

**Edge Security**

# **User Guide**

**Issue**            07  
**Date**             2024-07-16



**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.

## **Huawei Cloud Computing Technologies Co., Ltd.**

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

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

---

# Contents

---

|   |          |
|---|----------|
| <b>1 Enabling EdgeSec.....</b>  | <b>1</b> |
| <b>2 Site Acceleration.....</b>   | <b>3</b> |
| <b>3 Security Protection.....</b>   | <b>4</b> |
| 3.1 Website Settings.....   | 4        |
| 3.1.1 Adding a Website to EdgeSec.....  | 4        |
| 3.1.2 Viewing the Basic Information.....  | 5        |
| 3.1.3 Switching Working Mode.....   | 7        |
| 3.1.4 Configuring a Traffic Identifier for a Known Attack Source.....                               | 8        |
| 3.2 Dashboard.....  | 9        |
| 3.3 Managing Events.....  | 11       |
| 3.3.1 Managing Web Protection Events.....   | 11       |
| 3.3.1.1 Viewing Web Protection Events.....  | 11       |
| 3.3.1.2 Handling False Alarms.....  | 13       |
| 3.3.2 Managing DDoS Protection Events.....  | 20       |
| 3.3.2.1 Viewing DDoS Protection Events.....   | 20       |
| 3.3.2.2 Downloading DDoS Protection Events.....   | 21       |
| 3.4 Statistical Analysis.....   | 21       |
| 3.4.1 Web Protection Trend Statistics.....  | 21       |
| 3.4.2 Web Top Statistics.....   | 23       |
| 3.5 Protection Policy.....  | 24       |
| 3.5.1 Creating a Protection Policy.....   | 24       |
| 3.5.2 Applying a Policy to Your Website.....  | 25       |
| 3.5.3 Configuring Protection Policies.....  | 26       |
| 3.5.3.1 Configuration Guidance.....   | 26       |
| 3.5.3.2 Configuring Basic Protection Rules to Defend Against Common Web Attacks.....                | 30       |
| 3.5.3.3 Configuring CC Attack Protection Rules to Defend Against CC Attacks.....                    | 33       |
| 3.5.3.4 Configuring a Precise Protection Rule.....  | 38       |
| 3.5.3.5 Creating a Reference Table to Configure Protection Metrics In Batches.....                  | 45       |
| 3.5.3.6 Configuring IP Address Blacklist and Whitelist Rules to Block Specified IP Addresses.....   | 48       |
| 3.5.3.7 Configuring a Known Attack Source Rule.....   | 52       |
| 3.5.3.8 Configuring Geolocation Access Control Rules to Block Requests from Specific Locations..... | 57       |
| 3.5.3.9 Configuring Anti-Crawler Rules.....   | 59       |

|   |           |
|---|-----------|
| 3.5.3.10 Configuring a Global Whitelist Rule to Ignore False Positives..... | 67        |
| 3.5.3.11 Configuring a Data Masking Rule.....                               | 70        |
| 3.6 Address Group Management.....   | 74        |
| 3.6.1 Adding a Blacklist or Whitelist IP Address Group.....                 | 74        |
| 3.6.2 Modifying or Deleting a Blacklist or Whitelist IP Address Group.....  | 76        |
| 3.7 DDoS Attack Monitoring.....   | 77        |
| <b>4 Permissions Management.....</b>  | <b>78</b> |
| 4.1 Creating a User Group and Granting Permissions.....                     | 78        |
| <b>5 Key Operations Recorded by CTS.....</b>                                | <b>80</b> |
| 5.1 EdgeSec Operations Recorded by CTS.....                                 | 80        |
| 5.2 Querying Traces.....  | 83        |
| <b>6 Monitoring.....</b>  | <b>84</b> |
| 6.1 EdgeSec Monitored Metrics.....  | 84        |
| 6.2 Configuring a Monitoring Alarm Rule.....                                | 97        |
| 6.3 Viewing Monitored Metrics.....  | 98        |
| <b>7 Change History.....</b>  | <b>99</b> |

# 1 Enabling EdgeSec

## Prerequisites

- The current account has the BSS Administrator and EdgeSec\_FullAccess permissions.
- The Huawei Cloud CDN has been enabled.

### NOTE

EdgeSec works on the basis of Content Delivery Network (CDN) sites. To use EdgeSec, you need to enable CDN.

## Specification Limitations


- A domain name expansion package supports a maximum of 10 domain names.
- A maximum of 10 IP blacklist and whitelist protection rules can be added to a rule extension package.
- [Table 1-1](#) lists the specifications of the Enterprise Edition.

**Table 1-1** Description

| Service Scale                            | Enterprise Edition |
|--|--------------------|
| Number of domain names                   | 20                 |
| CC attack prevention rules               | 100                |
| Precise protection rules                 | 100                |
| Reference table rules                    | 100                |
| IP address blacklist and whitelist rules | 1,000              |
| Geolocation access control rules         | 100                |
| Global protection whitelist rules        | 1,000              |
| Data masking rules                       | 100                |

## Procedure

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security.**

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

**Step 4** Click **Buy.** The **Buy EdgeSec** page is displayed. Set the product parameters.

- **Package:** The enterprise edition is supported.
- Billing mode.
  - **Traffic:** the protected service traffic
  - By request: billed by number of HTTP/HTTPS requests that are protected by EdgeSec.
  - Dynamic acceleration: Billed by number of CDN dynamic acceleration requests.

### NOTE

- You are billed by the traffic used per hour. You can also buy traffic packages to deduct traffic used.
- You are billed at tiered traffic prices. The billing cycle is one calendar month.
- **Domain Expansion Package:** A domain expansion package can protect a maximum of 10 domain names.
- **Rule Expansion Package:** A rule expansion package contains 10 IP blacklist and whitelist protection rules.

If the quota of IP address whitelist and blacklist rules cannot meet your requirements, you can purchase rule expansion packages under the current instance edition to increase such quota.

**Step 5** Set **Required Duration.**

### NOTE

The **Auto-renew** option enables the system to renew your service by the purchased period when the service is about to expire.

**Step 6** Confirm the parameter settings, select **I have read and agree to the [Huawei Cloud EdgeSec Service Agreement](#)**, and click **Submit** in the lower right corner of the page.

**Step 7** Confirm the order details and click **Pay Now.**

----End

# 2 Site Acceleration

---

The site acceleration provides the following functions:

- [Domain Name Management](#)
- [Analysis](#)
- [Analysis \(New\)](#)
- [Cache Purge and Prefetch](#)
- [Node IP Address Query](#)
- [Certificate Management](#)
- [Log Management](#)
- [Resource Package Management](#)

# 3 Security Protection

---

## 3.1 Website Settings

### 3.1.1 Adding a Website to EdgeSec

This section describes how to access a domain name.

#### Prerequisites

A domain name has been added on the **Domains** page. For details about domain name management, see [Domain Name Management](#).

#### Constraints


- Only website domain names on the **Domains** page can be added. For details about the service types, see [Adding a Domain Name](#).
- A protected domain name can only be added once.
- A maximum of 20 domain names can be added.

#### Specification Limitations

After your website is connected, the file visitors can upload each time cannot exceed 512 MB.

#### Procedure

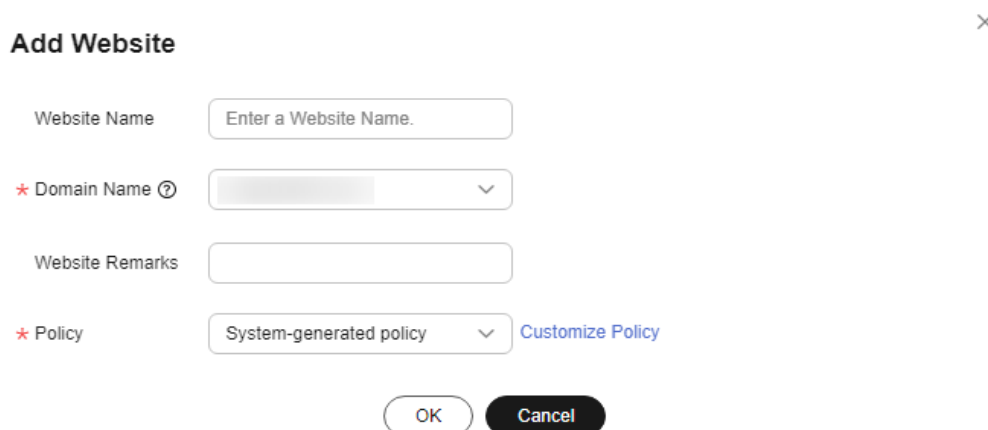
**Step 1** [Log in to the management console](#).

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

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

**Step 4** In the upper left corner of the list, click **Add Website**. For details about the parameters, see [Table 3-1](#).



**Figure 3-1** Adding a website

**Add Website** ×

Website Name

\* Domain Name ?

Website Remarks

\* Policy  [Customize Policy](#)

**Table 3-1** 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


### 3.1.2 Viewing the Basic Information

This section describes how to view the policy name and protection status of a protected domain name on the EdgeSec management console.

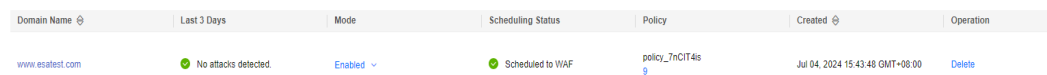
#### Prerequisites

A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

## Procedure

- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security.**
- Step 3** In the navigation pane on the left, choose **Website Setting** under **Edge Security.**
- Step 4** View the protected website information, as shown in [Figure 3-2](#). For details about the parameters, see [Table 3-2](#).

**Figure 3-2** Website list



| Domain Name     | Last 3 Days          | Mode    | Scheduling Status | Policy          | Created                         | Operation |
|-----------------|----------------------|---------|-------------------|-----------------|---------------------------------|-----------|
| www.esatest.com | No attacks detected. | Enabled | Scheduled to WAF  | policy_TnCIT4is | Jul 04, 2024 15:43:48 GMT+08:00 | Delete    |


**Table 3-2** Website list parameters

| Parameter         | Description  |
|-------------------|--|
| Domain Name       | Protected domain name  |
| Last 3 Days       | Protection status of the domain name over the past three days  |
| Mode              | Protection mode. Click ▼ to select one of the following protection modes: <ul style="list-style-type: none"><li>• <b>Enabled</b></li><li>• <b>Suspended</b> If a large number of normal requests are blocked, for example, status code 418 is frequently returned, then you can switch the mode to <b>Suspended</b>. In this mode, your website is not protected because EdgeSec only forwards requests. It does not scan for attacks. This mode is risky. You are advised to reduce false alarms by <a href="#">Configuring a Global Whitelist (Originally False Alarm Masking) Rule</a>.</li></ul> |
| Scheduling Status | Scheduling status of a domain name   |
| Policy            | Total number of protection policies You can click the number to go to the rule configuration page and configure specific protection rules. For details, see <a href="#">Configuring Protection Rules</a> .   |
| Created           | Time the website was added   |
| Operation         | To remove a protected website from EdgeSec, click <b>Delete</b> .  |

- Step 5** In the **Domain Name** column, click the domain name of the website to go to the basic information page.
- Step 6** View information about the protected website, as shown in [Figure 3-3](#).

**Figure 3-3** Viewing the basic information

| Basic Information |   | Traffic Identifier  |  |
|-------------------|---|--|--|
| Website Name      | -...     | Session Tag  | --  |
| Domain Name       | www.esatest.com   | User Tag   | --  |
| Website Remarks   | -...     |  |  |
| Policy Name       | policy_7nCiT4is   |  |  |
| Alarm Page        | Default  |  |  |

- Customize the alarm page: Click . In the displayed dialog box, select **Custom** or **Redirection** and complete required configurations. By default, **Alarm Page** is **Default**.
- For details about how to configure the traffic identifier, see [Configuring a Traffic Identifier for a Known Attack Source](#).

----End

### 3.1.3 Switching Working Mode

You can switch the protection status.

#### Prerequisites

A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

#### Application Scenarios



- **Enabled:** In this mode, EdgeSec defends your website against attacks based on configured policies.
- **Suspended:** If a large number of normal requests are blocked, for example, status code 418 is frequently returned, then you can switch the mode to **Suspended**. In this mode, your website is not protected because EdgeSec only forwards requests. It does not scan for or log attacks. This mode is risky. You are advised to use the global protection whitelist rules to reduce false alarms.

#### Impact on the System

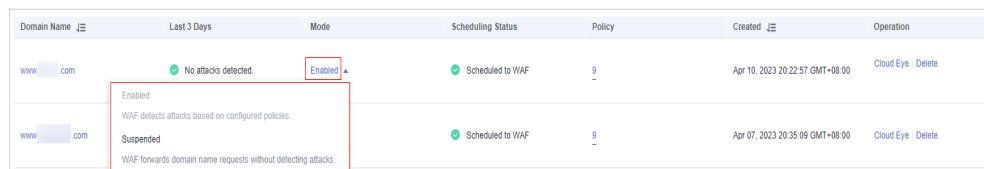
In the Suspended mode, your website is not protected because EdgeSec only forwards requests. It does not scan for attacks. To avoid normal requests from being blocked, configure [global protection whitelist \(formerly false alarm masking\) rules](#), instead of using the Suspended mode.

#### Procedure

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

- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.
- Step 3** In the navigation pane on the left, choose **Website Setting** under **Edge Security**.
- Step 4** In the row containing the target domain name, click  in the **Mode** column and select a mode you want.

**Figure 3-4** Switching working mode



| Domain Name | Last 3 Days                                       | Mode      | Scheduling Status | Policy | Created                         | Operation        |
|-------------|---|-----------|-------------------|--------|---------------------------------|------------------|
| www.com     | No attacks detected.                              | Enabled   | Scheduled to WAF  | 9      | Apr 10, 2023 20:22:57 GMT+08:00 | Cloud Eye Delete |
| www.com     | WAF detects attacks based on configured policies. | Suspended | Scheduled to WAF  | 9      | Apr 07, 2023 20:35:09 GMT+08:00 | Cloud Eye Delete |

- **Enabled:** In this mode, EdgeSec defends your website against attacks based on configured policies.
- **Suspended:** If a large number of normal requests are blocked, for example, status code 418 is frequently returned, then you can switch the mode to **Suspended**. In this mode, your website is not protected because EdgeSec only forwards requests. It does not scan for or log attacks. This mode is risky. You are advised to use the global protection whitelist rules to reduce false alarms.

----End

## Other Operations

- [Handling False Alarms](#)

### 3.1.4 Configuring a Traffic Identifier for a Known Attack Source

EdgeSec allows you to configure traffic identifiers by IP address, session, or user tag to block possibly malicious requests from known attack sources based on **IP address**, **Cookie**, or **Params**.


## Prerequisites


A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

## Constraints

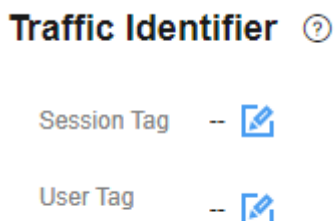
- Before enabling Cookie- or Params-based known attack source rules, configure a session or user tag for the corresponding website domain name.

## Procedure

- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.

- Step 3** In the navigation pane on the left, choose **Website Setting** under **Edge Security**.
- Step 4** In the **Domain Name** column, click the domain name of the website to go to the basic information page.
- Step 5** In the **Traffic Identifier** area, click  next to **Session Tag**, or **User Tag** to configure a traffic identifier by referring to [Table 3-3](#).

**Figure 3-5** Traffic Identifier



**Table 3-3** Traffic identifier parameters

| Identifier  | Description   | Example Value |
|-------------|---|---------------|
| Session Tag | This tag is used to block possibly malicious requests based on the cookie attributes of an attack source. Configure this parameter to block requests based on cookie attributes.    | jsessionid    |
| User Tag    | This tag is used to block possibly malicious requests based on the Params attribute of an attack source. Configure this parameter to block requests based on the Params attributes. | name          |

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

----End

## Other Operations

### [Configuring a Known Attack Source Rule](#)

## 3.2 Dashboard

On the **Dashboard** page, you can view the protection logs of all protected websites or instances for a specified time range, including yesterday, today, past 3 days, past 7 days, or past 30 days. On this page, event logs are displayed by different dimensions, including the number of attack types, top 10 attacked

domain names, top 10 attack source IP addresses, top 10 attacked URLs, top 10 attack source locations, and top 10 error pages.

Statistics on the security overview page are updated every minute.

## Prerequisites


- A domain name has been added and connected. For details, see [Adding a Website to EdgeSec](#).
- At least one protection rule has been configured for the domain name.

## Specification Limitations

On the **Dashboard** page, protection data of a maximum of 30 days can be viewed.

## Procedure

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

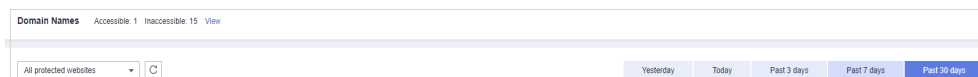
**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.

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

**Step 4** In the upper part of the page, specify the domain, website, and time period you want to query.

- **Domain Names:** shows information about website domain names added to the EdgeSec instance in the selected enterprise project. Click **View** to go to the **Website Settings** page and view details about domain names of protected websites.
- **All protected websites:** By default, the information about all websites you add to EdgeSec in all enterprise projects are displayed.
- Query time: You can select **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, or **Past 30 days**.

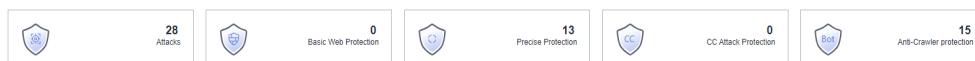
**Figure 3-6** Setting search criteria



**Step 5** View how many requests, attacks, and pages under each type of attacks.

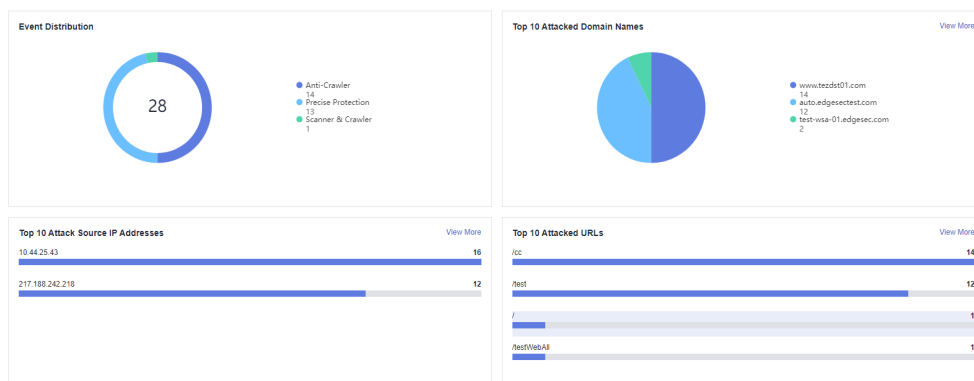
- **Attacks:** shows how many times the website are attacked.
- You can view how many pages are attacked by a certain type of attacks within a certain period of time.

**Figure 3-7** Protection action statistics



**Step 6** Query security data.

**Figure 3-8** Security Event Statistics



**Table 3-4** Security event statistics parameters

| Parameter                         | Description   |
|-----------------------------------|---|
| Event Distribution                | Types of attack events.<br>Click an area in the <b>Event Distribution</b> area to view the type, number, and proportion of an attack.   |
| Top 10 Attacked Domain Names      | The ten most attacked domain names and the number of attacks on each domain name.<br>Click <b>View More</b> to go to the <b>Events</b> page and view more protection data.                        |
| Top 10 Attack Source IP Addresses | The ten source IP addresses with the most attacks and the number of attacks from each source IP address.<br>Click <b>View More</b> to go to the <b>Events</b> page and view more protection data. |
| Top 10 Attacked URLs              | The ten most attacked URLs and the number of attacks on each URL.<br>Click <b>View More</b> to go to the <b>Events</b> page and view more protection data.  |

----End

## 3.3 Managing Events

### 3.3.1 Managing Web Protection Events

#### 3.3.1.1 Viewing Web Protection Events

You can search for security events, such as XSS attacks, SQL injection, CC attacks, and user-defined precise protection events in the event list to quickly locate attack sources or analyze attack events.

You can view event data of all protected domain names in the last 30 days.

**NOTICE**


If you switch the working mode for a website to **Suspended**, EdgeSec only forwards all requests to the website without inspection. It does not log any attack events neither.

**Prerequisites**

A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

**Procedure**

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

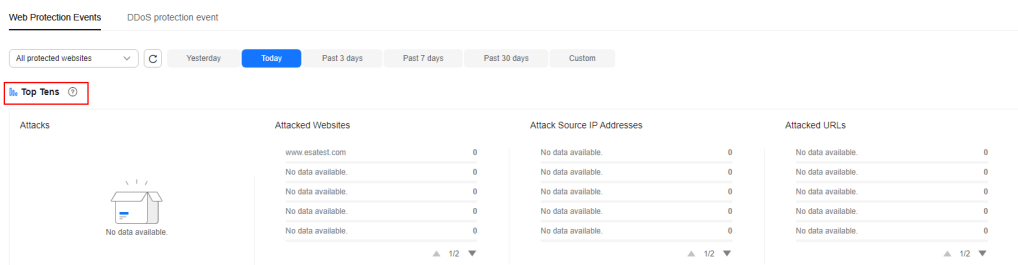
**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.

**Step 3** In the navigation pane on the left, choose **Edge Security > Events**. The **Events** page is displayed.


**Step 4** Select a website from the **Website** drop-down list. You can view protection logs of yesterday, today, past 3 days, past 7 days, past 30 days, or a user-defined time range.

**Top Tens:** Displays a summary of top tens about protected domain names you select for a time range.

**Figure 3-9** Events



**Step 5** In the **Events** area, view the event details.

- Configure a filter by combining several conditions. Click **Add** and select filter conditions displayed. Then, click **OK**. [Table 3-5](#) lists parameters for filter conditions.
- Click  to select fields you want to display in the event lists.
- To view event details, locate the row containing the event and click **Details** in the **Operation** column.

**Figure 3-10** Events





**Table 3-5** Description of the conditions

| Parameter         | Description   |
|-------------------|---|
| Event ID          | ID of the event   |
| Incident Type     | Type of the attack.<br>By default, <b>All</b> is selected. You can view logs of all attack types or select an attack type to view corresponding attack logs.  |
| Protective Action | The options are <b>Block</b> , <b>Log only</b> , and <b>Verification code</b> .   |
| Source IP         | Public IP address of the web visitor/attacker<br>By default, <b>All</b> is selected. You can view logs of all attack source IP addresses, select an attack source IP address, or enter an attack source IP address to view corresponding attack logs. |
| URL               | Attacked URL  |

**Table 3-6** Parameters in the event list

| Parameter         | Description  | Example Value       |
|-------------------|--|---------------------|
| Time              | When the attack occurred   | 2023/03/04 13:20:04 |
| Source IP Address | Public IP address of the web visitor/attacker  | -                   |
| Domain Name       | Attacked domain name   | www.example.com     |
| Geolocation       | Location where the IP address of the attack originates from  | -                   |
| URL               | Attacked URL   | /admin              |
| Incident Type     | Type of the attack.  | Precise Defense     |
| Protective Action | The options are <b>Block</b> , <b>Log only</b> , and <b>Verification code</b> .<br><b>NOTE</b><br>If an access request matches a data masking rule, the protective action is marked as <b>Mismatch</b> . | <b>Block</b>        |

----End

### 3.3.1.2 Handling False Alarms

If you confirm that an attack event on the **Events** page is a false alarm, you can handle the event as false alarm by ignoring the URL and rule ID in basic web protection, or by deleting or disabling the corresponding protection rule you

configured. After you set an attack event to a false alarm, the event is no longer displayed on the **Events** page

EdgeSec detects attacks by using built-in basic web protection rules, built-in features in anti-crawler protection, and custom rules you configured (such as CC attack protection, precise access protection, blacklist, whitelist, and geolocation access control rules). EdgeSec will respond to detected attacks based on the protective actions (such as **Block** and **Log only**) defined in the rules and display attack events on the **Events** page.

## Prerequisites

There is at least one false alarm event in the event list.

## Constraints

- Only attack events blocked or recorded by preconfigured basic web protection rules and features in anti-crawler protection can be handled as false alarms.
- For events generated based on custom rules (such as a CC attack protection rule, precise protection rule, blacklist rule, whitelist rule, or geolocation access control rule), they cannot be handled as false alarms. To ignore such an event, delete or disable the custom rule hit by the event.
- An attack event can only be handled as a false alarm once.

## Application Scenarios


Normal service requests are intercepted. For example, suppose you deploy a web application on a Huawei Cloud ECS and then add the public domain name associated with that application to EdgeSec. If you enable basic web protection for that application, EdgeSec may block the access requests that match the basic web protection rules. As a result, the website cannot be accessed through its domain name. However, the website can still be accessed through the IP address. In this case, you can handle the false alarms to allow normal access requests to the application.

## Impact on the System

After the blocked event is falsely reported, the event is no longer displayed on the **Events** page.

## Procedure

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.

**Step 3** In the navigation pane on the left, choose **Edge Security > Events**. The **Events** page is displayed.

**Step 4** In the event list, handle events.

- If you confirm that an event is a false alarm, locate the row containing the event. In the **Operation** column, click **Handle > Handle as False Alarm** and handle the hit rule.

**Figure 3-11** Handling a false alarm

**Handle False Alarm** ×

\* Scope  All domain names  Specified domain names

\* Domain Name ⌵  
  
+ Add

\* Condition List

| Field | Subfield | Logic   | Content |
|-------|----------|---------|---------|
| URL   | --       | Include | /       |

+ Add You can add 29 more conditions.

\* Ignore WAF Protection  All protection  Basic web protection

Rule Description

**OK** Cancel

**Table 3-7** Parameter description

| Parameter   | Description   | Example Value          |
|-------------|---|------------------------|
| Scope       | <ul style="list-style-type: none"> <li>– <b>All domain names:</b> By default, this rule will be used to all domain names that are protected by the current policy.</li> <li>– <b>Specify domain names:</b> Specify a domain name range this rule applies to.</li> </ul>                     | Specified domain names |
| Domain Name | <p>This parameter is mandatory when you select <b>Specified domain names</b> for <b>Scope</b>.</p> <p>Enter a single domain name that matches the wildcard domain name being protected by the current policy.</p> <p>To add more domain names, click <b>Add</b> to add them one by one.</p> | www.example.com        |

| Parameter                 | Description   | Example Value            |
|---------------------------|---|--------------------------|
| Condition List            | <p>Click <b>Add</b> to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. A condition includes the following parameters:</p> <p>Parameters for configuring a condition are described as follows:</p> <ul style="list-style-type: none"><li>- Field</li><li>- <b>Subfield</b>: Configure this field only when <b>Params</b>, <b>Cookie</b>, or <b>Header</b> is selected for <b>Field</b>.</li></ul> <p><b>NOTICE</b><br/>The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.</p> <ul style="list-style-type: none"><li>- <b>Logic</b>: Select a logical relationship from the drop-down list.</li><li>- <b>Content</b>: Enter or select the content that matches the condition.</li></ul> | Path, Include, / product |
| Ignore EdgeSec Protection | <ul style="list-style-type: none"><li>- <b>All protection</b>: All EdgeSec rules do not take effect, and EdgeSec allows all request traffic to the domain names in the rule.</li><li>- <b>Basic web protection</b>: You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule.</li></ul>  | Basic web protection     |
| Ignored Protection Type   | <p>If you select <b>Basic web protection</b> for <b>Ignored Protection Type</b>, specify the following parameters:</p> <ul style="list-style-type: none"><li>- <b>Attack type</b>: Configure the rule by attack event type, such as XSS and SQL injection. One type contains one or more rule IDs.</li><li>- <b>All built-in rules</b>: all checks enabled in <b>Basic Web Protection</b>.</li></ul>  | Attack type              |

| Parameter         | Description  | Example Value |
|-------------------|--|---------------|
| Attack type       | This parameter is displayed when <b>Ignored Protection Type</b> is set to <b>Attack type</b> .   | SQL injection |
| Rule Description  | A brief description of the rule. This parameter is optional.   | -             |
| Advanced Settings | <p>To ignore attacks of a specific field, specify the field in the <b>Advanced Settings</b> area. After you add the rule, EdgeSec will stop blocking attack events of the specified field.</p> <p>Select the target field from the first drop-down list box. The following fields are supported: <b>Params, Cookie, Header, Body, and Multipart</b>.</p> <ul style="list-style-type: none"><li>- If you select <b>Params, Cookie, or Header</b>, you can select <b>All</b> or <b>Specified field</b> to configure a subfield.</li><li>- If you select <b>Body</b> or <b>Multipart</b>, you can select <b>All</b>.</li><li>- If you select <b>Cookie</b>, the <b>Domain Name</b> box for the rule can be empty.</li></ul> <p><b>NOTE</b><br/>If <b>All</b> is selected, EdgeSec will not block all attack events of the selected field.</p> | Params<br>All |

- Add the source IP address to an address group. Locate the row containing the desired event, in the **Operation** column, click **Handle > Add to Address Group**. The source IP address of the event will be blocked or allowed based on the policy used for the address group.

**Add to:** You can select an existing address group or create an address group.

Figure 3-12 Add to Address Group

✕

### Add to Address Group

Attack source IP addresses added to an address group will be allowed or blocked in accordance with the policy used for the address group.

\* Attack Source IP Address 10. [ ]

\* Add to Existing address group New address group

\* Group Name  Policies the address group is used for: 1

Confirm
Cancel

- Add the source IP address to a blacklist or whitelist rule of the corresponding protected domain name. Locate the row containing the desired event. In the **Operation** column, click **Handle** > **Add to Blacklist/Whitelist**. Then, the source IP address will be blocked or allowed based on the protective action configured in the blacklist or whitelist rule.

Figure 3-13 Add to Blacklist/Whitelist

✕

### Add to Blacklist/Whitelist

Attack source IP addresses added to the policy used for the target domain name will be always allowed or blocked by the policy.

|             |              |          |        |
|-------------|--------------|----------|--------|
| Domain Name | www [ ] .com | Policies | zctest |
|-------------|--------------|----------|--------|

IP addresses or IP address ranges that can be added: 9,996

\* Attack Source IP Address 10. [ ]

\* Add to Existing rule New rule

\* Rule Name

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

\* Protective Action

Known Attack Source

Rule Description

Confirm
Cancel

**Table 3-8** Parameters for adding a record to the blacklist or whitelist

| Parameter              | Description  |
|------------------------|--|
| Add to                 | <ul style="list-style-type: none"><li>- Existing rule</li><li>- New rule</li></ul>   |
| Rule Name              | <ul style="list-style-type: none"><li>- If you select <b>Existing rule</b> for <b>Add to</b>, select a rule name from the drop-down list.</li><li>- If you select <b>New rule</b> for <b>Add to</b>, customize a blacklist or whitelist rule.</li></ul>  |
| IP Address/Range/Group | This parameter is mandatory when you select <b>New rule</b> for <b>Add to</b> .<br>You can select <b>IP address/Range</b> or <b>Address Group</b> to add IP addresses a blacklist or whitelist rule.   |
| Group Name             | This parameter is mandatory if you select <b>Address group</b> for <b>IP Address/Range/Group</b> .<br>Select an address group from the drop-down list. You can also click <b>Add Address Group</b> to create an address group. For details, see <a href="#">Adding a Blacklist or Whitelist IP Address Group</a> . |
| Protective Action      | <ul style="list-style-type: none"><li>- <b>Block</b>: Select <b>Block</b> if you want to blacklist an IP address or IP address range.</li><li>- <b>Log only</b>: Select <b>Log only</b> if you want to observe an IP address or IP address range.</li></ul>  |
| Known Attack Source    | If you select <b>Block</b> for <b>Protective Action</b> , you can select a blocking type of a known attack source rule. EdgeSec will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.   |
| Rule Description       | A brief description of the rule. This parameter is optional.   |

----End

## Effective Conditions

A false alarm will be deleted within about a minute after the handling configuration is done. It will no longer be displayed in the attack event details list. You can refresh the browser cache and access the page where the global whitelist rule is configured again to check whether the configuration is successful.

## Other Operations

If an event is handled as a false alarm, the rule hit will be added to the global protection whitelist rule list. You can go to the **Policies** page and then switch to the **Global Protection Whitelist** page to manage the rule, including querying,

disabling, deleting, and modifying the rule. For details, see [Configuring a Global Whitelist Rule](#).

## 3.3.2 Managing DDoS Protection Events



### 3.3.2.1 Viewing DDoS Protection Events

You can view event data of all protected domain names in the last 7 days.

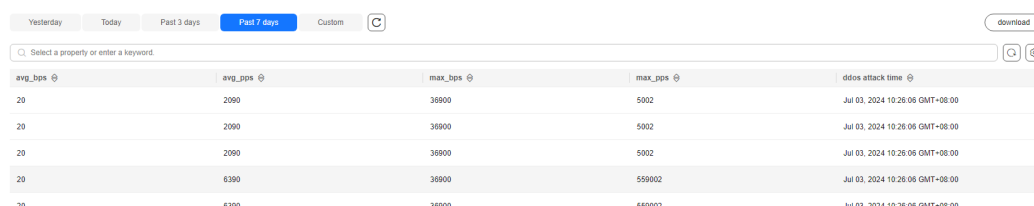
#### Prerequisites

A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

#### Procedure

- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.
- Step 3** In the navigation pane on the left, choose **Edge Security > Events**. The **Events** page is displayed.
- Step 4** Click the **DDoS Protection Events** tab to view protection logs of **yesterday**, **today**, **past 3 days**, **past 7 days**, or a custom time range.
- Step 5** In the event list, view the event details.
  - Select a filtering criterion or enter a keyword to search for specific events.
  - Click  to select fields you want to display in the event lists.

**Figure 3-14** Event list



| avg_bps | avg_pps | max_bps | max_pps | ddos attack time                |
|---------|---------|---------|---------|---------------------------------|
| 20      | 2090    | 38900   | 5002    | Jul 03, 2024 10:26:06 GMT+08:00 |
| 20      | 2090    | 38900   | 5002    | Jul 03, 2024 10:26:06 GMT+08:00 |
| 20      | 2090    | 38900   | 5002    | Jul 03, 2024 10:26:06 GMT+08:00 |
| 20      | 6390    | 38900   | 559002  | Jul 03, 2024 10:26:06 GMT+08:00 |

**Table 3-9** Parameters in the event list

| Parameter        | Description                               |
|------------------|---|
| avg_bps          | Average bandwidth of DDoS attack traffic. |
| max_bps          | Maximum bandwidth of DDoS attack traffic. |
| avg_pps          | Average forwarding rate of data packets.  |
| max_pps          | Maximum forwarding rate of data packets.  |
| ddos attack time | Time when a DDoS attack occurs.           |



----End


### 3.3.2.2 Downloading DDoS Protection Events

You can view event data of all protected domain names in the last 7 days.

#### Prerequisites

A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

#### Procedure

- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.
- Step 3** In the navigation pane on the left, choose **Edge Security > Events**. The **Events** page is displayed.
- Step 4** Choose **DDoS Protection Events**. In the upper right corner of the event list, click **Download** to download event data.

**Table 3-10** Parameters of the event table

| Parameter   | Description      |
|-------------|------------------|
| attack time | ddos attack time |
| avg bps     | avg_bps          |
| avg pps     | avg_pps          |
| max bps     | max_bps          |
| max pps     | max_pps          |

----End


## 3.4 Statistical Analysis

### 3.4.1 Web Protection Trend Statistics

On the **Web Protection Trend Statistics** page, you can view response action data of yesterday, today, past 3 days, past 7 days, past 30 days, or a custom time range.

## Procedure

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.

**Step 3** In the navigation pane on the left, choose **Edge Security > Statistics**. The **Statistics** page is displayed.

**Step 4** In the upper part of the **Web Protection Trend Statistics** page, set the domain name, website, time range, and time granularity.

- **All protected websites:** By default, the information about all websites you add to EdgeSec in all enterprise projects are displayed.
- **Time range:** You can select **Yesterday, Today, Past 3 Days, Past 7 Days, Past 30 Days**, or **Custom**.

### NOTICE

The maximum time range is **Past 30 Days**.

- **Time granularity:** This parameter depends on the selected query time range. For details, see [Table 3-11](#).

**Table 3-11** Time granularity

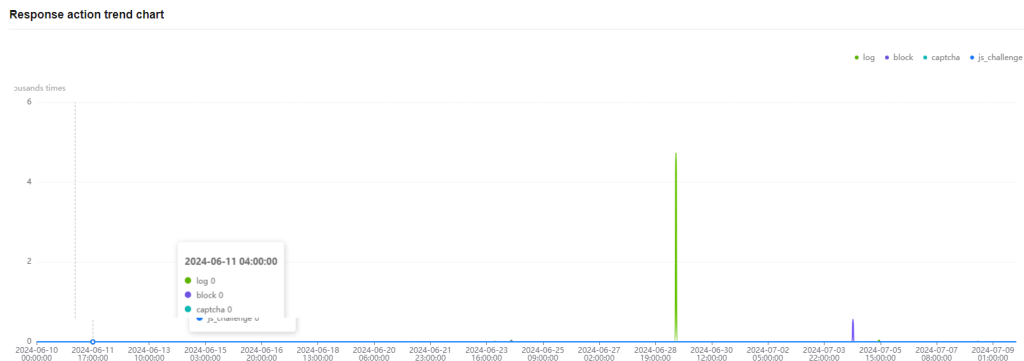
| Time Range                | Time Granularity                      |
|---------------------------|---------------------------------------|
| 1 hour                    | 1 minute or 5 minutes                 |
| Within 1 day (> 1 hour)   | 1 minute, 5 minutes, or 1 hour        |
| Within 3 days (> 1 day)   | 1 minute, 5 minutes, 1 hour, or 1 day |
| Within 7 days (> 3 days)  | 5 minutes, 1 hour, or 1 day           |
| Within 30 days (> 7 days) | 1 hour or 1 day                       |

**Step 5** View the number requests that trigger different response actions, including **log only, block, verification code**, and **JS challenge**.

- **Log only:** A request that matches the rule is logged but not blocked.
- **Block:** A request that matches the rule is blocked and the block response page is returned to the client that initiates the request.
- **Verification code:** If the JavaScript challenge fails, a verification code is required. Requests will be blocked unless the visitor enters a correct verification code.
- **JS challenge:** EdgeSec returns a piece of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes the JavaScript code, EdgeSec allows all requests from the client within a period of time (30 minutes by default). During this period, no

verification is required. If the client fails to execute the code, WAF blocks the requests.

**Figure 3-15** Response action trend chart




----End

## 3.4.2 Web Top Statistics

On the **Web Top Statistics** page, you can view key request statistics such as client IP addresses, URLs, and server domain names for the last 30 minutes, today, or a user-defined period.

### Procedure

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.

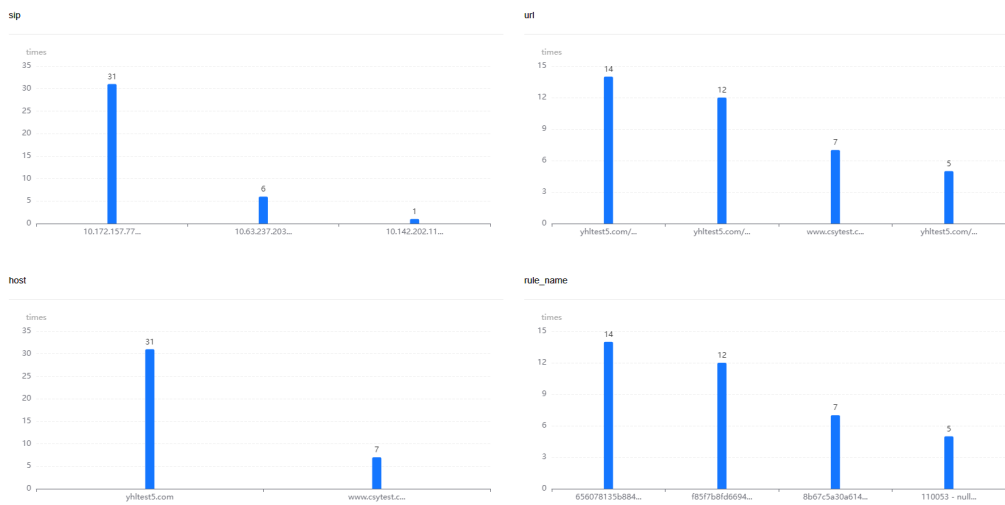
**Step 3** In the navigation pane on the left, choose **Edge Security > Statistics**. The **Statistics** page is displayed.

**Step 4** In the upper part of the page, specify the domain, website, and time period you want to query.

- **All protected websites:** By default, the information about all websites you add to EdgeSec in all enterprise projects are displayed.
- **Time period:** You can select **Last 30 Minutes**, **Today**, or **Custom**.

**Step 5** Data display

**Figure 3-16** Web TOP statistics



**Table 3-12** Web TOP statistics parameters

| Parameter      | Description  |
|----------------|--|
| sip            | IP address of the client that initiates the request.   |
| url            | URL that receives the request.   |
| host           | Domain name of the server that receives the request.   |
| rule_name      | The type structure is policy ID-policy_name.   |
| User agent     | HTTP request header, which contains information about the user agent application that sends the request, including the browser ID, operating system ID, language, and version details. |
| Request method | HTTP request method.   |

----End

## 3.5 Protection Policy

### 3.5.1 Creating a Protection Policy

A policy is a combination of rules, such as basic web protection, blacklist, whitelist, and precise protection rules. A policy can be applied to multiple domain names, but only one policy can be used for a domain name. This section describes how to add a protection policy.


#### Constraints

- A protected domain name can use only one policy.

- A maximum of 3,000 protection policies can be added.

## Procedure

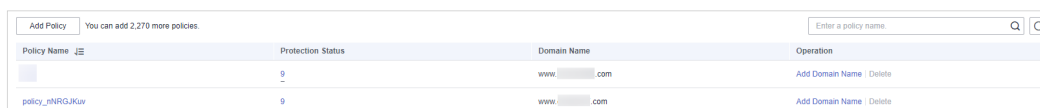
**Step 1** [Log in to the management console.](#)

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

**Step 3** In the navigation pane on the left, choose **Edge Security** > **Policies**. The **Policies** page is displayed.

**Step 4** In the upper left corner, click **Add Policy**.

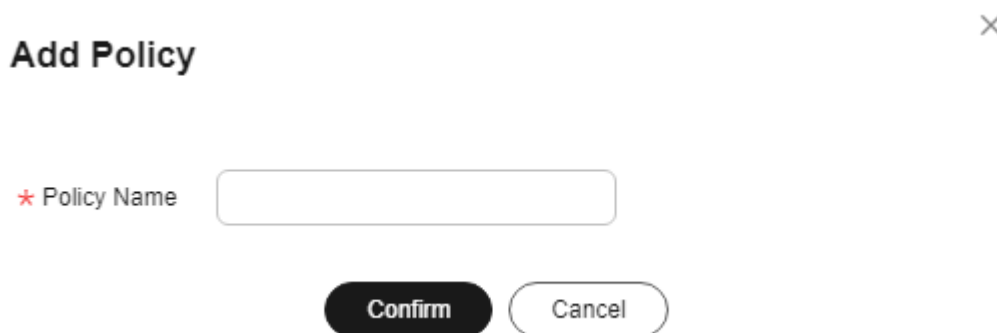
**Figure 3-17** Adding a protection policy



| Policy Name     | Protection Status | Domain Name | Operation                |
|-----------------|-------------------|-------------|--------------------------|
|                 | 0                 | www. .com   | Add Domain Name   Delete |
| policy_nNRGJKuv | 0                 | www. .com   | Add Domain Name   Delete |

**Step 5** In the dialog box that is displayed, enter a policy name and click **confirm**.

**Figure 3-18** Add Policy



**Add Policy** ✕

\* Policy Name


**Confirm** **Cancel**

**Step 6** The added policy is displayed in the policy list.

**Step 7** In the **Policy Name** column, click the policy name. On the displayed page, add rules to the policy by referring to [Configuring Protection Rules](#).

----End

## Other Operations


- To modify a policy name, click  next to the policy name. In the dialog box displayed, enter a new policy name.
- To delete a rule, click **Delete** in the **Operation** column.

## 3.5.2 Applying a Policy to Your Website

This section describes how to apply a policy to your protected website.

## Procedure

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

**Step 3** In the navigation pane on the left, choose **Edge Security** > **Policies**. The **Policies** page is displayed.

**Step 4** In the row containing the target policy, click **Add Domain Name** in the **Operation** column.

**Step 5** Select a **Domain Name** that applies to the policy.

---

### NOTICE

- A protected domain name can use only one policy,
  - but one policy can be applied to multiple domain names.
  - To delete a policy that has been applied to domain names, add these domain names to other policies first. Then, click **Delete** in the **Operation** column of the policy you want to delete.
- 

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

----End

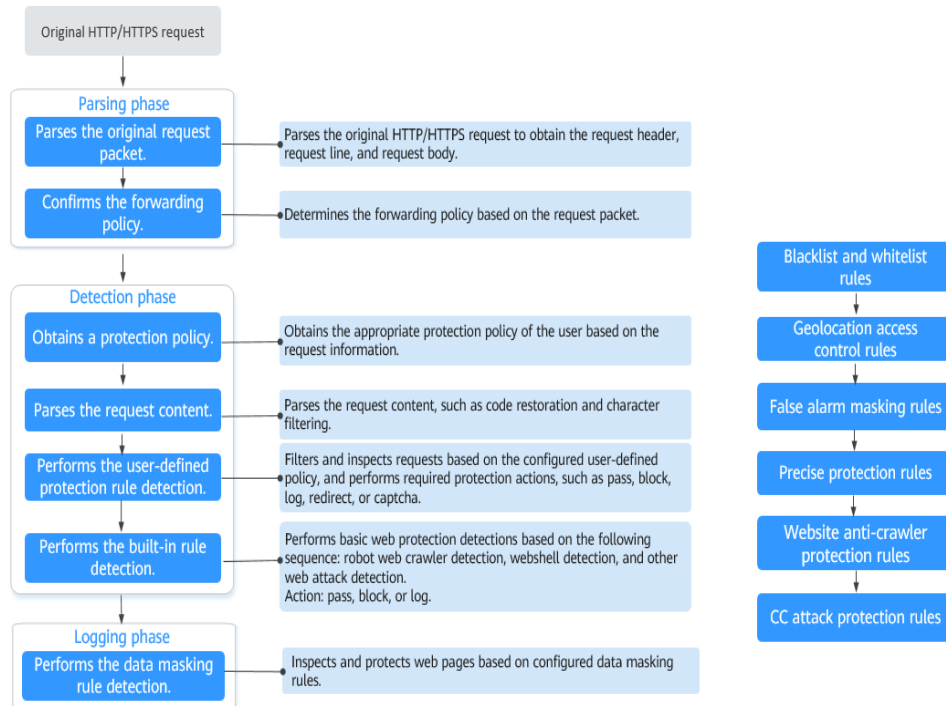
## 3.5.3 Configuring Protection Policies

### 3.5.3.1 Configuration Guidance

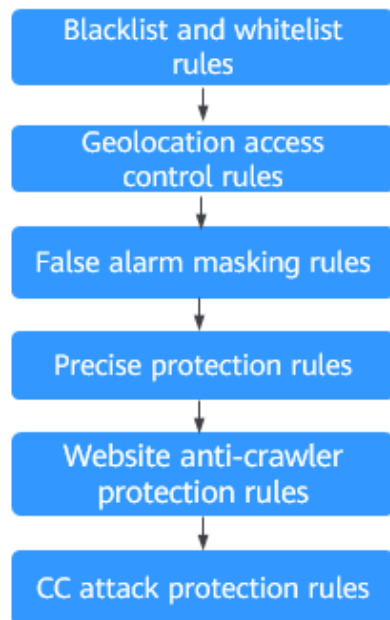
#### How EdgeSec Engine Works

The built-in protection rules of EdgeSec help you defend against common web application attacks, including XSS attacks, SQL injection, crawlers, and web shells. You can customize protection rules to let EdgeSec better protect your website services using these custom rules. [Figure 3-19](#) shows how EdgeSec engine built-in protection rules work. [Figure 3-20](#) shows the detection sequence of user-defined rules.

**Figure 3-19** EdgeSec engine detection process



**Figure 3-20** Priorities of custom protection rules



**Response actions**

- **Pass:** The current request is unconditionally permitted after a protection rule is matched.
- **Block:** The current request is blocked after a rule is matched.

- CAPTCHA: The system will perform human-machine verification after a rule is matched.
- Redirect: The system will notify you to redirect the request after a rule is matched.
- Log: Only attack information is recorded after a rule is matched.
- Mask: The system will anonymize sensitive information after a rule is matched.

## Protection Rule Configuration Methods

EdgeSec provides the following customized configuration methods to simplify the configuration process. Select a proper configuration method to meet your service requirements.



This method is recommended when you have few domain name services or have different configuration rules for domain name services.

### NOTE

After a domain name is added, EdgeSec automatically associates a protection policy with the domain name, and protection rules configured for the domain name are also added to the protection policy by default. If there are domain names applicable to the protection policy, you can directly add them to the policy. For details, see [Applying a Policy to Your Website](#).

- Where to configure
  - In the navigation pane on the left, choose **Website Settings**.
  - In the **Policy** column of the row containing the target domain name, click the number to go to the **Policies** page.

**Figure 3-21** Website list

| Domain Name     | Last 3 Days  | Mode    | Scheduling Status  | Policy         | Created                         | Operation |
|-----------------|--|---------|--|----------------|---------------------------------|-----------|
| www.esatest.com |  No attacks detected. | Enabled |  Scheduled to WAF | policy_7n0t4is | Jul 04, 2024 15:43:48 GMT+08:00 | Delete    |

- Protection rules you can configure on the rule configuration page

**Table 3-13** Configurable protection rules

| Protection Rule      | Description  | Reference   |
|----------------------|--|---|
| Basic Web Protection | With an extensive reputation database, EdgeSec defends against Open Web Application Security Project (OWASP) top 10 threats, and detects and blocks threats, such as malicious scanners, IP addresses, and web shells. | <a href="#">Configuring Basic Protection Rules to Defend Against Common Web Attacks</a> |



| Protection Rule                   | Description  | Reference  |
|-----------------------------------|--|--|
| CC Attack Protection              | CC attack protection rules can be customized to restrict access to a specific URL on your website based on a unique IP address, mitigating CC attacks.   | <a href="#">Configuring CC Attack Protection Rules to Defend Against CC Attacks</a>                    |
| Precise Protection                | You can customize protection rules by combining HTTP headers, cookies, URLs, request parameters, and client IP addresses.  | <a href="#">Configuring a Precise Protection Rule</a>  |
| Blacklist and Whitelist           | You can configure blacklist and whitelist rules to block or log only access requests from specified IP addresses.  | <a href="#">Configuring IP Address Blacklist and Whitelist Rules to Block Specified IP Addresses</a>   |
| Known Attack Source               | If EdgeSec blocks a malicious request by IP address, Cookie, or Params, you can configure a known attack source rule to let EdgeSec automatically block all requests from the attack source for a blocking duration set in the known attack source rule. | <a href="#">Configuring a Known Attack Source Rule</a>   |
| Geolocation Access Control        | You can customize these rules to allow or block requests from a specific country or region.  | <a href="#">Configuring Geolocation Access Control Rules to Block Requests from Specific Locations</a> |
| Anti-Crawler                      | This function dynamically analyzes website service models and accurately identifies crawler behavior based on data risk control and bot identification systems, such as JS Challenge.  | <a href="#">Configuring Anti-Crawler Rules</a>   |
| Global protection whitelist rules | You can configure these rules to let EdgeSec ignore certain rules for specific requests.   | <a href="#">Configuring a Global Whitelist Rule to Ignore False Positives</a>                          |
| Data Masking                      | You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.   | <a href="#">Configuring a Data Masking Rule</a>  |

### 3.5.3.2 Configuring Basic Protection Rules to Defend Against Common Web Attacks

After this function is enabled, EdgeSec can defend against common web 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. You can also enable basic web protection, such as web shell detection.

#### Prerequisites


A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

#### Constraints

- Basic web protection has two modes: **Block** and **Log only**.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- If you select **Block** for **Basic Web Protection**, you can [configure access control criteria for a known attack source](#). EdgeSec will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.

#### Procedure



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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.

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

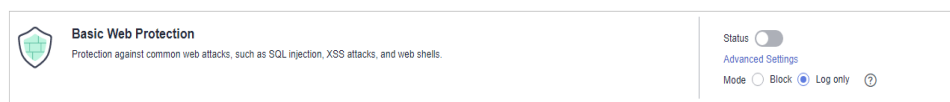
**Step 4** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

**Figure 3-22** Website list



| Domain Name     | Last 3 Days  | Mode    | Scheduling Status  | Policy          | Created                         | Operation |
|-----------------|--|---------|--|-----------------|---------------------------------|-----------|
| www.esatest.com |  No attacks detected. | Enabled |  Scheduled to WAF | policy_7nClT4is | Jul 04, 2024 15:43:48 GMT+08:00 | Delete    |

**Step 5** In the **Basic Web Protection** configuration area, change **Status** and **Mode** as needed by referring to [Table 3-14](#).

**Figure 3-23** Basic Web Protection configuration area

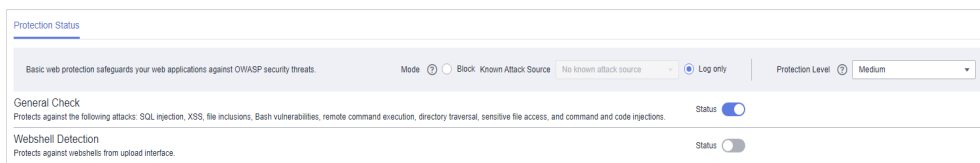


**Table 3-14** Parameter description

| Parameter | Description  |
|-----------|--|
| Status    | Status of Basic Web Protection <ul style="list-style-type: none"> <li> : enabled.</li> <li> : disabled.</li> </ul> |
| Mode      | <ul style="list-style-type: none"> <li><b>Block</b>: The detected attacks are blocked and logged.</li> <li><b>Log only</b>: The detected attacks are logged only.</li> </ul>   |

**Step 6** In the **Basic Web Protection** configuration area, click **Advanced Settings**.

**Step 7** On the **Protection Status** tab page, enable protection types you need by referring to [Table 3-16](#).

**Figure 3-24** 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](#).

1. 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 3-15** 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.  |

| Protection Level | Description   |
|------------------|---|
| High             | <p>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.</p> <p>Configure global whitelist rules after the service has been running for a period of time, and then enable the strict mode.</p> |

2. Set the protection type.

---

**NOTICE**

By default, **General Check** is enabled. You can enable other protection types by referring to [Table 3-16](#).

---

**Table 3-16** Protection types

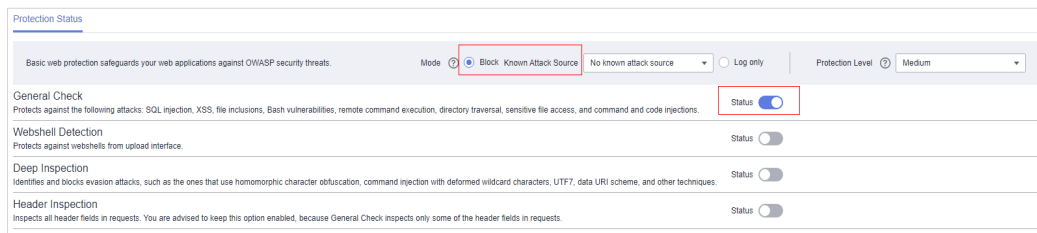
| Type               | Description   |
|--------------------|---|
| General Check      | <p>Defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code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

----End

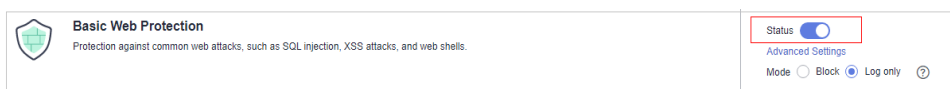
## Example - Blocking SQL Injection Attacks

If domain name **www.example.com** has been connected to EdgeSec, perform the following steps to verify that EdgeSec can block SQL injection attacks.

- Step 1** Enable **General Check** in **Basic Web Protection** and set the protection mode to **Block**.

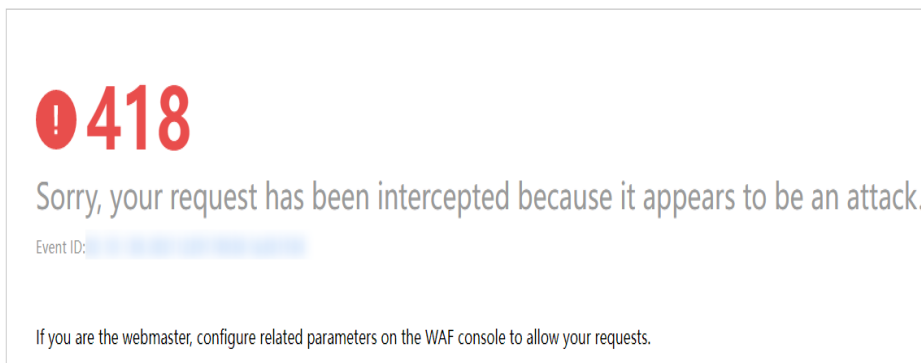
**Figure 3-25** Enabling General Check

**Step 2** Enable EdgeSec basic web protection.

**Figure 3-26** Enabling EdgeSec basic web protection

**Step 3** Clear the browser cache and enter a simulated SQL injection (for example, `http://www.example.com?id=' or 1=1`) in the address box.

The access request is intercepted, as shown in [Figure 3-27](#).


**Figure 3-27** Block page

**Step 4** Go to the EdgeSec console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page.

----End

### 3.5.3.3 Configuring CC Attack Protection Rules to Defend Against CC Attacks

CC attack protection can limit the access to a protected website based on a single IP address. To use this protection, ensure that you have toggled on **CC Attack**

**Protection** (its status should be ).

#### Prerequisites


A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

## Constraints

- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- A reference table can be added to a CC attack protection rule. The reference table takes effect for all protected domain names.
- A CC attack protection rule offers protective actions such as **Verification code** and **Block** for your choice. For example, you can configure a CC attack protection rule to block requests from a visit for 600 seconds if the visitor accessed a URL (for example, /admin\*) of your website over 10 times within 60 seconds.

## Procedure



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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge 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 domain name, click the number to go to the **Policies** page.

**Figure 3-28** Website list

| Domain Name     | Last 3 Days  | Mode    | Scheduling Status  | Policy                     | Created                         | Operation |
|-----------------|--|---------|--|----------------------------|---------------------------------|-----------|
| www.esatest.com |  No attacks detected. | Enabled |  Scheduled to WAF | policy_7nDIT4is<br>9<br>.. | Jul 04, 2024 15:43:48 GMT+08:00 | Delete    |

**Step 5** In the **CC Attack Protection** configuration area, change **Status** as needed and click **Customize Rule** to go to the **CC Attack Protection** page.

**Figure 3-29** CC Attack Protection configuration area



**Step 6** In the upper left corner of the **CC Attack Protection** page, click **Add Rule**.

**Step 7** In the displayed dialog box, configure a CC attack protection rule by referring to [Table 3-17](#).

**Table 3-17** Rule parameters

| Parameter        | Description  | Example Value |
|------------------|--|---------------|
| Rule Name        | Name of the rule   | test          |
| Rule Description | A brief description of the rule. This parameter is optional. | --            |

| Parameter       | Description  | Example Value                                   |
|-----------------|--|---|
| Rate Limit Mode | <ul style="list-style-type: none"><li>● <b>Source:</b>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, EdgeSec limits traffic rate of the IP address (or user) in the way you configure.<br/><b>Per IP address:</b> A website visitor is identified by the IP address.</li></ul>   | --  |
| Trigger         | <p>Click <b>Add</b> to add conditions. At least one condition is required, but up to 30 conditions are allowed. If you add more than one condition, the rule will only take effect if all of the conditions are met.</p> <ul style="list-style-type: none"><li>● <b>Fields:</b> include geolocation, path, IP address, cookie, header, Params, and HTTP code.</li><li>● <b>Subfield:</b> Configure this field only when <b>Cookie, Header, or Params</b> is selected for <b>Field</b>.</li></ul> <p><b>NOTICE</b><br/>The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.</p> <ul style="list-style-type: none"><li>● <b>Logic:</b> Select a logical relationship from the drop-down list.</li></ul> <p><b>NOTE</b><br/>If you set <b>Logic</b> to <b>Include any value, Exclude any value, Equal to any value, Not equal to any value, Prefix is any value, Prefix is not any of them, Suffix is any value, or Suffix is not any of them</b>, select an existing reference table. For details, see <a href="#">Creating a Reference Table to Configure Protection Metrics In Batches</a>.</p> <ul style="list-style-type: none"><li>● <b>Content:</b> Enter or select the content that matches the condition.</li></ul> | <b>Path Include / admin</b>                     |
| Rate Limit      | The maximum requests that a website visitor can initiate within the configured period. If the configured rate limit has been reached, EdgeSec will respond according to the protective action configured.  | <b>10</b> requests allowed in <b>60</b> seconds |

| Parameter         | Description   | Example Value   |
|-------------------|---|---|
| Protective Action | <p>The action that EdgeSec will take if the number of requests exceeds <b>Rate Limit</b> you configured. The options are as follows:</p> <ul style="list-style-type: none"><li>• <b>Verification code:</b> EdgeSec allows requests that trigger the rule as long as your website visitors complete the required verification. Currently, certification code supports English.</li><li>• <b>Block:</b> EdgeSec blocks requests that trigger the rule.</li><li>• <b>Log only:</b> EdgeSec only logs requests that trigger the rule.</li></ul> | Block   |
| Block Duration    | Period of time for which to block the item when you set <b>Protective Action</b> to <b>Block</b> .  | <b>600</b> seconds  |
| Block Page        | <p>The page displayed if the maximum number of requests has been reached. This parameter is configured only when <b>Protective Action</b> is set to <b>Block</b>.</p> <ul style="list-style-type: none"><li>• If you select <b>Default settings</b>, the default block page is displayed.</li><li>• If you select <b>Custom</b>, a custom error message is displayed.</li></ul>   | Custom  |
| Block Page Type   | If you select <b>Custom</b> for <b>Block Page</b> , select a type of the block page among options <b>application/json</b> , <b>text/html</b> , and <b>text/xml</b> .  | text/html   |
| Page Content      | If you select <b>Custom</b> for <b>Block Page</b> , configure the content to be returned.   | <p>Page content styles corresponding to different page types are as follows:</p> <ul style="list-style-type: none"><li>• <b>text/html:</b><br/>&lt;html&gt;&lt;body&gt;Forbidden&lt;/body&gt;&lt;/html&gt;</li><li>• <b>application/json:</b> {"msg": "Forbidden"}</li><li>• <b>text/xml:</b> &lt;?xml version="1.0" encoding="utf-8"?&gt;&lt;error&gt;&lt;msg&gt;Forbidden&lt;/msg&gt;&lt;/error&gt;</li></ul> |



**Step 8** Click **OK**. You can then view the added CC attack protection rule in the CC rule list.

- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

----End

## Configuration Example - Verification Code

If domain name **www.example.com** has been connected to EdgeSec, perform the following steps to verify that EdgeSec CAPTCHA verification is enabled.

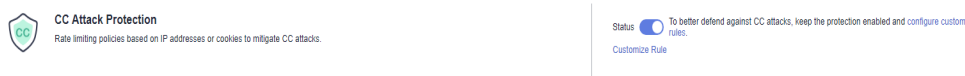
**Step 1** Add a CC attack protection rule with **Protection Action** set to **Verification code**.

**Figure 3-30** Verification code



**Step 2** Enable CC attack protection.

**Figure 3-31** CC Attack Protection configuration area



**Step 3** Clear the browser cache and access <http://www.example.com/admin/>.

If you access the page 10 times within 60 seconds, a verification code is required when you attempt to access the page for the eleventh time. You need to enter the verification code to continue the access.

### NOTE

There is a delay before the blocking takes effect. If the operation proceeds too quickly, the eleventh visiting attempt may not be blocked.



### Verification Required

Your requests are too frequent!

Please input the verification code:   

**Step 4** Go to the EdgeSec console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page.

----End

### 3.5.3.4 Configuring a Precise Protection Rule

EdgeSec allows you to customize protection rules by combining HTTP headers, cookies, URLs, request parameters, and client IP addresses.

You can combine common HTTP fields, such as **IP**, **Path**, **Referer**, **User Agent**, and **Params** in a protection rule to let EdgeSec block or only log the requests that match the combined conditions.

A reference table can be added to a precise protection rule. The reference table takes effect for all protected domain names.

## Prerequisites

A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

## Constraints


- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- If you configure **Protective Action** to **Block** for a precise protection rule, you can configure a known attack source rule by referring to [Configuring a Known Attack Source Rule](#). EdgeSec will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.

## Application Scenarios

Precise protection rules are used for anti-leeching and website management background protection.

## Procedure



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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

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

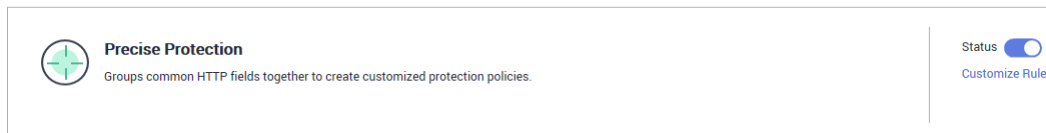
**Step 4** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

**Figure 3-32** Website list

| Domain Name                     | Last 3 Days  | Mode    | Scheduling Status  | Policy                     | Created                         | Operation |
|---------------------------------|--|---------|--|----------------------------|---------------------------------|-----------|
| <a href="#">www.esalest.com</a> |  No attacks detected. | Enabled |  Scheduled to WAF | policy_7nDIT4is<br>9<br>.. | Jul 04, 2024 15:43:48 GMT+08:00 | Delete    |

**Step 5** In the **Precise Protection** configuration area, change **Status** as needed and click **Customize Rule** to go to the **Precise Protection** page.

**Figure 3-33** Precise Protection configuration area



**Step 6** On the **Precise Protection** page, set **Detection Mode**.

Two detection modes are available:

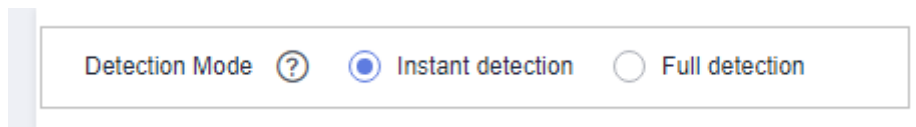
- **Instant Detection:** If a request matches a configured precise protection rule, EdgeSec immediately ends threat detection and blocks the request.

 **NOTE**

When the request meets the blocking conditions in Precise Protection, CC attack detection is still performed.

- **Full Detection:** If a request matches a configured precise protection rule, EdgeSec finishes its scan first and then blocks all requests that match the configured precise protection rule.

**Figure 3-34** Setting Detection Mode



**Step 7** Click **Add Rule**.

**Step 8** In the displayed dialog box, add a rule by referring to [Table 3-18](#) and [Table 3-19](#).

The settings shown in [Figure 3-35](#) are used as an example. If a visitor tries to access a URL containing `/admin`, EdgeSec will block the request.

---

**NOTICE**

To ensure that EdgeSec blocks only attack requests, configure **Protective Action** to **Log only** first and check whether normal requests are blocked on the **Events** page. If no normal requests are blocked, configure **Protective Action** to **Block**.

---

**Figure 3-35 Add Precise Protection Rule**

✕

**Add Precise Protection Rule**

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              |
|-------|----------|---------|----------------------|
| Path  | --       | Include | <input type="text"/> |

[Add Reference Table](#)

⊕ Add You can add 29 more conditions. (The protective action is executed only when all the conditions are met.)

\* Protective Action

\* Known Attack Source

\* Priority  A smaller value indicates a higher priority.

\* Effective Date  Immediate  Custom

**Table 3-18 Rule parameters**

| Parameter | Description                                     | Example Value |
|-----------|---|---------------|
| Rule Name | Name of a user-defined precise protection rule. | --            |

| Parameter      | Description   | Example Value   |
|----------------|---|---|
| Condition List | <p>Click <b>Add</b> to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. A condition includes the following parameters:</p> <p>Parameters for configuring a condition are described as follows:</p> <ul style="list-style-type: none"><li>• <b>Field</b></li><li>• <b>Subfield:</b> Configure this field only when <b>IP</b>, <b>Params</b>, <b>Cookie</b>, or <b>Header</b> is selected for <b>Field</b>.</li></ul> <p><b>NOTICE</b><br/>The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.</p> <ul style="list-style-type: none"><li>• <b>Logic:</b> Select a logical relationship from the drop-down list.</li></ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"><li>- If <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> is selected, select an existing reference table in the <b>Content</b> drop-down list. For details, see <a href="#">Creating a Reference Table to Configure Protection Metrics In Batches</a>.</li><li>- <b>Exclude any value</b>, <b>Not equal to any value</b>, <b>Prefix is not any of them</b>, and <b>Suffix is not any of them</b> indicates, respectively, that EdgeSec performs the protection action (block or log only) when the field in the access request does not contain, is not equal to, or the prefix or suffix is not any value set in the reference table. For example, assume that <b>Path</b> field is set to <b>Exclude any value</b> and the <b>test</b> reference table is selected. If <i>test1</i>, <i>test2</i>, and <i>test3</i> are set in the <b>test</b> reference table, EdgeSec performs the protection action when the path of the access request does not contain <i>test1</i>, <i>test2</i>, or <i>test3</i>.</li></ul> | <ul style="list-style-type: none"><li>• <b>Path Include /admin</b></li><li>• <b>User Agent Prefix is not mozilla/5.0</b></li><li>• <b>IP Equal to 192.168.2.3</b></li><li>• <b>Cookie key1 Prefix is not jsessionid</b></li></ul> |

| Parameter           | Description   | Example Value                        |
|---------------------|---|--------------------------------------|
|                     | <ul style="list-style-type: none"> <li>• <b>Content:</b> Enter or select the content of condition matching.</li> </ul> <p><b>NOTE</b><br/>For more details about the configurations in general, see <a href="#">Table 3-19</a>.</p>   |                                      |
| Protective Action   | You can select <b>Block Log only</b> , or <b>JS Challenge</b> (EdgeSec returns JavaScript code).  | <b>Block</b>                         |
| Known Attack Source | If you set <b>Protective Action</b> to <b>Block</b> , you can select a blocking type for a known attack source rule. EdgeSec will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.   | <b>Long-term IP address blocking</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.<br><br><b>NOTICE</b><br>If multiple precise access control rules have the same priority, EdgeSec matches the rules in the sequence of time the rules are added. | <b>5</b>                             |
| Effective Date      | Select <b>Immediate</b> to enable the rule immediately, or select <b>Custom</b> to configure when you wish the rule to be enabled.  | <b>Immediate</b>                     |

**Table 3-19** Condition list configurations

| Field  | Subfield | Logic  | Example Content  |
|--|----------|--|--|
| <b>Path:</b> Part of a URL that does not include a domain name. This value supports exact matches only. For example, if the path to be protected is <b>/admin</b> , <b>Path</b> must be set to <b>/admin</b> . | None     | Select a logical relationship from the drop-down list. | <b>/buy/phone/</b><br><b>NOTICE</b><br>If <b>Path</b> is set to <b>/</b> , all paths of the website are protected. |

| Field  | Subfield   | Logic | Example Content  |
|--|--|-------|--|
| <b>User Agent:</b> A user agent of the scanner to be checked.  | None   |       | <b>Mozilla/5.0 (Windows NT 6.1)</b>  |
| <b>IP:</b> An IP address of the visitor to be protected.   | <ul style="list-style-type: none"> <li>Client IP Address</li> <li>X-Forwarded-For</li> </ul>       |       | XXX.XXX.1.1  |
| <b>Params:</b> A request parameter.  | None   |       | <b>201901150929</b>  |
| <b>Cookie:</b> A small piece of data to identify web visitors  | <ul style="list-style-type: none"> <li>All fields</li> <li>Any subfield</li> <li>Custom</li> </ul> |       | jsessionId   |
| <b>Referer:</b> A user-defined request resource.<br>For example, if the protected path is / <b>admin/xxx</b> and you do not want visitors to access the page from <b>www.test.com</b> , set <b>Content</b> to <b>http://www.test.com</b> . | None   |       | http://www.test.com  |
| <b>Header:</b> A user-defined HTTP header.   | <ul style="list-style-type: none"> <li>All fields</li> <li>Any subfield</li> <li>Custom</li> </ul> |       | <b>text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8</b> |
| <b>Method:</b> the user-defined request method.  | None   |       | <b>GET, POST, PUT, DELETE, and PATCH</b>   |
| <b>Request Line:</b> Length of a user-defined request line.  | None   |       | <b>50</b>  |

| Field   | Subfield | Logic  | Example Content   |
|---|----------|--|---|
| <b>Request:</b> Length of a user-defined request. It includes the request header, request line, and request body. | None     |  | None  |
| <b>Protocol:</b> the protocol of the request.   | None     |  | http  |
| Request message body.   | None     |  | None  |
| ASN: AS number  | --       | <ul style="list-style-type: none"><li>• Include</li><li>• Exclude</li><li>• Greater than</li><li>• Less than</li></ul> | --  |
| Geolocation   | --       | <ul style="list-style-type: none"><li>• Include</li><li>• Exclude</li></ul>  | --  |
| Known feature crawler   | --       | <ul style="list-style-type: none"><li>• Match</li><li>• Mismatch</li></ul>   | <ul style="list-style-type: none"><li>• Search engine</li><li>• Scanner</li><li>• Script tool</li><li>• Other</li></ul> |

**Step 9** Click **Confirm**. You can then view the added precise protection rule in the protection rule list.

- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

----End

## Protection Effect

If you have configured a precise protection rule as shown in [Figure 3-35](#) for your domain name, to verify EdgeSec is protecting your website (**www.example.com**) against the rule:

**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 EdgeSec by following the instructions in [Adding a Website to EdgeSec](#).
- If the website is accessible, go to [2](#).



**Step 2** Clear the browser cache and enter **http://www.example.com/admin** (or any page containing **/admin**) in the address bar. Normally, EdgeSec blocks the requests that meet the conditions and returns the block page.

----End

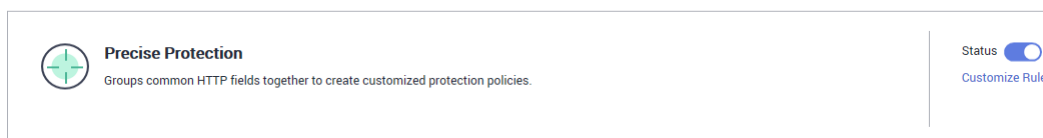
## Configuration Example - Disallowing Access Requests from IP Addresses in a Specified Region

Assume that domain name *www.example.com* has been connected to EdgeSec and you want to disallow only IP addresses in **BeijingSingapore**, to access the domain name. Perform the following steps:

**Step 1** Add a precise protection rule. Set the **Field** to **Geolocation**, **Content** to **BeijingSingapore**, and **Protective Action** to **Block**.

**Step 2** Enable the precise protection rule.

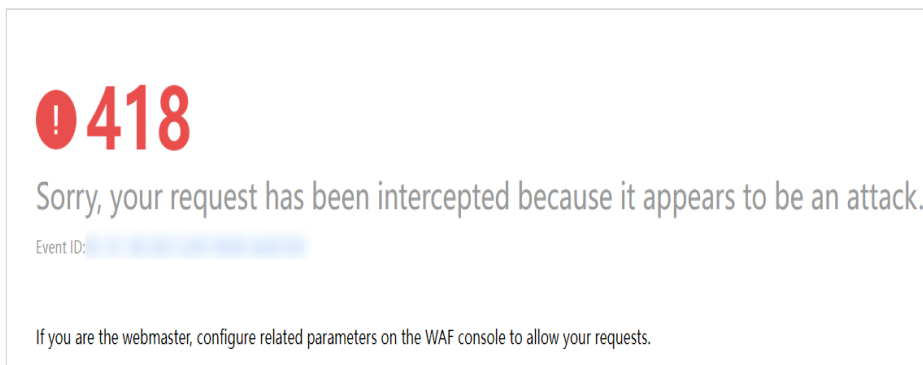
**Figure 3-36** Precise Protection configuration area



**Step 3** Clear the browser cache and access <http://www.example.com>.

When an access request from IP addresses in **BeijingSingapore** accesses a page, EdgeSec blocks the access request, as shown in [Block page](#).

**Figure 3-37** Block page



**Step 4** Go to the EdgeSec console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page. You will see that all requests from **BeijingSingapore** have been blocked.

----End

### 3.5.3.5 Creating a Reference Table to Configure Protection Metrics In Batches

This topic describes how to create a reference table to batch configure protection metrics of a single type, such as **Path**, **User Agent**, **IP**, **Params**, **Cookie**, **Referer**,

and **Header**. A reference table can be referenced by CC attack protection rules and precise protection rules.

## Prerequisites

A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

## Constraints


A maximum of 100 reference tables can be created.

## Application Scenarios

You can use a reference table when you configure protection fields in batches for CC attack protection rules and precise access protection rules.

## Procedure



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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge 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 domain name, click the number to go to the **Policies** page.

**Figure 3-38** Website list

| Domain Name     | Last 3 Days  | Mode    | Scheduling Status  | Policy                          | Created                         | Operation              |
|-----------------|--|---------|--|---------------------------------|---------------------------------|------------------------|
| www.esatest.com |  No attacks detected. | Enabled |  Scheduled to WAF | <a href="#">policy_7nCiT4is</a> | Jul 04, 2024 15:43:48 GMT+08:00 | <a href="#">Delete</a> |

**Step 5** In the **CC Attack Protection** or **Precise Protection** area, click **Customize Rule**.

**Step 6** Click **Reference Table Management** in the upper left corner of the list.

**Step 7** On the **Reference Table Management** page, click **Add Reference Table**.

**Step 8** In the **Add Reference Table** dialog box, specify the parameters by referring to [Table 3-20](#).

**Figure 3-39** Adding a reference table

### Add Reference Table

×

\* Name

\* Type

\* Value

[+](#) Add You can add 99 more conditions.

Rule Description

Confirm
Cancel

**Table 3-20** Parameter description

| Parameter | Description            | Example Value |
|-----------|------------------------|---------------|
| Name      | Table name you entered | test          |

| Parameter | Description   | Example Value      |
|-----------|---|--------------------|
| Type      | <ul style="list-style-type: none"><li>• <b>Path:</b> A URL to be protected, excluding a domain name</li><li>• <b>User Agent:</b> A user agent of the scanner to be protected</li><li>• <b>IP:</b> An IP address of the visitor to be protected.</li><li>• <b>Params:</b> A request parameter to be protected</li><li>• <b>Cookie:</b> A small piece of data to identify web visitors</li><li>• <b>Referer:</b> A user-defined request resource.<br/>For example, if the protected path is /<b>admin/xxx</b> and you do not want visitors to access it from <i>www.test.com</i>, set <b>Value</b> to <b>http://www.test.com</b>.</li><li>• <b>Header:</b> A user-defined HTTP header</li></ul> | <b>Path</b>        |
| Value     | Value of the corresponding <b>Type</b> . Wildcards are not allowed.<br><b>NOTE</b><br>Click <b>Add</b> to add more than one value.  | <b>/buy/phone/</b> |

**Step 9** Click **Confirm**. You can then view the added reference table in the reference table list.

----End

## Other Operations

- To modify a reference table, click **Modify** in the row containing the reference table.
- To delete a reference table, click **Delete** in the row containing the reference table.

### 3.5.3.6 Configuring IP Address Blacklist and Whitelist Rules to Block Specified IP Addresses

By default, all IP addresses are allowed to access your website. You can configure blacklist and whitelist rules to block or log only, or allow access requests from specified IP addresses or IP address ranges. You can add a single IP address or import an IP address group to the blacklist or whitelist.

## Prerequisites

A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

## Constraints

- EdgeSec supports batch import of IP address blacklists and whitelists. You can use address groups to add multiple IP addresses or IP address ranges quickly to a blacklist or whitelist rule. For details, see [Adding a Blacklist or Whitelist IP Address Group](#).
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- The address 0.0.0.0/0 cannot be added to the IP address blacklist or whitelist. If you want to block all IP addresses within a range of blocked addresses, add a blacklist rule to block the range.
- If you configure **Protective Action** to **Block** for a blacklist or whitelist rule, you can configure a known attack source rule by referring to [Configuring a Known Attack Source Rule](#). EdgeSec will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.

## Precautions

- If you configure an IP address blacklist/whitelist rule in both EdgeSec and [CDN](#), the blacklist/whitelist rule in CDN is executed first.
- If the quota of IP address whitelist and blacklist rules of your EdgeSec instance cannot meet your requirements, you can purchase rule expansion packages under the current EdgeSec instance edition (a rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules) to increase such quota.

## Impact on the System


If an IP address is added to a blacklist, EdgeSec blocks requests from that IP address without checking whether the requests are malicious.

### NOTE

After an IP address or IP address segment is added to the blacklist, CC attack detection is still performed.

## Procedure

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

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

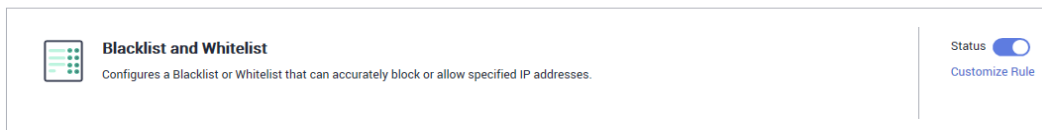
**Step 4** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

**Figure 3-40** Website list

| Domain Name     | Last 3 Days          | Mode    | Scheduling Status | Policy          | Created                         | Operation |
|-----------------|----------------------|---------|-------------------|-----------------|---------------------------------|-----------|
| www.esatest.com | No attacks detected. | Enabled | Scheduled to WAF  | policy_7nCiT4is | Jul 04, 2024 15:43:48 GMT+08:00 | Delete    |

**Step 5** In the **Blacklist and Whitelist** configuration area, change **Status** as needed and click **Customize Rule**.

**Figure 3-41** Blacklist and Whitelist configuration area



**Step 6** In the upper left corner of the **Blacklist and Whitelist** page, click **Add Rule**.

**Step 7** In the displayed dialog box, add a blacklist or whitelist rule, as shown in **Figure 3-42**.

**NOTE**

- If you select **Log only** for **Protective Action** for an IP address, EdgeSec only identifies and logs requests from the IP address.
- Other IP addresses are evaluated based on other configured EdgeSec protection rules.

**Figure 3-42** Adding a blacklist or whitelist rule

×

### Add Blacklist or Whitelist Rule

\* Rule Name

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

\* IP Address/Range

\* Protective Action

Known Attack Source

Rule Description

Table 3-21 Rule parameters

| Parameter                  | Description  | Example Value                 |
|----------------------------|--|-------------------------------|
| Rule Name                  | Rule name you entered.   | EdgeSectest                   |
| IP Address/<br>Range/Group | You can select <b>IP address/Range</b> or <b>Address Group</b> to add IP addresses a blacklist or whitelist rule.  | IP Address/Range              |
| IP Address/<br>Range       | This parameter is mandatory if you select <b>IP address/range</b> for <b>IP Address/Range/Group</b> .<br>The value can be an IP address or an IP address range. <ul style="list-style-type: none"><li>• IP address: IP address to be added to the blacklist or whitelist</li><li>• IP address range: IP address and subnet mask defining a network segment</li></ul> | XXX.XXX.2.3                   |
| Select Address Group       | This parameter is mandatory if you select <b>Address group</b> for <b>IP Address/Range/Group</b> . Select an IP address group from the drop-down list. You can also click <b>Add Address Group</b> to create an address group. For details, see <a href="#">Adding a Blacklist or Whitelist IP Address Group</a> .   | -                             |
| Protective Action          | <ul style="list-style-type: none"><li>• <b>Block</b>: Select <b>Block</b> if you want to blacklist an IP address or IP address range.</li><li>• <b>Log only</b>: Select <b>Log only</b> if you want to observe an IP address or IP address range.</li></ul>  | Block                         |
| Known Attack Source        | If you select <b>Block</b> for <b>Protective Action</b> , you can select a blocking type of a known attack source rule. EdgeSec will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.   | Long-term IP address blocking |
| Rule Description           | A brief description of the rule. This parameter is optional.   | None                          |

**Step 8** Click **OK**. You can then view the added rule in the list of blacklist and whitelist rules.

- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

----End

### 3.5.3.7 Configuring a Known Attack Source Rule

If EdgeSec blocks a malicious request by IP address, Cookie, or Params, you can configure a known attack source rule to let EdgeSec automatically block all requests from the attack source for a blocking duration set in the known attack source rule. For example, if a blocked malicious request originates from an IP address 192.168.1.1 and you set the blocking duration to 500 seconds, EdgeSec will block the IP address for 500 seconds after the known attack source rule takes effect.

#### Prerequisites

A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

#### Constraints


- For a known attack source rule to take effect, it must be enabled when you configure basic web protection, precise protection, blacklist, or whitelist protection rules.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- Before adding a known attack source rule for malicious requests blocked by Cookie or Params, a traffic identifier must be configured for the corresponding domain name. For details, see [Configuring a Traffic Identifier for a Known Attack Source](#).

#### Specification Limitations

- You can configure up to six blocking types. Each type can have one known attack source rule configured.
- The maximum time an IP address can be blocked for is 30 minutes.

#### Procedure

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

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



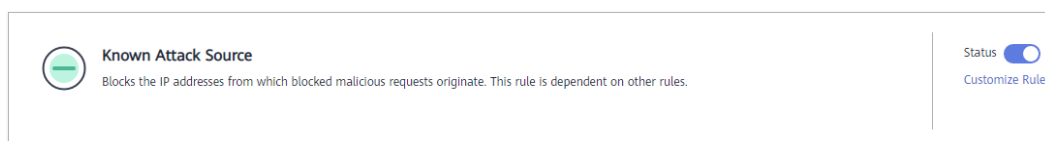
**Step 4** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

**Figure 3-43** Website list

| Domain Name     | Last 3 Days          | Mode    | Scheduling Status | Policy          | Created                         | Operation |
|-----------------|----------------------|---------|-------------------|-----------------|---------------------------------|-----------|
| www.esatest.com | No attacks detected. | Enabled | Scheduled to WAF  | policy_TnCIT4is | Jul 04, 2024 15:43:48 GMT+08:00 | Delete    |

**Step 5** In the **Known Attack Source** configuration area, change **Status** if needed and click **Customize Rule** to go to the **Known Attack Source** page.

**Figure 3-44** Known Attack Source configuration



**Step 6** In the upper left corner of the known attack source rules, click **Add Known Attack Source Rule**.

**Step 7** In the displayed dialog box, specify the parameters by referring to [Table 3-22](#).

**Figure 3-45** Add Known Attack Source Rule

×

### Add Known Attack Source Rule

**i** When **Cookie** or **Params** is selected, you need to set the traffic identifier on the domain name details page to complete the configuration of the known attack source rule.

Blocking Type ▼  
Long-term IP address blocking

★ Blocking Duration (s) ▭

Rule Description ▭

Note: The maximum short-term blocking duration and long-term blocking duration are 300 seconds and 1800 seconds, respectively. When the blocking duration is 0, the known attack source rule does not take effect.

Confirm
Cancel

**Table 3-22** Known attack source parameters

| Parameter             | Description  | Example Value                        |
|-----------------------|--|--------------------------------------|
| Blocking Type         | Specifies the blocking type. The options are: <ul style="list-style-type: none"><li>• <b>Long-term IP address blocking</b></li><li>• <b>Short-term IP address blocking</b></li><li>• <b>Long-term Cookie blocking</b></li><li>• <b>Short-term Cookie blocking</b></li><li>• <b>Long-term Params blocking</b></li><li>• <b>Short-term Params blocking</b></li></ul> | <b>Long-term IP address blocking</b> |
| Blocking Duration (s) | The blocking duration must be an integer and range from: <ul style="list-style-type: none"><li>• (300, 1800] for long-term blocking</li><li>• (0, 300] for short-term blocking</li></ul>   | 500                                  |
| Rule Description      | A brief description of the rule. This parameter is optional.   | None                                 |

**Step 8** Click **Confirm**. You can then view the added known attack source rule in the list.

----End

## Other Operations

- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

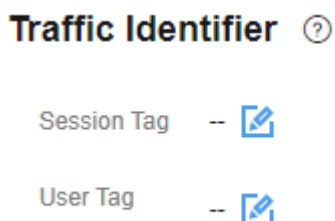
## Configuration Example - Blocking Known Attack Source Identified by Cookie

Assume that domain name *www.example.com* has been connected to EdgeSec and a visitor has sent one or more malicious requests through IP address *XXX.XXX.248.195*. You want to block access requests from this IP address and whose cookie is **jsessionid** for 10 minutes. Refer to the following steps to configure a rule and verify its effect.

**Step 1** On the **Website Settings** page, click *www.example.com* to go to its basic information page.

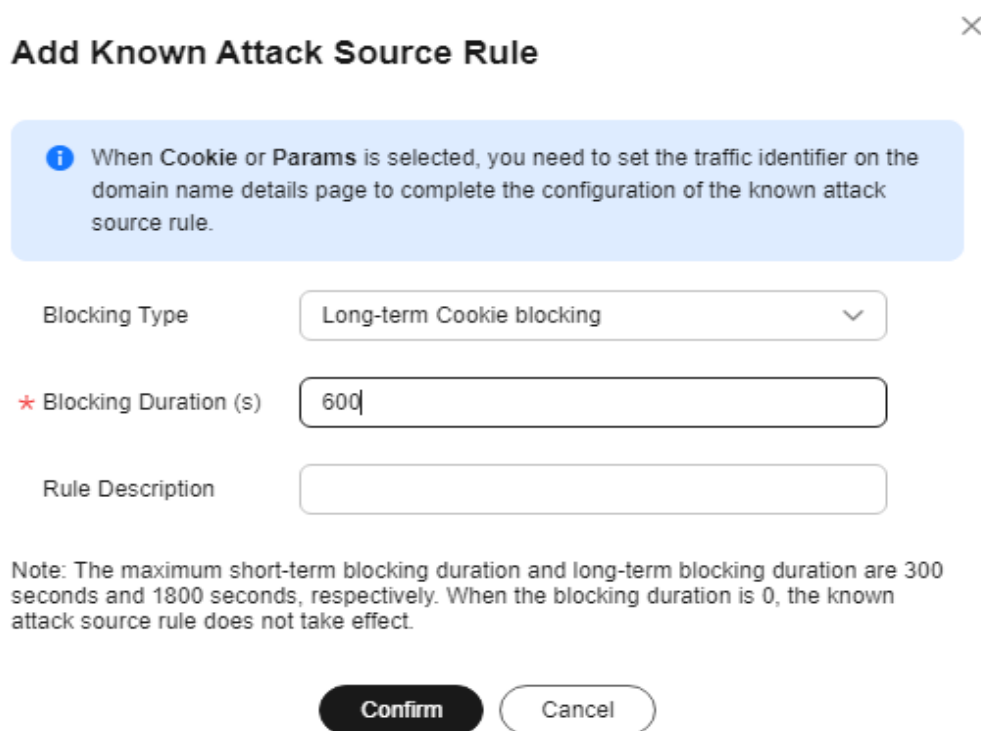
**Step 2** In the **Traffic Identifier** area, configure the cookie in the **Session Tag** field.

Figure 3-46 Traffic Identifier



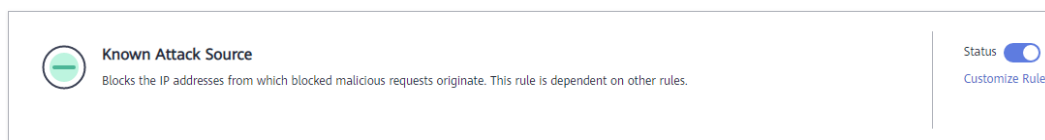
**Step 3** Add a known attack source, select **Long-term Cookie blocking** for **Blocking Type**, and set block duration to 600 seconds.

Figure 3-47 Adding a Cookie-based known attack source rule



**Step 4** Enable the known attack source protection.

Figure 3-48 Known Attack Source configuration



**Step 5** Add a blacklist and whitelist rule to block *XXX.XXX.248.195*. Select **Long-term Cookie blocking** for **Known Attack Source**.

**Figure 3-49** Specifying a known attack source rule

**Add Blacklist or Whitelist Rule** ×

\* Rule Name

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

\* IP Address/Range

\* Protective Action

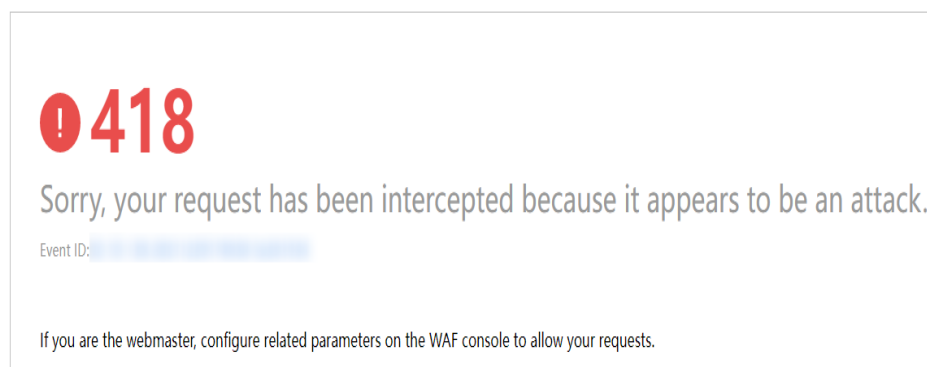
Known Attack Source

Rule Description

**Step 6** Clear the browser cache and access <http://www.example.com>.

When a request from IP address *XXX.XXX.248.195*, EdgeSec blocks the access. When EdgeSec detects that the cookie of the access request from the IP address is **jsessionid**, EdgeSec blocks the access request for 10 minutes.

**Figure 3-50** Block page



**Step 7** Go to the EdgeSec console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page.

----End

### 3.5.3.8 Configuring Geolocation Access Control Rules to Block Requests from Specific Locations

This section describes how to configure a geolocation access control rule. A geolocation access control rule allows you to control IP addresses forwarded from or to specified countries and regions.

#### Prerequisites

A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

#### Constraints


- One region can be configured in only one geolocation access control rule. For example, if you have blocked requests from Singapore with a geolocation access control rule, then Singapore cannot be added to other geolocation access control rules.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

#### Precautions

If you configure a regional access control rule in both EdgeSec and CDN, the rule in CDN is executed first.

#### Procedure



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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.

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

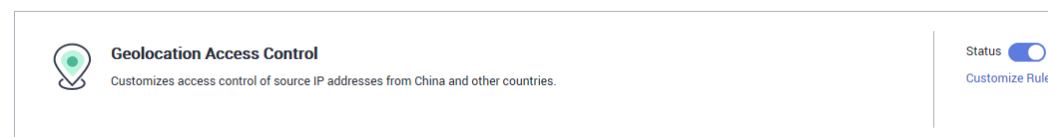
**Step 4** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

**Figure 3-51** Website list

| Domain Name     | Last 3 Days  | Mode    | Scheduling Status  | Policy          | Created                         | Operation |
|-----------------|--|---------|--|-----------------|---------------------------------|-----------|
| www.esatest.com |  No attacks detected. | Enabled |  Scheduled to WAF | policy_7nCiT4is | Jul 04, 2024 15:43:48 GMT+08:00 | Delete    |

**Step 5** In the **Geolocation Access Control** configuration area, change **Status** if needed and click **Customize Rule**.

**Figure 3-52** Geolocation Access Control configuration area



**Step 6** In the upper left corner of the **Geolocation Access Control** page, click **Add Rule**.

**Step 7** In the displayed dialog box, specify the parameters by referring to [Table 3-23](#).

**Figure 3-53** Adding a geolocation access control rule

**Table 3-23** Rule parameters

| Parameter         | Description   | Example Value |
|-------------------|---|---------------|
| Rule Name         | Rule name you configured  | -             |
| Rule Description  | A brief description of the rule. This parameter is optional.                                  | -             |
| Geolocation       | Geographical location from which an IP address is originated                                  | -             |
| Protective Action | Action EdgeSec will take if the rule is hit. You can select <b>Block</b> or <b>Log only</b> . | <b>Block</b>  |

**Step 8** Click **Confirm**. You can then view the added rule in the list of the geolocation access control rules.

- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

----End

## Protection Effect

To verify EdgeSec is protecting your website (**www.example.com**) against a rule:

**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 EdgeSec by following the instructions in [Adding a Website to EdgeSec](#).
- If the website is accessible, go to **2**.

**Step 2** Add a geolocation access control rule by referring to [Procedure](#).

**Step 3** Clear the browser cache and access **http://www.example.com**. Normally, EdgeSec blocks such requests and returns the block page.

----End

### 3.5.3.9 Configuring Anti-Crawler Rules

You can configure website anti-crawler protection rules to protect against search engines, scanners, script tools, and other crawlers, and use JavaScript to create custom anti-crawler protection rules.

## Prerequisites

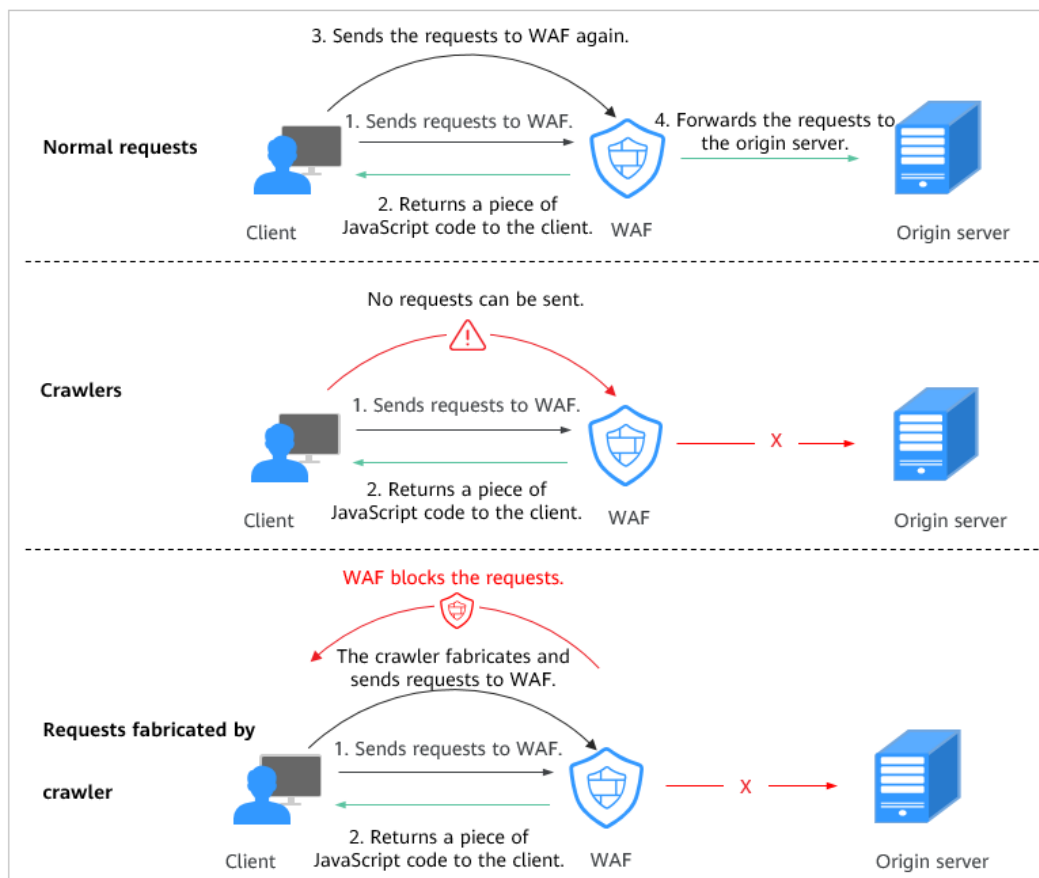
A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

## Constraints

- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- If your service is connected to CDN, exercise caution when using this function. CDN caching may impact Anti-Crawler performance and page accessibility.

## How JavaScript Anti-Crawler Protection Works

[Figure 3-54](#) shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

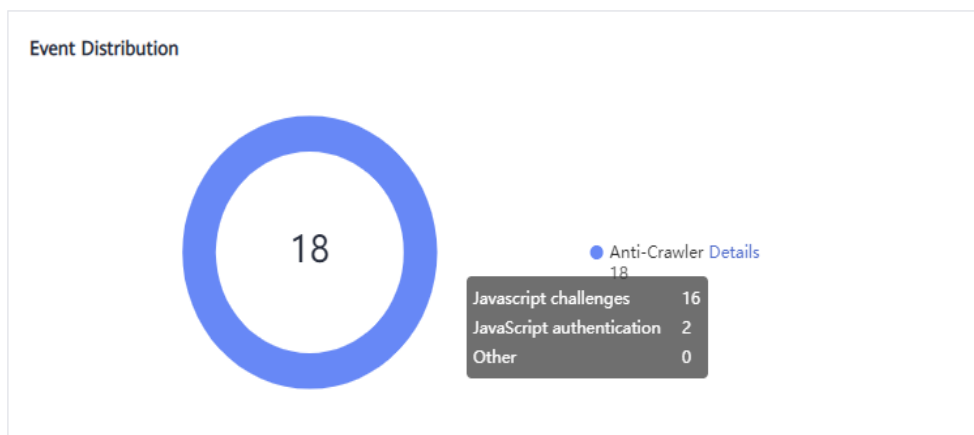
**Figure 3-54** JavaScript Anti-Crawler protection process

If JavaScript anti-crawler is enabled when a client sends a request, EdgeSec 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 EdgeSec again. EdgeSec 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 EdgeSec again. The client fails JavaScript authentication.
- If a client crawler fabricates an EdgeSec authentication request and sends the request to EdgeSec, the EdgeSec 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 3-55](#), the JavaScript anti-crawler has logged 18 events, 16 of which are JavaScript challenge responses, and 2 of which are JavaScript authentication responses. **Others** is the number of EdgeSec authentication requests fabricated by the crawler.




**Figure 3-55** Parameters of a JavaScript anti-crawler protection rule**NOTICE**

EdgeSec only logs JavaScript challenge and JavaScript authentication events. No other protective actions can be configured for JavaScript challenge and authentication.

**Procedure**

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

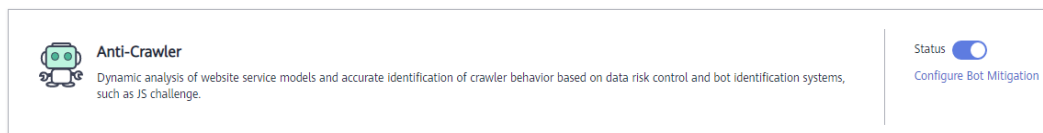
**Step 3** In the navigation pane on the left, choose **Website Setting** under **Edge Security**.

**Step 4** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

**Figure 3-56** Website list

| Domain Name     | Last 3 Days          | Mode    | Scheduling Status | Policy          | Created                         | Operation |
|-----------------|----------------------|---------|-------------------|-----------------|---------------------------------|-----------|
| www.esatest.com | No attacks detected. | Enabled | Scheduled to WAF  | policy_TnCiT4is | Jul 04, 2024 15:43:48 GMT+08:00 | Delete    |

**Step 5** In the **Anti-Crawler** configuration area, toggle on the anti-crawler function. If you enable this function, click **Configure Bot Mitigation**.

**Figure 3-57** Anti-Crawler configuration area

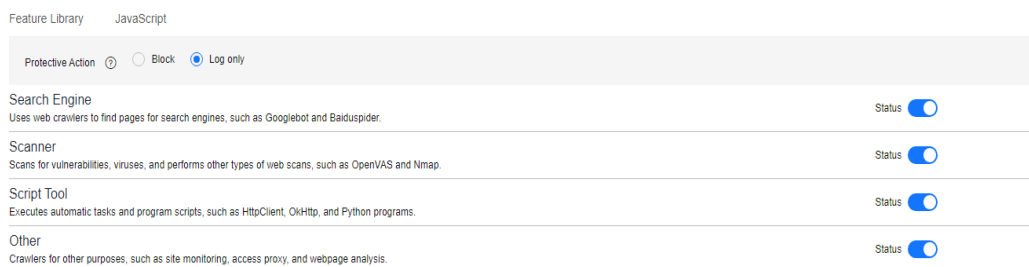
**Step 6** Select the **Feature Library** tab and enable the protection by referring to [Figure 3-58](#).

A feature-based anti-crawler rule has two protective actions:

- **Block**  
EdgeSec blocks and logs detected attacks.
- **Log only**  
Detected attacks are logged only. This is the default protective action.

**Scanner** is enabled by default, but you can enable other protection types if needed.

**Figure 3-58** Feature Library




**Table 3-24** Anti-crawler detection features

| Type          | Description   | Remarks   |
|---------------|---|---|
| Search Engine | This rule is used to block web crawlers, such as Googlebot and Baiduspider, from collecting content from your site.   | If you enable this rule, EdgeSec detects and blocks search engine crawlers.<br><b>NOTE</b><br>If <b>Search Engine</b> is not enabled, EdgeSec does not block POST requests from Googlebot or Baiduspider. If you want to block POST requests from Baiduspider, use the configuration described in <a href="#">Configuration Example - Search Engine</a> . |
| Scanner       | This rule is used to block scanners, such as OpenVAS and Nmap. A scanner scans for vulnerabilities, viruses, and other jobs.  | If you enable this rule, EdgeSec detects and blocks scanner crawlers.   |
| Script Tool   | This rule is used to block script tools. A script tool is often used to execute automatic tasks and program scripts, such as HttpClient, OkHttp, and Python programs. | If you enable this rule, EdgeSec detects and blocks the execution of automatic tasks and program scripts.<br><b>NOTE</b><br>If your application uses scripts such as HttpClient, OkHttp, and Python, disable <b>Script Tool</b> . Otherwise, EdgeSec will identify such script tools as crawlers and block the application.                               |

| Type  | Description  | Remarks  |
|-------|--|--|
| Other | <p>This rule is used to block crawlers used for other purposes, such as site monitoring, using access proxies, and web page analysis.</p> <p><b>NOTE</b><br/>To avoid being blocked by EdgeSec, crawlers may use a large number of IP address proxies.</p> | If you enable this rule, EdgeSec detects and blocks crawlers that are used for various purposes. |

**Step 7** Select the **JavaScript** tab and configure **Status** and **Protective Action**.

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

---

**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 8** Configure a JavaScript-based anti-crawler rule by referring to [Table 3-25](#).

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 **Confirm**.

**Figure 3-59 Exclude Path**

**Exclude Rule**

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

\* Rule Name

Rule Description

\* Effective Date  Immediate

\* Condition List

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

[Add Reference Table](#)

[Add](#) You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)

\* Priority  A smaller value indicates a higher priority.

**Confirm**

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

**Figure 3-60 Add Rule**

**Add Rule**

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

\* Rule Name

Rule Description

\* Effective Date  Immediate

\* Condition List

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

[Add Reference Table](#)

[Add](#) You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)

\* Priority  A smaller value indicates a higher priority.

**Confirm**

**Table 3-25** Parameters of a JavaScript-based anti-crawler protection rule

| Parameter | Description      | Example Value |
|-----------|------------------|---------------|
| Rule Name | Name of the rule | EdgeSec       |

| Parameter        | Description  | Example Value              |
|------------------|--|----------------------------|
| Rule Description | A brief description of the rule. This parameter is optional.   | -                          |
| Effective Date   | Time the rule takes effect.  | Immediate                  |
| Condition List   | <p>Parameters for configuring a condition are described 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><br/>If you select <b>Include any value, Exclude any value, Equal to any value, Not equal to any value, Prefix is any value, Prefix is not any of them, Suffix is any value, or Suffix is not any of them</b>, a reference table must be selected for <b>Content</b>. For details about reference tables, see <a href="#">Creating a Reference Table</a>.</p> <ul style="list-style-type: none"><li>● <b>Content:</b> Enter or select the content that matches the condition.</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

## Other Operations

- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

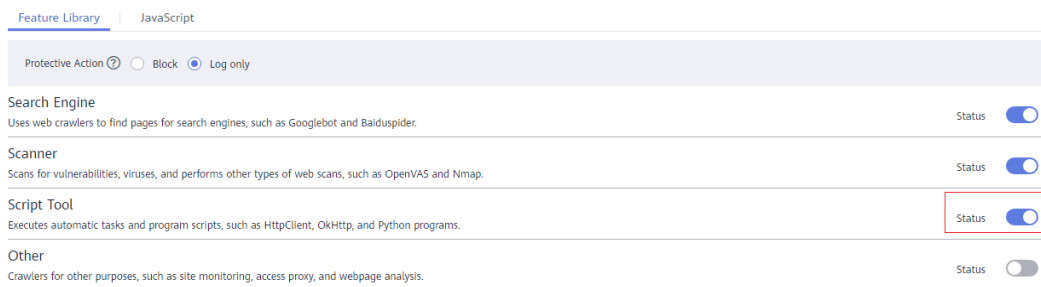
## Configuration Example - Logging Script Crawlers Only

To verify that EdgeSec is protecting domain name **www.example.com** against an anti-crawler rule:

**Step 1** Execute a JavaScript tool to crawl web page content.

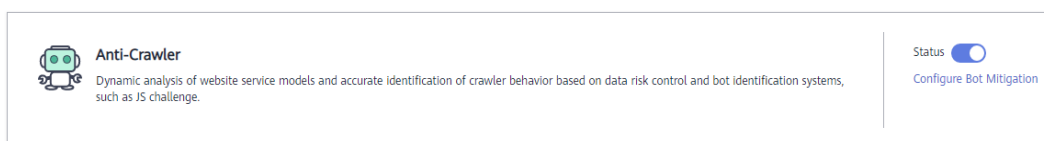
**Step 2** On the **Feature Library** tab, enable **Script Tool** and select **Log only** for **Protective Action**. (If EdgeSec detects an attack, it logs the attack only.)

**Figure 3-61** Enabling Script Tool



**Step 3** Enable anti-crawler protection.

**Figure 3-62** Anti-Crawler configuration area



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

**Figure 3-63** Viewing Events - Script crawlers

| Time                         | Source IP Address | Geolocation | Domain Name | URL                       | Malicious Load | Event Type        | Protective Action | Operation                  |
|------------------------------|-------------------|-------------|-------------|---------------------------|----------------|-------------------|-------------------|----------------------------|
| Dec 29, 2021 14:07:50 GMT... | [Redacted]        | Beijing     | [Redacted]  | /HNAP1                    | js_verified    | Scanner & Crawler | Block             | Details Handle False Alarm |
| Dec 29, 2021 14:07:50 GMT... | [Redacted]        | Beijing     | [Redacted]  | /nmaplowercheck1640758... | js_challenge   | Scanner & Crawler | Block             | Details Handle False Alarm |

----End

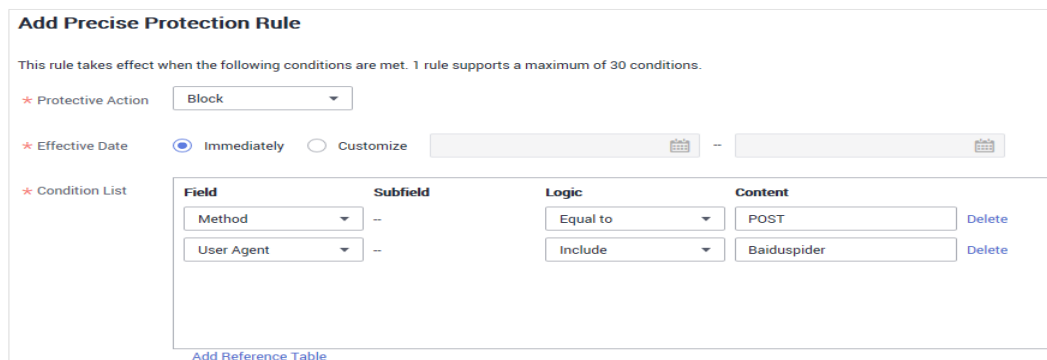
## Configuration Example - Search Engine

The following shows how to allow the search engine of Baidu or Google and block the POST request of Baidu.

**Step 1** Set **Status** of **Search Engine** to  by referring to the instructions in [Step 5](#).

**Step 2** Configure a precise protection rule by referring to [Configuring a Precise Protection Rule](#).

**Figure 3-64** Blocking POST requests



----End

### 3.5.3.10 Configuring a Global Whitelist Rule to Ignore False Positives

When EdgeSec detects a malicious attack that matches the basic web protection rule or custom rules you configure, it processes the attack event based on the protective action in the hit rule.

You can add false alarm masking rules to let EdgeSec ignore certain rule IDs or event types (for example, skip XSS checks for a specific URL).

- If you select **All protection** for **Ignore EdgeSec Protection**, all EdgeSec rules do not take effect, and EdgeSec allows all request traffic to the domain names in the rule.
- If you select **Basic Web Protection** for **Ignore EdgeSec Protection**, you can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule.

#### Prerequisites


A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

#### Constraints

- If you select **All protection** for **Ignore EdgeSec Protection**, all EdgeSec rules do not take effect, and EdgeSec allows all request traffic to the domain names in the rule.
- If you select **Basic web protection** for **Ignore Protection**, global protection whitelist rules take effect only for events triggered against EdgeSec built-in rules in **Basic Web Protection** and anti-crawler rules under **Feature Library**.
  - Basic web protection rules  
Basic web protection defends against common web attacks, such as SQL injection, XSS attacks, remote buffer overflow attacks, file inclusion, Bash vulnerability exploits, remote command execution, directory traversal, sensitive file access, and command and code injections. Basic web protection also detects web shells and evasion attacks.
  - Feature-based anti-crawler protection  
Feature-based anti-crawler identifies and blocks crawler behavior from search engines, scanners, script tools, and other crawlers.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- You can configure a global protection whitelist rule by referring to [Handling False Alarms](#). After handling a false alarm, you can view the rule in the global protection whitelist rule list.

#### Procedure

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.

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

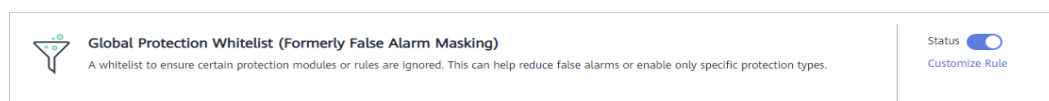
**Step 4** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

**Figure 3-65** Website list

| Domain Name     | Last 3 Days          | Mode    | Scheduling Status | Policy          | Created                         | Operation |
|-----------------|----------------------|---------|-------------------|-----------------|---------------------------------|-----------|
| www.esatest.com | No attacks detected. | Enabled | Scheduled to WAF  | policy_7nCiT4is | Jul 04, 2024 15:43:48 GMT+08:00 | Delete    |

**Step 5** In the **Global Protection Whitelist** configuration area, change **Status** if needed and click **Customize Rule**.

**Figure 3-66** Global Protection Whitelist configuration area



**Step 6** In the upper left corner of the **Global Protection Whitelist** page, click **Add Rule**.

**Step 7** Add a global whitelist rule by referring to [Table 3-26](#).

**Figure 3-67** Add Global Protection Whitelist Rule

**Add Global Protection Whitelist Rule** ×

\* Scope  All domain names  Specified domain names

\* Domain Name    
 + Add

\* Condition List

| Field | Subfield | Logic   | Content              |
|-------|----------|---------|----------------------|
| Path  | --       | Include | <input type="text"/> |

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

\* Ignore WAF Protection  All protection  Basic web protection

Rule Description

**Table 3-26** Parameters

| Parameter | Description   | Example Value          |
|-----------|---|------------------------|
| Scope     | <ul style="list-style-type: none"> <li><b>All domain names:</b> By default, this rule will be used to all domain names that are protected by the current policy.</li> <li><b>Specified domain names:</b> This rule will be used to the specified domain names that match the wildcard domain name being protected by the current policy.</li> </ul> | Specified domain names |



| Parameter                 | Description  | Example Value                              |
|---------------------------|--|--|
| Domain Name               | <p>This parameter is mandatory when you select <b>Specified domain names</b> for <b>Scope</b>.</p> <p>Enter a single domain name that matches the wildcard domain name being protected by the current policy.</p>  | www.example.com                            |
| Condition List            | <p>Click <b>Add</b> to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. A condition includes the following parameters:</p> <p>Parameters for configuring a condition are described as follows:</p> <ul style="list-style-type: none"><li>• <b>Field</b></li><li>• <b>Subfield:</b> Configure this field only when <b>Params, Cookie, or Header</b> is selected for <b>Field</b>.</li></ul> <p><b>NOTICE</b><br/>The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.</p> <ul style="list-style-type: none"><li>• <b>Logic:</b> Select a logical relationship from the drop-down list.</li><li>• <b>Content:</b> Enter or select the content that matches the condition.</li></ul> | Path, Include, / product                   |
| Ignore EdgeSec Protection | <ul style="list-style-type: none"><li>• <b>All protection:</b> All EdgeSec rules do not take effect, and EdgeSec allows all request traffic to the domain names in the rule.</li><li>• <b>Basic Web Protection:</b> You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule.</li></ul>   | Basic Web Protection                       |
| Rule Description          | A brief description of the rule. This parameter is optional.   | SQL injection attacks are not intercepted. |

**Step 8** Click **OK**.

----End

## Other Operations

- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

### 3.5.3.11 Configuring a Data Masking Rule

This section describes how to configure data masking rules. You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.

#### NOTE

CC attack protection does not support data masking rules.

## Prerequisites

A protected website has been added. For details, see [Adding a Website to EdgeSec](#).

## Constraints


It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

## Impact on the System

Sensitive data in the events will be masked to protect your website visitor's privacy.

## Procedure

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

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

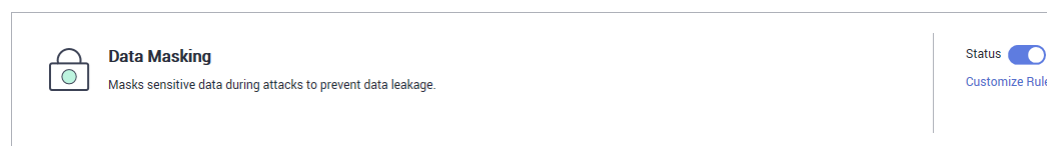
**Step 4** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

**Figure 3-68** Website list

| Domain Name     | Last 3 Days          | Mode    | Scheduling Status | Policy                      | Created                         | Operation |
|-----------------|----------------------|---------|-------------------|-----------------------------|---------------------------------|-----------|
| www.esatest.com | No attacks detected. | Enabled | Scheduled to WAF  | policy_7nCiT4is<br>9<br>... | Jul 04, 2024 15:43:48 GMT+08:00 | Delete    |

**Step 5** In the **Data Masking** configuration area, change **Status** if needed and click **Customize Rule**.

**Figure 3-69** Data Masking configuration area



**Step 6** In the upper left corner of the **Data Masking** page, click **Add Rule**.

**Step 7** In the displayed dialog box, specify the parameters by referring to [Table 3-27](#).

**Figure 3-70** Adding a data masking rule

**Table 3-27** Rule parameters

| Parameter | Description  | Example Value   |
|-----------|--|---|
| Path      | <p>Part of the URL that does not include the domain name.</p> <ul style="list-style-type: none"> <li>Prefix match: The path ending with * indicates that the path is used as a prefix. For example, if the path to be protected is <b>/admin/test.php</b> or <b>/adminabc</b>, set <b>Path</b> to <b>/admin*</b>.</li> <li>Exact match: The path to be entered must match the path to be protected. If the path to be protected is <b>/admin</b>, set <b>Path</b> to <b>/admin</b>.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>The path supports prefix and exact matches only and 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>, EdgeSec converts <b>///</b> to <b>/</b>.</li> </ul> | <p><b>/admin/login.php</b></p> <p>For example, if the URL to be protected is <b>http://www.example.com/admin/login.php</b>, set <b>Path</b> to <b>/admin/login.php</b>.</p> |

| Parameter        | Description   | Example Value  |
|------------------|---|--|
| Masked Field     | <p>A field set to be masked</p> <ul style="list-style-type: none"> <li>• <b>Params:</b> A request parameter</li> <li>• <b>Cookie:</b> A small piece of data to identify web visitors</li> <li>• <b>Header:</b> A user-defined HTTP header</li> <li>• <b>Form:</b> A form parameter</li> </ul> | <ul style="list-style-type: none"> <li>• If <b>Masked Field</b> is <b>Params</b> and <b>Field Name</b> is <b>id</b>, content that matches <b>id</b> is masked.</li> <li>• If <b>Masked Field</b> is <b>Cookie</b> and <b>Field Name</b> is <b>name</b>, content that matches <b>name</b> is masked.</li> </ul> |
| Field Name       | <p>Set the parameter based on <b>Masked Field</b>. The masked field will not be displayed in logs.</p> <p><b>NOTICE</b><br/>The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.</p>                                       |  |
| Rule Description | A brief description of the rule. This parameter is optional.  | None   |

**Step 8** Click **OK**. The added data masking rule is displayed in the list of data masking rules.

----End

## Other Operations

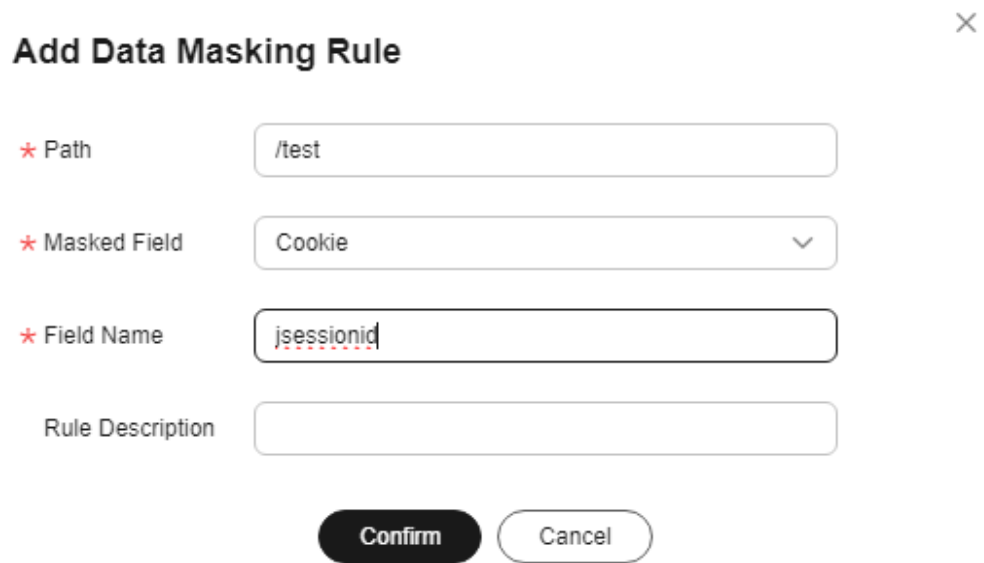
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

## Configuration Example - Masking the Cookie Field

To verify that EdgeSec is protecting your domain name *www.example.com* against a data masking rule (with **Cookie** selected for **Masked Field** and **jsessionid** entered in **Field Name**):

**Step 1** Add a data masking rule.

**Figure 3-71** Select **Cookie** for **Masked Field** and enter **jsessionid** in **Field Name**.



**Add Data Masking Rule** ×

\* Path

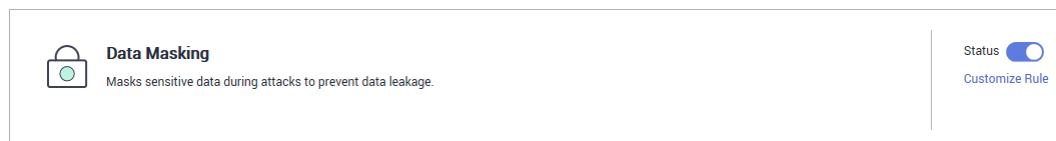
\* Masked Field

\* Field Name

Rule Description

**Step 2** Enable data masking.

**Figure 3-72** Data Masking configuration area



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

**Step 4** In the row containing the event hit the rule, click **Details** in the **Operation** column and view the event details.

Data in the **jsessionid** cookie field is masked.

**Figure 3-73** Viewing events - privacy data masking

The screenshot displays three sections of an event log entry:

- Event Details:** A table with the following data:

|                    |  |                       |               |
|--------------------|--|-----------------------|---------------|
| Time               | Dec 02, 2021 15:17:51 GMT+08:00                  | Event Type            | SQL Injection |
| Source IP Address  | [Redacted]                                       | Geolocation           | Guangdong     |
| Domain Name        | www.[Redacted].com                               | URL                   | /             |
| Malicious Payload  | body   | Protective Action     | Block         |
| Event ID           | 02-0000-0000-0000-147202112021517<br>51-54796454 | Status Code           | 418           |
| Response Time (ms) | 0  | Response Body (bytes) | 3,545         |
- Malicious Load:** A code block containing the payload: `<' or '1'='1'>testhere</xml>`
- Request Details:** A code block showing the following request information:

```
POST /
content-length: 29
postman-token: 487222b0-8003-4ae6-a6ce-4e28bc873403
host: www.[Redacted].com
content-type: text/xml
cache-control: no-cache
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Cookie: HWWAFSESID=f3ece7308c3e8feff3; HWWAFSESTIME=1637135543680; jsessionid=*** **
```

----End

## 3.6 Address Group Management

### 3.6.1 Adding a Blacklist or Whitelist IP Address Group

With IP address groups, you can quickly add IP addresses or IP address ranges to a blacklist or whitelist rule.

#### Constraints

- Do not add the same IP address or IP address range to different IP address groups, or the IP address groups will fail to be created.

## Specification Limitations


- A maximum of 50 address groups can be created. A maximum of 200 IP addresses or IP address ranges can be added to an address group.
- Before adding an address group to a blacklist or whitelist rule, ensure that the quota of IP address blacklist and whitelist rules has not been used up.

### NOTE

- To obtain the quota of IP address blacklist and whitelist rules, see [Configuring IP Address Blacklist and Whitelist Rules to Block Specified IP Addresses](#).
- If the quota of IP address whitelist and blacklist rules of your EdgeSec instance cannot meet your requirements, you can purchase rule expansion packages under the current EdgeSec instance edition or upgrade your EdgeSec instance edition to increase such quota. A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules.

## Procedure

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

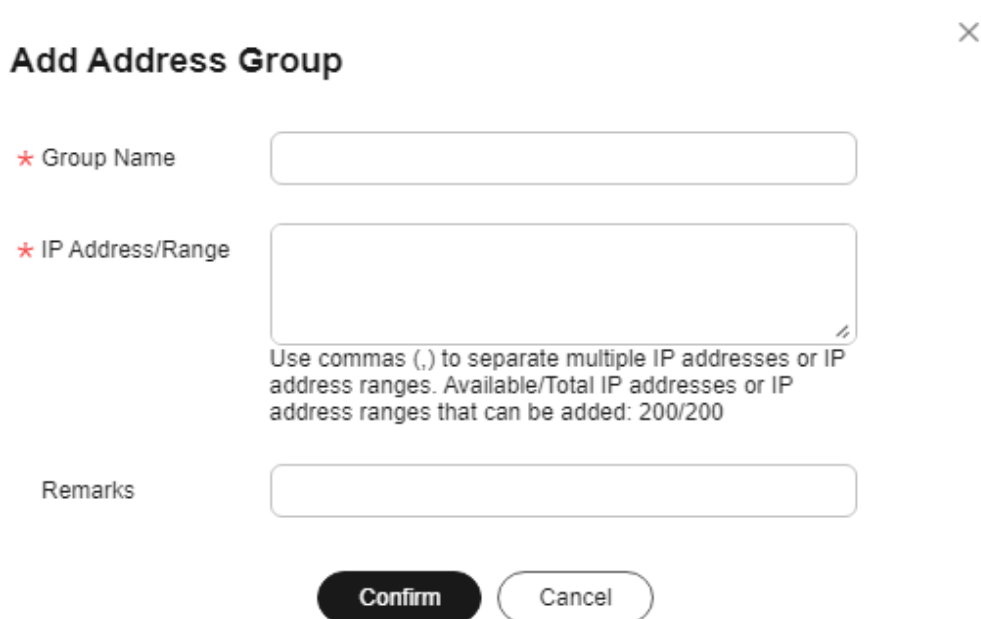
**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.

**Step 3** In the navigation pane on the left, choose **Edge Security > Address Groups**. The **Address Groups** page is displayed.

**Step 4** On the upper left of the address group list, click **Add Address Group**.

**Step 5** In the **Add Address Group** dialog box, enter an address group name and IP addresses or IP address ranges.

**Figure 3-74** Add Address Group



**Add Address Group** ×

\* Group Name

\* IP Address/Range

Use commas (,) to separate multiple IP addresses or IP address ranges. Available/Total IP addresses or IP address ranges that can be added: 200/200

Remarks

**Confirm**

 NOTE

- Use commas (,) to separate multiple IP addresses or IP address ranges. The value cannot contain line breaks.
- A maximum of 200 IP addresses or IP address ranges are allowed.

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

----End

## 3.6.2 Modifying or Deleting a Blacklist or Whitelist IP Address Group

This topic describes how to modify or delete an IP address group.

### Prerequisites


You have created an IP address group.

### Constraints

- An IP address or IP address range that has been added to an IP address group cannot be added to any other IP address group.
- Only address groups not used by any rules can be deleted. Before you delete an address group that is being used by a blacklist or whitelist rule, remove the address group from the rule first.

### Procedure

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

**Step 2** Click  in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

**Step 3** In the navigation pane on the left, choose **Edge Security** > **Address Groups**. The **Address Groups** page is displayed.

**Step 4** In the address group list, view the address group information.

**Table 3-28** Parameter description

| Parameter            | Description  |
|----------------------|--|
| Group Name           | Address group name you configured                            |
| IP Address/<br>Range | IP addresses or IP address ranges added to the address group |
| Rule                 | Rules that are using the address group                       |
| Remarks              | Supplementary information about the address group            |

**Step 5** Modify or delete an IP address group.




- **Modify an address group.**  
In the row containing the address group you want to modify, click **Modify** in the **Operation** column. In the **Modify Address Group** dialog box, change the group name or IP address/IP address range, and click **Confirm**.
- **Delete an address group.**  
In the row containing the address group you want to delete, click **Delete** in the **Operation** column. In the displayed dialog box, click **Confirm**.

----End

## 3.7 DDoS Attack Monitoring

After a service is connected, you can view the protection information to learn about the security status of the current service.

### Procedure

- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the page and choose **Security & Compliance > Edge Security**.
- Step 3** In the navigation pane on the left, choose **Edge Security > DDoS Attack Monitoring**. The **DDoS Attack Monitoring** page is displayed.
- Step 4** In the upper part of the page, view the anti-DDoS logs. For details about the parameters, see [Table 3-29](#).

**Table 3-29** DDoS attack protection parameters

| Parameter           | Description   |
|---------------------|---|
| Peak Attack Traffic | Maximum attack traffic bandwidth within a specified period. |

#### NOTE

In the traffic or packet chart on the **DDoS Attack Protection** page, the display granularity varies according to the query interval. The details are as follows:

- If the query interval is less than or equal to 3 days, the display granularity is 1 minute.
- If the query interval is greater than 3 days and less than or equal to 30 days, the display granularity is 1 hour.

----End

# 4 Permissions Management

## 4.1 Creating a User Group and Granting Permissions

This section describes how to use [IAM](#) to implement fine-grained permissions control for your EdgeSec resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to EdgeSec resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a Huawei account or a cloud service to perform efficient O&M on your EdgeSec resources.

If your Huawei account does not require individual IAM users, skip this section.

This section describes the procedure for granting permissions. [Figure 4-1](#) shows the procedure.

### Prerequisites

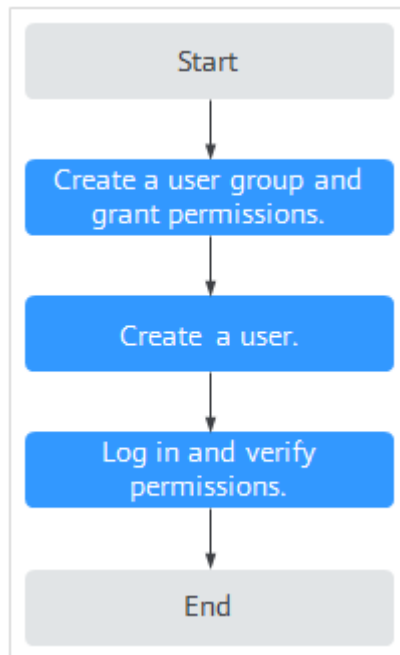
Before granting permissions to a user group, you need to learn about the permissions supported by EdgeSec in [Table 4-1](#) and choose policies or roles based on your requirements.

**Table 4-1** EdgeSec system roles

| System Role/<br>Policy Name | Description                        | Type             | Dependency |
|-----------------------------|------------------------------------|------------------|------------|
| EdgeSec<br>FullAccess       | All permissions of<br>EdgeSec      | System<br>policy | None       |
| EdgeSec<br>ReadOnlyAccess   | Read-only permission<br>of EdgeSec | System<br>policy |            |

## Permission Granting Process

Figure 4-1 Process for granting permissions



1. **Create a user group and assign permissions.**  
Create a user group on the IAM console and assign the **EdgeSec FullAccess** permissions to the group.
2. **Create a user and add it to a user group.**  
Create a user on the IAM console and add the user to the group created in **1**.
3. **Log in** and verify permissions.  
Log in to the EdgeSec console by using the created user, and verify that the user only has permissions of EdgeSec.  
Choose any other service from **Service List**. If a message appears indicating that you do not have permissions to access the service, the **EdgeSec FullAccess** policy has already taken effect.

# 5 Key Operations Recorded by CTS

## 5.1 EdgeSec Operations Recorded by CTS

CTS records operations on EdgeSec. With CTS, you can query, audit, and backtrack these operations. For details, see the *Cloud Trace Service User Guide*.

**Table 5-1** lists the EdgeSec operations recorded by CTS.

**Table 5-1** EdgeSec operations recorded by CTS

| Operation  | Resource Type         | Trace                     |
|--|-----------------------|---------------------------|
| Adding a CDN domain name scheduling task               | cdnDomainScheduleTask | addCdnDomainScheduleTask  |
| Adding a domain name to be protected                   | bsgDomainName         | addBsgDomainName          |
| Deleting a protected domain name                       | bsgDomainName         | deleteBsgDomainName       |
| Updating a protected domain name                       | bsgDomainName         | updateBsgDomainName       |
| Subscribing to the service                             | serviceInfo           | addServiceInfo            |
| Unsubscribing from the service                         | serviceInfo           | deleteServiceInfo         |
| Adding a domain name to be protected from DDoS attacks | ddosDomainNames       | addEdgeDDosDomainNames    |
| Deleting a domain name protected from DDoS attacks     | ddosDomainNames       | deleteEdgeDDosDomainNames |

| Operation  | Resource Type          | Trace                        |
|--|------------------------|------------------------------|
| Updating a domain name protected from DDoS attacks | ddosDomainNames        | updateEdgeDDosDomainNames    |
| Creating a script anti-crawler rule                | EdgeSecAntiCrawlerRule | createEdgeSecAntiCrawlerRule |
| Deleting a script anti-crawler rule                | EdgeSecAntiCrawlerRule | deleteEdgeSecAntiCrawlerRule |
| Changing the script anti-crawler mode              | EdgeSecAntiCrawlerRule | switchEdgeSecAntiCrawlerRule |
| Updating a script anti-crawler rule                | EdgeSecAntiCrawlerRule | updateEdgeSecAntiCrawlerRule |
| Creating a CC attack protection rule               | EdgeSecCcRule          | createEdgeSecCcRule          |
| Deleting a CC attack protection rule               | EdgeSecCcRule          | deleteEdgeSecCcRule          |
| Updating a CC attack protection rule               | EdgeSecCcRule          | updateEdgeSecCcRule          |
| Creating a certificate                             | EdgeSecCertificate     | createEdgeSecCertificate     |
| Deleting a certificate                             | EdgeSecCertificate     | deleteEdgeSecCertificate     |
| Updating a certificate                             | EdgeSecCertificate     | updateEdgeSecCertificate     |
| Creating a precise protection rule                 | EdgeSecCustomRule      | createEdgeSecCustomRule      |
| Deleting a precise protection rule                 | EdgeSecCustomRule      | deleteEdgeSecCustomRule      |
| Updating a precise protection rule                 | EdgeSecCustomRule      | updateEdgeSecCustomRule      |
| Creating a domain name to be protected             | EdgeSecDomain          | createEdgeSecDomain          |
| Deleting a protected domain name                   | EdgeSecDomain          | deleteEdgeSecDomain          |
| Updating a protected domain name                   | EdgeSecDomain          | updateEdgeSecDomain          |
| Creating a geolocation access control rule         | EdgeSecGeolpRule       | createEdgeSecGeolpRule       |
| Deleting a geolocation access control rule         | EdgeSecGeolpRule       | deleteEdgeSecGeolpRule       |

| Operation  | Resource Type          | Trace                        |
|--|------------------------|------------------------------|
| Updating a geolocation access control rule                     | EdgeSecGeolpRule       | updateEdgeSecGeolpRule       |
| Creating a false alarm masking rule                            | EdgeSecIgnoreRule      | createEdgeSecIgnoreRule      |
| Deleting a false alarm masking rule                            | EdgeSecIgnoreRule      | deleteEdgeSecIgnoreRule      |
| Resetting a false alarm masking rule                           | EdgeSecIgnoreRule      | recountEdgeSecIgnoreRule     |
| Updating a false alarm masking rule                            | EdgeSecIgnoreRule      | updateEdgeSecIgnoreRule      |
| Creating an IP address group                                   | EdgeSecIpGroup         | CreateEdgeSecIpGroup         |
| Deleting an IP address group                                   | EdgeSecIpGroup         | DeleteEdgeSecIpGroup         |
| Updating an IP address group                                   | EdgeSecIpGroup         | UpdateEdgeSecIpGroup         |
| Updating the domain names to which a protection policy applies | EdgeSecPolicy          | applyEdgeSecPolicy           |
| Creating a protection policy                                   | EdgeSecPolicy          | createEdgeSecPolicy          |
| Deleting a protection policy                                   | EdgeSecPolicy          | deleteEdgeSecPolicy          |
| Updating a protection policy                                   | EdgeSecPolicy          | updateEdgeSecPolicy          |
| Creating a privacy masking rule                                | EdgeSecPrivacyMaskRule | createEdgeSecPrivacyMaskRule |
| Deleting a privacy masking rule                                | EdgeSecPrivacyMaskRule | deleteEdgeSecPrivacyMaskRule |
| Updating a privacy masking rule                                | EdgeSecPrivacyMaskRule | updateEdgeSecPrivacyMaskRule |
| Creating a known attack source rule                            | EdgeSecPunishmentRule  | createEdgeSecPunishmentRule  |
| Deleting a known attack source rule                            | EdgeSecPunishmentRule  | deleteEdgeSecPunishmentRule  |
| Updating a known attack source rule                            | EdgeSecPunishmentRule  | updateEdgeSecPunishmentRule  |

| Operation  | Resource Type           | Trace                          |
|--|-------------------------|--------------------------------|
| Creating a reference table                         | EdgeSecValueList        | createEdgeSecValueList         |
| Deleting a reference table                         | EdgeSecValueList        | deleteEdgeSecValueList         |
| Updating a reference table                         | EdgeSecValueList        | updateEdgeSecValueList         |
| Adding an IP address blacklist or whitelist rule   | EdgeSecWhiteBlackIpRule | createEdgeSecWhite-BlackIpRule |
| Deleting an IP address blacklist or whitelist rule | EdgeSecWhiteBlackIpRule | deleteEdgeSecWhite-BlackIpRule |
| Updating an IP address blacklist or whitelist rule | EdgeSecWhiteBlackIpRule | updateEdgeSecWhite-BlackIpRule |

## 5.2 Querying Traces

After you enable CTS, the system starts recording operations on EdgeSec. You can view the operation records of the last 7 days on the CTS console.

For details about how to view audit logs, see [Querying Real-Time Traces \(for New Console\)](#).

# 6 Monitoring

---

## 6.1 EdgeSec Monitored Metrics

### Description

This section describes metrics reported by EdgeSec to Cloud Eye as well as their namespaces and dimensions. You can query the metrics and alarms generated for EdgeSec on the Cloud Eye console or using the APIs provided by Cloud Eye.

### Namespaces

SYS.EdgeSec

#### NOTE

A namespace is an abstract collection of resources and objects. Multiple namespaces can be created in a single cluster with the data isolated from each other. This enables namespaces to share the same cluster services without affecting each other.



## Metrics

**Table 6-1** EdgeSec metrics

| ID               | Name                      | Description   | Value Range              | Monitored Object      | Monitoring Period (Original Metric) |
|------------------|---------------------------|---|--------------------------|-----------------------|-------------------------------------|
| requests         | Number of Requests        | Number of requests returned by EdgeSec in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of requests for accessing the protected domain name. | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |
| EdgeSec_http_2xx | EdgeSec Status Code (2XX) | Number of 2XX status codes returned by EdgeSec in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of 2XX status codes returned.                | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |
| EdgeSec_http_3xx | EdgeSec Status Code (3XX) | Number of 3XX status codes returned by EdgeSec in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of 3XX status codes returned.                | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |

| ID                      | Name                      | Description  | Value Range              | Monitored Object      | Monitoring Period (Original Metric) |
|-------------------------|---------------------------|--|--------------------------|-----------------------|-------------------------------------|
| EdgeSec_http_4xx        | EdgeSec Status Code (4XX) | Number of 4XX status codes returned by EdgeSec in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of 4XX status codes returned.   | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |
| EdgeSec_http_5xx        | EdgeSec Status Code (5XX) | Number of 5XX status codes returned by EdgeSec in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of 5XX status codes returned.   | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |
| EdgeSec_failed_requests | EdgeSec Traffic Threshold | Number of requests destined for the protected domain name in the last 5 minutes during breakdown protection duration<br>Unit: count<br>Collection method: Number of requests to the protected domain name while the website was down | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |

| ID                     | Name                       | Description   | Value Range                     | Monitored Object      | Monitoring Period (Original Metric) |
|------------------------|----------------------------|---|---------------------------------|-----------------------|-------------------------------------|
| inbound_traffic        | Total Inbound Traffic      | Total inbound traffic in the last 5 minutes<br>Unit: Mbit/s<br>Collection method: Collect the total inbound traffic in the last 5 minutes.  | ≥ 0 Mbit/s<br>Value type: Float | Protected domain name | 5 minutes                           |
| outbound_traffic       | Total Outbound Traffic     | Total outbound traffic in the last 5 minutes<br>Unit: Mbit/s<br>Collection method: Collect the total outbound traffic in the last 5 minutes.  | ≥ 0 Mbit/s<br>Value type: Float | Protected domain name | 5 minutes                           |
| EdgeSec_process_time_0 | EdgeSec Latency [0, 10) ms | Number of requests processed by EdgeSec at a latency from 0 ms (included) to 10 ms (excluded) in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of requests processed by EdgeSec at a latency from 0 ms (included) to 10 ms (excluded) in the last 5 minutes. | ≥ 0<br>Value type: Float        | Protected domain name | 5 minutes                           |

| ID                      | Name                        | Description  | Value Range                         | Monitored Object      | Monitoring Period (Original Metric) |
|-------------------------|-----------------------------|--|-------------------------------------|-----------------------|-------------------------------------|
| EdgeSec_process_time_10 | EdgeSec Latency [10, 20) ms | <p>Number of requests processed by EdgeSec at a latency from 10 ms (included) to 20 ms (excluded) in the last 5 minutes</p> <p>Unit: count</p> <p>Collection method: Collect the number of requests processed by EdgeSec at a latency from 10 ms (included) to 20 ms (excluded) in the last 5 minutes.</p> | <p>≥ 0</p> <p>Value type: Float</p> | Protected domain name | 5 minutes                           |
| EdgeSec_process_time_20 | EdgeSec Latency [20, 50) ms | <p>Number of requests processed by EdgeSec at a latency from 20 ms (included) to 50 ms (excluded) in the last 5 minutes</p> <p>Unit: count</p> <p>Collection method: Collect the number of requests processed by EdgeSec at a latency from 20 ms (included) to 50 ms (excluded) in the last 5 minutes.</p> | <p>≥ 0</p> <p>Value type: Float</p> | Protected domain name | 5 minutes                           |

| ID                       | Name                            | Description   | Value Range                   | Monitored Object      | Monitoring Period (Original Metric) |
|--------------------------|---------------------------------|---|-------------------------------|-----------------------|-------------------------------------|
| EdgeSec_process_time_50  | EdgeSec Latency [50, 100) ms    | Number of requests processed by EdgeSec at a latency from 50 ms (included) to 100 ms (excluded) in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of requests processed by EdgeSec at a latency from 50 ms (included) to 100 ms (excluded) in the last 5 minutes.       | $\geq 0$<br>Value type: Float | Protected domain name | 5 minutes                           |
| EdgeSec_process_time_100 | EdgeSec Latency [100, 1,000) ms | Number of requests processed by EdgeSec at a latency from 100 ms (included) to 1,000 ms (excluded) in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of requests processed by EdgeSec at a latency from 100 ms (included) to 1,000 ms (excluded) in the last 5 minutes. | $\geq 0$<br>Value type: Float | Protected domain name | 5 minutes                           |

| ID                        | Name                              | Description   | Value Range              | Monitored Object      | Monitoring Period (Original Metric) |
|---------------------------|-----------------------------------|---|--------------------------|-----------------------|-------------------------------------|
| EdgeSec_process_time_1000 | EdgeSec Latency [1,000, above) ms | Number of requests processed by EdgeSec at a latency greater than or equal to 1,000 ms in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of requests processed by EdgeSec at a latency greater than or equal to 1,000 ms in the last 5 minutes. | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |
| qps_peak                  | Peak QPS                          | Peak QPS of the protected domain name in the last 5 minutes<br>Unit: count<br>Collection method: Collect the peak QPS of the protected domain name in the last 5 minutes.   | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |
| qps_mean                  | Average QPS                       | Average QPS of the protected domain name in the last 5 minutes<br>Unit: count<br>Collection method: Collect the average QPS of the protected domain name in the last 5 minutes.   | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |

| ID                | Name  | Description   | Value Range              | Monitored Object      | Monitoring Period (Original Metric) |
|-------------------|---|---|--------------------------|-----------------------|-------------------------------------|
| EdgeSec_http_0    | No EdgeSec Status Code                          | Number of requests with no status code returned by EdgeSec in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of requests with no status code returned by EdgeSec in the last 5 minutes.                           | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |
| upstream_code_2xx | Status Code Returned by the Origin Server (2XX) | Number of requests with a 2XX status code returned by the origin server in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of requests with a 2XX status code returned by the origin server in the last 5 minutes. | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |

| ID                | Name  | Description   | Value Range              | Monitored Object      | Monitoring Period (Original Metric) |
|-------------------|---|---|--------------------------|-----------------------|-------------------------------------|
| upstream_code_3xx | Status Code Returned by the Origin Server (3XX) | Number of requests with a 3XX status code returned by the origin server in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of requests with a 3XX status code returned by the origin server in the last 5 minutes. | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |
| upstream_code_4xx | Status Code Returned by the Origin Server (4XX) | Number of requests with a 4XX status code returned by the origin server in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of requests with a 4XX status code returned by the origin server in the last 5 minutes. | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |



| ID                   | Name  | Description   | Value Range                          | Monitored Object      | Monitoring Period (Original Metric) |
|----------------------|---|---|--------------------------------------|-----------------------|-------------------------------------|
| upstream_code_5xx    | Status Code Returned by the Origin Server (5XX) | Number of requests with a 5XX status code returned by the origin server in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of requests with a 5XX status code returned by the origin server in the last 5 minutes. | $\geq 0$<br>Value type: Float        | Protected domain name | 5 minutes                           |
| upstream_code_0      | No Origin Server Status Code                    | Number of requests with no status code returned in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of requests with no status code returned in the last 5 minutes.   | $\geq 0$<br>Value type: Float        | Protected domain name | 5 minutes                           |
| inbound_traffic_peak | Peak Inbound Traffic                            | Peak inbound traffic to the domain name in the last 5 minutes<br>Unit: Mbit/s<br>Collection method: Collect the peak inbound traffic to the domain name in the last 5 minutes.  | $\geq 0$ Mbit/s<br>Value type: Float | Protected domain name | 5 minutes                           |

| ID                    | Name                     | Description  | Value Range                     | Monitored Object      | Monitoring Period (Original Metric) |
|-----------------------|--------------------------|--|---------------------------------|-----------------------|-------------------------------------|
| inbound_traffic_mean  | Average Inbound Traffic  | Average inbound traffic to the domain name in the last 5 minutes<br>Unit: Mbit/s<br>Collection method: Collect the average inbound traffic to the domain name in the last 5 minutes.   | ≥ 0 Mbit/s<br>Value type: Float | Protected domain name | 5 minutes                           |
| outbound_traffic_peak | Peak Outbound Traffic    | Peak outbound traffic to the domain name in the last 5 minutes<br>Unit: Mbit/s<br>Collection method: Collect the peak outbound traffic to the domain name in the last 5 minutes.       | ≥ 0 Mbit/s<br>Value type: Float | Protected domain name | 5 minutes                           |
| outbound_traffic_mean | Average Outbound Traffic | Average outbound traffic to the domain name in the last 5 minutes<br>Unit: Mbit/s<br>Collection method: Collect the average outbound traffic to the domain name in the last 5 minutes. | ≥ 0 Mbit/s<br>Value type: Float | Protected domain name | 5 minutes                           |

| ID                     | Name  | Description   | Value Range              | Monitored Object      | Monitoring Period (Original Metric) |
|------------------------|---|---|--------------------------|-----------------------|-------------------------------------|
| attacks                | Number of Attacks                                 | Number of attacks against the domain name in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of attacks against the domain name in the last 5 minutes.                                 | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |
| crawlers               | Number of Crawler Attacks                         | Number of crawler attacks against the domain name in the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of crawler attacks against the domain name in the last 5 minutes.                 | ≥ 0<br>Value type: Float | Domain Name           | 5                                   |
| base_protection_counts | Number of Attacks Blocked by Basic Web Protection | Number of attacks blocked by basic web protection rules over the last 5 minutes<br>Unit: count<br>Collection method: Collect the number of attacks blocked by basic web protection rules over the last 5 minutes. | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |

| ID                        | Name  | Description   | Value Range              | Monitored Object      | Monitoring Period (Original Metric) |
|---------------------------|---|---|--------------------------|-----------------------|-------------------------------------|
| precise_protection_counts | Number of Attacks Blocked by Precise Protection | Number of attacks blocked by precise protection rules over the last 5 minutes<br><br>Unit: count<br><br>Collection method: Collect the number of attacks blocked by precise protection rules over the last 5 minutes. | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |
| cc_protection_counts      | Number of Attacks Blocked by CC Protection      | Number of attacks blocked by CC protection rules over the last 5 minutes<br><br>Unit: count<br><br>Collection method: Collect the number of attacks blocked by CC protection rules over the last 5 minutes.           | ≥ 0<br>Value type: Float | Protected domain name | 5 minutes                           |

## Dimensions

| Key                 | Value                                    |
|---------------------|--|
| instance_id         | ID of the dedicated EdgeSec instance     |
| EdgeSec_instance_id | ID of the website protected with EdgeSec |

## Example of Raw Data Format of Monitored Metrics

```
[
  {
    "metric": {
      // Namespace
      "namespace": "SYS.EdgeSec",
      "dimensions": [
        {
```

```
    // Dimension name, for example, protected website
    "name": "EdgeSec_instance_id",
    // ID of the monitored object in this dimension, for example, ID of the protected website
    "value": "082db2f542e0438aa520035b3e99cd99"
  }
},
// Metric ID
"metric_name": "EdgeSec_http_2xx"
},
// Time to live, which is predefined for the metric
"ttl": 172800,
// Metric value
"value": 0.0,
// Metric unit
"unit": "Count",
// Metric value type
"type": "float",
// Collection time for the metric
"collect_time": 1637677359778
}
]
```


## 6.2 Configuring a Monitoring Alarm Rule

You can set EdgeSec alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring period, and whether to send notifications. This helps you learn the EdgeSec protection status in a timely manner.


### Prerequisites

The domain name to be protected has been connected to EdgeSec.

### Procedure

- Step 1** Click  in the upper left corner of the page and choose **Management & Governance > Cloud Eye**.
- Step 2** In the navigation pane on the left, choose **Alarm Management > Alarm Rules**.
- Step 3** In the upper right corner of the page, click **Create Alarm Rule**.
- Step 4** Set the parameters as prompted. The key parameters are as follows. For details about more parameters, see [Creating an Alarm Rule](#).
  - **Alarm Type:** Events
  - **Event Type:** system event and customized event

**Figure 6-1** EdgeSec monitoring alarm rule

|                 |  |
|-----------------|--|
| ★ Alarm Type    | <input checked="" type="radio"/> Metric <input type="radio"/> Event  |
| ★ Resource Type | <input type="text" value="EdgeSec"/>  |
| ★ Dimension     | <input type="text" value="EdgeSec-DDoS"/>  |

**Step 5** Click **Create**. In the displayed dialog box, click **OK**.

----End


## 6.3 Viewing Monitored Metrics

You can view EdgeSec metrics on the management console to learn about the EdgeSec protection status in a timely manner and set protection policies based on the metrics.

### Prerequisites

A monitoring alarm rule has been configured for EdgeSec in Cloud Eye. For details, see [Configuring a Monitoring Alarm Rule](#).

### Procedure

**Step 1** Click  in the upper left corner of the page and choose **Management & Governance > Cloud Eye**.

**Step 2** In the navigation pane on the left, choose **Cloud Service Monitoring > EdgeSec**.

**Step 3** In the row containing the target EdgeSec instance, click **View Metric** in the **Operation** column.

----End

# 7 Change History

| Date       | Description   |
|------------|---|
| 2024-07-16 | <p>This issue is the seventh official release.</p> <p>Added:</p> <ul style="list-style-type: none"><li>• <a href="#">Managing DDoS Protection Events</a>.</li><li>• <a href="#">Statistical Analysis</a>.</li></ul> <p>Optimized:</p> <ul style="list-style-type: none"><li>• Added <b>Geographical Location</b> to the rate limiting conditions in section <a href="#">Configuring CC Attack Protection Rules to Defend Against CC Attacks</a>.</li><li>• Optimized the page for viewing basic information in section <a href="#">Website Settings</a>.</li><li>• Removed the <b>Allow</b> option for protection actions in sections <a href="#">Configuring a Precise Protection Rule</a>, <a href="#">Configuring IP Address Blacklist and Whitelist Rules to Block Specified IP Addresses</a>, and <a href="#">Configuring Geolocation Access Control Rules to Block Requests from Specific Locations</a>.</li><li>• Changed the Edge Security portal.</li><li>• Optimized the pages for configuring different policies in section <a href="#">Configuring Protection Policies</a>.</li></ul> |
| 2024-05-24 | <p>This is the sixth official release.</p> <p>Optimized:</p> <p>Adjusted the document architecture and added sections <b>Site Acceleration</b> and <b>Security Protection</b>.</p>  |

| Date       | Description   |
|------------|---|
| 2024-01-25 | <p>This issue is the fifth official release.</p> <p>Added:</p> <p>Configuration example of allowing access requests from the source IP addresses in a specified region in section <a href="#">Configuring a Precise Protection Rule</a>.</p> <p>Optimized:</p> <ul style="list-style-type: none"><li>Parameters and descriptions in section <a href="#">DDoS Attack Monitoring</a>.</li><li>Configuration procedure and parameters in section <a href="#">Configuring a Monitoring Alarm Rule</a>.</li></ul> <p>Deleted:</p> <p>Region parameter in <a href="#">Enabling EdgeSec</a>.</p> |
| 2023-12-05 | <p>This issue is the fourth official release.</p> <p>Deleted:</p> <ul style="list-style-type: none"><li>Anti-DDoS overview page section.</li><li>The DDoS log fields in section "Managing Full Logs".</li></ul>   |
| 2023-10-31 | <p>This issue is the third official release.</p> <p>Optimized:</p> <p><a href="#">Enabling EdgeSec</a>.</p>   |
| 2023-08-08 | <p>This issue is the second official release.</p> <p>Added:</p> <ul style="list-style-type: none"><li>The description about enterprise projects in "EdgeSec Management" and "Edge Anti-DDoS Management".</li><li>Managing Logs</li><li>Managing Projects and Enterprise Projects</li></ul>  |
| 2023-03-30 | <p>This issue is the first official release.</p>  |