

**Edge Security**

# **Best Practices**

**Issue**            03  
**Date**             2024-10-31



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. 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 Basic Web Protection.....</b>  | <b>1</b> |
| <b>2 CC Attack Protection.....</b>  | <b>7</b> |
| 2.1 Overview.....   | 7        |
| 2.2 IP Address-based Rate Limiting.....   | 7        |
| 2.3 Cookie-based CC Attack Protection.....                                      | 8        |
| 2.4 Preventing Bonus Hunting by Configuring Service Cookies and System IDs..... | 10       |

# 1 Basic Web Protection

---

This topic walks you through how to enable web attack defense using EdgeSec.


## Prerequisites

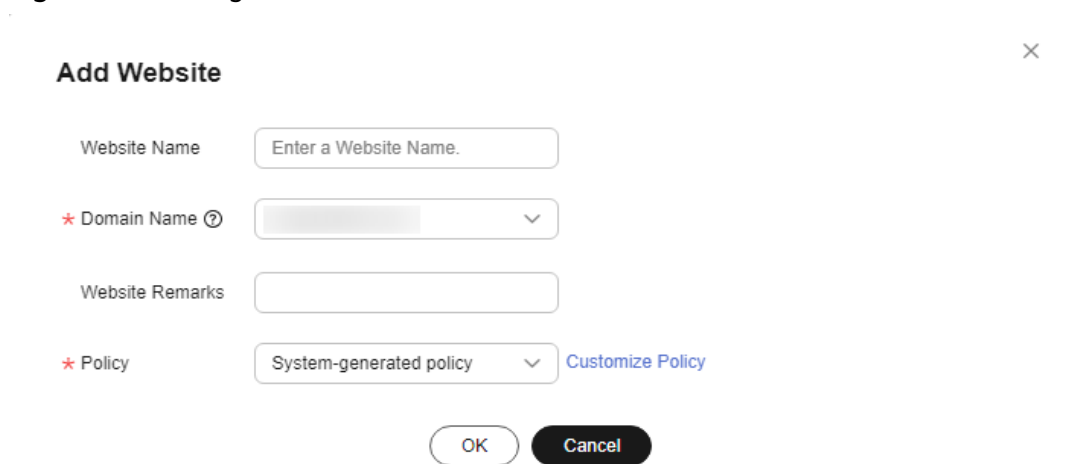
You have added domain names to the **Domains** module in the Content Delivery Network (CDN) service. For details, see [Domain Name Management](#).

## Application Scenarios

Use EdgeSec to enable web protection for domain names.

## Adding a Website to EdgeSec

- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the page and choose **Content Delivery & Edge Computing > CDN and Security**.
- Step 3** In the navigation pane on the left, choose **Edge Security > Website Settings**. The **Website Settings** page is displayed.
- Step 4** In the upper left corner of the list, click **Add Website**. For details about the parameters, see [Table 1-1](#).

**Figure 1-1** Adding a website

**Add Website** ×

Website Name

\* Domain Name ?

Website Remarks

\* Policy  [Customize Policy](#)

**Table 1-1** Parameters for adding a protected website

| Parameter       | Description  |
|-----------------|--|
| Website Name    | Name of the website you want to protect. It must meet the following requirements: <ul style="list-style-type: none"><li>• The name must be unique.</li><li>• The name must start with a letter.</li><li>• The length cannot exceed 128 characters.</li><li>• The value can contain uppercase letters, lowercase letters, digits, and special characters (-_.).</li></ul> |
| Domain Name     | Select a domain name to be protected. You can only select a domain name whose <b>Service Type</b> is <b>Website</b> on the <b>Domains</b> page of CDN.   |
| Website Remarks | A brief description of the website   |
| Policy          | The <b>System-generated policy</b> is selected by default. You can select a policy you configured before.  |

**Step 5** Click **OK**.

----End

## Configuring a Protection Policy

**Step 1** In the navigation pane on the left, choose **Edge Security** > **Website Settings**. The **Website Settings** page is displayed.

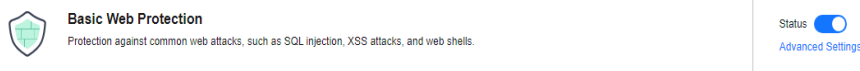
**Step 2** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

**Figure 1-2** Website list



| Domain Name     | Last 3 Days          | Mode    | Scheduling Status | Policy           | Created                         | Operation |
|-----------------|----------------------|---------|-------------------|------------------|---------------------------------|-----------|
| www.esatest.com | No attacks detected. | Enabled | Scheduling to CDN | policy_mNNSs4hIL | Oct 16, 2024 22:57:26 GMT+08:00 | Delete    |

**Step 3** In the **Basic Web Protection** configuration area, change **Status** and **Mode** as needed by referring to [Table 1-2](#).

**Figure 1-3** Basic Web Protection configuration area



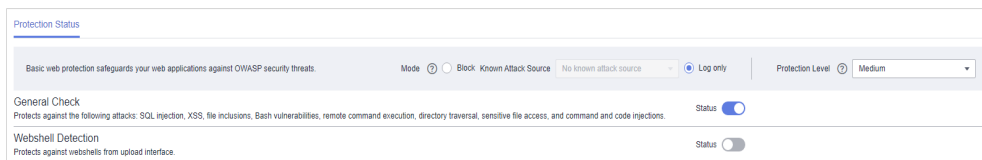
**Table 1-2** Parameter description

| Parameter | Description  |
|-----------|--|
| Status    | Status of Basic Web Protection <ul style="list-style-type: none"> <li> : enabled.</li> <li> : disabled.</li> </ul> |

**Step 4** In the **Basic Web Protection** configuration area, click **Advanced Settings**.

**Step 5** On the **Protection Status** tab page, enable protection types you need by referring to [Table 1-4](#).

**Figure 1-4** Basic web protection



**NOTICE**

If you select **Mode** for **Block** on the **Protection Status** tab, you can select a known attack source rule to let EdgeSec block requests accordingly. For details, see [Configuring a Known Attack Source Rule](#).

- Set the protection level.  
In the upper right part of the page, set **Protection Level** to **Low**, **Medium**, or **High**. The default value is **Medium**.

**Table 1-3** Protection levels

| Protection Level | Description  |
|------------------|--|
| Low              | EdgeSec only blocks the requests with obvious attack signatures.<br>If a large number of false alarms are reported, <b>Low</b> is recommended.   |
| Medium           | The default level is <b>Medium</b> , which meets a majority of web protection requirements.  |
| High             | At this level, EdgeSec provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks.<br>Configure global whitelist rules after the service has been running for a period of time, and then enable the strict mode. |

2. Set the protection type.

---

**NOTICE**

By default, **General Check** is enabled. You can enable other protection types by referring to [Table 1-4](#).

---

**Table 1-4** Protection types

| Type               | Description  |
|--------------------|--|
| General Check      | Defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections. SQL injection attacks are mainly detected based on semantics.<br><b>NOTE</b><br>If you enable <b>General Check</b> , EdgeSec checks your websites based on the built-in rules. |
| Webshell Detection | Protects against web shells from upload interface.<br><b>NOTE</b><br>If you enable <b>Webshell Detection</b> , EdgeSec detects web page Trojan horses inserted through the upload interface.   |

----End

## Suggestions

- If you are not familiar with your website's traffic pattern, select the **Log only** mode for one to two weeks and analyze the logs for those days.
  - If no record of blocking legitimate requests is found, switch to the **Block** mode.
  - If legitimate requests are blocked, adjust the protection level or configure global protection whitelist (formerly false alarm masking) rules to prevent legitimate requests from being blocked.
- Note the following points in your operations:
  - Do not transfer the original SQL statement or JAVA SCRIPT code in a legitimate HTTP request.
  - Do not use special keywords (such as UPDATE and SET) in a legitimate URL. For example, **https://www.example.com/abc/update/mod.php?set=1**.
  - Use Object Storage Service (OBS) or other secure methods to upload files that exceed 50 MB rather than via a web browser.

## Protection Effect

To check whether basic web protection takes effect, enter a test domain name in the address bar of your browser and simulate an SQL injection attack. If Edge WAF blocks the attack, the configuration works. You can view attack event logs on the **Dashboard** page.

Figure 1-5 Blocking SQL attacks

! 418

Sorry, your request has been intercepted because it appears to be an attack.

False alarm ID: 888974223

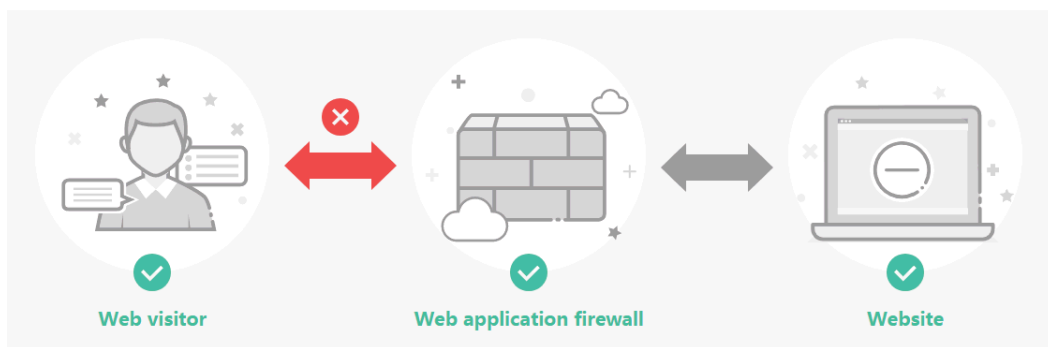
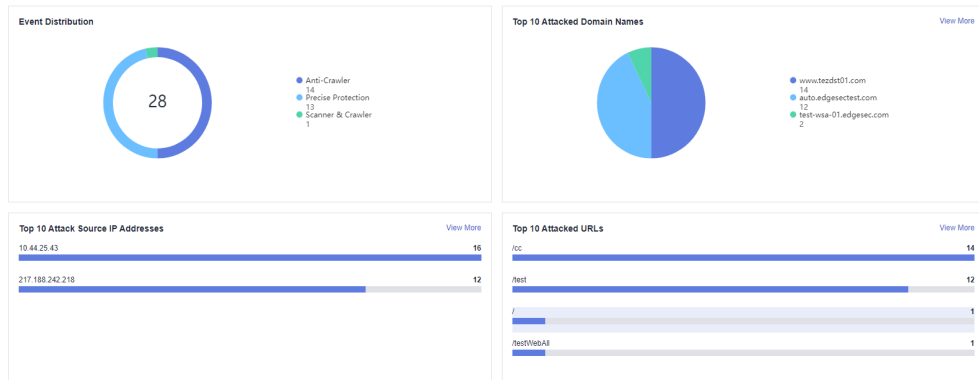


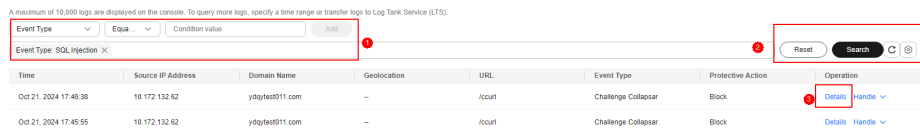


Figure 1-6 Web security event statistics



You can also view protection logs generated in yesterday, today, past 3 days, past 7 days, 30 days, or user-defined time range on the **Events** page. Click **Details** to view event details.

Figure 1-7 Events



# 2 CC Attack Protection

---

## 2.1 Overview

This topic walks you through how to configure protection rules to limit traffic rate by IP addresses defend against Challenge Collapsar (CC) attacks.

### How Can We Know Whether a CC Attack Occurs?

If you find that the website processing speed decreases and network bandwidth usage is high, your website may suffer from CC attacks. In this case, check whether the number of access logs or network connections increases significantly. If yes, your website is suffering from CC attacks. Then you can configure Edge WAF protection policies to block CC attacks, thereby ensuring website availability.

 **NOTE**

Edge WAF protects application-layer traffic against DoS attacks, such as HTTP GET attacks.

### Prerequisites

Your website has been connected to EdgeSec. For details, see [Adding a Website to EdgeSec](#).



## 2.2 IP Address-based Rate Limiting

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

### Attack Example

Attackers can 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 normal requests and its competitiveness decreases sharply.

## 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 is hit by CC attacks.
2. [Log in to the management console.](#)
3. Click  in the upper left corner of the page and choose **Content Delivery & Edge Computing > CDN and Security**.
4. In the navigation pane on the left, choose **Website Setting** under **Edge Security**.
5. In the **Policy** column of the row containing the target domain name, click the number of enabled protection rules. On the page displayed, confirm that the status of CC attack protection is enabled (  ) and click **Customize Rule**.

**Figure 2-1** CC Attack Protection configuration area



6. Then, customize a CC attack protection rule. In the upper left corner of the page, click **Add Rule**. In the displayed dialog box, specify the path and rule name, and set **Rate Limit Mode** to **Per IP address**, **Rate Limit** based on 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 website 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:** EdgeSec allows requests that trigger the rule as long as your website visitors complete the required verification. Currently, certification code supports English.
    - **Block:** EdgeSec blocks requests that trigger the rule.
    - **Log only:** EdgeSec only logs requests that trigger the rule.

If the number of access requests exceeds the configured rate limit, the visitors are required to enter a verification code to continue the access.
7. Go to the **Events** page, view details about attack events. For details, see [Viewing Events](#).

## 2.3 Cookie-based CC Attack Protection



In some cases, it may be difficult to obtain source IP addresses of visitors for a website. For example, websites use proxies that do not use the **X-Forwarded-For**

HTTP header field. The cookie field should be configured to identify visitors and **All WAF instances** should be enabled for precise user-based rate limiting.

## Attack Examples

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 is hit by CC attacks.
2. [Log in to the management console.](#)
3. Click  in the upper left corner of the page and choose **Content Delivery & Edge Computing > CDN and Security**.
4. In the navigation pane on the left, choose **Website Setting** under **Edge Security**.
5. In the **Policy** column of the row containing the target domain name, click the number of enabled protection rules. On the page displayed, confirm that the status of CC attack protection is enabled (  ) and click **Customize Rule**.

**Figure 2-2** CC Attack Protection configuration area



6. In the upper left corner of the **CC Attack Protection** page, click **Add Rule**. In the displayed dialog box, set **Rate Limit Mode** and specify **User Identifier** in the **Cookie** field.

### NOTE

With a CC attack protection rule, you can set **Protective Action** to **Block** and specify **Block Duration**. Then, 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.

Figure 2-3 Per user

\* Rate Limit Mode:  Source  Destination

Requests from a specific source are limited. For example, if traffic from an IP address (or user) exceeds the rate limit you configure in this rule, WAF limits traffic rate of the IP address (or user) in the way you configure.

Per IP address  Per user  Other

\* User Identifier:  Enter a field name.

\* Request Aggregation:

\* Trigger:

| Field | Subfield | Logic    | Content |
|-------|----------|----------|---------|
| Path  | --       | Inclu... |         |

[Add Reference Table](#)

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

\* Rate Limit:  requests  seconds

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

- **Rate Limit Mode:** Select **Source** and then **Per user** to distinguish a single web visitor based on cookies.
- **User Identifier:** Enter a user identifier, which is the variable name in the **Cookie** field.
- **Rate Limit:** Number of requests allowed from a website visitor in the rate limiting period. The visitor's access request is denied if the limit is reached.
- **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:** EdgeSec allows requests that trigger the rule as long as your website visitors complete the required verification. Currently, certification code supports English.
  - **Block:** EdgeSec blocks requests that trigger the rule.
  - **Log only:** EdgeSec only logs requests that trigger the rule.
- **Block Page:** Select **Default settings** or **Custom**.

## 2.4 Preventing Bonus Hunting by Configuring Service Cookies and System IDs

This topic introduces how to configure service cookies and system IDs to restrict malicious bonus hunting and downloads.

## 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 a System ID to Configure a Path-based 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.](#)

**Step 2** Click  in the upper left corner of the page and choose **Content Delivery & Edge Computing > CDN and Security.**

**Step 3** In the navigation pane on the left, choose **Website Setting** under **Edge Security.**

**Step 4** In the **Policy** column of the row containing the target domain name, click the number of enabled protection rules. On the page displayed, confirm that the status of CC attack protection is enabled (  ) and click **Customize Rule.**

**Figure 2-4** CC Attack Protection configuration area



**Step 5** In the upper left corner of the **CC Attack Protection** page, click **Add Rule.** In the displayed dialog box, specify the path to be protected, configure **Rate Limit Mode** with service cookies (or user ID), and complete other settings based on your service needs. [Figure 2-5](#) shows an example rule.

Figure 2-5 Configuring service cookies

\* Rate Limit Mode  Source  Destination

Requests from a specific source are limited. For example, if traffic from an IP address is configured in this rule, WAF limits traffic rate of the IP address (or user) in the way you specify.

Per IP address  Per user  Other

\* User Identifier

\* Request Aggregation

\* Trigger

| Field                             | Subfield | Logic                                 | Content                        |
|-----------------------------------|----------|---------------------------------------|--------------------------------|
| <input type="text" value="Path"/> | --       | <input type="text" value="Inclu..."/> | <input type="text" value="/"/> |

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

\* Rate Limit    requests    seconds

- **User Identifier:** Enter the service cookie or user ID.

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

----End

## Using a System ID to Configure a Path-based CC Attack Protection Rule

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

**Step 2** In the navigation pane on the left, choose **Website Setting** under **Edge Security**.

**Step 3** In the **Policy** column of the row containing the target domain name, click the number of enabled protection rules. On the page displayed, confirm that the status of CC attack protection is enabled (  ) and click **Customize Rule**.

Figure 2-6 CC Attack Protection configuration area



**Step 4** In the upper left corner of the **CC Attack Protection** page, click **Add Rule**. Configure a CC attack protection rule using system ID like HWSESID to limit traffic to the path. **Figure 2-7** shows an example rule.

**Figure 2-7** System ID

The screenshot shows the configuration interface for a CC Attack Protection rule. The 'Rate Limit Mode' is set to 'Source'. The 'User Identifier' is set to 'Cookie' with the value 'HWSESID'. The 'Trigger' is set to 'Path' with the content '/'. The 'Rate Limit' is set to 10 requests per 60 seconds. The 'Protective Action' is set to 'Block'.

★ Rate Limit Mode:  Source  Destination

Requests from a specific source are limited. For example, if traffic from an IP address (or user) exceeds the rate limit you configure in this rule, WAF limits traffic rate of the IP address (or user) in the way you configure.

Per IP address  Per user  Other

★ User Identifier: Cookie

★ Request Aggregation:

★ Trigger:

| Field | Subfield | Logic    | Content |
|-------|----------|----------|---------|
| Path  | --       | Inclu... | /       |

[Add Reference Table](#)

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

★ Rate Limit:  requests  seconds

---

★ Protective Action:  Verification code  Block  Block dynamically  Log only

- **User Identifier:** Enter the system ID as the cookie.

**Step 5** Click **Confirm**.

----End