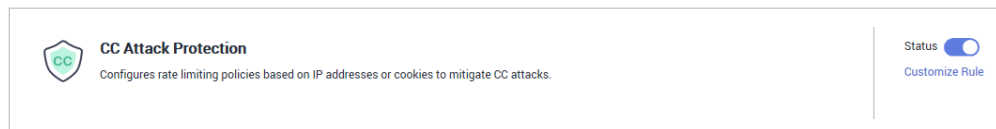
of requests reaches the threshold, the CC attack protection rule will be triggered. Now, let's see how to use this field to configure a CC attack protection rule.

- Step 1** Log in to the management console and connect your website to WAF.
- Cloud WAF: [Adding a Domain Name to WAF \(Cloud Mode - CNAME Access\)](#)
  - Dedicated WAF instances: [Adding a Website to WAF \(Dedicated Mode\)](#)
- Step 2** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.
- Step 3** In the **CC Attack Protection** configuration area, toggle **CC Attack Protection** on (  ) if needed.

**Figure 5-8** CC Attack Protection configuration area



**Figure 5-9** CC Attack Protection configuration area



- Step 4** In the upper left corner of the **CC Attack Protection** page, click **Add Rule**.
- Step 5** Configure a CC attack protection rule using HWWAFSESID to limit traffic to the path. For details, see [Figure 5-10](#).
- **Rate Limit Mode:** Select **Source** and then **Per user**.
  - **User Identifier:** Select **Cookie** and set it to **HWWAFSESID**.
  - **Trigger:** Set **Field** to **Path**, and set **Logic** and **Content** based on site requirements.
  - **Other parameters:** Set them to meet your service requirements.

Figure 5-10 HWWAFSESID-based rate limiting

**Add CC Attack Protection Rule**

Restrictions and precautions vary by mode. ⓘ

Rule Description: wafest

\* Rate Limit Mode: **1** Source (highlighted) 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 **2**  Per user (highlighted)  Other

\* User Identifier: **3** Cookie (highlighted) HWWAFSESID (highlighted)

If this field is not in a request, BENSESSCC\_TAG will be used for counting by default. If this field exists but is empty, the request will be counted.

\* Request Aggregation:

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: **4** Field: Path (highlighted) Subfield: -- Logic: Include (highlighted) Content:

[Add Reference Table](#)

**Confirm** **Cancel**

**Step 6** Click **Confirm**.

**----End**

# 6 Using WAF to Block Crawler Attacks

---

## Application Scenarios

Web crawlers make network information collection and query easy, but they also introduce the following negative impacts:

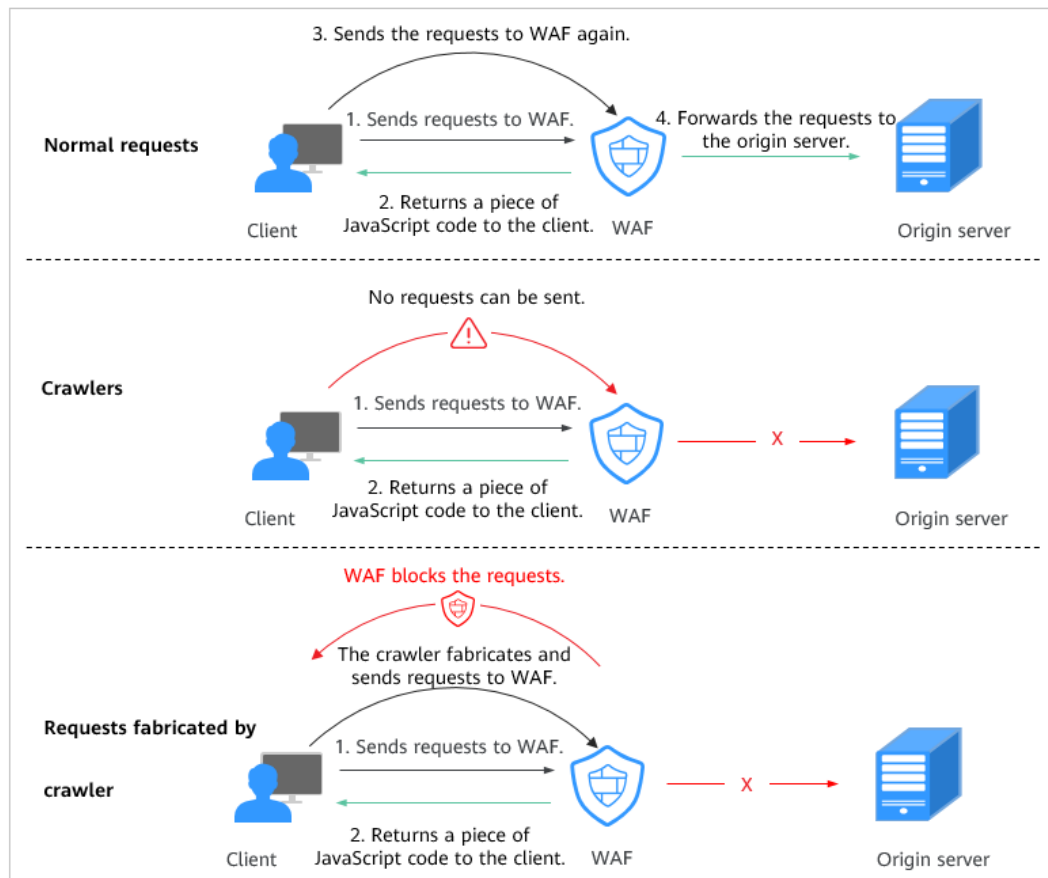
- Web crawlers always consume too much server bandwidth and increase server load as they use specific policies to browser as much information of high value on a website as possible.
- Bad actors may use web crawlers to launch DoS attacks against websites. As a result, websites may fail to provide normal services due to resource exhaustion.
- Bad actors may use web crawlers to steal mission-critical data on your websites, which will damage your economic interests.

To comprehensively mitigate crawler attacks against websites, WAF provides three anti-crawler policies, general check and web shell detection by identifying User-Agent, website anti-crawler by checking browser validity, and CC attack protection by limiting the access traffic rate.

## Overview

**Figure 6-1** shows how WAF detects crawlers, where step 1 and step 2 are called JS challenges and step 3 is called JS authentication.

**Figure 6-1** JavaScript Anti-Crawler protection process

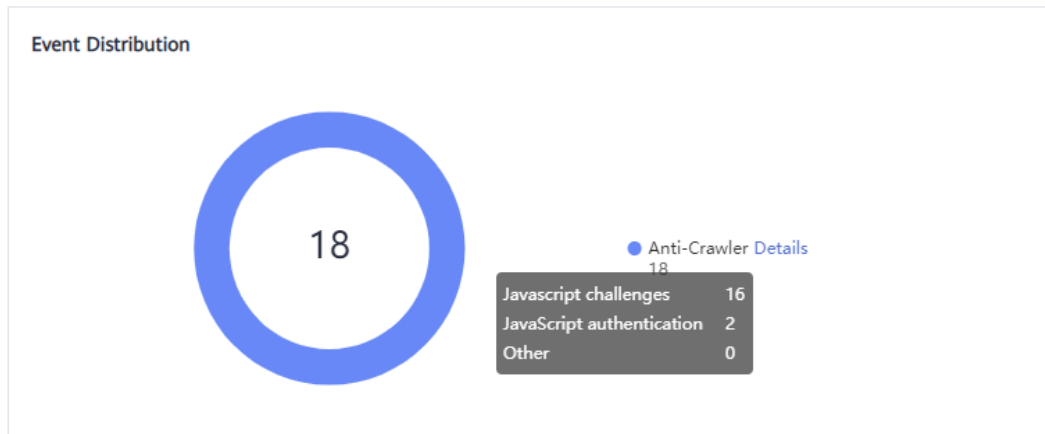


If JavaScript anti-crawler is enabled when a client sends a request, WAF returns a piece of JavaScript code to the client.

- If the client sends a normal request to the website, triggered by the received JavaScript code, the client will automatically send the request to WAF again. WAF then forwards the request to the origin server. This process is called JavaScript verification.
- If the client is a crawler, it cannot be triggered by the received JavaScript code and will not send a request to WAF again. The client fails JavaScript authentication.
- If a client crawler fabricates a WAF authentication request and sends the request to WAF, the WAF will block the request. The client fails JavaScript authentication.

By collecting statistics on the number of JavaScript challenges and authentication responses, the system calculates how many requests the JavaScript anti-crawler defends. In **Figure 6-2**, the JavaScript anti-crawler has logged 18 events, 16 of which are JavaScript challenge responses, and 2 of which are JavaScript authentication responses. **Other** indicates the number of WAF authentication requests fabricated by the crawler.

**Figure 6-2** Parameters of a JavaScript anti-crawler protection rule



### Limitations and Constraints

- The cloud WAF standard edition does not support the website anti-crawler function.
- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.
- If your service is connected to CDN, exercise caution when using the JS anti-crawler function.  
CDN caching may impact JS anti-crawler performance and page accessibility.

### Resource and Cost Planning

**Table 6-1** Resources and costs

Resource	Description	Monthly Fee
Web Application Firewall	Cloud - professional edition: <ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Number of domain names that can be protected: 50</li> <li>• QPS quota: 5,000 QPS</li> <li>• Peak bandwidth: 200 Mbit/s inside the cloud and 50 Mbit/s outside the cloud</li> </ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

### Step 1: Buy the Professional Edition Cloud WAF

The following describes how to buy the standard edition cloud WAF.

- Step 1** [Log in to Huawei Cloud management console](#).

- Step 2** On the management console page, choose **Security & Compliance > Web Application Firewall**.
- Step 3** In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select **Cloud Mode** for **WAF Mode**.
- **Region:** Select the region nearest to your services WAF will protect.
  - **Edition:** Select **Professional**.
  - **Expansion Package and Required Duration:** Set them based on site requirements.
- Step 4** Confirm the product details and click **Buy Now** in the lower right corner of the page.
- Step 5** Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
- Step 6** On the payment page, select a payment method and pay for your order.
- End

## Step 2: Add Website Information to WAF

The following example shows how to add a website information to WAF in cloud CNAME access mode.

- For details about the cloud load balancer access mode, see [Connecting a Website to WAF \(Cloud Mode - ELB Access\)](#).
  - For details about the dedicated mode, see [Connecting a Website to WAF \(Dedicated Mode\)](#).
- Step 1** In the navigation pane on the left, choose **Website Settings**.
- Step 2** In the upper left corner of the website list, click **Add Website**.
- Step 3** Select **Cloud - CNAME** and click **Configure Now**.
- Step 4** Configure website information as prompted.

**Figure 6-3** Configuring basic information

**Basic Settings**

Protected Domain Name ?  
 [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  
 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 <span style="float: right;">v</span>	HTTP <span style="float: right;">v</span>	IPv4 <span style="float: right;">v</span> <input type="text" value="Enter a public IP ad"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	Delete

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

Use Layer-7 Proxy ?

**Table 6-2** Key parameters

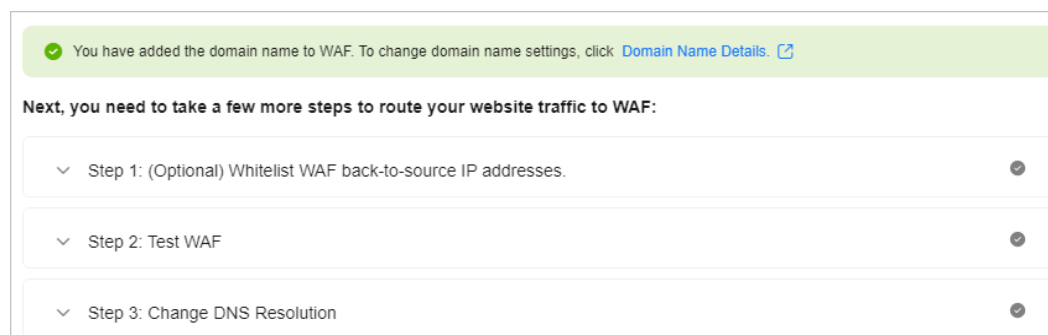
Parameter	Description	Example Value
Domain Name	Domain name you want to add to WAF for protection. <ul style="list-style-type: none"> <li>The domain name has an ICP license.</li> <li>You can enter a single domain name (for example, top-level domain name <b>example.com</b> or level-2 domain name <b>www.example.com</b>) or a wildcard domain name (<b>*.example.com</b>).</li> </ul>	www.example.com
Protected Port	The port over which the website traffic goes	Standard ports



Parameter	Description	Example Value
Server Configuration	<p>Web server address settings. You need to configure the client protocol, server protocol, server weights, server address, and server port.</p> <ul style="list-style-type: none"> <li>● <b>Client Protocol:</b> protocol used by a client to access a server. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Protocol:</b> protocol used by WAF to forward client requests. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Address:</b> 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.</li> <li>● <b>Server Port:</b> service port over which the WAF instance forwards client requests to the origin server.</li> <li>● <b>Weight:</b> Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.</li> </ul>	<p><b>Client Protocol:</b> Select <b>HTTP</b>.</p> <p><b>Server Protocol:</b> <b>HTTP</b></p> <p><b>Server Address:</b> <i>IPv4 XXX.XXX.1.1</i></p> <p><b>Server Port:</b> <b>80</b></p>
Use Layer-7 Proxy	<p>You need to configure whether you deploy layer-7 proxies in front of WAF.</p> <p>Set this parameter based on your website deployment.</p>	Yes

**Step 5** Click **Next**. Then, [whitelist WAF back-to-source IP address](#), [test WAF](#), and [modify DNS records](#) as prompted.


**Figure 6-4** Domain name added to WAF



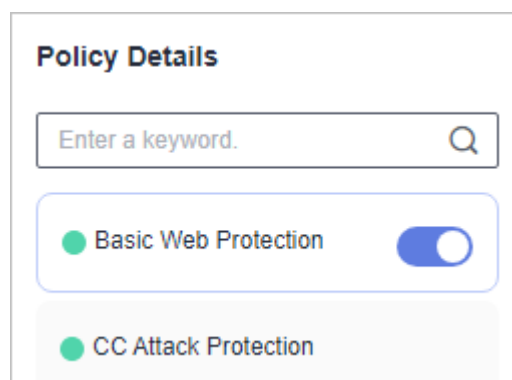
----End

### Step 3: Enable General Check and Web Shell Detection (Identifying User-Agent)

General check and web shell detection in WAF can help detect and block threats such as malicious crawlers and web shells.

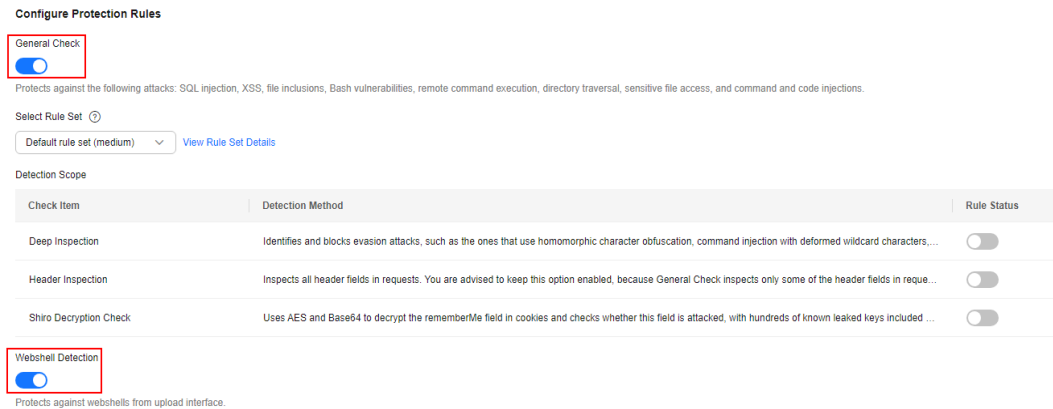
- Step 1** In the navigation pane on the left, choose **Website Settings**.
- Step 2** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.
- Step 3** Ensure that **Basic Web Protection** is enabled (status: ).

**Figure 6-5** Basic Web Protection configuration area



- Step 4** On the **Protection Status** page, enable **General Check** and **Webshell Detection**.

**Figure 6-6** Protection configuration



If WAF detects that a malicious crawler is crawling your website, WAF immediately blocks it and logs the event. You can view the crawler protection logs on the **Events** page.

Time	Source IP Address	Domain Name	URL	Malicious Load	Event Type	Protective Action	Operation
Oct 16, 2018 10:01:03 GMT+08:00	192.168.1.1	www.guoshan.com	/	curl/7.29.0	Scanner & Crawler	Log only	<a href="#">Details</a> <a href="#">Handle False Alarm</a>

----End

### Step 4: Enable Anti-Crawler Protection to Verify Browser Validity

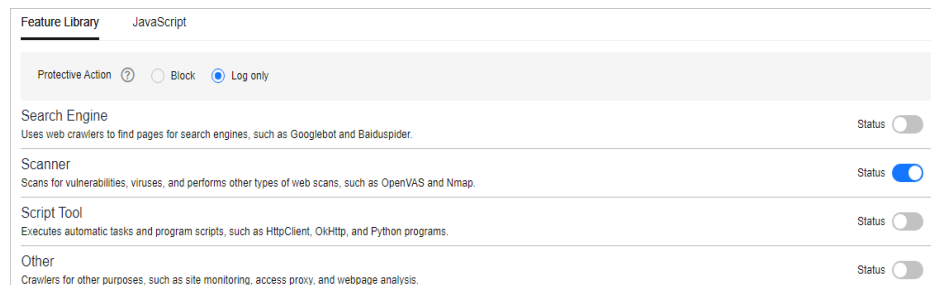
If you enable anti-crawler protection, WAF dynamically analyzes website service models and accurately identifies crawler behavior based on data risk control and bot identification approaches.

**Step 1** Click the **Anti-Crawler** configuration area and toggle it on.



-  : enabled.
-  : disabled.

**Step 2** On the **Feature Library** page, enable **Scanner** and set other parameters based on your service requirements.

**Figure 6-7** Feature Library



**Step 3** Select the **JavaScript** tab and change **Status** if needed.

**JavaScript** anti-crawler is disabled by default. To enable it, click  and then click **OK** in the displayed dialog box to toggle on .

**Protective Action: Block or Log only.** You can also select **Verification code**. If the JavaScript challenge fails, a verification code is required. As long as the visitor provides a valid verification code, their request will not be restricted.

**NOTICE**

- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.
- If your service is connected to CDN, exercise caution when using the JS anti-crawler function.  
CDN caching may impact JS anti-crawler performance and page accessibility.

**Step 4** Configure a JavaScript-based anti-crawler rule by referring to [Table 6-3](#).

Two protective actions are provided: **Protect all requests** and **Protect specified requests**.

- To protect all requests except requests that hit a specified rule  
Set **Protection Mode** to **Protect all requests**. Then, click **Exclude Rule**, configure the request exclusion rule, and click **OK**.

**Figure 6-8** Exclude Rule

Field	Subfield	Logic	Content	Case-Sensitive
Path	--	Include		<input checked="" type="checkbox"/>

- To protect a specified request only  
Set **Protection Mode** to **Protect specified requests**, click **Add Rule**, configure the request rule, and click **OK**.

**Figure 6-9 Add Rule**

**Add Rule**

Restrictions and precautions vary by mode. ⓘ

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

\* Rule Name

Rule Description

\* Condition List

Field	Subfield	Logic	Content	Case-Sensitive
Path	--	Include	<input type="text"/>	<input checked="" type="checkbox"/>

[Add Reference Table](#)

+ Add You can add 29 more conditions. (The rule is only applied when all conditions are met.)

\* Application Schedule  Immediate

\* Priority  A smaller value indicates a higher priority.

**Table 6-3** Parameters of a JavaScript-based anti-crawler protection rule

Parameter	Description	Example Value
Rule Name	Name of the rule	waf
Rule Description	A brief description of the rule. This parameter is optional.	-
Effective Date	Time the rule takes effect.	Immediate

Parameter	Description	Example Value
Condition List	<p>Parameters for configuring a condition are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Field:</b> Select the field you want to protect from the drop-down list. Currently, only <b>Path</b> and <b>User Agent</b> are included.</li> <li>• <b>Subfield</b></li> <li>• <b>Logic:</b> Select a logical relationship from the drop-down list.</li> </ul> <p><b>NOTE</b> If you set <b>Logic</b> to <b>Include any value</b>, <b>Exclude any value</b>, <b>Equal to any value</b>, <b>Not equal to any value</b>, <b>Prefix is any value</b>, <b>Prefix is not any of them</b>, <b>Suffix is any value</b>, or <b>Suffix is not any of them</b>, you need to select a reference table.</p> <ul style="list-style-type: none"> <li>• <b>Content:</b> Enter or select the content that matches the condition.</li> <li>• <b>Case-Sensitive:</b> This parameter can be configured if <b>Path</b> is selected for <b>Field</b>. If you enable this, the system matches the case-sensitive path. It helps the system accurately identify and handle various crawler requests, improving the accuracy and effectiveness of anti-crawler policies.</li> </ul>	<b>Path Include /admin</b>
Priority	Rule priority. If you have added multiple rules, rules are matched by priority. The smaller the value you set, the higher the priority.	5

----End

If you enable anti-crawler, web visitors can only access web pages through a browser.

```

</body>
</html>
[root@VM_0_9_centos ~]# curl http://cloudsecuritylab.tech/ --user-agent 'xpymp.exe'
<html>
<head>
<meta http-equiv="Server" content="HuaweiCloudWAF">
</head>
<body>
<noscript>
<h1><strong>Please Enable JavaScript and Cookie.</strong></h1>
</noscript>
<h1> <span id = "open_cookie"/> </h1>
<script type="text/javascript">
(function(t,a,c){function===typeof window.define&&window.define.amd?window.define(c):"undefined"!
=typeof module&&module.exports?module.exports=c():a.exports?a.exports=c():a[t]=c()}("fe",this,funct
ion(){var t=function(a){if(!(this instanceof t))return new t(a);this.options=this.extend(a,{swfConta
inerId:"fingerprintjs2",swfPath:"flash/compiled/FontList.swf",detectScreenOrientation:!0,sortPugins
For:[/palemoon/i],userDefinedFonts:[]});this.nativeForEach=Array.prototype.forEach;this.nativeMap=Ar
ray.prototype.map};t.prototype={extend:function(a,c){if(null==a)return c;for(var b in a)null!=a[b]&&c[b]
!=a[b]&&c[b]=a[b];return c},get:function(a){var c=this,b={data:[],addPreprocessedComponent:function(a){
var b=a.v
alue;"function"===typeof c.options.preprocessor&&(b=c.options.preprocessor(a.key,b));this.data.push(
{key:a.key,value:b})}},b=this.userAgentKey(b),b=this.languageKey(b),b=this.colorDepthKey(b),b=this.d
eviceMemoryKey(b),b=this.pixelRatioKey(b),b=this.hardwareConcurrencyKey(b),b=this.screenResolutionKe
y(b),
b=this.availableScreenResolutionKey(b),b=this.timezoneOffsetKey(b),b=this.platformKey(b),b=this.plug

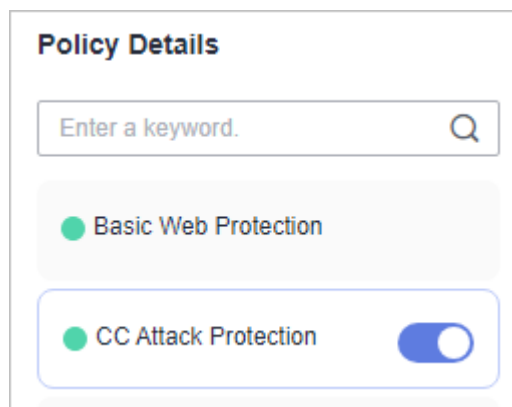
```

### Step 5: Configure CC Attack Protection to Limit Access Frequency

A CC attack protection rule uses a specific IP address, cookie, or referer to limit the access to a specific path (URL), mitigating the impact of CC attacks on web services.

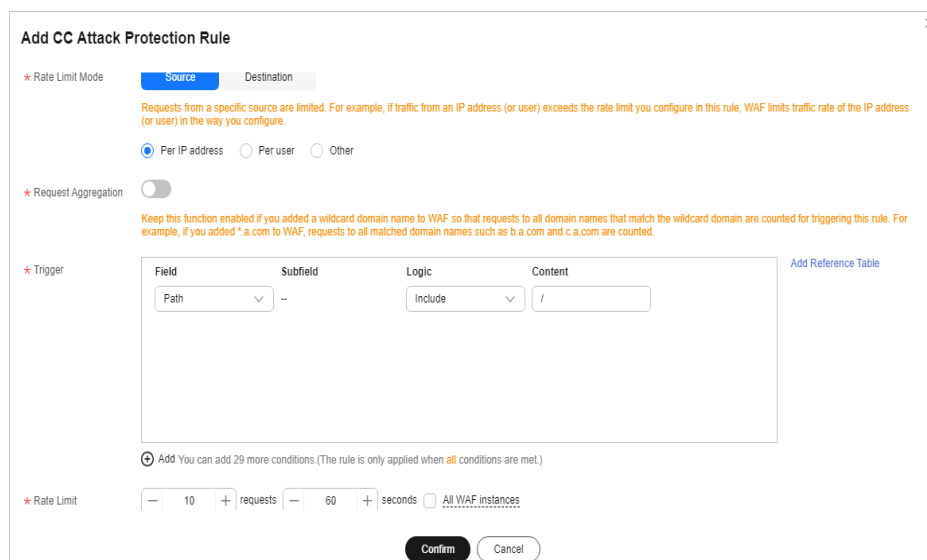
**Step 1** Ensure that the **Status** of **CC Attack Protection** is enabled (  ).

**Figure 6-10** CC Attack Protection configuration area

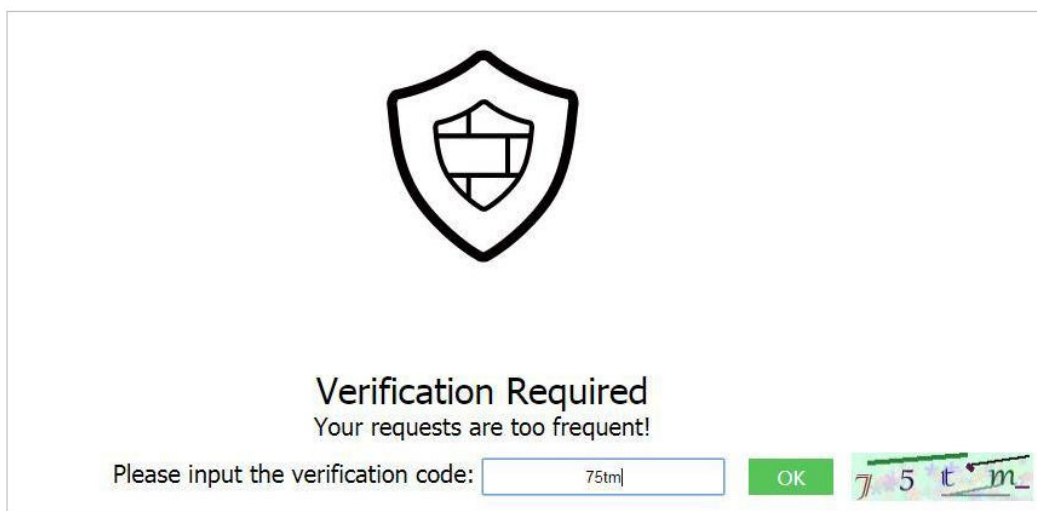


**Step 2** In the upper left corner above the **CC Attack Protection** rule list, click **Add Rule**. The following uses IP address-based rate limiting and human-machine verification as examples to describe how to add an IP address-based rate limiting rule, as shown in [Figure 6-11](#).

**Figure 6-11** Per IP address



If the number of access requests exceeds the configured rate limit, the visitors are required to enter a verification code to continue the access.



----End



# 7 Verifying a Global Protection Whitelist Rule by Simulating Requests with Postman

## Application Scenarios

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 rule.

## Example

Assume that your workloads are deployed in the **/product** directory, and parameter ID contains scripts or text in Rich Text Format (RTF) submitted by your customers. To ensure service running and improve WAF protection accuracy, you plan to mask false alarms generated for content submitted by the customers.

## Resource and Cost Planning

Table 7-1 Resources and costs

Resource	Description	Monthly Fee
Web Application Firewall	Cloud - Standard edition <ul style="list-style-type: none"><li>Billing mode: Yearly/ Monthly</li><li>Number of domain names that can be protected: 10</li><li>QPS quota: 2,000 QPS</li><li>Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li></ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

## Step 1: Buy the Standard Edition Cloud WAF

The following describes how to buy the standard edition cloud WAF.

- Step 1** [Log in to Huawei Cloud management console.](#)
- Step 2** On the management console page, choose **Security & Compliance > Web Application Firewall**.
- Step 3** In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select **Cloud Mode** for **WAF Mode**.
- **Region:** Select the region nearest to your services WAF will protect.
  - **Edition:** Select **Standard**.
  - **Expansion Package and Required Duration:** Set them based on site requirements.
- Step 4** Confirm the product details and click **Buy Now** in the lower right corner of the page.
- Step 5** Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
- Step 6** On the payment page, select a payment method and pay for your order.
- End

## Step 2: Add Website Information to WAF

The following example shows how to add a website information to WAF in cloud CNAME access mode.

- For details about the cloud load balancer access mode, see [Connecting a Website to WAF \(Cloud Mode - ELB Access\)](#).
  - For details about the dedicated mode, see [Connecting a Website to WAF \(Dedicated Mode\)](#).
- Step 1** In the navigation pane on the left, choose **Website Settings**.
- Step 2** In the upper left corner of the website list, click **Add Website**.
- Step 3** Select **Cloud - CNAME** and click **Configure Now**.
- Step 4** Configure website information as prompted.

**Figure 7-1** Configuring basic information

**Basic Settings**

Protected Domain Name ?  
 [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  
 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 <span style="float: right;">v</span>	HTTP <span style="float: right;">v</span>	IPv4 <span style="float: right;">v</span> <input type="text" value="Enter a public IP ad"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	Delete

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

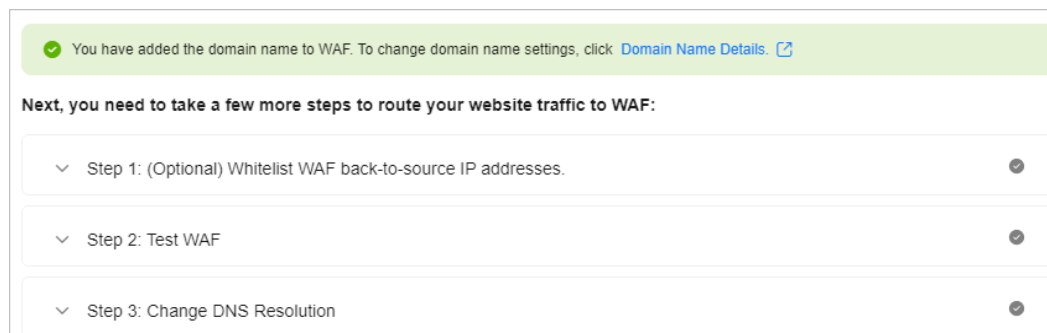
Use Layer-7 Proxy ?  
 Yes  No

**Table 7-2** Key parameters

Parameter	Description	Example Value
Domain Name	Domain name you want to add to WAF for protection. <ul style="list-style-type: none"> <li>The domain name has an ICP license.</li> <li>You can enter a single domain name (for example, top-level domain name <b>example.com</b> or level-2 domain name <b>www.example.com</b>) or a wildcard domain name (<b>*.example.com</b>).</li> </ul>	www.example.com
Protected Port	The port over which the website traffic goes	Standard ports

Parameter	Description	Example Value
Server Configuration	<p>Web server address settings. You need to configure the client protocol, server protocol, server weights, server address, and server port.</p> <ul style="list-style-type: none"> <li>● <b>Client Protocol:</b> protocol used by a client to access a server. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Protocol:</b> protocol used by WAF to forward client requests. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Address:</b> 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.</li> <li>● <b>Server Port:</b> service port over which the WAF instance forwards client requests to the origin server.</li> <li>● <b>Weight:</b> Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.</li> </ul>	<p><b>Client Protocol:</b> Select <b>HTTP</b>.</p> <p><b>Server Protocol:</b> <b>HTTP</b></p> <p><b>Server Address:</b> <i>IPv4 XXX.XXX.1.1</i></p> <p><b>Server Port:</b> <b>80</b></p>
Use Layer-7 Proxy	<p>You need to configure whether you deploy layer-7 proxies in front of WAF.</p> <p>Set this parameter based on your website deployment.</p>	Yes

**Step 5** Click **Next**. Then, **whitelist WAF back-to-source IP address**, **test WAF**, and **modify DNS records** as prompted.

**Figure 7-2** Domain name added to WAF

----End



### Step 3: Verify a Global Protection Whitelist Rule by Simulating Requests with Postman

**Step 1** Ensure that **Basic Web Protection** is enabled and its mode is **Block**. Enable **General Check** under it.

**Step 2** [Download](#) and install Postman.

**Step 3** On Postman, set the request path to **/product** and parameter ID to a common test script and send the request. The access request to the protected website is blocked.

**Step 4** Handle the false alarm.

1. [Log in to the management console](#).
2. Click  in the upper left corner of the management console and select a region or project.
3. Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
4. In the navigation pane on the left, choose **Events**.
5. On the **Events** page, WAF **010000** rule for **XSS Attack** is hit.
6. In the row containing the event, click **Handle as False Alarm**.
7. In the **Handle False Alarm** dialog box, add a global protection whitelist rule as shown in [Figure 7-3](#).

**Figure 7-3** Add Global Protection Whitelist Rule

**Handle False Alarm**

Restrictions and precautions vary by mode. ?

\* Policy Name: policy\_YXu0amUA x

\* Scope:  All domain names  Specified domain names

\* Condition List

Field	Subfield	Logic	Content
URL	--	Include	/product

+ Add You can add 29 more conditions.

\* Ignore WAF Protection:  All protection  Basic web protection  Invalid requests ?

\* Ignored Protection Type:  ID  Attack type  All built-in rules

\* Rule ID: 090806/Remote Command Execution / High x

Rule Description:

Advanced Settings ?

8. Click **OK**.

It takes about 5 minutes for a protection rule to take effect.

**Step 5** On Postman, set the request path to **/product** and parameter ID to a common test script and send the request again. The access request to the protected website is blocked again.

**Step 6** Handle the false alarms that hit the **110053 XSS attack** rule by referring to [Step 4](#).

**Figure 7-4** Add Global Protection Whitelist Rule

**Handle False Alarm**

Restrictions and precautions vary by mode. ?

\* Policy Name: policy\_YXu0amUA x

\* Scope:  All domain names  Specified domain names

\* Condition List

Field	Subfield	Logic	Content
URL	--	Include	/product

+ Add You can add 29 more conditions.

\* Ignore WAF Protection:  All protection  Basic web protection  Invalid requests ?

\* Ignored Protection Type:  ID  Attack type  All built-in rules

\* Rule ID: 090806/Remote Command Execution / High x

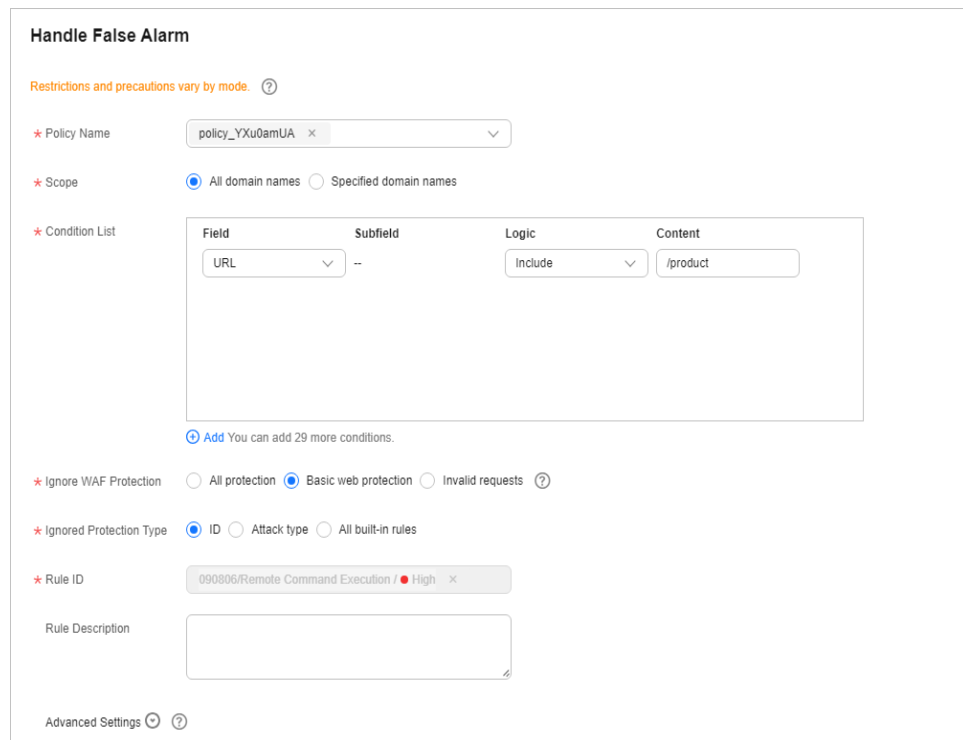
Rule Description:

Advanced Settings ?

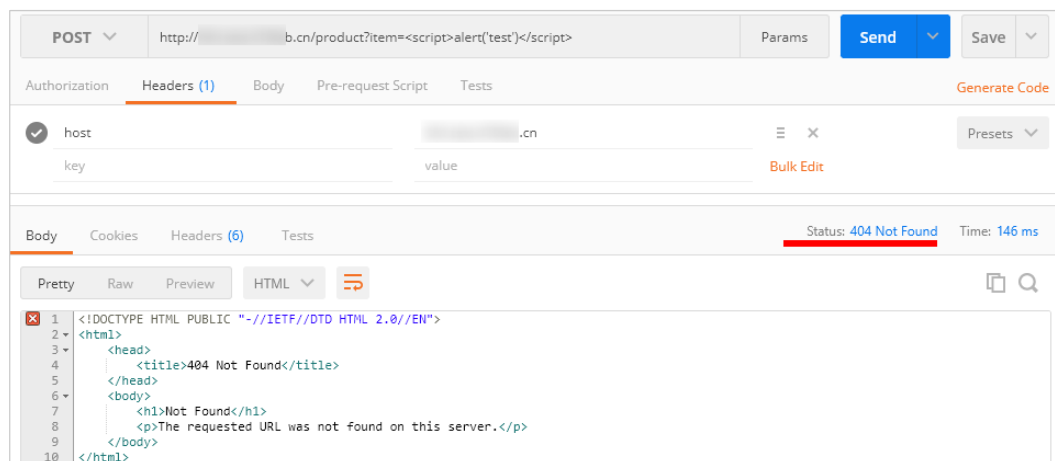
**Step 7** On Postman, set the request path to **/product** and parameter ID to a common test script and send the request third time. The access request to the protected website is still blocked.

**Step 8** Handle the false alarm that hits the **110060** rule for **XSS attack** by referring to [Step 4](#).

**Figure 7-5** Add Global Protection Whitelist Rule



**Step 9** On Postman, set the request path to **/product** and the parameter ID to a common test script and send the request forth time. In this case, the access request to the protected website is not blocked. All global protection whitelist rules have taken effect.



Go to the **Event** page, no new XSS attack event is displayed.

**Step 10** Simulate an attack on Postman to verify that the configured global protection whitelist rules do not stop WAF from blocking XSS attacks against other parameters.

1. On Postman, set the request path to **/product** and parameter **item** to a common test script and send the request. The access request to the protected website is blocked.
2. On the **Events** page, view the XSS attack against parameter **item**.



**Step 11** Simulate an attack on Postman to verify that the configured global protection whitelist rules do not stop WAF from blocking XSS attacks against other paths.

1. On Postman, set the request path to **/order** and parameter ID to a common test script and send the request. The access request to the protected website is blocked.
2. On the **Events** page, view the event generated for blocked XSS attack against **/order (URL)** and parameter ID.

----**End**

# 8 Combining WAF and HSS to Improve Web Page Tampering Protection

---

## Application Scenarios

Web tampering is a type of cyberattack that exploits vulnerabilities in web applications to tamper with web application content or to insert hidden links. Web tampering attacks are often used to spread malicious information, incite unrest, and steal money.

Links to pornographic or otherwise illegal content may be inserted into normal web pages. Tampered web pages can permanently damage the brand image of your organization.

This topic describes how to use the combination of WAF and HSS to protect dynamic and static web pages from being tampered with.

## Solution Architecture and Advantages

WAF examines HTTP/HTTPS requests. If an attacker attempts to tamper with web pages using attacks like SQL injection, WAF can identify and block the attacks in a timely manner, so they cannot sneak into or change anything in the OSs of your web servers.

Even if attacks bypass the first layer of protection, HSS WTP provides multi-level defenses. HSS WTP protects files in the web file directories from any unauthorized access. Only your website administrator can update the website content through the privileged process. Apart from that, HSS WTP also backs up web file directories locally and remotely. Once a file is tampered with, it can be quickly restored with backups. For dynamic web pages such as applications on web servers, HSS WTP uses Runtime Application Self-Protection (RASP) to monitor application access. It can detect tampering on dynamic data such as databases and prevent attackers from using applications to tamper with web pages in real time.

With HSS and WAF in place, you can stop worrying about web page tampering.

**Table 8-1** Differences between the web tamper protection functions of HSS and WAF

Type	HSS	WAF
Static web pages	Locks files in driver and web file directories to prevent attackers from tampering with them.	Caches static web pages on servers.
Dynamic web pages	<ul style="list-style-type: none"> <li>• Dynamic WTP Protects your data while Tomcat is running, detecting dynamic data tampering in databases.</li> <li>• Privileged process management Allows only privileged processes to modify web pages.</li> </ul>	Not supported
Backup and restoration	<ul style="list-style-type: none"> <li>• Proactive backup and restoration If WTP detects that a file in the protection directory is tampered with, it immediately uses the backup file on the local server to restore the file.</li> <li>• Remote backup and restoration If a file directory or backup directory on the local server becomes invalid, you can use the remote backup service to restore the tampered web page.</li> </ul>	Not supported
Protection object	Web tamper prevention. This function is suitable for websites that have high protection requirements.	Websites that only require application-layer protection

## Resource and Cost Planning


**Table 8-2** Resources and costs


Resource	Description	Monthly Fee
Host Security Service (HSS)	<ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Edition: WTP.</li> <li>• Server quota: 1</li> </ul>	For details about billing rules, see <a href="#">Billing Description</a> .

Resource	Description	Monthly Fee
Web Application Firewall	Cloud - Standard edition <ul style="list-style-type: none"><li>• Billing mode: Yearly/ Monthly</li><li>• Number of domain names that can be protected: 10</li><li>• QPS quota: 2,000 QPS</li><li>• Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li></ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

## Step 1: Configure a Web Tamper Protection Rule in WAF

**Step 1** [Log in to the management console](#).

**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

**Step 4** In the navigation pane on the left, choose **Policies**.

**Step 5** Click the name of the target policy to go to the protection configuration page.

**Step 6** Click the **Web Tamper Protection** configuration area and toggle it on or off if needed.

-  : enabled.
-  : disabled.

**Step 7** In the upper left corner above the **Web Tamper Protection** rule list, click **Add Rule**.

**Step 8** In the displayed dialog box, specify the parameters by referring to [Table 8-3](#).

**Figure 8-1** Adding a web tamper protection rule

**Add Web Tamper Protection Rule** ✕

\* Domain Name

\* Path

Rule Description

**OK**

**Table 8-3** Rule parameters


Parameter	Description	Example Value
Domain Name	Domain name of the website to be protected	<b>www.example.com</b>
Path	<p>A part of the URL, not including the domain name</p> <p>A URL is used to define the address of a web page. The basic URL format is as follows:</p> <p>Protocol name://Domain name or IP address[:Port]/[Path/.../File name].</p> <p>For example, if the URL is <b>http://www.example.com/admin</b>, set <b>Path</b> to <b>/admin</b>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>The path does not support regular expressions.</li> <li>The path cannot contain two or more consecutive slashes. For example, <b>///admin</b>. If you enter <b>///admin</b>, WAF converts <b>///</b> to <b>/</b>.</li> </ul>	<b>/admin</b>
Rule Description	A brief description of the rule. This parameter is optional.	None

**Step 9** Click **OK**. You can view the rule in the list of web tamper protection rules.

----End

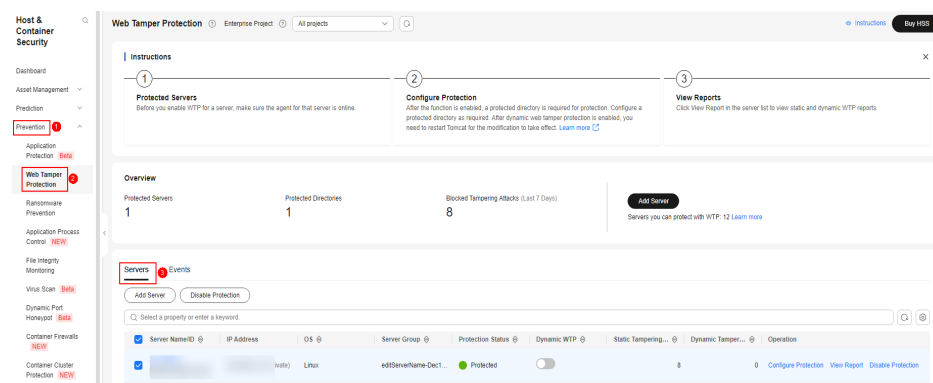
## Step 2: Enable HSS Web Tamper Protection

**Step 1** [Log in to the management console](#).

**Step 2** Click  in the upper left corner of the page, select a region, and choose **Security & Compliance** > **HSS** to go to the HSS management console.

**Step 3** In the navigation pane, choose **Server Protection** > **Web Tamper Protection**. On the **Web Tamper Protection** page, click **Add Server**.

**Figure 8-2** Adding a protected server



**Step 4** On the **Add Server** page, click the **Available servers** tab. Select the target server, select a quota from the drop-down list or retain the default value, and click **Add and Enable Protection**.

**Step 5** View the server status on the **Web Tamper Protection** page.

- Choose **Server Protection** > **Web Tamper Protection**. If the **Protection Status** of the server is **Protected**, WTP has been enabled.
- Choose **Asset Management** > **Servers & Quota** and click the **Servers** tab. If the protection status of the target server is **Enabled** and the **Edition/Expiration Date** of it is **Web Tamper Protection**, the WTP edition is enabled.

----End

#### NOTICE

- Before disabling WTP, perform a comprehensive detection on the server, handle known risks, and record operation information to prevent O&M errors and attacks on the server.
  - If WTP is disabled, web applications are more likely to be tampered with. Therefore, you need to delete important data on the server, stop important services on the server, and disconnect the server from the external network in a timely manner to avoid unnecessary losses caused by attacks on the server.
  - After you or disable WTP, files in the protected directory are no longer protected. You are advised to process files in the protected directory before performing these operations.
  - If you find some files missing after disabling WTP, search for them in the local or remote backup path.
  - The premium edition will be disabled when you disable WTP.
-

# 9 Configuring Header Field Forwarding to Disable Response Packet Compression

## Application Scenarios

The client usually declares that response compression is supported in the Accept-Encoding header, for example, Accept-Encoding: gzip. After the response passes through WAF, WAF considers that the response meets the compression standard and compresses the response. However, after receiving the response, the client cannot automatically decompress the response packet. The website then responds abnormally.

To address this issue, you can configure **Forward Field** to rewrite the **Accept-Encoding** header for the domain name on the WAF console so that WAF does not compress the response.

## Resource and Cost Planning

Table 9-1 Resources and costs

Resource	Description	Monthly Fee
Web Application Firewall	Cloud - professional edition: <ul style="list-style-type: none"><li>• Billing mode: Yearly/ Monthly</li><li>• Number of domain names that can be protected: 50</li><li>• QPS quota: 5,000 QPS</li><li>• Peak bandwidth: 200 Mbit/s inside the cloud and 50 Mbit/s outside the cloud</li></ul>	For details about pricing rules, see <a href="#">Billing Description</a> .



## Limitations and Constraints

Header field forwarding can be configured only in cloud CNAME access mode and dedicated mode.

### Step 1: Buy the Professional Edition Cloud WAF

The following describes how to buy the standard edition cloud WAF.

- Step 1** [Log in to Huawei Cloud management console](#).
  - Step 2** On the management console page, choose **Security & Compliance > Web Application Firewall**.
  - Step 3** In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select **Cloud Mode** for **WAF Mode**.
    - **Region:** Select the region nearest to your services WAF will protect.
    - **Edition:** Select **Professional**.
    - **Expansion Package** and **Required Duration:** Set them based on site requirements.
  - Step 4** Confirm the product details and click **Buy Now** in the lower right corner of the page.
  - Step 5** Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
  - Step 6** On the payment page, select a payment method and pay for your order.
- End

### Step 2: Add Website Information to WAF

The following example shows how to add a website information to WAF in cloud CNAME access mode.

- For details about the cloud load balancer access mode, see [Connecting a Website to WAF \(Cloud Mode - ELB Access\)](#).
  - For details about the dedicated mode, see [Connecting a Website to WAF \(Dedicated Mode\)](#).
- Step 1** In the navigation pane on the left, choose **Website Settings**.
  - Step 2** In the upper left corner of the website list, click **Add Website**.
  - Step 3** Select **Cloud - CNAME** and click **Configure Now**.
  - Step 4** Configure website information as prompted.

**Figure 9-1** Configuring basic information

**Basic Settings**

Protected Domain Name ?  
 [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  
 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 <span style="font-size: small;">v</span>	HTTP <span style="font-size: small;">v</span>	IPv4 <span style="font-size: small;">v</span> <input type="text" value="Enter a public IP ad"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	Delete

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

Use Layer-7 Proxy ?

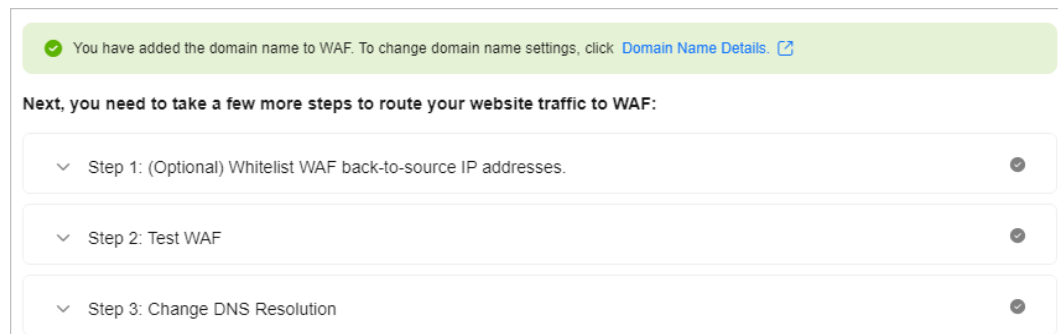
**Table 9-2** Key parameters

Parameter	Description	Example Value
Domain Name	Domain name you want to add to WAF for protection. <ul style="list-style-type: none"> <li>The domain name has an ICP license.</li> <li>You can enter a single domain name (for example, top-level domain name <b>example.com</b> or level-2 domain name <b>www.example.com</b>) or a wildcard domain name (<b>*.example.com</b>).</li> </ul>	www.example.com
Protected Port	The port over which the website traffic goes	Standard ports

Parameter	Description	Example Value
Server Configuration	<p>Web server address settings. You need to configure the client protocol, server protocol, server weights, server address, and server port.</p> <ul style="list-style-type: none"> <li>• <b>Client Protocol:</b> protocol used by a client to access a server. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>• <b>Server Protocol:</b> protocol used by WAF to forward client requests. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>• <b>Server Address:</b> 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.</li> <li>• <b>Server Port:</b> service port over which the WAF instance forwards client requests to the origin server.</li> <li>• <b>Weight:</b> Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.</li> </ul>	<p><b>Client Protocol:</b> Select <b>HTTP</b>.</p> <p><b>Server Protocol:</b> <b>HTTP</b></p> <p><b>Server Address:</b> <i>IPv4 XXX.XXX.1.1</i></p> <p><b>Server Port:</b> <b>80</b></p>
Use Layer-7 Proxy	<p>You need to configure whether you deploy layer-7 proxies in front of WAF.</p> <p>Set this parameter based on your website deployment.</p>	Yes

**Step 5** Click **Next**. Then, **whitelist WAF back-to-source IP address**, **test WAF**, and **modify DNS records** as prompted.

**Figure 9-2** Domain name added to WAF




----End

### Step 3: Configure Header Field Forwarding

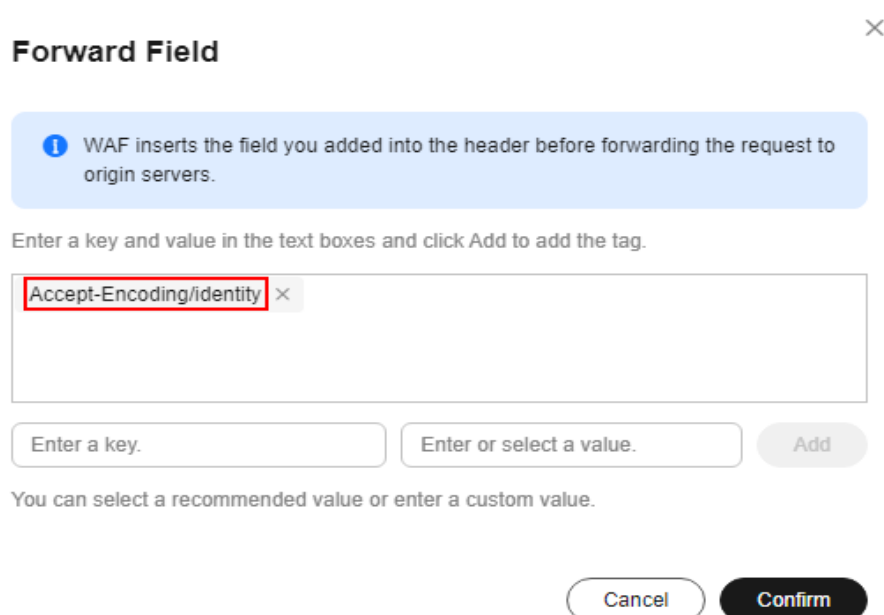
**Step 1** In the navigation pane on the left, choose **Website Settings**.

**Step 2** In the **Domain Name** column, click the website domain name to go to the basic information page.

**Step 3** In the **Forward Field** column, click . In the displayed **Forward Field** dialog box, enter a key/value pair, and click **Add**.

Set **Key** to **Accept-Encoding** and **Value** to **identity**.

**Figure 9-3** Forward Field



**Step 4** Click **Confirm**.

----End

# 10 Configuring Origin Server Security

## 10.1 Using WAF to Improve Connection Security

### Application Scenarios

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. The details are as follows:

- Minimum TLS version

The minimum TLS version that can be used by a client to access the website. After you configure the minimum TLS version, only the requests over the connections secured with the minimum TLS version or the later version can access your website. This helps you meet security requirements for industrial websites.

#### NOTE

- Up to now, three TLS versions (TLS v1.0, TLS v1.1, and TLS v1.2) have been released, among which TLS v1.0 and TLS v1.1 have been released for a long time. Some encryption algorithms (such as SHA1 and RC4) used by TLS v1.0 and TLS v1.1 are vulnerable to attacks. TLS v1.0 and TLS v1.1 cannot meet the geometric growth of data transmission encryption requirements, which might bring potential security risks. To secure the communication and meet the Payment Card Industry Data Security Standard (PCI DSS), PCI Security Standards Council (PCI SSC) stated that it no longer accepted TLS v1.0 as of June 30, 2018. Vendors of mainstream browsers, such as Mozilla Firefox, Apple Safari, Google Chrome, and Microsoft Edge, also declared that they would stop supporting TLS v1.0 and TLS v1.1 by 2020.
- You can query the TLS version supported by the website through other tools.
- Cipher suites

A cipher suite is a set of algorithms that help secure a network connection through TLS. A more secure cipher suite can better secure the confidentiality and data integrity of websites.

## Resource and Cost Planning

**Table 10-1** Resources and costs

Resource	Description	Monthly Fee
Web Application Firewall	Cloud - Standard edition <ul style="list-style-type: none"> <li>Billing mode: Yearly/ Monthly</li> <li>Number of domain names that can be protected: 10</li> <li>QPS quota: 2,000 QPS</li> <li>Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li> </ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

## Minimum TLS Versions Supported

The default minimum TLS version configured in WAF is **TLS v1.0**. To better secure your website, configure an appropriate TLS version. [Table 10-2](#) lists the minimum TLS versions supported for different scenarios.

**Table 10-2** Minimum TLS versions supported

Scenario	Minimum TLS Version (Recommended)	Protection Effect
Websites that handle critical business data, such as sites used in banking, finance, securities, and e-commerce.	TLS v1.2	WAF automatically blocks website access requests that use TLS v1.0 or TLS v1.1.
Websites with basic security requirements, for example, small- and medium-sized enterprise websites.	TLS v1.1	WAF automatically blocks website access requests that use TLS v1.0.
Client applications with no special security requirements	TLS v1.0	Requests using any TLS protocols can access the website.

## Cipher Suites Supported

The default cipher suite in WAF is **Cipher suite 1**. Cipher suite 1 offers a good mix of browser compatibility and security. For details about each cipher suite, see [Table 10-3](#).

**Table 10-3** Description of cipher suites

Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
<p>Classic cipher suite</p> <p><b>NOTE</b> By default, <b>Security cipher suite</b> is configured for websites. However, if the request does not carry the server name indication (SNI), WAF uses the <b>Classic cipher suite</b>.</p>	<ul style="list-style-type: none"> <li>• ECDHE-RSA-AES256-SHA384</li> <li>• AES256-SHA256</li> <li>• RC4</li> <li>• HIGH</li> </ul>	<ul style="list-style-type: none"> <li>• MD5</li> <li>• aNULL</li> <li>• eNULL</li> <li>• NULL</li> <li>• DH</li> <li>• EDH</li> <li>• AESGCM</li> </ul>	<ul style="list-style-type: none"> <li>• Compatibility: Good. A wide range of browsers are supported.</li> <li>• Security: Average</li> </ul>
Cipher suite 1	<ul style="list-style-type: none"> <li>• ECDHE-ECDSA-AES256-GCM-SHA384</li> <li>• HIGH</li> </ul>	<ul style="list-style-type: none"> <li>• MEDIUM</li> <li>• LOW</li> <li>• aNULL</li> <li>• eNULL</li> <li>• DES</li> <li>• MD5</li> <li>• PSK</li> <li>• RC4</li> <li>• kRSA</li> <li>• 3DES</li> <li>• DSS</li> <li>• EXP</li> <li>• CAMELLIA</li> </ul>	<p>Recommended configuration.</p> <ul style="list-style-type: none"> <li>• Compatibility: Good. A wide range of browsers are supported.</li> <li>• Security: Good</li> </ul>

Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
Cipher suite 2	<ul style="list-style-type: none"> <li>• ECDH+AESGCM</li> <li>• EDH+AESGCM</li> </ul>	-	<ul style="list-style-type: none"> <li>• Compatibility: Average. Strict compliance with forward secrecy requirements of PCI DSS and excellent protection, but browsers of earlier versions may be unable to access the website.</li> <li>• Security: Excellent</li> </ul>
Cipher suite 3	<ul style="list-style-type: none"> <li>• ECDHE-RSA-AES128-GCM-SHA256</li> <li>• ECDHE-RSA-AES256-GCM-SHA384</li> <li>• ECDHE-RSA-AES256-SHA384</li> <li>• RC4</li> <li>• HIGH</li> </ul>	<ul style="list-style-type: none"> <li>• MD5</li> <li>• aNULL</li> <li>• eNULL</li> <li>• NULL</li> <li>• DH</li> <li>• EDH</li> </ul>	<ul style="list-style-type: none"> <li>• Compatibility: Average. Earlier versions of browsers may be unable to access the website.</li> <li>• Security: Excellent. Multiple algorithms, such as ECDHE, DHE-GCM, and RSA-AES-GCM, are supported.</li> </ul>
Cipher suite 4	<ul style="list-style-type: none"> <li>• ECDHE-RSA-AES256-GCM-SHA384</li> <li>• ECDHE-RSA-AES128-GCM-SHA256</li> <li>• ECDHE-RSA-AES256-SHA384</li> <li>• AES256-SHA256</li> <li>• RC4</li> <li>• HIGH</li> </ul>	<ul style="list-style-type: none"> <li>• MD5</li> <li>• aNULL</li> <li>• eNULL</li> <li>• NULL</li> <li>• EDH</li> </ul>	<ul style="list-style-type: none"> <li>• Compatibility: Good. A wide range of browsers are supported.</li> <li>• Security: Average. The GCM algorithm is supported.</li> </ul>



Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
Cipher suite 5	<ul style="list-style-type: none"> <li>• AES128-SHA:AES256-SHA</li> <li>• AES128-SHA256:AES256-SHA256</li> <li>• HIGH</li> </ul>	<ul style="list-style-type: none"> <li>• MEDIUM</li> <li>• LOW</li> <li>• aNULL</li> <li>• eNULL</li> <li>• EXPORT</li> <li>• DES</li> <li>• MD5</li> <li>• PSK</li> <li>• RC4</li> <li>• DHE</li> </ul>	Supported algorithms: RSA-AES-CBC only
Cipher suite 6	<ul style="list-style-type: none"> <li>• ECDHE-ECDSA-AES256-GCM-SHA384</li> <li>• ECDHE-RSA-AES256-GCM-SHA384</li> <li>• ECDHE-ECDSA-AES128-GCM-SHA256</li> <li>• ECDHE-RSA-AES128-GCM-SHA256</li> <li>• ECDHE-ECDSA-AES256-SHA384</li> <li>• ECDHE-RSA-AES256-SHA384</li> <li>• ECDHE-ECDSA-AES128-SHA256</li> <li>• ECDHE-RSA-AES128-SHA256</li> </ul>	-	<ul style="list-style-type: none"> <li>• Compatibility: Average</li> <li>• Security: Good</li> </ul>

Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
Security cipher suite	<ul style="list-style-type: none"> <li>• ECDHE-ECDSA-AES256-GCM-SHA384</li> <li>• HIGH</li> </ul>	<ul style="list-style-type: none"> <li>• MEDIUM</li> <li>• LOW</li> <li>• aNULL</li> <li>• eNULL</li> <li>• DES</li> <li>• MD5</li> <li>• PSK</li> <li>• RC4</li> <li>• kRSA</li> <li>• SRP</li> <li>• 3DES</li> <li>• DSS</li> <li>• EXP</li> <li>• CAMELLIA</li> <li>• SHA1</li> <li>• SHA256</li> <li>• SHA384</li> </ul>	<p>This cipher suite supports all algorithms in cipher suite 1, except for the CBC algorithm. Recommended. This cipher suite can meet security requirements in most scenarios.</p> <ul style="list-style-type: none"> <li>• Compatibility: Average. Core suite: ECDHE-ECDSA-AES256-GCM-SHA384. Old protocols and weak algorithms are disabled. Browsers of earlier versions may fail to access the system.</li> <li>• Security: Excellent</li> </ul>
Cipher suite 8	<ul style="list-style-type: none"> <li>• AESGCM</li> <li>• HIGH</li> <li>• ECDHE</li> <li>• RSA</li> </ul>	<ul style="list-style-type: none"> <li>• DH</li> <li>• EXPORT</li> <li>• RC4</li> <li>• MEDIUM</li> <li>• LOW</li> <li>• aNULL</li> <li>• eNULL</li> </ul>	<p>Supports AES-GCM, providing strong encryption and data integrity protection.</p> <ul style="list-style-type: none"> <li>• Compatibility: Good. A wide range of browsers are supported.</li> <li>• Security: Good</li> </ul>

The cipher suites provided by WAF are compatible with the latest browsers and clients, but are incompatible with some browsers of earlier versions. Compatible browsers or clients of a certain cipher suite may vary depending on the TLS version configured. Using TLS v1.0 as an example, [Table 10-4](#) describes the browser and client compatibility.

**NOTICE**

It is recommended that compatibility tests should be carried out on the service environment to ensure service stability.

**Table 10-4** Incompatible browsers and clients for cipher suites under TLS v1.0

Browser/ Client	Classi c Ciphe r Suite	Ciph er Suite 1	Ciph er Suite 2	Ciph er Suite 3	Ciph er Suite 4	Ciphe r Suite 5	Cip her Suite 6	Secur ity Cip her Suite	Cip her Suite 8
Google Chrome 63 / macOS High Sierra 10.13.2	Not compatible	Compatible	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	√
Google Chrome 49/ Windows XP SP3	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Compatible	Compatible	Not compatible	√
Internet Explorer 6 /Windows XP	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Internet Explorer 8 /Windows XP	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Safari 6/iOS 6.0.1	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible	Not compatible	√
Safari 7/iOS 7.1	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible
Safari 7/OS X 10.9	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible


Browser/ Client	Classi c Ciphe r Suite	Ciph er Suite 1	Ciph er Suite 2	Ciph er Suite 3	Ciph er Suite 4	Ciphe r Suite 5	Cip her Suite 6	Secur ity Cip her Suite	Cip her Suite 8
Safari 8/iOS 8.4	Comp atible	Com patib le	Not com pati ble	Com patib le	Com patib le	Comp atible	Co mpa tible	Co mpa tible	Co mpa tible
Safari 8/OS X 10.10	Comp atible	Com patib le	Not com pati ble	Com patib le	Com patib le	Comp atible	Co mpa tible	Co mpa tible	Co mpa tible
Internet Explorer 7/Windows Vista	Comp atible	Com patib le	Not com pati ble	Com patib le	Com patib le	Not comp atible	√	Not com pati ble	√
Internet Explorer 8, 9, or 10 /Windows 7	Comp atible	Com patib le	Not com pati ble	Com patib le	Com patib le	Not comp atible	√	Not com pati ble	√
Internet Explorer 10 /Windows Phone 8.0	Comp atible	Com patib le	Not com pati ble	Com patib le	Com patib le	Not comp atible	√	Not com pati ble	√
Java 7u25	Comp atible	Com patib le	Not com pati ble	Com patib le	Com patib le	Not comp atible	√	Not com pati ble	√
OpenSSL 0.9.8y	Not comp atible	Not com pati ble	Not com pati ble	Not com pati ble	Not com pati ble	Not comp atible	Not com pati ble	Not com pati ble	√
Safari 5.1.9/OS X 10.6.8	Comp atible	Com patib le	Not com pati ble	Com patib le	Com patib le	Not comp atible	√	Not com pati ble	√


Browser/ Client	Classi c Ciphe r Suite	Ciph er Suite 1	Ciph er Suite 2	Ciph er Suite 3	Ciph er Suite 4	Ciphe r Suite 5	Cip her Suite 6	Sec urit y Cip her Suite	Cip her Suite 8
Safari 6.0.4/OS X 10.8.4	Comp atible	Com patib le	Not com pati ble	Com patib le	Com patib le	Not comp atible	√	Not com patib le	√

### Configuring the Minimum TLS Version and Cipher Suite

The following describes how to configure TLS v1.2 and cipher suite 1 as the minimum TLS version and how to verify that the configuration takes effect.

**Step 1** [Log in to the management console.](#)

**Step 2** Click  in the upper left corner of the management console and select a region or project.

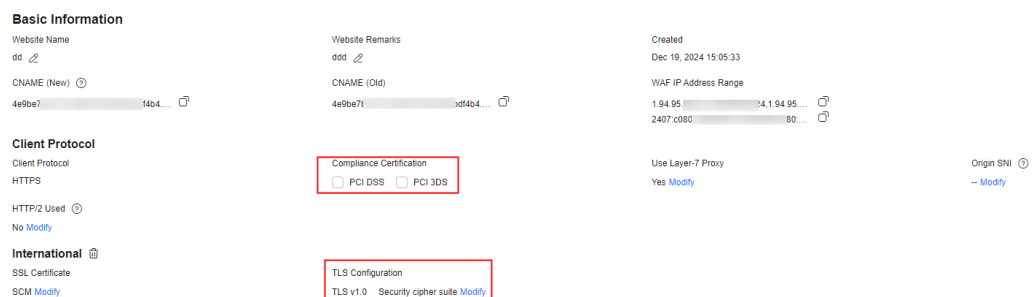
**Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

**Step 4** In the navigation pane on the left, choose **Website Settings**.

**Step 5** In the **Domain Name** column, click the website domain name to go to the basic information page.

**Step 6** Click  in the **TLS Configuration** row.

**Figure 10-1** TLS configuration modification



 **NOTE**

WAF allows you to enable PCI DSS and PCI 3-Domain Secure (3DS) compliance certification checks with just a few clicks. After they are enabled, WAF will configure the minimum TLS version in accordance with the PCI DSS and PCI 3DS compliance certification requirements.

- If you enable the PCI DSS certification check:
  - The minimum TLS version and cypher suite are automatically set to **TLS v1.2** and **EECDH+AESGCM:EDH+AESGCM**, respectively, and cannot be changed.
  - To change the minimum TLS version and cipher suite, disable the check.
- If you enable the PCI 3DS certification check:
  - The minimum TLS version is automatically set to **TLS v1.2** and cannot be changed.
  - The check cannot be disabled.

**Step 7** In the displayed **TLS Configuration** dialog box, select **TLS v1.2** as the minimum TLS version and **Cipher suite 1**.

**Figure 10-2** TLS Configuration

**TLS Configuration**

Certificate Name  
zrj-fun

Type  
International

Minimum TLS Version

Note: Requests to the domain must be made using the selected version or later. Otherwise, the requests will fail. TLS v1.2 is recommended because it is more secure.

Cipher Suite

Balanced security and compatibility.  
Encryption algorithms  
ECDHE-ECDSA-AES256-GCM-  
SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH

**Step 8** Click **Confirm**.

----End




## Verification

If the **Minimum TLS Version** is set to **TLS v1.2**, verify that the website can be accessed over connections secured by TLS v1.2 or later but cannot be accessed over connections secured by TLS v1.1 or earlier.

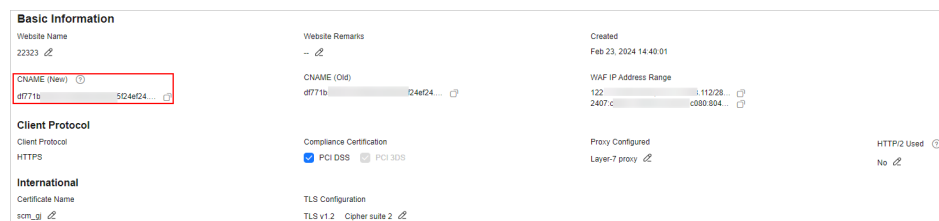
You can run commands on the local PC to check whether the TLS is configured successfully. Before the verification, ensure that **OpenSSL** has been installed on your local PC.

**Step 1** Copy the CNAME record of the protected domain name and use the CNAME record to obtain WAF access IP addresses.

1. [Log in to the management console](#).

2. Click  in the upper left corner of the management console and select a region or project.
3. Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
4. In the navigation pane on the left, choose **Website Settings**.
5. In the **Domain Name** column, click the domain name of the website to go to the basic information page.
6. In the **CNAME** row, click  to copy the CNAME record.

**Figure 10-3** Copying the CNAME record



**Step 2** Obtain the WAF access IP addresses.

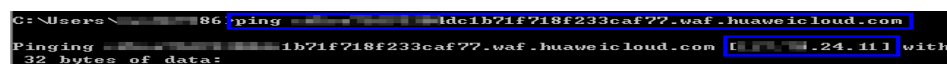
- Cloud mode

In the command line interface (CLI) of Windows OSs, run the following command to obtain WAF access IP addresses:

**ping** *CNAME record*

The command output displays WAF access IP addresses. [Figure 10-4](#) shows an example.

**Figure 10-4** ping cname



- Dedicated mode
  - a. In the navigation pane on the left, choose **Instances Management > Dedicated Engine** to go to the dedicated WAF instance page.
  - b. In the **IP Address** column, obtain the subnet IP addresses of all dedicated WAF instances. Those subnet IP addresses are access IP addresses of dedicated WAF instances.

**Step 3** Run the following command to verify that the protected website can be accessed using TLS v1.2.

**openssl s\_client -connect** *WAF access IP address* **-servername** "*Domain name of the protected website*" **-tls1\_2**

If the certificate information similar to the one shown in [Figure 10-5](#) is displayed, the website can be accessed using TLS v1.2.

**Figure 10-5** Verifying TLS v1.2

```
[root@VM_159_141_centos ~]# openssl s_client -connect 10.0.0.24.32:443 -servername "10.0.0.24.32.com" -tls1_2
CONNECTED(00000003)
depth=0 C = XX, L = Default City, O = Default Company Ltd, CN = waf.com
verify error:num=18:self signed certificate
verify return:1
depth=0 C = XX, L = Default City, O = Default Company Ltd, CN = waf.com
verify error:num=10:certificate has expired
notAfter=Oct 27 13:05:38 2018 GMT
verify return:1
depth=0 C = XX, L = Default City, O = Default Company Ltd, CN = waf.com
notAfter=Oct 27 13:05:38 2018 GMT
verify return:1
---
Certificate chain
 0 s:/C=XX/L=Default City/O=Default Company Ltd/CN=waf.com
 1 i:/C=XX/L=Default City/O=Default Company Ltd/CN=waf.com
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgIJAMJcdOLsrN3iMA0GCSqGSIb3DQEBCwUAMFQxCzAJBgNV
```

**Step 4** Run the following command to verify that the protected website cannot be accessed using TLS v1.1.

**openssl s\_client -connect** *WAF access IP address* **-servername** "*Protected domain name*" **-tls1\_1**

If no certificate information is displayed, as shown in [Figure 10-6](#), WAF has blocked the access that used TLS v1.1.

**Figure 10-6** Verifying TLS v1.1

```
[root@VM_159_141_centos ~]# openssl s_client -connect 10.0.0.24.32:443 -servername "10.0.0.24.32.com" -tls1_1
CONNECTED(00000003)
139740601669520:error:14094438:SSL routines:ssl3_read_bytes:tlsv1 alert internal error:s3_pkt.c:1493:SSL alert number 80
139740601669520:error:1409E0E5:SSL routines:ssl3_write_bytes:ssl handshake failure:s3_pkt.c:659:
---
no peer certificate available
---
no client certificate CA names sent
---
SSL handshake has read 7 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol  : TLSv1.1
  Cipher    : 0000
  Session-ID:
  Session-ID-ctx:
  Master-Key:
  Key-Ang   : None
  Krb5 Principal: None
  PSK identity: None
  PSK identity hint: None
  Start Time: 1556527943
  Timeout   : 7200 (sec)
  Verify return code: 0 (ok)
---
```

----End

## 10.2 Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers

### Application Scenarios

After you connect your website to Web Application Firewall (WAF), configure an access control policy on your origin server to allow only the WAF back-to-source IP



addresses. This prevents hackers from obtaining your origin server IP addresses and then bypassing WAF to attack origin servers.

This topic walks you through how to check whether origin servers have exposure risks and how to configure access control policies. This topic applies to scenarios where your origin servers are deploying on ECSs or have been added to backend servers of an ELB load balancer.

#### NOTE

- WAF will forward incoming traffic destined for the origin servers no matter whether you configure access control rules on the origin servers. However, if you have no access control rules configured on origin servers, bad actors may bypass WAF and directly attack your origin servers once they obtain your origin server IP addresses.
- If you use an NAT gateway before an ECS for forwarding data, you also need to configure an inbound rule in the security group the ECS belongs to by referring to [Configuring an Inbound Rule for an ECS](#). This rule allows only WAF IP addresses to access origin servers to keep them secure.

## Precautions

- Before configuring an access control policy on an origin server, ensure that you have connected all domain names of websites hosted on Elastic Cloud Server (ECS) or having Elastic Load Balance (ELB) deployed to WAF.
- The following issued should be considered when you configure a security group:
  - If you enable the WAF bypassed mode for your website but do not disable security group and network ACL configurations, the origin server may become inaccessible from the Internet.
  - If new WAF back-to-source IP addresses are assigned to WAF after a security group is configured for your website, the website may respond 5xx errors frequently.

## How Do I Check Whether the Origin Server IP Address Is Exposed?

In a non-Huawei Cloud environment, use a Telnet tool to establish a connection over the service port of the public IP address of your origin server (or enter the IP address of your web application in the browser). Then, check whether the connection is established.

- Connection established  
The origin server has exposed to the public. Once a hacker obtains the public IP address of the origin server, the hacker can bypass WAF and directly attack the origin server.
- Connection not established  
The origin server is hidden from the public and there is no exposure risk.

For example, to check whether the origin server is exposed, check whether the origin server IP address that has been protected by WAF can be connected over port 443. If information similar to that shown in [Figure 10-7](#) is displayed, the connection is established and the origin server IP address is exposed.


**Figure 10-7** Testing


```
[root@VM_0_4_centos ~]# telnet 14.215.177.20 443
Trying 14.215.177.20...
Connected to 14.215.177.20.
Escape character is '^]'.
```

## Obtaining WAF Back-to-Source IP Addresses

A back-to-source IP address is a source IP address used by WAF to forward client requests to origin servers. To origin servers, all web requests come from WAF and all source IP addresses are WAF back-to-source IP addresses. The real client IP address is encapsulated into the HTTP X-Forwarded-For (XFF) header field. For more details, see [How Do I Whitelist the WAF Back-to-Source IP Address Ranges?](#)

**Step 1** [Log in to the management console.](#)

**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

**Step 4** In the navigation pane on the left, choose **Website Settings**.

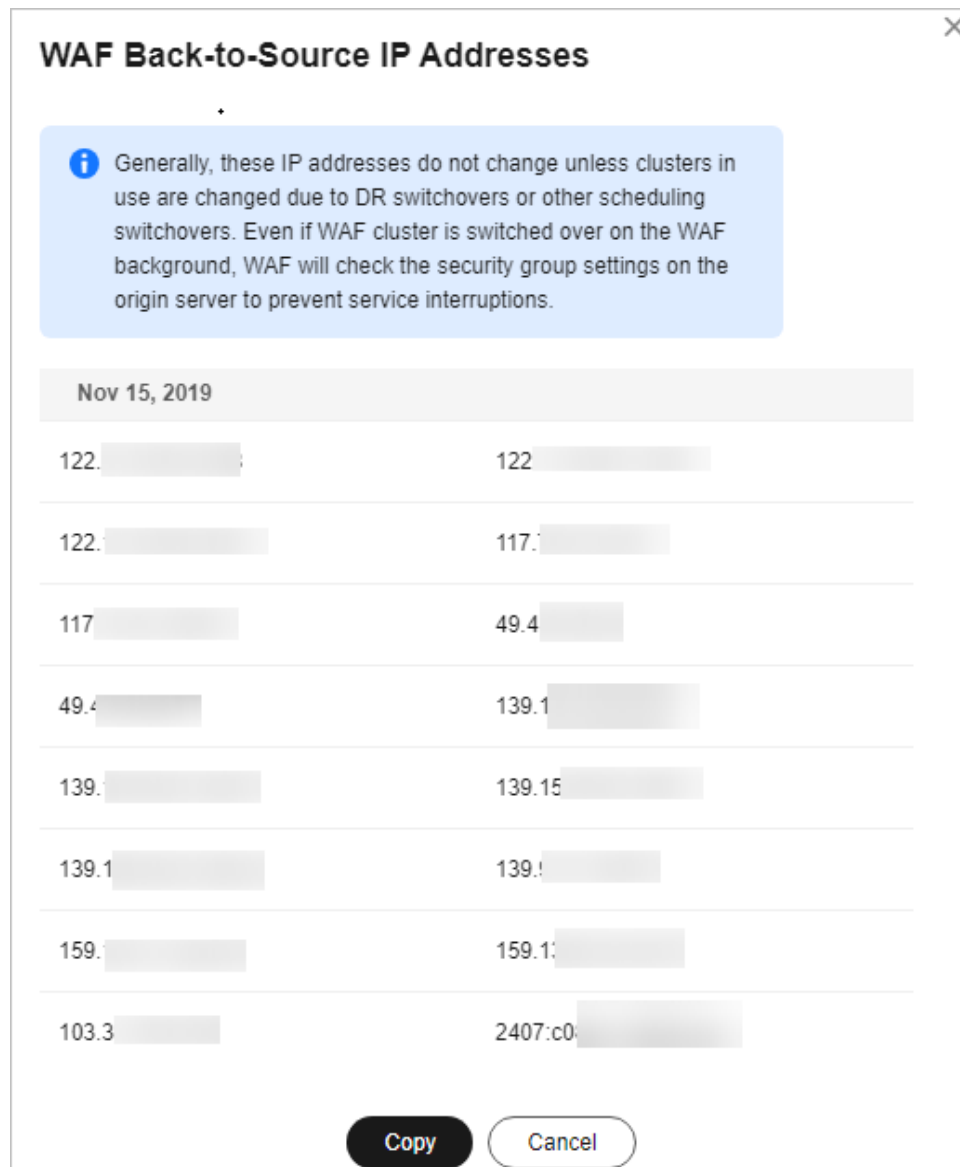
**Step 5** In the upper right corner above the website list, click the **WAF Back-to-Source IP Addresses** link.

 **NOTE**

WAF back-to-source IP addresses are periodically updated. Whitelist the new IP addresses in time to prevent those IP addresses from being blocked by origin servers.

**Step 6** In the displayed dialog box, click **Copy** to copy all the addresses.

Figure 10-8 WAF Back-to-Source IP Addresses dialog box





----End

## Configuring an Inbound Rule for an ECS

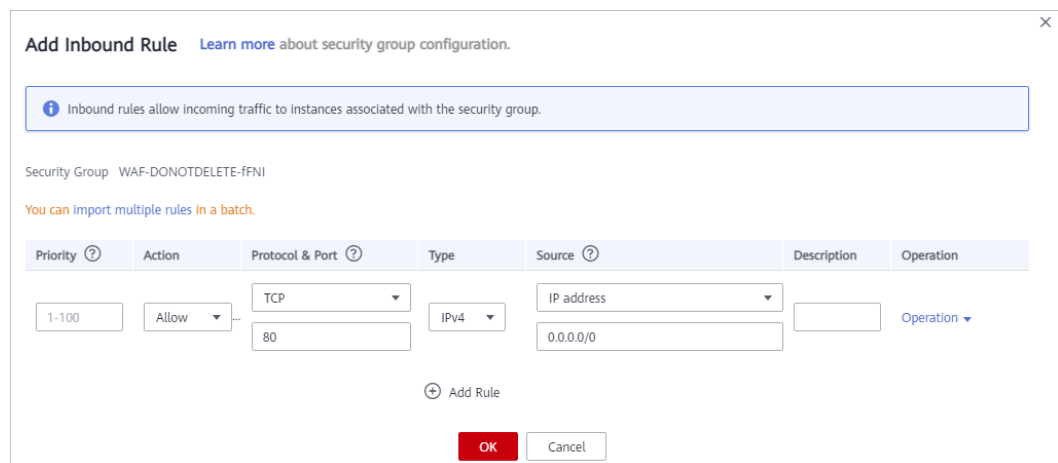
If your origin server is deployed on an ECS, perform the following steps to configure a security group rule to allow only the WAF back-to-source IP addresses to access the origin server.

### NOTICE

Ensure that all WAF back-to-source IP addresses are whitelisted by an inbound rule of the security group configured for the ECS. Otherwise, website may become inaccessible.

- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner of the page and choose **Compute > Elastic Cloud Server**.
- Step 4** Locate the row containing the ECS you want. In the **Name/ID** column, click the ECS name to go to the ECS details page.
- Step 5** Click the **Security Groups** tab. Then, click **Change Security Group**.
- Step 6** Click the security group ID and view the details.
- Step 7** Click the **Inbound Rules** tab and click **Add Rule**. Then, specify parameters in the **Add Inbound Rule** dialog box. For details, see [Table 10-5](#).

**Figure 10-9** Add Inbound Rule



**Table 10-5** Inbound rule parameters

Parameter	Description
Protocol & Port	Protocol and port for which the security group rule takes effect. If you select <b>TCP (Custom ports)</b> , enter the origin server port number in the text box below the TCP box.
Source	Add all WAF back-to-source IP addresses copied in <a href="#">Step 6</a> one by one. <b>NOTE</b> One IP address is configured in a rule. Click <b>Add Rule</b> to add more rules. A maximum of 10 rules can be added.

- Step 8** Click **OK**.
- Then, the security group rules allow all inbound traffic from the WAF back-to-source IP addresses.
- To check whether the security group rules take effect, refer to [How Do I Check Whether the Origin Server IP Address Is Exposed?](#) If a connection cannot be


established over the service port but the website is still accessible, the configuration takes effect.


----End

## Enabling ELB Access Control

If your origin server is deployed on backend servers of an ELB load balancer, perform the following steps to configure an access control list to allow only the WAF back-to-source IP addresses to access the origin server.

**Step 1** [Log in to the management console](#).

**Step 2** Click  in the upper left corner of the management console and select a region or project.



**Step 3** Click  in the upper left corner of the page and choose **Networking > Elastic Load Balance**.

**Step 4** Locate the load balancer you want. In the **Listener** column, click the listener name to go to the details page.

**Step 5** In the **Access Control** row of the target listener, click **Configure**.

**Figure 10-10** Listener list



NameID	Monitoring	Frontend Protocol/Port	Health Check	Default Backend Server Group	Access Control	Operation
listener-79c-f723959e-69f2-40be-b512-77054b127a29		HTTP/80	 Healthy	server_group-0001 <a href="#">View/Add Backend Server</a>	All IP addresses <a href="#">Configure</a>	<a href="#">Add/EB Forwarding Policy</a>   <a href="#">Edit</a>   <a href="#">Delete</a>

**Step 6** In the displayed dialog box, select **Whitelist** for **Access Control**.

1. Click **Create IP Address Group** and add the dedicated WAF instance IP addresses obtained in [Step 6](#) to the group being created.
2. Select the IP address group created in [Step 6.1](#) from the **IP Address Group** drop-down list.

**Step 7** Click **OK**.

To check whether the security group rules take effect, refer to [How Do I Check Whether the Origin Server IP Address Is Exposed?](#) If a connection cannot be established over the service port but the website is still accessible, the configuration takes effect.

----End

# 11 Using LTS to Analyze WAF Logs

## 11.1 Using LTS to Query and Analyze WAF Access Logs

### Application Scenarios

After you authorize WAF to access Log Tank Service (LTS), you can use the WAF logs recorded by **LTS** for quick and efficient real-time analysis, device O&M management, and analysis of service trends.

This practice uses the access log stream **lts-waf-access** of log group **lts-waf** as an example to describe how to use LTS to quickly query and analyze logs.

### Resource and Cost Planning

**Table 11-1** Resources and costs

Resource	Description	Monthly Fee
Log Tank Service (LTS)	<ul style="list-style-type: none"><li>Billing mode: Pay-per-use</li><li>New log volume: 10 GB/day</li><li>Log retention period: 7 days</li></ul>	For details about billing rules, see <a href="#">Billing Description</a> .

Resource	Description	Monthly Fee
Web Application Firewall	Cloud - Standard edition <ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Number of domain names that can be protected: 10</li> <li>• QPS quota: 2,000 QPS</li> <li>• Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li> </ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

### Step 1: Buy the Standard Edition Cloud WAF

The following describes how to buy the standard edition cloud WAF.

- Step 1** [Log in to Huawei Cloud management console](#).
  - Step 2** On the management console page, choose **Security & Compliance > Web Application Firewall**.
  - Step 3** In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select **Cloud Mode** for **WAF Mode**.
    - **Region**: Select the region nearest to your services WAF will protect.
    - **Edition**: Select **Standard**.
    - **Expansion Package** and **Required Duration**: Set them based on site requirements.
  - Step 4** Confirm the product details and click **Buy Now** in the lower right corner of the page.
  - Step 5** Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
  - Step 6** On the payment page, select a payment method and pay for your order.
- End

### Step 2: Add Website Information to WAF

The following example shows how to add a website information to WAF in cloud CNAME access mode.

- For details about the cloud load balancer access mode, see [Connecting a Website to WAF \(Cloud Mode - ELB Access\)](#).
- For details about the dedicated mode, see [Connecting a Website to WAF \(Dedicated Mode\)](#).

- Step 1** In the navigation pane on the left, choose **Website Settings**.

- Step 2** In the upper left corner of the website list, click **Add Website**.
- Step 3** Select **Cloud - CNAME** and click **Configure Now**.
- Step 4** Configure website information as prompted.

**Figure 11-1** Configuring basic information

**Basic Settings**

Protected Domain Name ?

[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

[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
<input type="text" value="HTTP"/>	<input type="text" value="HTTP"/>	<input type="text" value="IPv4"/> <input type="text" value="Enter a public IP ad"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	<input type="button" value="Delete"/>

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

Use Layer-7 Proxy ?

**Table 11-2** Key parameters

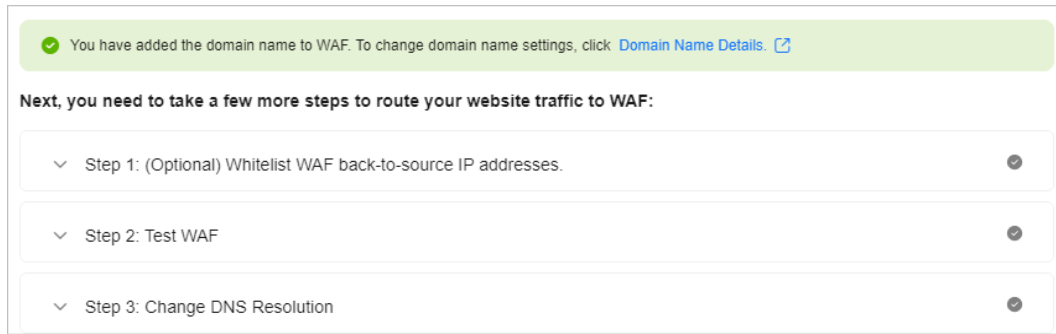
Parameter	Description	Example Value
Domain Name	Domain name you want to add to WAF for protection. <ul style="list-style-type: none"> <li>The domain name has an ICP license.</li> <li>You can enter a single domain name (for example, top-level domain name <b>example.com</b> or level-2 domain name <b>www.example.com</b>) or a wildcard domain name (<b>*.example.com</b>).</li> </ul>	www.example.com
Protected Port	The port over which the website traffic goes	Standard ports



Parameter	Description	Example Value
Server Configuration	<p>Web server address settings. You need to configure the client protocol, server protocol, server weights, server address, and server port.</p> <ul style="list-style-type: none"> <li>• <b>Client Protocol:</b> protocol used by a client to access a server. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>• <b>Server Protocol:</b> protocol used by WAF to forward client requests. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>• <b>Server Address:</b> 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.</li> <li>• <b>Server Port:</b> service port over which the WAF instance forwards client requests to the origin server.</li> <li>• <b>Weight:</b> Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.</li> </ul>	<p><b>Client Protocol:</b> Select <b>HTTP</b>.</p> <p><b>Server Protocol:</b> <b>HTTP</b></p> <p><b>Server Address:</b> <i>IPv4 XXX.XXX.1.1</i></p> <p><b>Server Port:</b> <b>80</b></p>
Use Layer-7 Proxy	<p>You need to configure whether you deploy layer-7 proxies in front of WAF.</p> <p>Set this parameter based on your website deployment.</p>	Yes

**Step 5** Click **Next**. Then, [whitelist WAF back-to-source IP address](#), [test WAF](#), and [modify DNS records](#) as prompted.


**Figure 11-2** Domain name added to WAF




----End


### Step 3: Enable LTS for Protection Logs

**Step 1** [Log in to the management console](#).

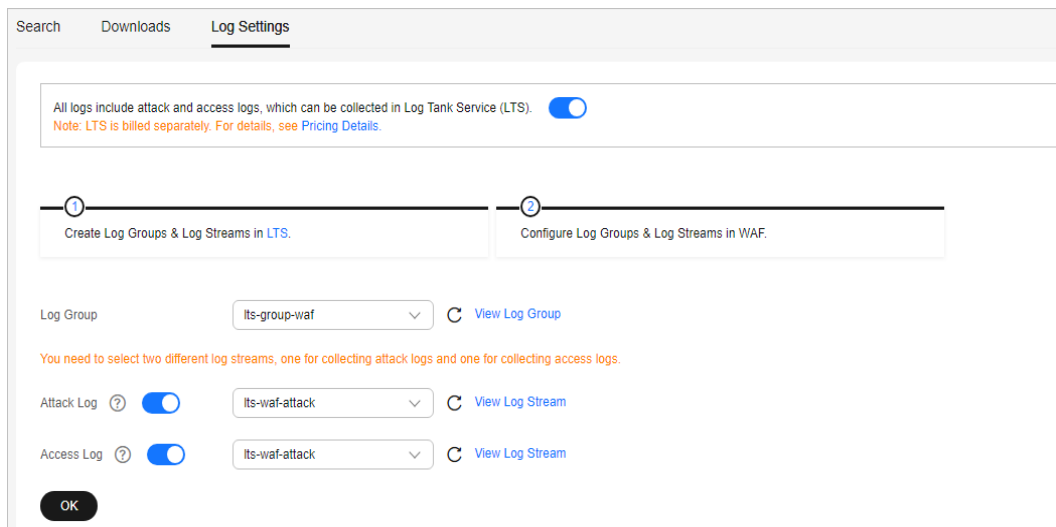
**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

**Step 4** In the navigation pane on the left, choose **Events**.

**Step 5** Click the **Log Settings** tab, enable LTS (  ), and select a log group and log stream. [Table 11-3](#) describes the parameters.

**Figure 11-3** Log settings



**Table 11-3** Log configuration


Parameter	Description	Example Value
Log Group	Select a log group or click <b>View Log Group</b> to go to the LTS console and create a log group.	lts-group-waf
Attack Log	Select a log stream or click <b>View Log Stream</b> to go to the LTS console and create a log stream.  An attack log includes information about event type, protective action, and attack source IP address of each attack.	lts-topic-waf-attack
Access Log	Select a log stream or click <b>View Log Stream</b> to go to the LTS console and create a log stream.  An access log includes key information about access time, client IP address, and resource URL of each HTTP access requests.	lts-topic-waf-access

**Step 6** Click **OK**.

You can view WAF protection event logs on the LTS console.

----End

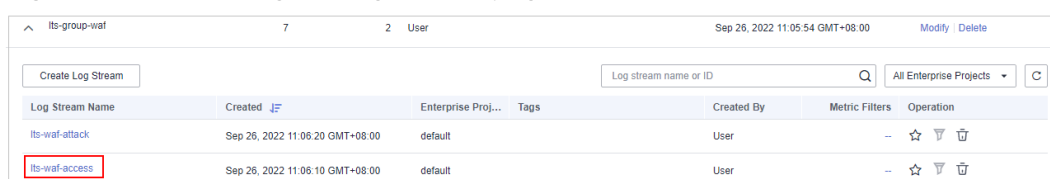
## Step 4: Query and Analyze WAF Access Logs in LTS


**Step 1** Click  in the upper left corner of the page and choose **Management & Governance > Log Tank Service**.

**Step 2** In the **Log Group Name** column, click the name of the target log group (for example, **lts-waf**) to go the log stream page.

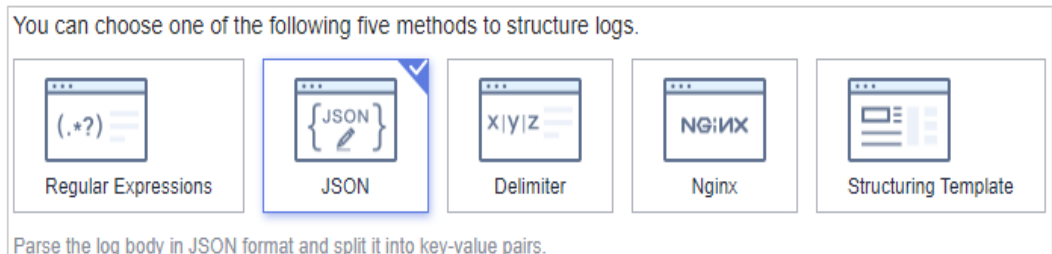
**Step 3** In the **Log Stream Name** column, click the name of the log stream used for WAF access logs (for example, **lts-waf-access**). Then, select the **Log Stream** tab.

**Figure 11-4** Accessing the log stream page



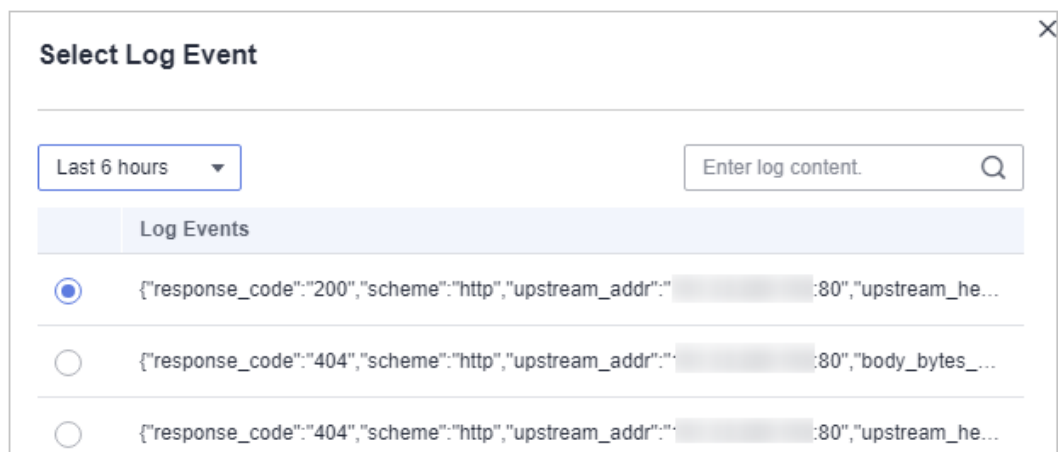
- Step 4** On the log stream details page, click  in the upper right corner. On the page displayed, click the **Cloud Structured Parsing** tab.
- Step 5** Select **JSON** as the log structure, as shown in [Figure 11-5](#).

**Figure 11-5** JSON



- Step 6** In the **Step 1 Select a sample log event** area, click **Select from existing log events**. In the displayed **Select Log Event** dialog box, select a log and click **OK**.

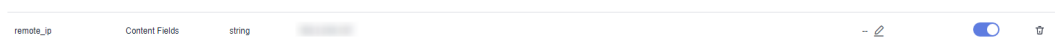
**Figure 11-6** Select Log Event



- Step 7** In the **Step 2 Extract fields** area, click **Intelligent Extraction** and enable quick analysis for the log field you want to analyze (for example, **remote\_ip**).

**remote\_ip**: IP address of a client from which the request originates.

**Figure 11-7** Selecting log fields for quick analysis



- Step 8** Click **Save**. Then, LTS will start a quick analysis and do statistics for logs collected in a certain period.

Figure 11-8 Quickly analysis of access logs



**Step 9** In the navigation pane, choose **Visualization**. On the right pane, select a log query time range, enter an SQL statement in the search box, and click **Query** to query the specified log.

You can enter either of the following SQL statements in the search box to query logs of a specified IP address:

**select \* where remote\_ip = 'xx.xx.xx.xx' or select \* where remote\_ip like 'xx.xx.xx%'**

----End

## 11.2 Using LTS to Analyze How WAF Blocks Spring Core RCE Vulnerabilities

### Application Scenarios

After you authorize WAF to access Log Tank Service (LTS), you can use the attack logs recorded by **LTS** for quick and efficient real-time analysis, device O&M management, and analysis of service trends.

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.

### Resource and Cost Planning

Table 11-4 Resources and costs

Resource	Description	Monthly Fee
Log Tank Service (LTS)	<ul style="list-style-type: none"> <li>Billing mode: Pay-per-use</li> <li>New log volume: 10 GB/day</li> <li>Log retention period: 7 days</li> </ul>	For details about billing rules, see <a href="#">Billing Description</a> .

Resource	Description	Monthly Fee
Web Application Firewall	Cloud - Standard edition <ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Number of domain names that can be protected: 10</li> <li>• QPS quota: 2,000 QPS</li> <li>• Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li> </ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

## Step 1: Buy the Standard Edition Cloud WAF

The following describes how to buy the standard edition cloud WAF.

- Step 1** [Log in to Huawei Cloud management console](#).
  - Step 2** On the management console page, choose **Security & Compliance > Web Application Firewall**.
  - Step 3** In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select **Cloud Mode** for **WAF Mode**.
    - **Region**: Select the region nearest to your services WAF will protect.
    - **Edition**: Select **Standard**.
    - **Expansion Package** and **Required Duration**: Set them based on site requirements.
  - Step 4** Confirm the product details and click **Buy Now** in the lower right corner of the page.
  - Step 5** Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
  - Step 6** On the payment page, select a payment method and pay for your order.
- End

## Step 2: Add Website Information to WAF

The following example shows how to add a website information to WAF in cloud CNAME access mode.

- For details about the cloud load balancer access mode, see [Connecting a Website to WAF \(Cloud Mode - ELB Access\)](#).
- For details about the dedicated mode, see [Connecting a Website to WAF \(Dedicated Mode\)](#).

- Step 1** In the navigation pane on the left, choose **Website Settings**.

- Step 2** In the upper left corner of the website list, click **Add Website**.
- Step 3** Select **Cloud - CNAME** and click **Configure Now**.
- Step 4** Configure website information as prompted.

**Figure 11-9** Configuring basic information

**Basic Settings**

Protected Domain Name ?

[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

[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
<input type="text" value="HTTP"/>	<input type="text" value="HTTP"/>	<input type="text" value="IPv4"/> <input type="text" value="Enter a public IP ad"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	<input type="button" value="Delete"/>

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

Use Layer-7 Proxy ?

**Table 11-5** Key parameters

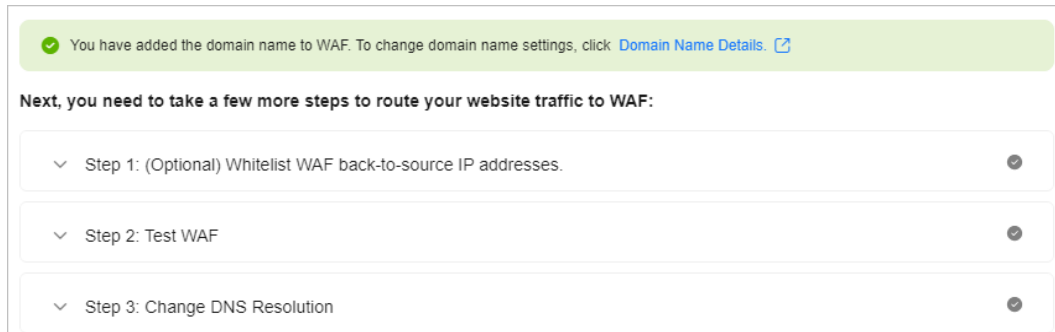
Parameter	Description	Example Value
Domain Name	Domain name you want to add to WAF for protection. <ul style="list-style-type: none"> <li>The domain name has an ICP license.</li> <li>You can enter a single domain name (for example, top-level domain name <b>example.com</b> or level-2 domain name <b>www.example.com</b>) or a wildcard domain name (<b>*.example.com</b>).</li> </ul>	www.example.com
Protected Port	The port over which the website traffic goes	Standard ports

Parameter	Description	Example Value
Server Configuration	<p>Web server address settings. You need to configure the client protocol, server protocol, server weights, server address, and server port.</p> <ul style="list-style-type: none"> <li>• <b>Client Protocol:</b> protocol used by a client to access a server. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>• <b>Server Protocol:</b> protocol used by WAF to forward client requests. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>• <b>Server Address:</b> 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.</li> <li>• <b>Server Port:</b> service port over which the WAF instance forwards client requests to the origin server.</li> <li>• <b>Weight:</b> Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.</li> </ul>	<p><b>Client Protocol:</b> Select <b>HTTP</b>.</p> <p><b>Server Protocol:</b> <b>HTTP</b></p> <p><b>Server Address:</b> <i>IPv4 XXX.XXX.1.1</i></p> <p><b>Server Port:</b> <b>80</b></p>
Use Layer-7 Proxy	<p>You need to configure whether you deploy layer-7 proxies in front of WAF.</p> <p>Set this parameter based on your website deployment.</p>	Yes

**Step 5** Click **Next**. Then, [whitelist WAF back-to-source IP address](#), [test WAF](#), and [modify DNS records](#) as prompted.




**Figure 11-10** Domain name added to WAF




----End


### Step 3: Enable LTS for Protection Logs

**Step 1** [Log in to the management console](#).

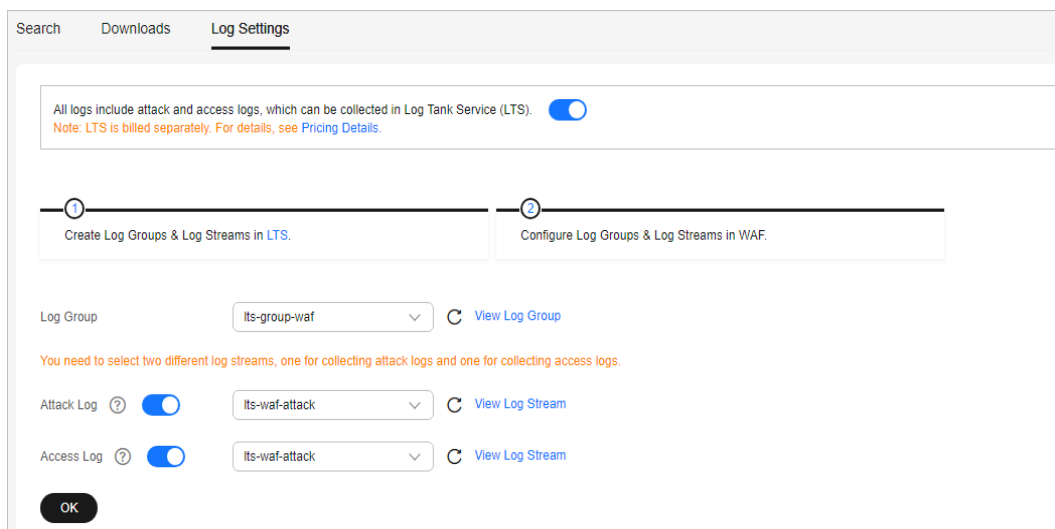
**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

**Step 4** In the navigation pane on the left, choose **Events**.

**Step 5** Click the **Log Settings** tab, enable LTS (  ), and select a log group and log stream. [Table 11-6](#) describes the parameters.

**Figure 11-11** Log settings



**Table 11-6** Log configuration


Parameter	Description	Example Value
Log Group	Select a log group or click <b>View Log Group</b> to go to the LTS console and create a log group.	lts-group-waf
Attack Log	Select a log stream or click <b>View Log Stream</b> to go to the LTS console and create a log stream.  An attack log includes information about event type, protective action, and attack source IP address of each attack.	lts-topic-waf-attack
Access Log	Select a log stream or click <b>View Log Stream</b> to go to the LTS console and create a log stream.  An access log includes key information about access time, client IP address, and resource URL of each HTTP access requests.	lts-topic-waf-access

**Step 6** Click **OK**.

You can view WAF protection event logs on the LTS console.

----End

## Step 4: Use LTS to Analyze How WAF Blocks Spring Core RCE Vulnerabilities

**Step 1** Click  in the upper left corner of the page and choose **Management & Governance > Log Tank Service**.

**Step 2** In the log group list, expand the WAF log group and choose log stream **attack**.

**Step 3** On the log stream details page, click  in the upper right corner. On the page displayed, click the **Cloud Structured Parsing** tab.

**Step 4** Select **JSON** for log structuring. Then, click **Select from existing events** and select a log in the dialog box displayed on the right.

**Step 5** Click **Intelligent Extraction** to find the fields you want to analyze quickly. Enable these fields in the **Quick Analysis** column. After this, you can collect and analyze periodic logs.

Figure 11-12 Log extraction field

Field	Source	Type	Example Value	Alias	Quick A...	Operation
action	Content Fields	string	block	--	<input checked="" type="checkbox"/>	
attack	Content Fields	string	custom_custom	--	<input checked="" type="checkbox"/>	
attack-time	Content Fields	string	2020-12-14T11:49:11.000Z	--	<input checked="" type="checkbox"/>	
attack_stream_id	Content Fields	string	d54c: [redacted] j6f067	--	<input checked="" type="checkbox"/>	
backend.alive	Content Fields	string	true	--	<input checked="" type="checkbox"/>	

**Step 6** Find the **category** field, click in the **Alias** column, change the field name, and click to save the settings.

**NOTE**

There is already a built-in **category** field in the system so you need to change the alias name of the **category** field, or your settings cannot be saved.

**Step 7** In the lower right corner of the list, click **Save**. LTS quickly analyzes and collects statistics on logs in the specified period.

**Step 8** In the navigation pane on the left, choose **Visualization**. Enter the following command and click **Query** to view the logs of the blocked Spring core RCE vulnerability.

**select rule, hit\_data where rule IN('XX','XX','XX','XX');**

Figure 11-13 Visualization query

rule	hit_data
091052	rf_http/rhc: [redacted] iserionstatus_123
091052	class module classloa [redacted]
091052	rf_http// [redacted] class module

----End

## 11.3 Using LTS to Configure Block Alarms for WAF Rules

### Application Scenarios

After you authorize WAF to access Log Tank Service (LTS), you can use the attack logs recorded by **LTS** for quick and efficient real-time analysis, device O&M management, and analysis of service trends.

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.

## Resource and Cost Planning

**Table 11-7** Resources and costs

Resource	Description	Monthly Fee
Log Tank Service (LTS)	<ul style="list-style-type: none"> <li>Billing mode: Pay-per-use</li> <li>New log volume: 10 GB/day</li> <li>Log retention period: 7 days</li> </ul>	For details about billing rules, see <a href="#">Billing Description</a> .
Simple Message Notification (SMN)	<p>SMN is billed based on downstream Internet traffic and notification messages. The fee composition in different scenarios is as follows:</p> <ul style="list-style-type: none"> <li>SMS: number of SMS notifications</li> <li>Email: Email notifications + Downstream Internet traffic</li> <li>HTTP or HTTPS: HTTP or HTTPS notifications + Downstream Internet traffic</li> </ul>	For details about billing rules, see <a href="#">Billing Description</a> .
Web Application Firewall (WAF)	<p>Cloud - Standard edition</p> <ul style="list-style-type: none"> <li>Billing mode: Yearly/ Monthly</li> <li>Number of domain names that can be protected: 10</li> <li>QPS quota: 2,000 QPS</li> <li>Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li> </ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

### Step 1: Buy the Standard Edition Cloud WAF

The following describes how to buy the standard edition cloud WAF.

- Step 1** [Log in to Huawei Cloud management console.](#)
- Step 2** On the management console page, choose **Security & Compliance > Web Application Firewall**.
- Step 3** In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select **Cloud Mode** for **WAF Mode**.
- **Region:** Select the region nearest to your services WAF will protect.
  - **Edition:** Select **Standard**.
  - **Expansion Package** and **Required Duration:** Set them based on site requirements.
- Step 4** Confirm the product details and click **Buy Now** in the lower right corner of the page.
- Step 5** Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
- Step 6** On the payment page, select a payment method and pay for your order.
- End

## Step 2: Add Website Information to WAF

The following example shows how to add a website information to WAF in cloud CNAME access mode.

- For details about the cloud load balancer access mode, see [Connecting a Website to WAF \(Cloud Mode - ELB Access\)](#).
  - For details about the dedicated mode, see [Connecting a Website to WAF \(Dedicated Mode\)](#).
- Step 1** In the navigation pane on the left, choose **Website Settings**.
- Step 2** In the upper left corner of the website list, click **Add Website**.
- Step 3** Select **Cloud - CNAME** and click **Configure Now**.
- Step 4** Configure website information as prompted.

**Figure 11-14** Configuring basic information

**Basic Settings**

Protected Domain Name ?  
 [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  
 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 <span style="float: right;">v</span>	HTTP <span style="float: right;">v</span>	IPv4 <span style="float: right;">v</span> <input type="text" value="Enter a public IP ad"/>	<input type="text" value="80"/>	<input type="text" value="1"/>	Delete

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

Use Layer-7 Proxy ?

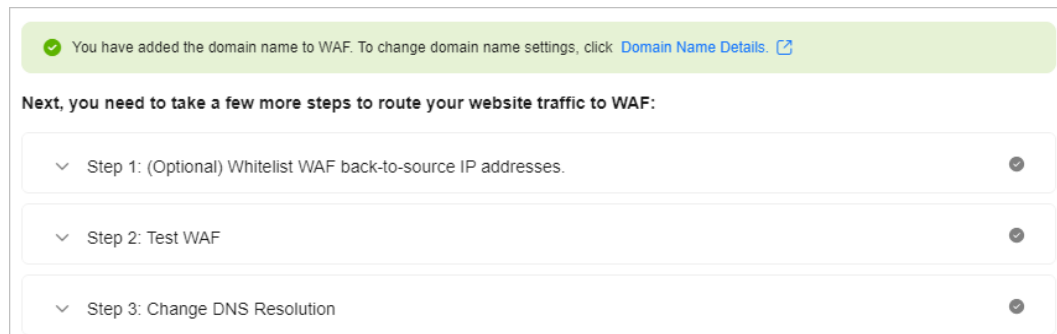
**Table 11-8** Key parameters

Parameter	Description	Example Value
Domain Name	Domain name you want to add to WAF for protection. <ul style="list-style-type: none"> <li>The domain name has an ICP license.</li> <li>You can enter a single domain name (for example, top-level domain name <b>example.com</b> or level-2 domain name <b>www.example.com</b>) or a wildcard domain name (<b>*.example.com</b>).</li> </ul>	www.example.com
Protected Port	The port over which the website traffic goes	Standard ports

Parameter	Description	Example Value
Server Configuration	<p>Web server address settings. You need to configure the client protocol, server protocol, server weights, server address, and server port.</p> <ul style="list-style-type: none"> <li>● <b>Client Protocol:</b> protocol used by a client to access a server. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Protocol:</b> protocol used by WAF to forward client requests. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Address:</b> 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.</li> <li>● <b>Server Port:</b> service port over which the WAF instance forwards client requests to the origin server.</li> <li>● <b>Weight:</b> Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.</li> </ul>	<p><b>Client Protocol:</b> Select <b>HTTP</b>.</p> <p><b>Server Protocol:</b> <b>HTTP</b></p> <p><b>Server Address:</b> <i>IPv4 XXX.XXX.1.1</i></p> <p><b>Server Port:</b> <b>80</b></p>
Use Layer-7 Proxy	<p>You need to configure whether you deploy layer-7 proxies in front of WAF.</p> <p>Set this parameter based on your website deployment.</p>	Yes

**Step 5** Click **Next**. Then, [whitelist WAF back-to-source IP address](#), [test WAF](#), and [modify DNS records](#) as prompted.


**Figure 11-15** Domain name added to WAF




----End


### Step 3: Enable LTS for Protection Logs

**Step 1** [Log in to the management console](#).

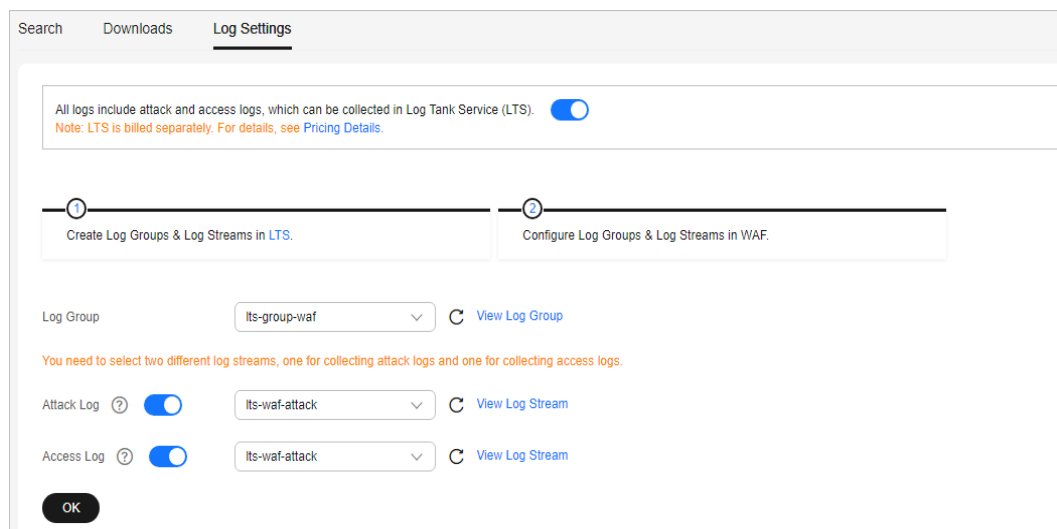
**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

**Step 4** In the navigation pane on the left, choose **Events**.

**Step 5** Click the **Log Settings** tab, enable LTS (  ), and select a log group and log stream. [Table 11-9](#) describes the parameters.

**Figure 11-16** Log settings





**Table 11-9** Log configuration


Parameter	Description	Example Value
Log Group	Select a log group or click <b>View Log Group</b> to go to the LTS console and create a log group.	lts-group-waf
Attack Log	Select a log stream or click <b>View Log Stream</b> to go to the LTS console and create a log stream.  An attack log includes information about event type, protective action, and attack source IP address of each attack.	lts-topic-waf-attack
Access Log	Select a log stream or click <b>View Log Stream</b> to go to the LTS console and create a log stream.  An access log includes key information about access time, client IP address, and resource URL of each HTTP access requests.	lts-topic-waf-access

**Step 6** Click **OK**.

You can view WAF protection event logs on the LTS console.

----End

## Step 4: Quickly Analyze Block Logs Generated by Protection Rules

**Step 1** Click  in the upper left corner of the page and choose **Management & Governance > Log Tank Service**.

**Step 2** In the log group list, expand the WAF log group and choose log stream **attack**.

**Step 3** On the log stream details page, click  in the upper right corner. On the page displayed, click the **Cloud Structured Parsing** tab.

**Step 4** Select **JSON** for log structuring. Then, click **Select from existing events** and select a log in the dialog box displayed on the right.

**Step 5** Click **Intelligent Extraction** to find the fields you want to analyze quickly. Enable these fields in the **Quick Analysis** column. After this, you can collect and analyze periodic logs.

**Figure 11-17** Log extraction field

Field	Source	Type	Example Value	Alias	Quick A...	Operation
action	Content Fields	string	block	-	<input checked="" type="checkbox"/>	
attack	Content Fields	string	custom_custom	-	<input checked="" type="checkbox"/>	
attack-time	Content Fields	string	2020-12-14T11:49:11.000Z	-	<input checked="" type="checkbox"/>	
attack_stream_id	Content Fields	string	d54f: [redacted] j5f067	-	<input checked="" type="checkbox"/>	
backend.alive	Content Fields	string	true	-	<input checked="" type="checkbox"/>	

**Step 6** Find the **category** field, click in the **Alias** column, change the field name, and click to save the settings.

**NOTE**

There is already a built-in **category** field in the system so you need to change the alias name of the **category** field, or your settings cannot be saved.

**Step 7** In the lower right corner of the list, click **Save**. LTS quickly analyzes and collects statistics on logs in the specified period.

**Step 8** In the navigation pane, choose **Visualization**. On the right pane, select a log query time range, enter an SQL statement in the search box, and click **Query**.

You can group logs by rule and URI. Enter the following SQL statement in the search box to query logs of a specified rule:

**select rule, uri, count(\*) as cnt where action = 'block' group by rule, uri order by cnt desc**

----End

## Step 5: Configure Alarm Rules

**Step 1** Click in the upper left corner of the page and choose **Management & Governance > Log Tank Service**.

**Step 2** In the navigation pane on the left, choose **Alarms > Alarm Rules**.

**Step 3** Click **Create**. In the dialog box displayed on the right, specify related parameters. [Table 11-10](#) describes the parameters.

**Figure 11-18** Create Alarm Rule

**Create Alarm Rule** ?

\* Rule Name: WAF

Description:

\* Statistics: By keyword | **By SQL**

\* Charts: 0

\* Log Group Name: waf

\* Log Stream Name: attack

Query Time Range: 1 h

Query Statement: `select rule,uri,count(*) as cnt where action='block' group by rule,uri order by cnt desc` [Preview](#)

+ Configure from Scratch | + Import Configuration

**Trigger**

\* Query Frequency: Custom int... | 1 | m

\* Conditional Expression: `cnt>5`

• If you have selected one chart and the query statement is `select count(*) as pv`, you can enter `pv > 10`.

• If you have selected two charts and the query statements are `select count(*) as pv` and `select count(*) as uv`, you can enter `$0.pv > 10 && $1.uv < 2`. [Learn more](#)

OK | Cancel

**Table 11-10** Parameter description

Parameter	Description	Example Value
Rule Name	Name of the custom rule	WAF alarms
Statistics	Select <b>By SQL</b> .	By SQL

Parameter	Description	Example Value
Charts	<p>Click <b>Configure from Scratch</b>.</p> <ul style="list-style-type: none"> <li>Specify <b>Log Group Name</b> and <b>Log Stream Name</b>.</li> <li><b>Query Time Range</b>: Time range for log statistics</li> <li><b>Query Statement</b>: Enter the SQL statement configured in <a href="#">Step 8</a>, for example, <b>select rule,uri,count(*) as cnt where action='block' group by rule,uri order by cnt desc</b>.</li> </ul>	None
Query Frequency	Frequency which triggers alarms Generally, a fixed custom interval of 5 minutes is selected.	Custom interval 5 minutes
Conditional Expression	Alarm threshold	cnt>5
Alarm Severity	Select an alarm severity based on the blocking emergency of the rule. The options are <b>critical</b> , <b>major</b> , <b>minor</b> , and <b>info</b> .	Major
Send Notification	Select <b>Yes</b> .	Yes
SMN Topic	<p>Select a topic from the drop-down list or create a topic.</p> <p>If there are no topics, click <b>View Topic</b> and perform the following steps to create a topic:</p> <ol style="list-style-type: none"> <li>Create a topic. For details, see <a href="#">Creating a Topic</a>.</li> <li>Add one or more subscriptions to the topic. You will need to provide a phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see <a href="#">Adding a Subscription</a>.</li> <li>Confirm the subscription. After the subscription is added, confirm the subscription.</li> </ol> <p>For details about topics and subscriptions, see the <i>Simple Message Notification User Guide</i>.</p>	None

Parameter	Description	Example Value
Time Zone/ Language	You can modify the language and time zone for receiving messages.	None
Message Templates	Select an existing template from the drop-down list box or click <b>Create Message Template</b> and create a template.	sql_template

**Step 4** Confirm all parameters and click **OK**. The alarm rule is configured. When the alarm rule is triggered, you will receive an alarm email or SMS message.

----End

# 12 Obtaining the Real Client IP Addresses

---

## Application Scenarios

A client IP address refers to an IP address of a visitor (or the device a visitor uses to initiate the request). Sometimes, a web application needs to require the client IP address. For example, a voting system needs to obtain the client IP addresses to ensure that each client casts only once.

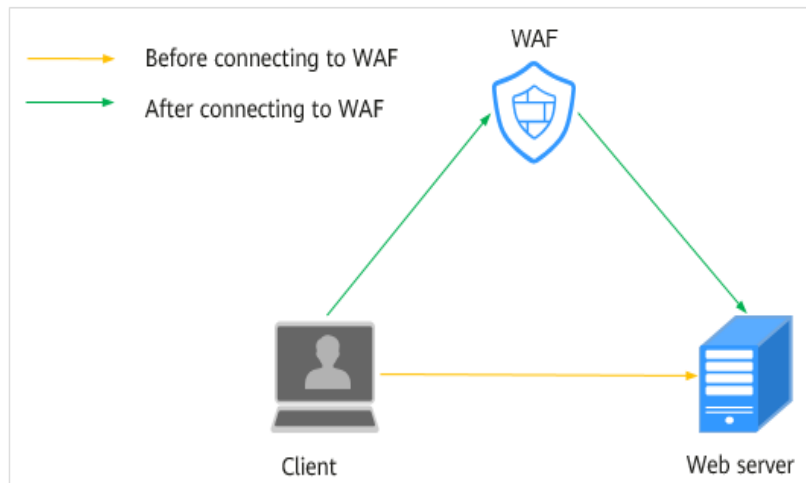
After your website is connected to WAF, WAF works as a reverse proxy between the client and the server. The real IP address of the server is hidden, and only the IP addresses of WAF are visible to web visitors. In this case, you can obtain the real IP address of the client through WAF or configure the website server to obtain the real IP address of the client.

The following 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.

## Architecture

Generally, a browser request does not directly reach the web server. Proxy servers, such as CDN, WAF, and advanced anti-DDoS, may be deployed between the browser and the origin server. Using WAF as an example, see [Figure 12-1](#).

**Figure 12-1** WAF deployment diagram



**NOTE**

- DNS resolves your domain name to the origin server IP address before your website is connected to WAF. Therefore, web visitors can directly access the server.
- After your website is connected to WAF, DNS resolves your domain name to the CNAME record of WAF. In this way, the traffic passes through WAF. WAF then filters out illegitimate traffic and only routes legitimate traffic back to the origin server.

In this case, the access request may be forwarded by multiple layers of security or acceleration proxies before reaching the origin server. So, how does the server obtain the real IP address of the client that initiates the request?

When forwarding HTTP requests to the downstream server, the transparent proxy server adds an **X-Forwarded-For** field to the HTTP header to identify the client IP address in the format of **X-Forwarded-For: client IP address, proxy 1-IP address, proxy 2-IP address, proxy 3-IP address, .....->....**

Then, you can obtain the client IP address from the **X-Forwarded-For** field, the first IP address in which is the client IP address.

**Constraints**

- Ensure that **Use Layer-7 Proxy** is configured correctly when you add a website to the WAF instance, or WAF cannot obtain the real IP address of your website visitors.  
To ensure that WAF obtains real client IP addresses and takes protective actions configured in protection policies, select **Yes** for **Use Layer-7 Proxy** when your website has a layer-7 proxy server such as CDN and cloud acceleration products deployed in front of WAF. In other cases, select **No** for **Use Layer-7 Proxy**.
- In normal cases, the first IP address in the **X-Forwarded-For** field is the real IP address of the client. If the length of an IPv6 address exceeds the length limit of the **X-Forwarded-For** field, the IP address cannot be read. In NAT64, the load balancer uses IPv4 listeners, which cannot read IPv6 addresses.

## Obtaining the Client IP Address from WAF

After a website is connected to WAF, WAF is deployed between the client and server as a reverse proxy to protect the website. The principles for WAF to obtain the real IP address are as follows:

- If you select **Yes** for **Use Layer-7 Proxy** when you add a domain name to WAF, WAF obtains the source IP address in the following sequence:
  - a. The source IP header list configured in **upstream** is preferentially used, that is, the IP address tag configured on the basic information page of the domain name. For details, see [Configuring a Traffic Identifier for a Known Attack Source](#). If no IP address is available, go to **b**.

### NOTE

If you want to use a TCP connection IP address as the client IP address, set **IP Tag** to **remote\_addr**.

- b. Obtain the value of the **cdn-src-ip** field in the source IP header list configured in the **config** file. If no value is obtained, go to **c**.
  - c. Obtain the value of the **x-real-ip** field. If no value is obtained, go to **d**.
  - d. Obtain the first public IP address from the left of the **x-forwarded-for** field. If no public IP address is obtained, go to **e**.
  - e. Obtain the value of the **remote\_addr** field, which includes the IP address used for establishing the TCP connection.
- If no proxy is used, that is, you select **No** for **Use Layer-7 Proxy** when adding the domain name to WAF, WAF obtains the source IP address from the **remote\_ip** field.

The following describes how WAF uses the X-Forwarded-For and X-Real-IP variables to obtain the real IP address of a client:

- Using the **X-Forwarded-For** field to obtain the client IP address  
The client IP address is placed in the **X-Forwarded-For** HTTP header field. The format is as follows:

```
X-Forwarded-For: Client IP address,Proxy 1-IP address,Proxy 2-IP address,...
```

### NOTE

The first IP address included in the **X-Forwarded-For** field is the client IP address.

The methods to obtain the **X-Forwarded-For** field by invoking the SDK interface in different programming languages are as follows:

- **ASP**  
`Request.ServerVariables("HTTP_X_FORWARDED_FOR")`
- **ASP.NET(C#)**  
`Request.ServerVariables["HTTP_X_FORWARDED_FOR"]`
- **PHP**  
`$_SERVER["HTTP_X_FORWARDED_FOR"]`
- **JSP**  
`request.getHeader("HTTP_X_FORWARDED_FOR")`

- Using the **X-Real-IP** field to obtain the client IP address (modifications caused by reverse proxies is considered)

The methods to obtain the **X-Real-IP** field by invoking the SDK interface in different programming languages are as follows:



- **ASP**  
Request.ServerVariables("HTTP\_X\_REAL\_IP")
- **ASP.NET(C#)**  
Request.ServerVariables["HTTP\_X\_REAL\_IP"]
- **PHP**  
\$\_SERVER["HTTP\_X\_REAL\_IP"]
- **JSP**  
request.getHeader("HTTP\_X\_REAL\_IP")

## How Does Tomcat Obtain the Client IP Address from Access Logs?

If Tomcat is deployed on your origin server, you can enable the X-Forwarded-For function of Tomcat to obtain the client IP address.

**Step 1** Open the **server.xml** file in the **tomcat/conf/** directory. Partial information about the AccessLogValue logging function is as follows:

```
<Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true">
  <Valve className="org.apache.catalina.valves.AccessLogValue" directory="logs"
    prefix="localhost_access_log." suffix=".txt"
    pattern="%h %l %u %t \"%r\" %s %b" />
```

**Step 2** Add **%{X-Forwarded-For}i** to **pattern**. Part of the modified **server.xml** file is as follows:

```
<Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true">
  <Valve className="org.apache.catalina.valves.AccessLogValue" directory="logs"
    prefix="localhost_access_log." suffix=".txt"
    pattern="%{X-Forwarded-For}i %h %l %u %t \"%r\" %s %b" />
</Host>
```

**Step 3** View the **localhost\_access\_log** file to obtain the client IP address from the **X-Forwarded-For** field.

----End

## How Does Apache Obtain the Client IP Address from Access Logs?

If Apache HTTP Server 2.4 or later is deployed on your origin server, you can use the **mod\_remoteip.so** file under **remoteip\_module** in the Apache installation package to obtain the real client IP address.

- CentOS 7.6
  - a. Add the following content to the **httpd.conf** file:

```
LoadModule remoteip_module modules/mod_remoteip.so ##Load the mod_remoteip.so module.
RemoteIPHeader X-Forwarded-For ## Set RemoteIPHeader.
RemoteIPInternalProxy WAF IP address range##Set the WAF back-to-source IP address range.
```

For more details, see [How Do I Whitelist the WAF Back-to-Source IP Address Ranges?](#)

### NOTE

- File **/etc/httpd/conf.modules.d/00-base.conf:46** has been added to the **mod\_remoteip.so** module.
- Use spaces to separate multiple back-to-source IP address ranges.
- b. Replace **%h** with **%a** in the log format file.

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

- c. Restart the Apache service to make the configuration take effect.
- Ubuntu 20.04.2
  - a. Add the following content to the **apache2.conf** file:

```
In -s ../mods-available/remotepip.load /etc/apache2/mods-enabled/remotepip.load ##Load the mod_remotepip.so module.
RemotepIPHeader X-Forwarded-For ## Set RemotepIPHeader.
RemotepIPInternalProxy WAF IP address range##Set the WAF back-to-source IP address range.
```

For more details, see [How Do I Whitelist the WAF Back-to-Source IP Address Ranges?](#)

#### NOTE

- You can also add the following content to load the **mod\_remotepip.so** module:

```
LoadModule remotepip_module /usr/lib/apache2/modules/
mod_remotepip.so
```
  - Use spaces to separate multiple back-to-source IP address ranges.
- b. Replace **%h** with **%a** in the log format file.

```
LogFormat "%a %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%a %l %u %t \"%r\" %>s %b" common
```
  - c. Restart the Apache service to make the configuration take effect.

If Apache 2.2 or earlier is deployed on your origin server, to obtain the real client IP address, you can run commands to install third-party module **mod\_rpaf** of Apache and modify the **httpd.conf** file

**Step 1** Run the following commands to install third-party module **mod\_rpaf** for Apache:

```
wget https://github.com/gnif/mod_rpaf/archive/v0.6.0.tar.gz
tar xvfz mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/usr/local/apache/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

**Step 2** Open the **httpd.conf** configuration file and modify the file content as follows:

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so ##Load module mod_rpaf.
<IfModule mod_rpaf.c>
RPAFenable On
RPAFsethostname On
RPAFproxy_ips 127.0.0.1 <Reverse proxy IP address>
RPAFheader X-Forwarded-For
</IfModule>
```

**Step 3** Define the log format.

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

**Step 4** Enable customized logs.

```
CustomLog "[Apache server directory]/logs/$access.log" common
```

**Step 5** Restart the Apache server for the configuration to take effect.

```
/[Apache server directory]/httpd/bin/apachectl restart
```

**Step 6** View the **access.log** file to obtain the client IP address from the **X-Forwarded-For** field.

----End

## How Does Nginx Obtain the Client IP Address from Access Logs?

If an Nginx reverse proxy is deployed on your origin server, you can configure location information on the Nginx reverse proxy so that the backend web server can use similar functions to obtain the client IP address

- Step 1** Configure the following information in the corresponding location of the Nginx reverse proxy to obtain the information about the client IP address:

```
Location ^ /<uri> {
    proxy_pass ....;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}
```

- Step 2** The backend web server obtains the real IP address of your website visitors by defining the Nginx log parameter `$http_x_forwarded_for`.

**Example**

```
log_format main ' "<$http_Cdn_Src_IP>" "${http_x_real_ip}" "[${http_x_forwarded_for}" "$remote_addr"
' '$http_user_agent - $remote_user [$time_local] "$request" ' ' $status $body_bytes_sent "$http_referer" ';
```

----End

## How Does IIS 6 Obtain the Client IP Address from Access Logs?

If you have deployed an IIS 6 server on your origin server, you can install the **F5XForwardedFor.dll** plug-in and obtain the client IP address from the access logs recorded by the IIS 6 server.

- Step 1** Download the [F5XForwardedFor](#) module.
- Step 2** Copy the **F5XForwardedFor.dll** file in the **x86\Release** or **x64\Release** directory to a specified directory (for example, **C:\ISAPIFilters**) based on the operating system version of your server. Ensure that the IIS process has the read permission for the directory.
- Step 3** Open the IIS manager, right-click the website that is currently open, and choose **Attribute** from the shortcut menu. The **Attribute** page is displayed.
- Step 4** On the **Attribute** page, switch to **ISAPI filter** and click **Add**. In the dialog box that is displayed, configure the following information:
- **Filter Name:** Set this parameter to **F5XForwardedFor**.
  - **Executable file:** Set this parameter to the full path of **F5XForwardedFor.dll**, for example, **C:\ISAPIFilters\F5XForwardedFor.dll**.
- Step 5** Click **OK** to restart the IIS 6 server.
- Step 6** View the access logs recorded by the IIS 6 server (the default log path is **C:\WINDOWS\system32\LogFiles\**, and the IIS log file name extension is **.log**). You can obtain client IP address from the **X-Forwarded-For** field.

----End

## How Does IIS 7 Obtain the Client IP Address from Access Logs?

If you have deployed an IIS 7 server on your origin server, you can install the **F5XForwardedFor.dll** module and obtain the client IP address from the access logs recorded by the IIS 7 server.

- Step 1** Download the [F5XForwardedFor](#) module.
- Step 2** Copy the **F5XFFHttpModule.dll** and **F5XFFHttpModule.ini** files in the **x86\Release** or **x64\Release** directory to a specified directory (for example, **C:\x\_forwarded\_for\x86** or **C:\x\_forwarded\_for\x64**) based on the operating

system version of your server. Ensure that the IIS process has the read permission for the directory.

- Step 3** On the server home page, double-click **Modules** to go to the **Modules** page.
- Step 4** Click **Configure Native Module**. In the dialog box displayed, click **Register**.
- Step 5** In the displayed dialog box, register the downloaded DLL file according to the operating system, and then click **OK**.
- x86 operating system: registration module **x\_forwarded\_for\_x86**
    - **Name:** x\_forwarded\_for\_x86
    - **Path:** C:\x\_forwarded\_for\x86\F5XFFHttpModule.dll
  - x64: Register the module **x\_forwarded\_for\_x64**.
    - **Name:** x\_forwarded\_for\_x64
    - **Path:** C:\x\_forwarded\_for\x64\F5XFFHttpModule.dll
- Step 6** After the registration is complete, select the newly registered module (**x\_forwarded\_for\_x86** or **x\_forwarded\_for\_x64**) and click **OK**.
- Step 7** In **ISAPI and CGI restriction**, add the registered DLL files by operating system and change **Restriction** to **Permitting**.
- x86 operating system:
    - **ISAPI or CGI path:** C:\x\_forwarded\_for\x86\F5XFFHttpModule.dll
    - **Description:** x86
  - x64 operating system:
    - **ISAPI or CGI path:** C:\x\_forwarded\_for\x64\F5XFFHttpModule.dll
    - **Description:** x64
- Step 8** Restart the IIS 7 server and wait for the configuration to take effect.
- Step 9** View the access logs recorded by the IIS 7 server (the default log path is **C:\WINDOWS\system32\LogFiles\**, and the IIS log file name extension is **.log**). You can obtain the client IP address from the **X-Forwarded-For** field.

----End

## How Does WAF Obtain the Real Client IP Addresses for Services Deployed in CCE?

If your service is deployed on Cloud Container Engine (CCE), CCE records the real client IP address in the **X-Original-Forwarded-For** field and records the WAF back-to-source address in the **X-Forwarded-For** field. You need to modify the CCE configuration file to enable Ingress to add the real IP address to the **X-Forwarded-For** field. In this way, WAF can obtain the real client IP address.

To modify the CCE configuration file, take the following steps:

- Step 1** Run the following command to modify the **kube-system/nginx-configuration** configuration file:

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

- Step 2** Add the following information to the configuration file:

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

**Step 3** Save the configuration file.

The configuration takes effect after you save the file. Ingress adds the real client IP addresses to the **X-Forwarded-For** field.

**Step 4** Modify the field for the service to obtain the real client IP addresses to **X-Original-Forwarded-For**.

----End

# 13 Configuring Alarms on Cloud Eye for Abnormal WAF Metrics

## Application Scenarios

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.

For details, see [WAF Monitored Metrics](#).

## Prerequisites

- [You have connected a website to WAF](#).
- You have enabled Cloud Eye.

## Resource and Cost Planning

Table 13-1 Resources and costs


Resource	Description	Monthly Fee
WAF	Cloud - Standard edition <ul style="list-style-type: none"><li>• Billing mode: Yearly/ Monthly</li><li>• Number of domain names that can be protected: 10</li><li>• QPS quota: 2,000 QPS</li><li>• Peak bandwidth: 100 Mbit/s inside the cloud and 30 Mbit/s outside the cloud</li></ul>	For details about pricing rules, see <a href="#">Billing Description</a> .


Resource	Description	Monthly Fee
Cloud Eye	<ul style="list-style-type: none"> <li>Basic functions of Cloud Eye, such as viewing monitoring panels, creating alarm rules, and adding monitoring items, are free of charge.</li> <li>If you want to receive alarm notifications, you need to pay for it. SMN is billed based on the usage of SMS, emails, or HTTP/HTTPS requests. For details, see <a href="#">Billing</a>.</li> </ul>	-

## Configuring a Monitoring Alarm Rule

You can set WAF alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring scope, and whether to send notifications. This helps you learn the WAF protection status in a timely manner.

**Step 1** [Log in to the management console](#).

**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Hover over  in the upper left corner of the page and choose **Management & Governance > Cloud Eye**.

**Step 4** In the navigation pane on the left, choose **Alarm Management > Alarm Rules**.

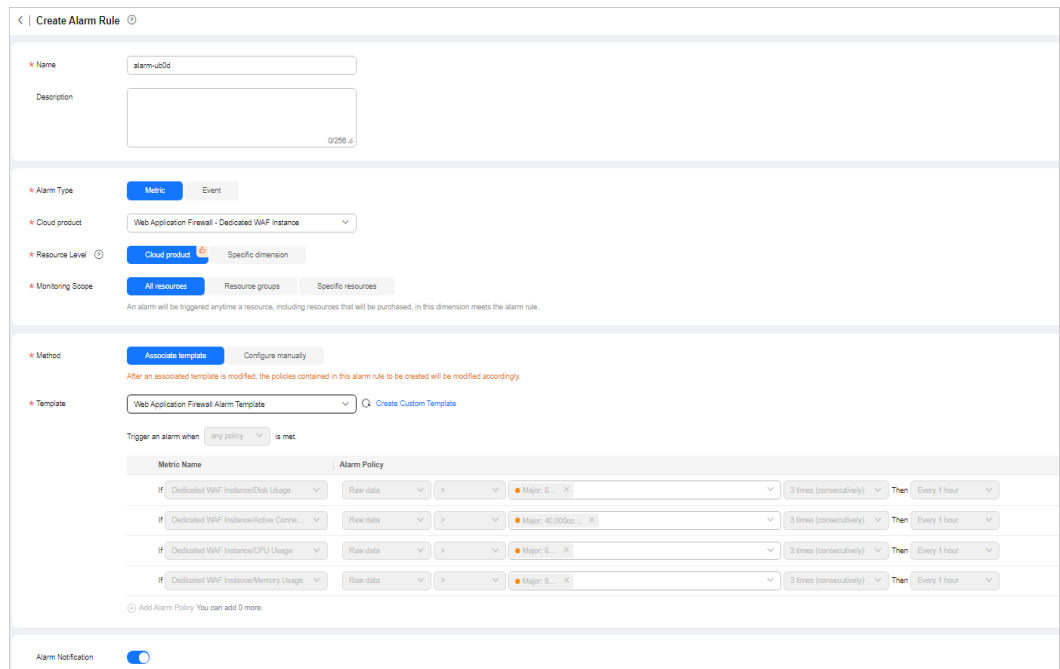
**Step 5** In the upper right corner of the page, click **Create Alarm Rule**.

**Step 6** Configure related parameters.

- **Name:** Enter a name.
- **Alarm Type:** Select **Metric**.
- **Cloud product:** Select **Web Application Firewall - Dedicated WAF Instance** or **Web Application Firewall - Domains**.
  - For dedicated instance metrics, select **Web Application Firewall - Dedicated WAF Instance** as the monitored metric.
  - For protected domain names, select **Web Application Firewall - Domains**.
- **Monitoring Scope:** Select **All resources**.
- **Method:** Select **Associated template** or create a custom template.
- **Alarm Notification:** If you want to receive alarms in real time, enable this option and select a notification mode.

- Other parameters: Set them based on site requirements.

**Figure 13-1** Create Alarm Rule



**Step 7** Click **Create**. In the displayed dialog box, click **OK**.

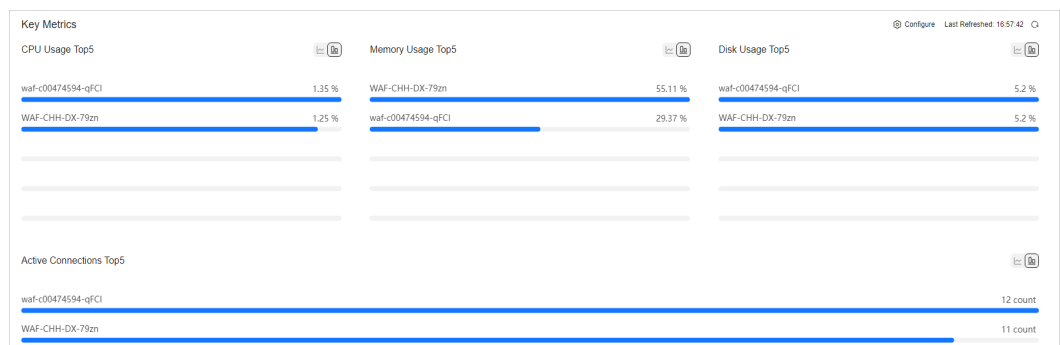
----End

## Viewing Monitored Metrics

You can view WAF metrics on the Cloud Eye console and learn about the WAF protection status in a timely manner.

- Step 1** In the navigation pane on the left, choose **Cloud Service Monitoring**.
- Step 2** Search for **Web Application Firewall WAF** by **Dashboard** in the search box. In the **Dashboard** column, click **Web Application Firewall WAF** to go to the **Details** page.
- Step 3** On the **Overview** tab, you can view metrics related to resource overview and alarm statistics.

**Figure 13-2** Viewing key metrics



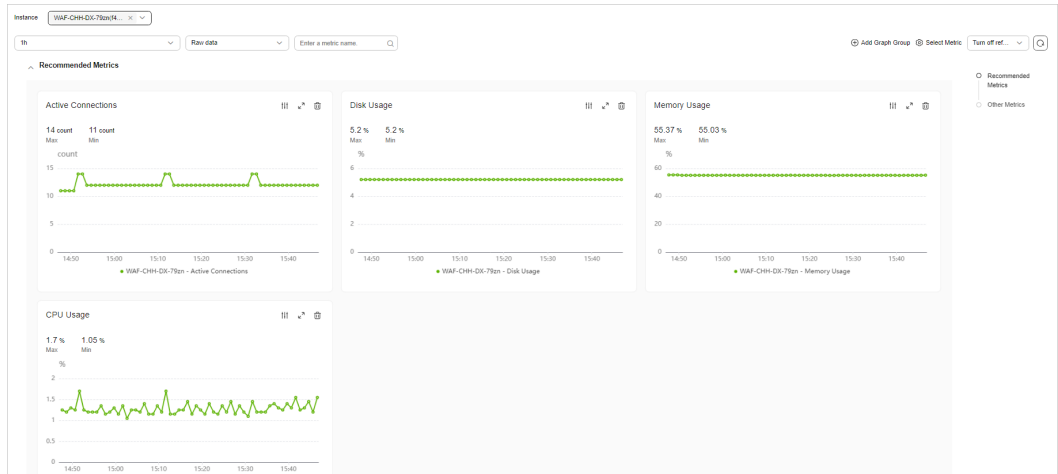


**Step 4** Click the **Resources** tab. In the **Operation** column of the instance list, click **View Metric**.

**NOTE**

To view the monitoring information about a specific website, you can go to the **Website Settings** page on the WAF console, locate the row containing the target domain name and click **Cloud Eye** in the **Operation** column.

**Figure 13-3** Viewing monitored metrics



----End

# 14 Migrating Protection Policies for Your Website

## Application Scenarios

This topic will walk you through on how to migrate your website protection policies from Alibaba Cloud WAF to Huawei Cloud WAF.

We will show how to complete the migration from Alibaba Cloud **pay-per-use WAF 3.0** to Huawei Cloud **professional edition cloud WAF**.

## Resource and Cost Planning

**Table 14-1** Resources and costs

Resource	Description	Monthly Fee
Web Application Firewall (WAF)	Cloud - professional edition: <ul style="list-style-type: none"> <li>• Billing mode: Yearly/ Monthly</li> <li>• Number of domain names that can be protected: 50</li> <li>• QPS quota: 5,000 QPS</li> <li>• Peak bandwidth: 200 Mbit/s inside the cloud and 50 Mbit/s outside the cloud</li> </ul>	For details about pricing rules, see <a href="#">Billing Description</a> .

## Step 1: Buy Huawei Cloud Professional Edition Cloud WAF

**Step 1** [Log in to Huawei Cloud management console](#).

**Step 2** On the management console page, choose **Security & Compliance > Web Application Firewall**.

**Step 3** In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select **Cloud Mode** for **WAF Mode**.

- **Region:** Select the region nearest to your services WAF will protect.
- **Edition:** Select **Professional**.
- **Expansion Package and Required Duration:** Set them based on site requirements.

**Step 4** Confirm the product details and click **Buy Now** in the lower right corner of the page.

**Step 5** Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.

**Step 6** On the payment page, select a payment method and pay for your order.

----End

## Step 2: Connect the Website to Huawei Cloud WAF

**Step 1** In the navigation pane on the left, choose **Website Settings**.

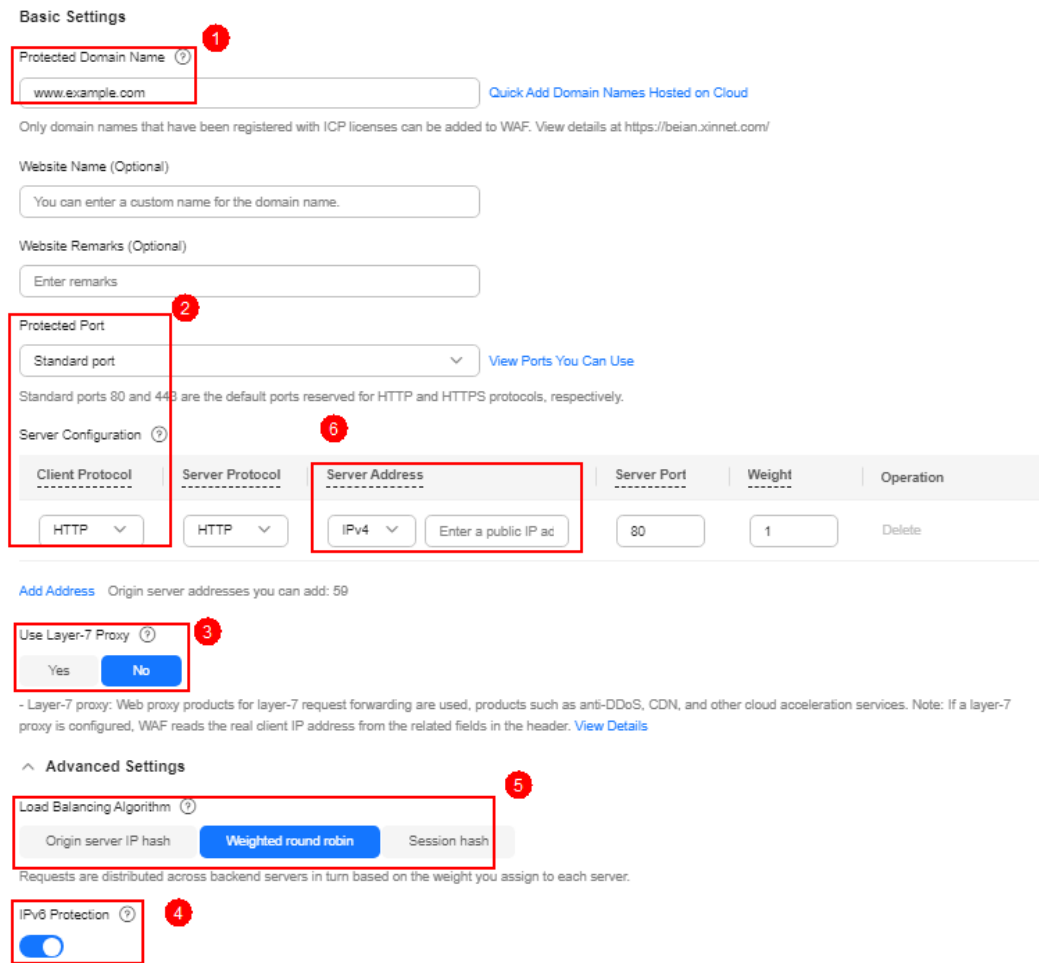
**Step 2** In the upper left corner of the website list, click **Add Website**.

**Step 3** Select **Cloud - CNAME** and click **Configure Now**.

**Step 4** Configure website details. [Table 14-2](#) describes the parameter mappings between Huawei Cloud and Alibaba Cloud.

On the Alibaba Cloud WAF console, choose **Website Configuration > CNAME Record**. In the **Actions** column of the row containing the target domain name, click **Edit** and check its configuration details.

**Figure 14-1** Domain name configuration page

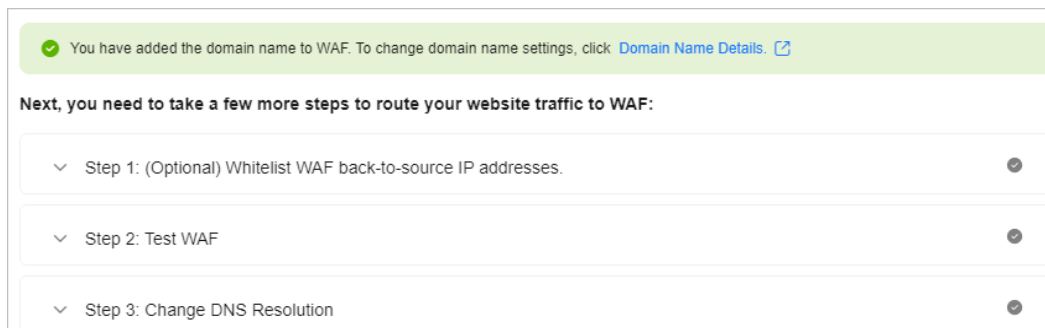


**Table 14-2** Parameter mappings

Parameter No. in Figure 14-1	Alibaba Cloud	Huawei Cloud
①	Domain Name	Domain Name
②	Protocol Type/Port	Client Protocol/Protected Port
③	Whether Layer 7 Proxy, Such as Anti-DDoS Pro, Anti-DDoS Premium, or Alibaba Cloud CDN, Is Deployed in Front of WAF	Use Layer-7 Proxy
④	IPv6	IPv6 Protection
⑤	Load Balancing Algorithm	Load Balancing Algorithm
⑥	Origin Server Address	Server Address
⑦	Protection Resource	<i>Automatically generated</i>

**Step 5** Click **Next**. Then, **whitelist WAF back-to-source IP address**, **test WAF**, and **modify DNS records** as prompted.

**Figure 14-2** Domain name added to WAF



----End

### Step 3: Migrating Protection Rules

**Table 14-3** summarizes mappings between Alibaba Cloud WAF rules and Huawei Cloud WAF rules.

**Table 14-3** Protection rule mappings

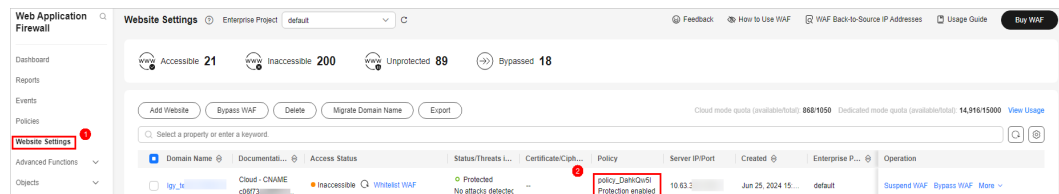
Alibaba Cloud	Huawei Cloud	Reference
Basic protection rule	Basic web protection	<a href="#">Configuring Basic Web Protection Rules to Defend Against Common Web Attacks</a>
Whitelist	<ul style="list-style-type: none"> <li>Blacklist and whitelist</li> <li>Global protection whitelist</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses</a></li> <li><a href="#">Configuring a Global Protection Whitelist Rule to Ignore False Alarms</a></li> </ul>
IP address blacklist	Blacklist and whitelist	<ul style="list-style-type: none"> <li><a href="#">Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses</a></li> </ul>
Custom rules	Precise protection	<a href="#">Configuring Custom Precise Protection Rules</a>
Scan protection	Scanning protection	<a href="#">Configuring Scan Protection Rules to Block Heavy-Traffic Attacks</a>
Custom response	Alarm page	<a href="#">Modifying the Alarm Page</a>

Alibaba Cloud	Huawei Cloud	Reference
HTTP flood protection (CC attack defense)	CC attack protection	<a href="#">Configuring a CC Attack Protection Rule</a>
Region blacklist rule	Geolocation access control	<a href="#">Configuring Geolocation Access Control Rules to Block or Allow Requests from Specific Locations</a>
Web Tamper Protection	Web tamper protection	<a href="#">Configuring Web Tamper Protection Rules to Prevent Static Web Pages from Being Tampered With</a>
Data leakage prevention	Information leakage prevention	<a href="#">Configuring Information Leakage Prevention Rules to Prevent Sensitive Information Leakage</a>

## Migrating Basic Protection Rules



- Step 1** Log in to the Alibaba Cloud WAF console. In the navigation pane on the left, choose **Protection Configuration > Protection Rules**. On the displayed page, expand the **Basic Protection Rule** area. In the **Action** column of the row containing the target rule, click **Edit** and check the rule details.
- Step 2** Log in to the Huawei Cloud WAF console and go to the Huawei Cloud WAF protection rule configuration page by referring to [Figure 14-3](#).

Figure 14-3 Protection rules



- Step 3** Select the **Basic Web Protection** configuration box, enable it, and migrate related configurations to Huawei Cloud WAF based on [Table 14-4](#).

Table 14-4 Parameter mappings

Alibaba Cloud	Huawei Cloud
Basic Protection Rule	Basic Web Protection
Create Template	Status <ul style="list-style-type: none"> <li> : enabled.</li> <li> : disabled.</li> </ul>

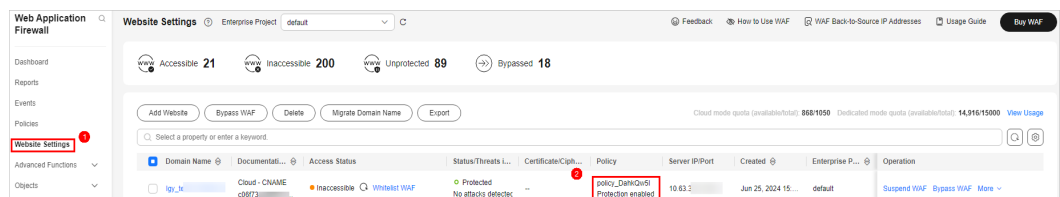
Alibaba Cloud	Huawei Cloud
Intelligent Whitelist	None
Rule Configuration	General Check/Deep Inspection/Header Inspection/Shiro Decryption Check
Protocol Compliance	None
Semantic Engine	General Check

----End

## Migrating Whitelist Rules



- Step 1** Log in to the Alibaba Cloud WAF console. In the navigation pane on the left, choose **Protection Configuration > Protection Rules**. On the displayed page, expand the **Whitelist** area. In the **Actions** column of the row containing the target rule, click **Edit** and check the rule details.
- Step 2** Log in to the Huawei Cloud WAF console and go to the Huawei Cloud WAF protection rule configuration page by referring to [Figure 14-4](#).

**Figure 14-4** Protection rules



- Step 3** In the **Global Protection Whitelist** configuration box, enable it, and click **Add Rule**. Then, migrate related configurations to Huawei Cloud WAF based on [Table 14-5](#).

**Table 14-5** Parameter mappings

Alibaba Cloud	Huawei Cloud
Whitelist	Global Protection Whitelist
Create Template	Status <ul style="list-style-type: none"> <li> : enabled.</li> <li> : disabled.</li> </ul>
Match Field	<b>Field</b> in the <b>Condition List</b> area
Logical Operator	Logic
Match Content	Content

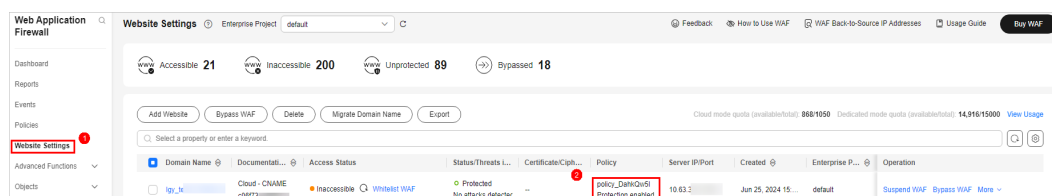
Alibaba Cloud	Huawei Cloud
Bypassed Modules Example: <b>Basic Protection Rule - All Rules</b>	Ignore WAF Protection Example: <b>Basic Web Protection - All built-in rules</b>

----End

## Migrating IP Address Blacklist Rules



- Step 1** Log in to the Alibaba Cloud WAF console. In the navigation pane on the left, choose **Protection Configuration > Protection Rules**. On the displayed page, expand the **IP Address Blacklist** area. In the **Actions** column of the row containing the target rule, click **Edit** and check the rule details.
- Step 2** Log in to the Huawei Cloud WAF console and go to the Huawei Cloud WAF protection rule configuration page by referring to [Figure 14-5](#).

**Figure 14-5** Protection rules



- Step 3** Choose **Blacklist and Whitelist**, enable it, and click **Add Rule**. Then, migrate related configurations to Huawei Cloud WAF based on [Table 14-6](#).

**Table 14-6** Parameter mappings

Alibaba Cloud	Huawei Cloud
IP Address Blacklist	Blacklist and Whitelist
Create Template	Status <ul style="list-style-type: none"> <li>●  : enabled.</li> <li>●  : disabled.</li> </ul>
IP Address Blacklist	IP Address/Range
Action	Protective Action

----End

## Migrating Custom Rules

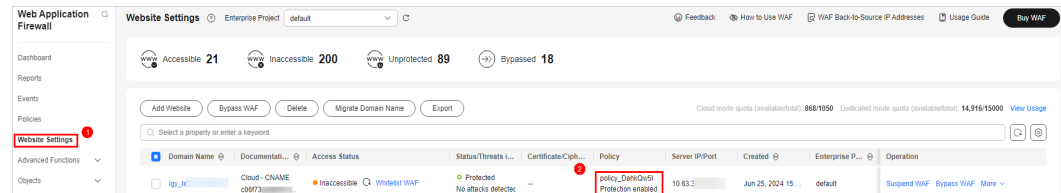
- Step 1** Log in to the Alibaba Cloud WAF console. In the navigation pane on the left, choose **Protection Configuration > Protection Rules**. On the displayed page,



expand the **Custom Rules** area. In the **Actions** column of the row containing the target rule, click **Edit** and check the rule details.



**Step 2** Log in to the Huawei Cloud WAF console and go to the Huawei Cloud WAF protection rule configuration page by referring to [Figure 14-6](#).

**Figure 14-6** Protection rules



**Step 3** Click the **Precise Protection** configuration box, enable it, and click **Add Rule**. Then, migrate related configurations to Huawei Cloud WAF based on [Table 14-7](#).

**Table 14-7** Parameter mappings

Alibaba Cloud	Huawei Cloud
Custom Rules	Precise Protection
Create Template	Status <ul style="list-style-type: none"> <li>●  : enabled.</li> <li>●  : disabled.</li> </ul>
Match Field	Field
Logical Operator	Logic
Match Content	Content
Protection Type	None
Action	Protective Action
Effective Mode	Apply

----End

## Migrating Custom Response Rules

**Step 1** Log in to the Alibaba Cloud WAF console. In the navigation pane on the left, choose **Protection Configuration > Protection Rules**. On the displayed page, expand the **Custom Response** area. In the **Actions** column of the row containing the target rule, click **Edit** and check the rule details.

**Step 2** Log in to the Huawei Cloud WAF console. In the navigation pane on the left, choose **Website Settings**. Click the target domain name to go to its details page.

**Step 3** Click the edit icon next to the page template name in the row where **Alarm Page** is located. In the displayed **Alarm Page** dialog box, specify **Page Template**.

Migrate related configurations to Huawei Cloud WAF based on [Table 14-8](#).

**Table 14-8** Parameter mappings

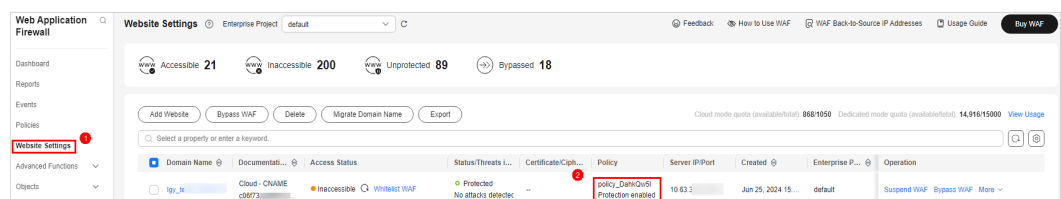
Alibaba Cloud	Huawei Cloud
Custom Response	Block Page
Create Template	Page Template
Status Code	HTTP Return Code
Response Body	Page Content

----End

## Migrating HTTP Flood Protection Rules



- Step 1** Log in to the Alibaba Cloud WAF console. In the navigation pane on the left, choose **Protection Configuration > Protection Rules**. On the displayed page, expand the **HTTP Flood Protection** area. In the **Actions** column of the row containing the target rule, click **Edit** and check the rule details.
- Step 2** Log in to the Huawei Cloud WAF console and go to the Huawei Cloud WAF protection rule configuration page by referring to [Figure 14-7](#).

**Figure 14-7** Protection rules



- Step 3** Click the **CC Attack Protection** configuration box, enable it, and click **Add Rule**. Then, migrate related configurations to Huawei Cloud WAF based on [Table 14-9](#).

**Table 14-9** Parameter mappings

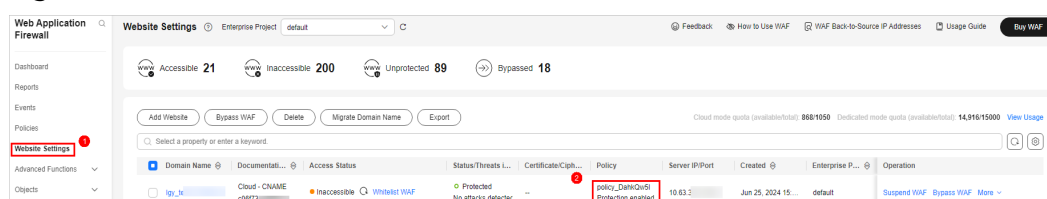
Alibaba Cloud	Huawei Cloud
HTTP Flood Protection (CC attack defense)	CC Attack Protection
Create Template	Status <ul style="list-style-type: none"> <li> : enabled.</li> <li> : disabled.</li> </ul>
Action	Protective Action
Protected objects	This parameter is not required for Huawei Cloud WAF.

----End

## Migrating Region Blacklist Rules



- Step 1** Log in to the Alibaba Cloud WAF console. In the navigation pane on the left, choose **Protection Configuration > Protection Rules**. On the displayed page, expand the **Region Blacklist** area. In the **Actions** column of the row containing the target rule, click **Edit** and check the rule details.
- Step 2** Log in to the Huawei Cloud WAF console and go to the Huawei Cloud WAF protection rule configuration page by referring to [Figure 14-8](#).

**Figure 14-8** Protection rules



- Step 3** In the **Geolocation Access Control** configuration box, enable it, and click **Add Rule**. Then, migrate related configurations to Huawei Cloud WAF based on [Table 14-10](#).

**Table 14-10** Parameter mappings

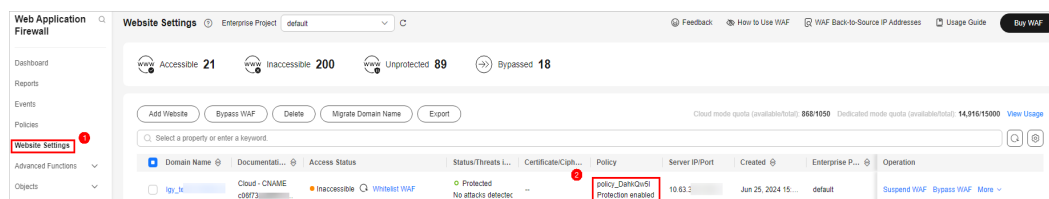
Alibaba Cloud	Huawei Cloud
Region Blacklist Rule	Geolocation Access Control
Create Template	Status <ul style="list-style-type: none"> <li>●  : enabled.</li> <li>●  : disabled.</li> </ul>
Action	Protective Action
Select Regions to Block	Geolocation

----End

## Migrating Website Tamper-Proofing Rules

- Step 1** Log in to the Alibaba Cloud WAF console. In the navigation pane on the left, choose **Protection Configuration > Protection Rules**. On the displayed page, expand the **Website Tamper-proofing** area. In the **Actions** column of the row containing the target rule, click **Edit** and check the rule details.
- Step 2** Log in to the Huawei Cloud WAF console and go to the Huawei Cloud WAF protection rule configuration page by referring to [Figure 14-9](#).

**Figure 14-9** Protection rules



**Step 3** In the **Web Tamper Protection** configuration box, enable it, and click **Add Rule**. Then, migrate related configurations to Huawei Cloud WAF based on [Table 14-11](#).

**Table 14-11** Parameter mappings

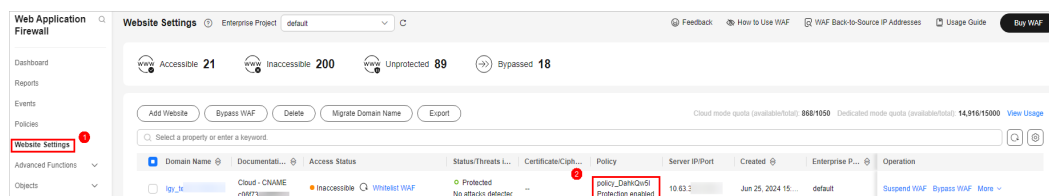
Alibaba Cloud	Huawei Cloud
Website Tamper-proofing	Web Tamper Protection
Create Template	Status <ul style="list-style-type: none"> <li>●  : enabled.</li> <li>●  : disabled.</li> </ul>
Address of Cached Page	Path

----End

## Migrating Data Leakage Prevention Rules



- Step 1** Log in to the Alibaba Cloud WAF console. In the navigation pane on the left, choose **Protection Configuration > Protection Rules**. On the displayed page, expand the **Data Leakage Prevention** area. In the **Actions** column of the row containing the target rule, click **Edit** and check the rule details.
- Step 2** Log in to the Huawei Cloud WAF console and go to the Huawei Cloud WAF protection rule configuration page by referring to [Figure 14-10](#).

**Figure 14-10** Protection rules



**Step 3** Click the **Information Leakage Prevention** configuration box, enable it, and click **Add Rule**. Then, migrate related configurations to Huawei Cloud WAF based on [Table 14-12](#).

**Table 14-12** Parameter mappings

Alibaba Cloud	Huawei Cloud
Data Leak Prevention	Information Leakage Prevention
Create Template	Status <ul style="list-style-type: none"><li> : enabled.</li><li> : disabled.</li></ul>
Match Condition	Type
Sensitive Info	Content
Action	Protective Action

----End