Edge Security

User Guide

Issue 05

Date 2024-01-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Purchasing EdgeSec.. 1

2 Managing Edge WAF.. 5

2.1 Dashboard.. 5

2.2 Managing Events... 8

2.2.1 Viewing Events.. 8

2.2.2 Handling False Alarms... 10

2.3 Protection Policy... 17

2.3.1 Creating a Protection Policy... 17

2.3.2 Applying a Policy to Your Website... 19

2.4 Configuring Protection Rules... 20

2.4.1 Configuration Guidance... 20

2.4.2 Configuring Basic Web Protection Rules... 24

2.4.3 Configuring a CC Attack Protection Rule.. 28

2.4.4 Configuring a Precise Protection Rule.. 35

2.4.5 Adding a Reference Table.. 44

2.4.6 Configuring an IP Address Blacklist or Whitelist Rule... 46

2.4.7 Configuring a Known Attack Source Rule... 53

2.4.8 Configuring a Geolocation Access Control Rule.. 57

2.4.9 Configuring an Anti-Crawler Rule.. 61

2.4.10 Configuring a Global Protection Whitelist (Formerly False Alarm Masking) Rule............ 69

2.4.11 Configuring a Data Masking Rule... 74

2.5 Website Settings.. 78

2.5.1 Adding a Website to Edge WAF.. 78

2.5.2 Viewing the Basic Information... 80

2.5.3 Switching Working Mode... 82

2.5.4 Configuring a Traffic Identifier for a Known Attack Source... 83

2.6 Certificate Management.. 85

2.6.1 Uploading a Certificate.. 85

2.6.2 Deleting a Certificate... 88

2.6.3 Viewing Certificate Information... 89

2.7 Address Group Management... 90

2.7.1 Adding a Blacklist or Whitelist IP Address Group.. 90

2.7.2 Modifying or Deleting a Blacklist or Whitelist IP Address Group..................................... 92

3 Edge Anti-DDoS Management..94

3.1 Viewing the Protection Information..94

3.2 Protecting Domain Names Using Policies..95

4 Managing Logs..97

5 Permissions Management..111

5.1 Creating a User Group and Granting Permissions..111

6 Key Operations Recorded by CTS..113

6.1 EdgeSec Operations Recorded by CTS..113

6.2 Querying Traces..116

7 Monitoring..117

7.1 EdgeSec Monitored Metrics..117

7.2 Configuring a Monitoring Alarm Rule..130

7.3 Viewing Monitored Metrics..131

8 Managing Projects and Enterprise Projects..132

9 Change History..134

1 Purchasing EdgeSec

Prerequisites

You have purchased Huawei Cloud Content Delivery Network (CDN) or Whole Site Acceleration (WSA).

NOTE

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

Specification Limitations

A domain package allows you to add 10 domain names, including one top-level domain and nine subdomains or wildcard domains related to the top-level domain.

NOTE

- If only one top-level domain can be added to a WAF instance, you can add one top-level domain and subdomain or wildcard domain names related to the top-level domain. For example, you can add one top-level domain name example.com and a maximum of nine sub-domains or generic domains, for example, www.example.com, *.example.com, mail.example.com, user.pay.example.com, and x.y.z.example.com. Each of these domain names (including the top-level domain name example.com) is counted toward a domain name quota in the domain name package.
- If a domain name maps to different ports, each port is considered to represent a different domain name. For example, **www.example.com:8080** and **www.example.com:8081** are counted towards your quota as two distinct domain names.

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 By default, the page for purchasing EdgeSec is displayed. Set the product type and region.

- **Enterprise Project**: Select an enterprise project from the drop-down list.

  This option is only available if you have logged in using an enterprise account, or if you have enabled enterprise projects. To learn more, see **Enabling Enterprise Center**. You can use enterprise projects to more efficiently manage cloud resources and project members.

  NOTE

  - Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.
  - The **default** option is available in the **Enterprise Project** drop-down list only after you purchase EdgeSec under the logged-in account.

- Resource: **Edge WAF** is selected by default. Select **Edge Anti-DDoS** as required.
  - Edge WAF provides web threat detection capabilities to effectively identify malicious features of service traffic, prevent website servers from being intruded, and ensure web service security and stability.
  - Edge anti-DDoS detects and cleans abnormal DDoS attack traffic in real time to protect your resources.

Step 4 **Parameters for purchasing EdgeSec** describes the parameters related to Edge WAF and Edge Anti-DDoS.

Table 1-1 Parameters for purchasing EdgeSec

Product Type	Parameter	Description
Edge WAF	Edition	Select edition specifications. For details about service edition differences, see **Service Edition Differences**. ● **Base**: perfect for small-and medium-sized websites. ● **Professional**: perfect for medium-and large-scale websites. ● **Enterprise**: perfect for large-scale websites that require customized rules.
	Charge Mode	By request: number of HTTP/HTPPS requests protected by Edge WAF.

Product Type	Parameter	Description
	Domain Expansion Package	A domain package allows you to add 10 domain names, including one top-level domain and nine subdomains or wildcard domains related to the top-level domain. For example, if you are using basic edition, 10 domain names can be protected, including only one top-level domain name. If you want to protect three top-level domain names, you can purchase two domain name expansion packages to increase the quota. EdgeSec editions offer different domain quotas. ● Base: A maximum of 10 domain names can be protected, including only one top-level domain name. ● Professional: A maximum of 50 domain names can be protected, including five top-level domain names. ● Enterprise: A maximum of 80 domain names can be protected, including eight top-level domain names. **NOTE** ● If only one top-level domain can be added to a WAF instance, you can add one top-level domain and subdomain or wildcard domain names related to the top-level domain. For example, you can add one top-level domain name example.com and a maximum of nine sub-domains or generic domains, for example, www.example.com, *.example.com, mail.example.com, user.pay.example.com, and x.y.z.example.com. Each of these domain names (including the top-level domain name example.com) is counted toward a domain name quota in the domain name package. ● If a domain name maps to different ports, each port is considered to represent a different domain name. For example, **www.example.com:8080** and **www.example.com:8081** are counted towards your quota as two distinct domain names.
	Rule Expansion Package	A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules. If the quota for 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.

Product Type	Parameter	Description
Edge Anti-DDoS	Charge Mode	By traffic: You are charged based on the hourly normal access traffic of CDN services protected by Edge DDoS.

Step 5 Set **Required Duration**. You can select one month, two months, or three months.

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 product details and click **Next**.

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

----End

2 Managing Edge WAF

2.1 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 requests and attack types, QPS, bandwidth, response code, event distribution, 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.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and view security statistics data of the project.

Prerequisites

- A domain name has been added and connected. For details, see **Adding a Website to Edge WAF**.
- 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.

How to Calculate QPS

The QPS calculation method varies depending on the time range. For details, see **Table 2-1**.

Table 2-1 QPS calculation

Time Range	Average QPS Description	Peak QPS Description
Yesterday or Today	The QPS curve is made with the average QPSs in every minute.	The QPS curve is made with each peak QPS in every minute.
Past 3 days	The QPS curve is made with the average QPSs in every five minutes.	The QPS curve is made with each peak QPS in every five minutes.
Past 7 days	The QPS curve is made with the maximum value among the average QPSs in every five minutes at a 10-minute interval.	The QPS curve is made with each peak QPS in every 10 minutes.
Past 30 days	The QPS curve is made with the maximum value among the average QPSs in every five minutes at a one-hour interval.	The QPS curve is made with the peak QPSs in every hour.

NOTE

Queries Per Second (QPS) indicates the number of requests per second. For example, an HTTP GET request is also called a query. The number of requests is the total number of requests in a specific time range.

Procedure

Step 1 Log in to the management console.

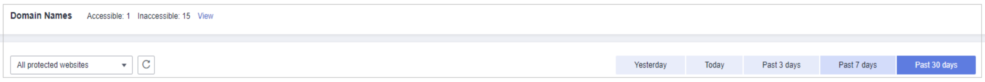
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

Step 3 In the navigation pane on the left, choose **Edge WAF** > **Dashboard**.

Step 4 In the upper part of the page, select a project from the **Enterprise Project** drop-down list. Specify the domain, website, and time period you want to query.

- **Domain Names**: shows information about website domain names added to the Edge WAF 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 Edge WAF in all enterprise projects are displayed. Select a region to view the corresponding website data.
- Query time: You can select **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, or **Past 30 days**.

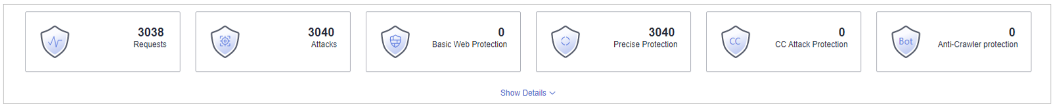
Figure 2-1 Setting search criteria



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

- **Requests**: shows the page views of the website, making it easy for you to view the total number of pages accessed by visitors in a certain period of time.
- **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.
- You can click **Show Details** to view the details of the 10 domain names with the most requests, attacks, and basic web protection, precise protection, CC attack protection, and anti-crawler protection actions.

Figure 2-2 Protection action statistics



Step 6 Query security data.

Figure 2-3 Security Event Statistics

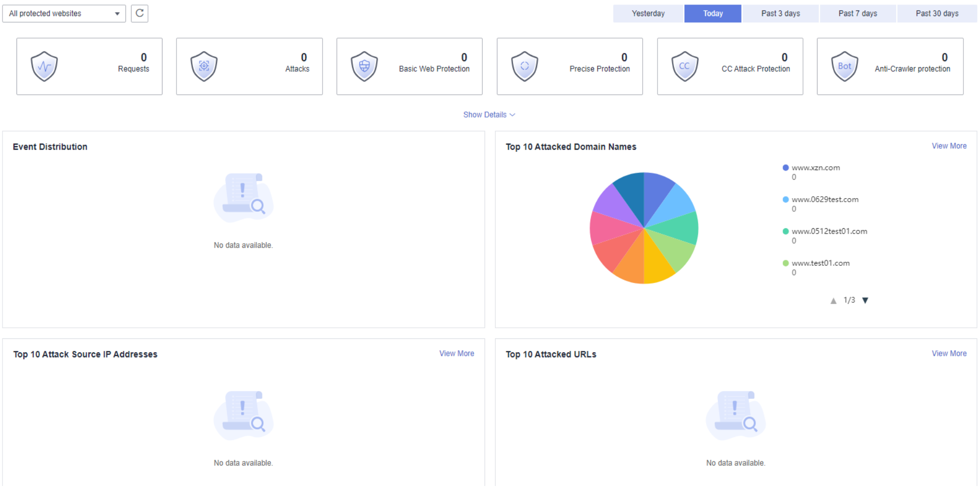


Table 2-2 Security event statistics parameters

Parameter	Description
Event Distribution	Types of attack events. Click an area in the **Event Distribution** 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. Click **View More** to go to the **Events** page and view more protection data.

Parameter	Description
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. Click **View More** to go to the **Events** page and view more protection data.
Top 10 Attacked URLs	The ten most attacked URLs and the number of attacks on each URL. Click **View More** to go to the **Events** page and view more protection data.

----End

2.2 Managing Events

2.2.1 Viewing 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 Edge WAF working mode for a website to **Suspended**, Edge WAF only forwards all requests to the website without inspection. It does not log any attack events neither.
- If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and view protection event logs in the project.

Prerequisites

A protected website has been added. For details, see **Adding a Website to Edge WAF**.

Constraints

If the security software installed on your server blocks the event file from being downloaded, close the software and download the file again.

Procedure

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

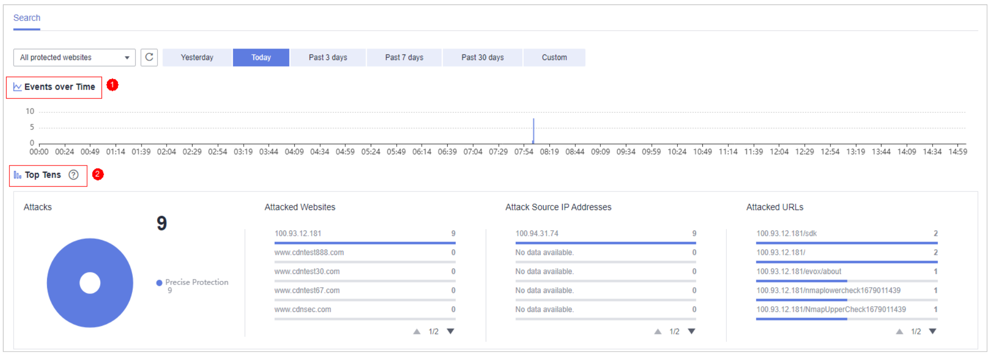
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

Step 3 In the navigation pane on the left, choose **Edge WAF** > **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.

- **Events over Time**: Displays the protection status of the selected website within the selected time range.
- **Top Tens**: Displays a summary of top tens about protected domain names you select for a time range.

Figure 2-4 Events

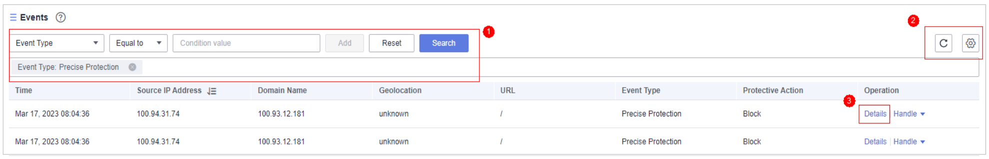


Attacked Websites		Attack Source IP Addresses		Attacked URLs	
100.93.12.181	9	100.94.31.74	9	100.93.12.181/sdk	2
www.cdntest888.com	0	No data available.	0	100.93.12.181/	2
www.cdntest30.com	0	No data available.	0	100.93.12.181/evox/about	1
www.cdntest67.com	0	No data available.	0	100.93.12.181/nmaplowercheck1679011439	1
www.cdnsec.com	0	No data available.	0	100.93.12.181/NmapUpperCheck1679011439	1

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 2-3 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 2-5 Events



Time	Source IP Address	Domain Name	Geolocation	URL	Event Type	Protective Action	Operation
Mar 17, 2023 08:04:36	100.94.31.74	100.93.12.181	unknown	/	Precise Protection	Block	Details Handle
Mar 17, 2023 08:04:36	100.94.31.74	100.93.12.181	unknown	/	Precise Protection	Block	Details Handle

Table 2-3 Description of the conditions

Parameter	Description
Event ID	ID of the event

Parameter	Description
Incident Type	Type of the attack By default, **All** is selected. You can view logs of all attack types or select an attack type to view corresponding attack logs.
Rule ID	ID of a built-in protection rule in basic web protection
Protective Action	The options are **Block**, **Log only**, and **Verification code**.
Source IP	Public IP address of the web visitor/attacker By default, **All** 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 2-4 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 **Block**, **Log only**, and **Verification code**. **NOTE** If an access request matches a data masking rule, the protective action is marked as **Mismatch**.	**Block**

----End

2.2.2 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

Edge WAF 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). Edge WAF 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.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your Edge WAF instance locates. Then, you can select the project from the **Enterprise Project** drop-down list and handle false alarms in the project.

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 Edge WAF. If you enable basic web protection for that application, Edge WAF 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.

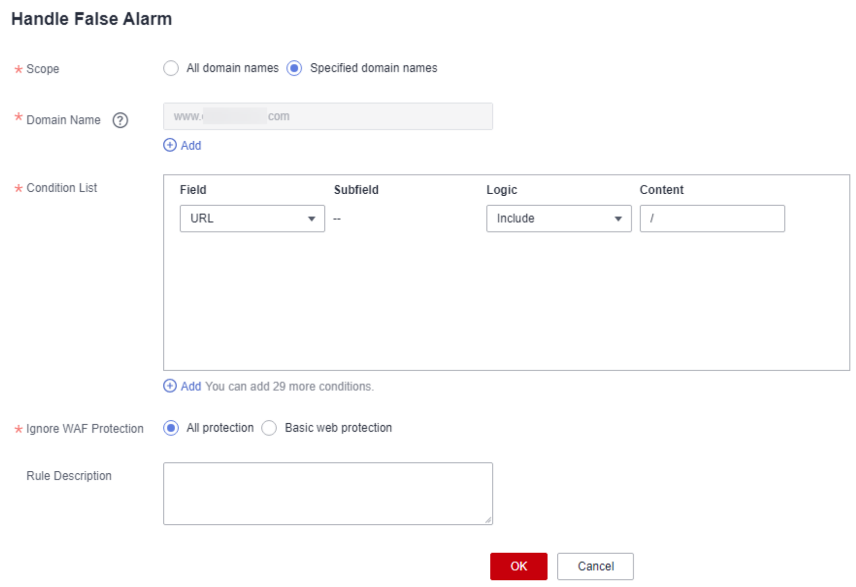
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

Step 3 In the navigation pane on the left, choose **Edge WAF** > **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 2-6 Handling a false alarm



Handle False Alarm

* Scope ○ All domain names ● Specified domain names

* Domain Name ? www.[redacted]com

⊕ 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 2-5 Parameter description

Parameter	Description	Example Value
Scope	– **All domain names**: By default, this rule will be used to all domain names that are protected by the current policy. – **Specify domain names**: Specify a domain name range this rule applies to.	Specified domain names
Domain Name	This parameter is mandatory when you select **Specified domain names** for **Scope**. Enter a single domain name that matches the wildcard domain name being protected by the current policy. To add more domain names, click **Add** to add them one by one.	www.example.com

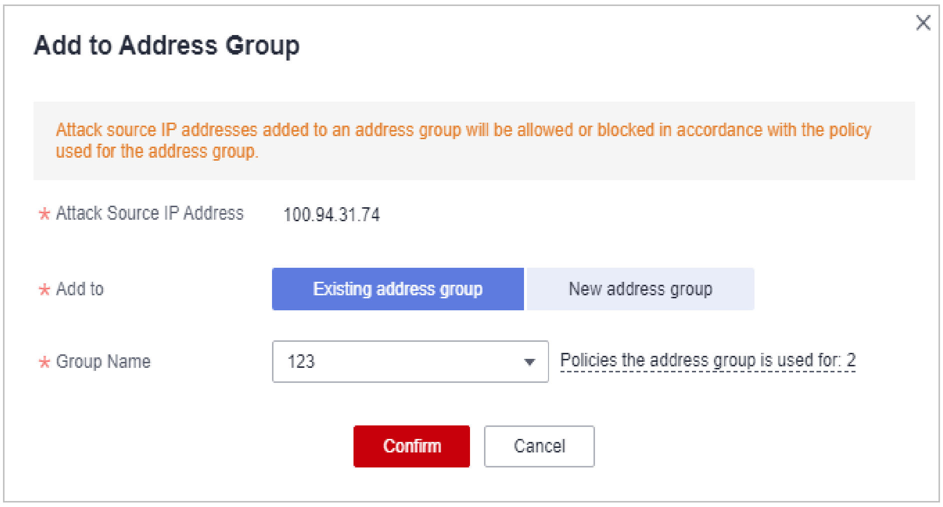
Parameter	Description	Example Value
Condition List	Click **Add** to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. A condition includes the following parameters: Parameters for configuring a condition are described as follows: – Field – **Subfield**: Configure this field only when **Params**, **Cookie**, or **Header** is selected for **Field**. NOTICE The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. – **Logic**: Select a logical relationship from the drop-down list. – **Content**: Enter or select the content that matches the condition.	Path, Include, / product
Ignore WAF Protection	– **All protection**: All Edge WAF rules do not take effect, and Edge WAF allows all request traffic to the domain names in the rule. – **Basic web 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.	Basic web protection
Ignored Protection Type	If you select **Basic web protection** for **Ignored Protection Type**, specify the following parameters: – **Attack type**: Configure the rule by attack event type, such as XSS and SQL injection. One type contains one or more rule IDs. – **All built-in rules**: all checks enabled in **Basic Web Protection**.	Attack type

Parameter	Description	Example Value
Attack type	This parameter is displayed when **Ignored Protection Type** is set to **Attack type**.	SQL injection
Rule Description	A brief description of the rule. This parameter is optional.	-
Advanced Settings	To ignore attacks of a specific field, specify the field in the **Advanced Settings** area. After you add the rule, Edge WAF will stop blocking attack events of the specified field. Select the target field from the first drop-down list box. The following fields are supported: **Params**, **Cookie**, **Header**, **Body**, and **Multipart**. – If you select **Params**, **Cookie**, or **Header**, you can select **All** or **Specified field** to configure a subfield. – If you select **Body** or **Multipart**, you can select **All**. – If you select **Cookie**, the **Domain Name** box for the rule can be empty. **NOTE** If **All** is selected, Edge WAF will not block all attack events of the selected field.	Params 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 2-7 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.

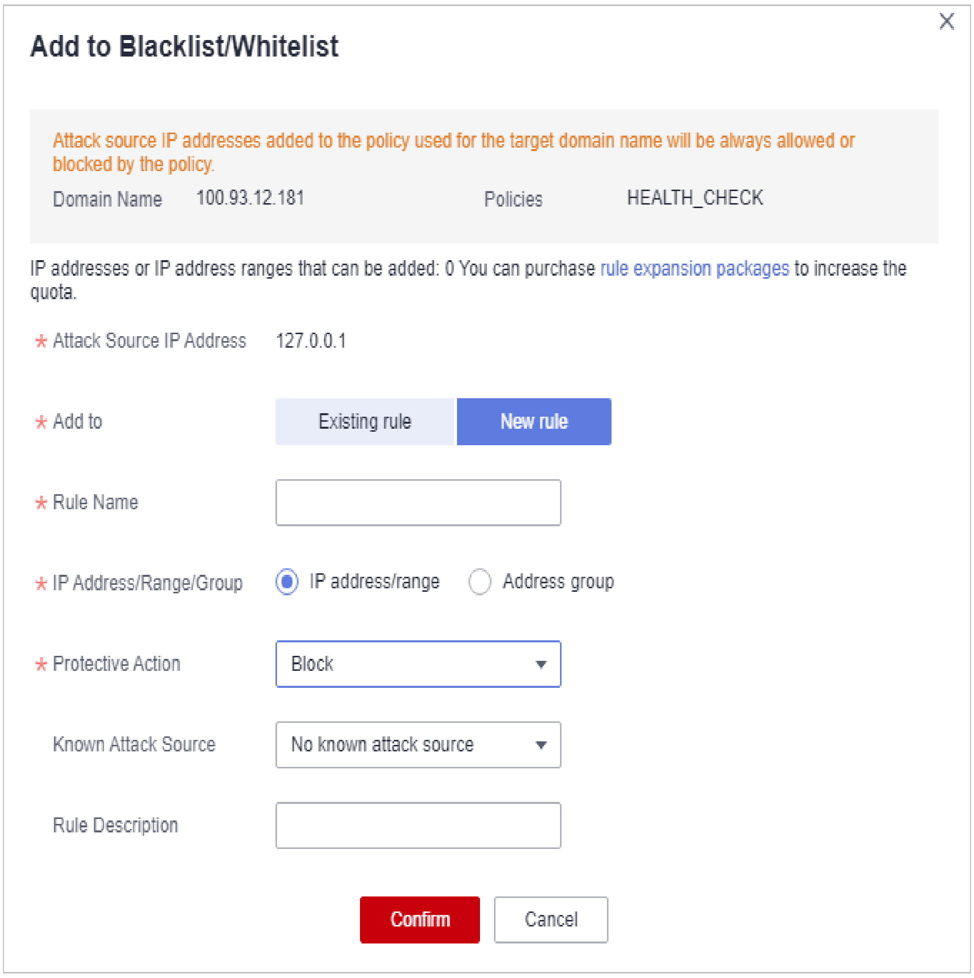
* Attack Source IP Address: 100.94.31.74

* Add to: Existing address group | New address group

* Group Name: 123 — Policies the address group is used for: 2

- 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 2-8 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 100.93.12.181 Policies HEALTH_CHECK

IP addresses or IP address ranges that can be added: 0 You can purchase rule expansion packages to increase the quota.

* Attack Source IP Address 127.0.0.1

* Add to: Existing rule | New rule

* Rule Name

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

* Protective Action: Block

Known Attack Source: No known attack source

Rule Description

Table 2-6 Parameters for adding a record to the blacklist or whitelist

Parameter	Description
Add to	– Existing rule – New rule
Rule Name	– If you select **Existing rule** for **Add to**, select a rule name from the drop-down list. – If you select **New rule** for **Add to**, customize a blacklist or whitelist rule.
IP Address/Range/Group	This parameter is mandatory when you select **New rule** for **Add to**. You can select **IP address/Range** or **Address Group** to add IP addresses a blacklist or whitelist rule.

Parameter	Description
Group Name	This parameter is mandatory when you select **Address group** for **IP Address/Range/Group**. Select an address group from the drop-down list. You can also click **Add Address Group** to create an address group. For details, see **Adding a Blacklist or Whitelist IP Address Group**.
Protective Action	– **Block**: Select **Block** if you want to blacklist an IP address or IP address range. – **Allow**: Select **Allow** if you want to whitelist an IP address or IP address range. – **Log only**: Select **Log only** if you want to observe an IP address or IP address range.
Known Attack Source	If you select **Block** for **Protective Action**, you can select a blocking type of a known attack source rule. Edge WAF 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 (original false alarm masking) 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 (formerly false alarm masking) rule list. You can go to the **Policies** page and then switch to the **Global Protection Whitelist (Formerly False Alarm Masking)** page to manage the rule, including querying, disabling, deleting, and modifying the rule. For details, see **Configuring a Global Whitelist (Originally False Alarm Masking) Rule**.

2.3 Protection Policy

2.3.1 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.

Procedure

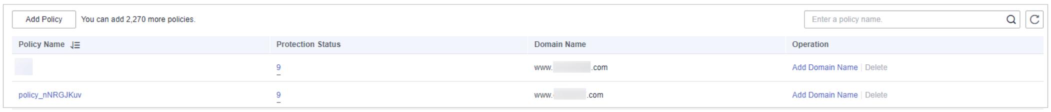
Step 1 Log in to the management console.

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 WAF** > **Policies**. The **Policies** page is displayed.

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

Figure 2-9 Adding a protection policy

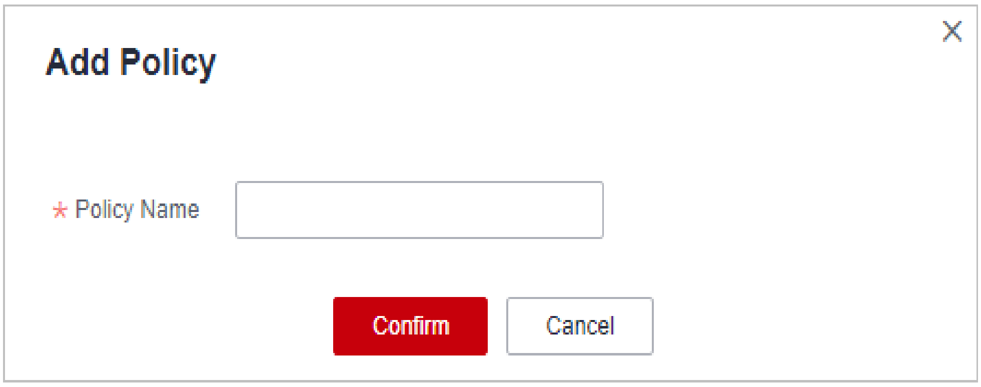


Add Policy   You can add 2,270 more policies.   Enter a policy name.

Policy Name	Protection Status	Domain Name	Operation
[redacted]	9	www.[redacted].com	Add Domain Name | Delete
policy_nNRGJKuv	9	www.[redacted].com	Add Domain Name | Delete

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

Figure 2-10 Add Policy



Add Policy

* Policy Name

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.

2.3.2 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 WAF** > **Policies**. The **Policies** page is displayed.

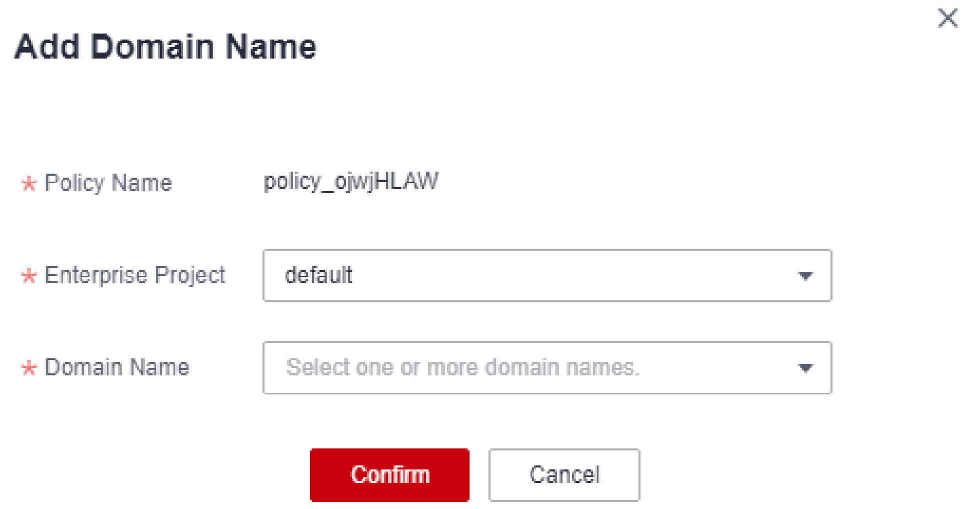
Step 4 In the row containing the target policy, click **Add Domain Name** in the **Operation** column.

Step 5 Select an **Enterprise Project** and **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.

Figure 2-11 Selecting one or more domain names



Add Domain Name

* Policy Name policy_ojwjHLAW

* Enterprise Project default

* Domain Name Select one or more domain names.

Step 6 Click **Confirm**.

----End

2.4 Configuring Protection Rules

2.4.1 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 2-12** shows how EdgeSec engine built-in protection rules work. **Figure 2-13** shows the detection sequence of user-defined rules.

Figure 2-12 EdgeSec engine detection process

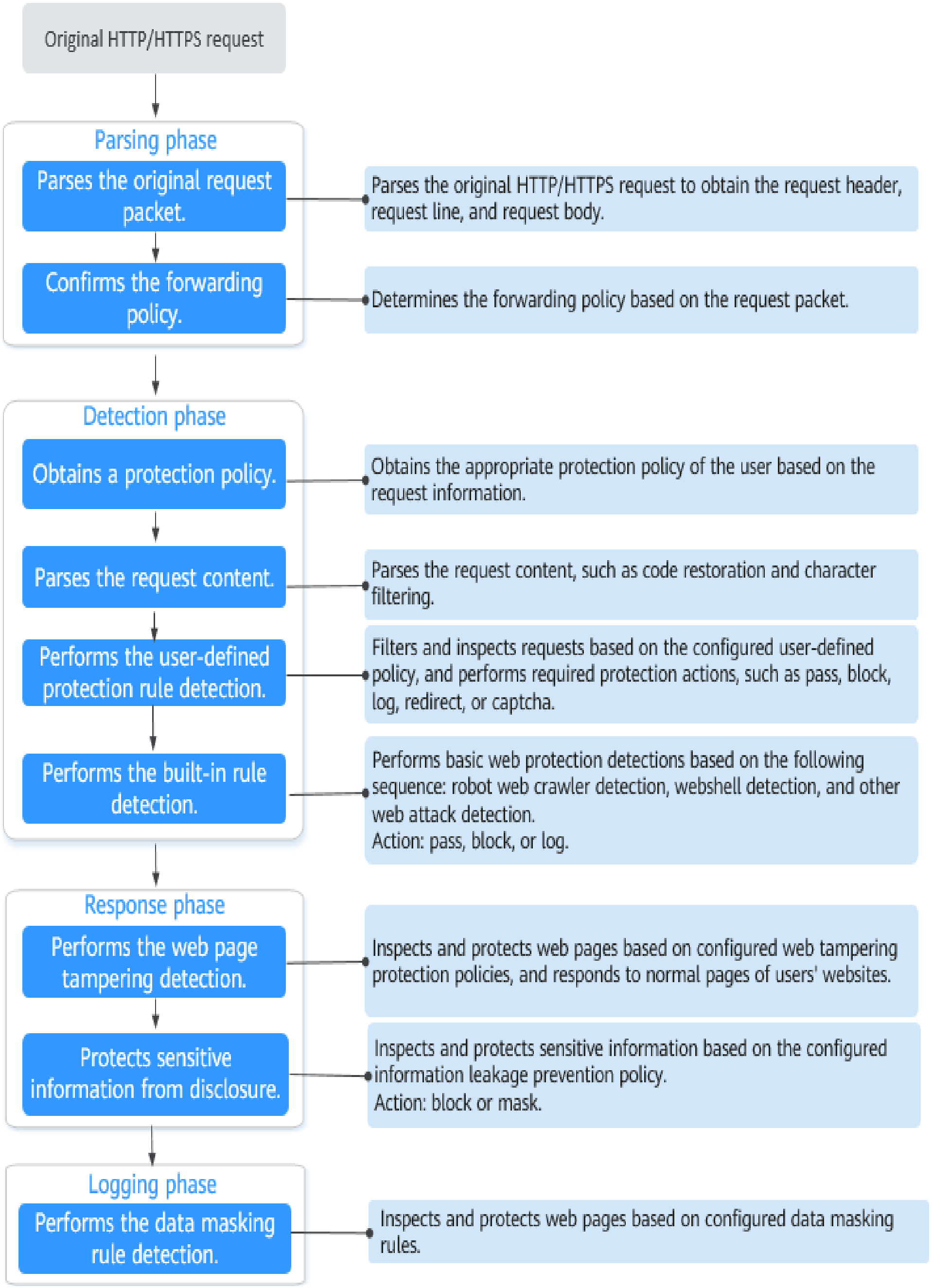
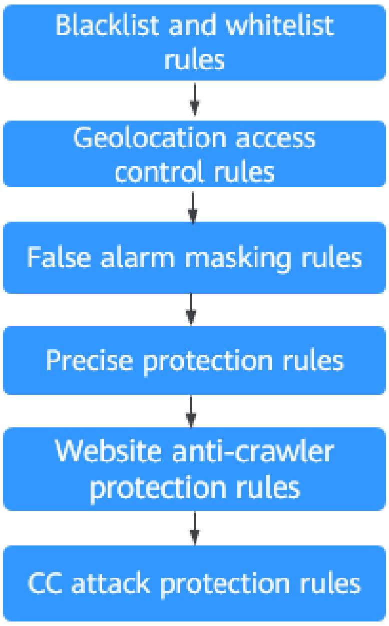

Original HTTP/HTTPS request
Parsing phase
Parses the original request packet.
Confirms the forwarding policy.
Parses the original HTTP/HTTPS request to obtain the request header, request line, and request body.
Determines the forwarding policy based on the request packet.
Detection phase
Obtains a protection policy.
Parses the request content.
Performs the user-defined protection rule detection.
Performs the built-in rule detection.
Obtains the appropriate protection policy of the user based on the request information.
Parses the request content, such as code restoration and character filtering.
Filters and inspects requests based on the configured user-defined policy, and performs required protection actions, such as pass, block, log, redirect, or captcha.
Performs basic web protection detections based on the following sequence: robot web crawler detection, webshell detection, and other web attack detection.
Action: pass, block, or log.
Response phase
Performs the web page tampering detection.
Protects sensitive information from disclosure.
Inspects and protects web pages based on configured web tampering protection policies, and responds to normal pages of users' websites.
Inspects and protects sensitive information based on the configured information leakage prevention policy.
Action: block or mask.
Logging phase
Performs the data masking rule detection.
Inspects and protects web pages based on configured data masking rules.

Figure 2-13 Priorities of custom protection rules


Blacklist and whitelist rules
Geolocation access control rules
False alarm masking rules
Precise protection rules
Website anti-crawler protection rules
CC attack 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

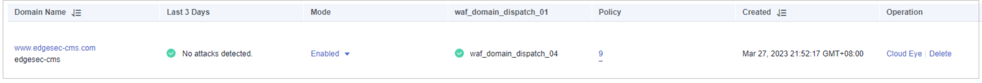
After a domain name is added to Edge WAF, Edge WAF automatically associates a protection policy with the domain name, and protection rules configured for the domain name are also added to the protection policy by default. If there are domain names applicable to the protection policy, you can directly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

- Where to configure

  a. In the navigation pane on the left, choose **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

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

Figure 2-14 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	No attacks detected.	Enabled	waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | Delete

- Protection rules you can configure on the rule configuration page

Table 2-7 Configurable protection rules

Protection Rule	Description	Reference
Basic Web Protection	With an extensive reputation database, WAF 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.	**Configuring Basic Web Protection Rules**
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, cookie, or referer field, mitigating CC attacks.	**Configuring a CC Attack Protection Rule**
Precise Protection	You can customize protection rules by combining HTTP headers, cookies, URLs, request parameters, and client IP addresses.	**Configuring a Precise Protection Rule**
Blacklist and Whitelist	You can configure blacklist and whitelist rules to block, log only, or allow access requests from specified IP addresses.	**Configuring an IP Address Blacklist or Whitelist Rule**

Protection Rule	Description	Reference
Known Attack Source	If Edge WAF blocks a malicious request by IP address, Cookie, or Params, you can configure a known attack source rule to let Edge WAF automatically block all requests from the attack source for a blocking duration set in the known attack source rule.	**Configuring a Known Attack Source Rule**
Geolocation Access Control	You can customize these rules to allow or block requests from a specific country or region.	**Configuring a Geolocation Access Control Rule**
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.	**Configuring an Anti-Crawler Rule**
Global protection whitelist (formerly false alarm masking) rules	You can configure these rules to let WAF ignore certain rules for specific requests.	**Configuring a Global Protection Whitelist (Formerly False Alarm Masking) Rule**
Data Masking	You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.	**Configuring a Data Masking Rule**

2.4.2 Configuring Basic Web Protection Rules

After this function is enabled, WAF 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 Edge WAF**.

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**. Edge WAF will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.

Procedure

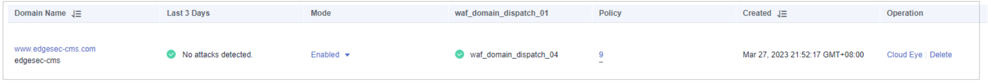
Step 1 **Log in to the management console.**

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 **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

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

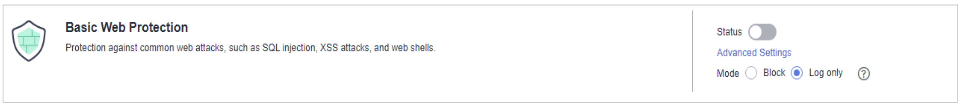
Figure 2-15 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	✓ No attacks detected.	Enabled ▾	✓ waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | Delete

Step 5 In the **Basic Web Protection** configuration area, change **Status** and **Mode** as needed by referring to **Table 2-8**.

Figure 2-16 Basic Web Protection configuration area



Basic Web Protection

Protection against common web attacks, such as SQL injection, XSS attacks, and web shells.

Status ○

Advanced Settings

Mode ○ Block ◉ Log only ⓘ

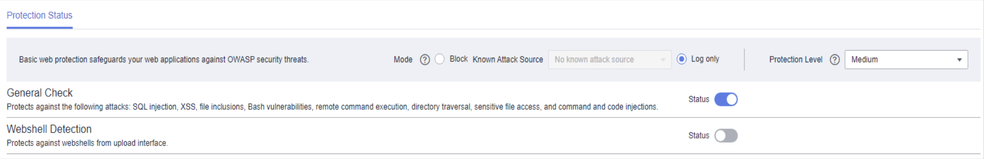
Table 2-8 Parameter description

Parameter	Description
Status	Status of Basic Web Protection - ◉: enabled. - ○: disabled.
Mode	- **Block**: The detected attacks are blocked and logged. - **Log only**:The detected attacks are logged only.

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 2-10**.

Figure 2-17 Basic web protection



Protection Status

Basic web protection safeguards your web applications against OWASP security threats.

Mode ○ Block Known Attack Source No known attack source ● Log only

Protection Level Medium

General Check
Protects against the following attacks: SQL injection, XSS, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command and code injections.
Status ●

Webshell Detection
Protects against webshells from upload interface.
Status ○

NOTICE

If you select **Mode** for **Block** on the **Protection Status** tab, you can select a known attack source rule to let WAF 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 2-9 Protection levels

Protection Level	Description
Low	WAF only blocks the requests with obvious attack signatures. If a large number of false alarms are reported, **Low** is recommended.
Medium	The default level is **Medium**, which meets a majority of web protection requirements.
High	At this level, WAF 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. To let Edge WAF defend against more attacks but make minimum effect on normal requests, observe your workloads for a period of time first. Then, configure a global protection whitelist (false alarm masking) rule and select **High**.

2. Set the protection type.

NOTICE

By default, **General Check** is enabled. You can enable other protection types by referring to **Table 2-10**.

Table 2-10 Protection types

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

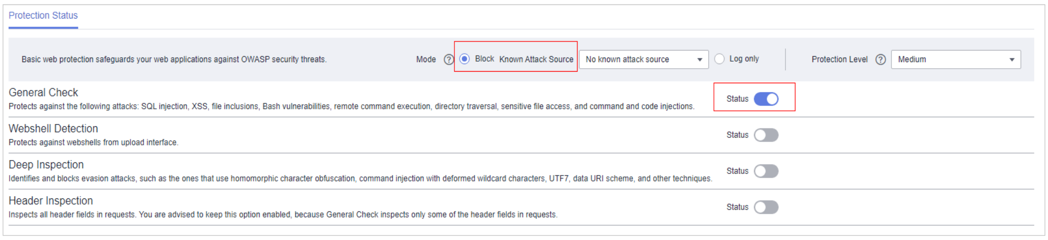
----End

Example - Blocking SQL Injection Attacks

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

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

Figure 2-18 Enabling General Check



Protection Status

Basic web protection safeguards your web applications against OWASP security threats.

Mode ⓘ ● Block Known Attack Source: No known attack source ○ Log only | Protection Level ⓘ Medium

General Check
Protects against the following attacks: SQL injection, XSS, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command and code injections.
Status: on

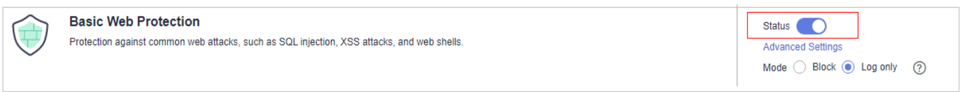
Webshell Detection
Protects against webshells from upload interface.
Status: off

Deep Inspection
Identifies and blocks evasion attacks, such as the ones that use homomorphic character obfuscation, command injection with deformed wildcard characters, UTF7, data URI scheme, and other techniques.
Status: off

Header Inspection
Inspects all header fields in requests. You are advised to keep this option enabled, because General Check inspects only some of the header fields in requests.
Status: off

Step 2 Enable WAF basic web protection.

Figure 2-19 Enabling WAF basic web protection



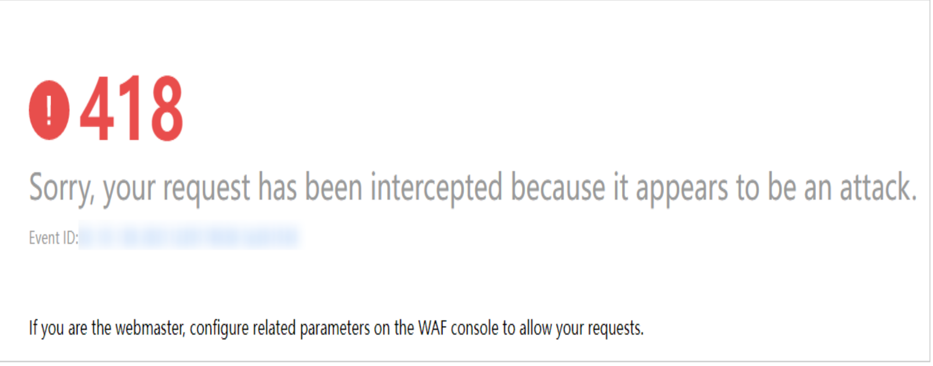
Basic Web Protection
Protection against common web attacks, such as SQL injection, XSS attacks, and web shells.

Status: on
Advanced Settings
Mode ○ Block ● Log only ⓘ

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.

Edge WAF blocks the access request. **Figure 2-20** shows an example block page.

Figure 2-20 Block page



418

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

Event ID: [redacted]

If you are the webmaster, configure related parameters on the WAF console to allow your requests.

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

----End

2.4.3 Configuring a CC Attack Protection Rule

CC attack protection can limit the access to a protected website based on a single IP address, cookie, or referer. Beyond that, CC attack protection can also limit access rate based on policies, domain names, and URLs to precisely mitigate CC attacks. In policy-based rate limiting, the number of requests for all domain names in the same policy are counted for triggering the rule. In domain-based rate limiting, the total number of requests for each domain name is counted separately for triggering the rule. In URL-based rate limiting, the number of requests for each URL is counted separately for triggering the rule. 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 Edge WAF**.

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 by identifying their cookie (name field) if the visitor accessed a URL (for example, /admin*) of your website over 10 times within 60 seconds.

Procedure

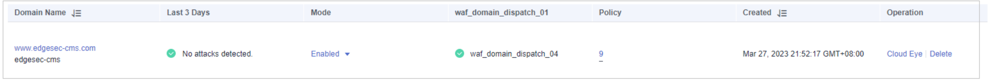
Step 1 **Log in to the management console.**

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 **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

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

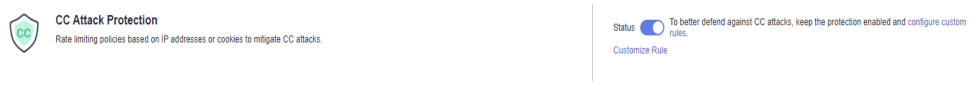
Figure 2-21 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	✓ No attacks detected.	Enabled ▾	✓ waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | Delete

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

Figure 2-22 CC Attack Protection configuration area



CC Attack Protection

Rate limiting policies based on IP addresses or cookies to mitigate CC attacks.

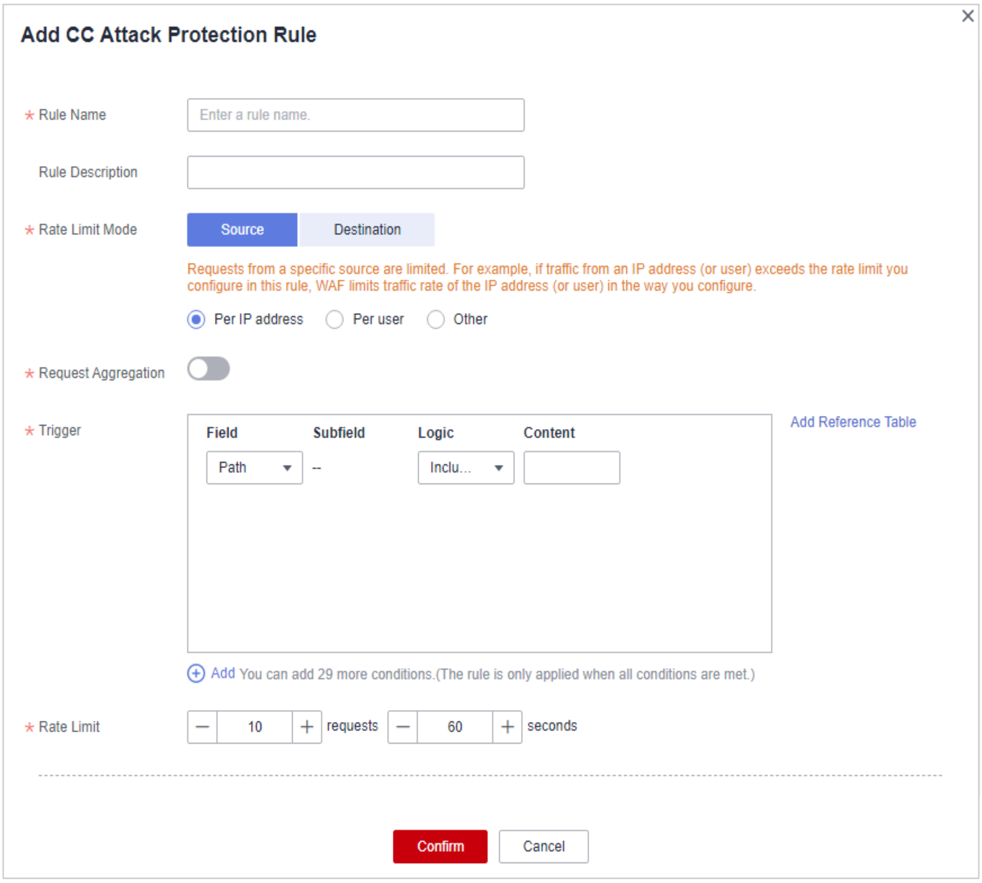
Status: enabled. To better defend against CC attacks, keep the protection enabled and configure custom rules.

Customize Rule

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 2-11**.

Figure 2-23 Adding a CC attack protection rule



Add CC Attack Protection Rule

* Rule Name: Enter a rule name.

Rule Description:

* Rate Limit Mode: Source | Destination

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

● Per IP address ○ Per user ○ Other

* Request Aggregation:

* Trigger:

Field	Subfield	Logic	Content
Path	--	Inclu...	

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

* Rate Limit: 10 requests 60 seconds

Table 2-11 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	● **Source**:Requests from a specific source are limited. For example, if traffic from an IP address (or user) exceeds the rate limit you configure in this rule, WAF limits traffic rate of the IP address (or user) in the way you configure. – **Per IP address**: A website visitor is identified by the IP address. – **Per user**: A website visitor is identified by the key value of **Cookie** or **Header**. – **Other**: A website visitor is identified by the Referer field (user-defined request source). **NOTE** If you set **Rate Limit Mode** to **Other**, set **Content** of **Referer** to a complete URL containing the domain name. The **Content** field supports prefix match and exact match only, but cannot contain two or more consecutive slashes, for example, **///admin**. If you enter **///admin**, WAF will convert it to **/admin**. For example, if **Path** is **/admin**, and you do not want visitors to access the page from **www.test.com**, set **Content** of **Referer** to **http://www.test.com**.	--
User Identifier	This parameter is mandatory when you select **Source** and **Per user** for **Rate Limit Mode**. ● **Cookie**: A cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the **name** field in the cookie to uniquely identify a website visitor, select **name**. ● **Header**: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements.	name

Parameter	Description	Example Value
Trigger	Click **Add** 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. ● **Field**: include path, IP address, cookie, header, Params, and HTTP code. ● **Subfield**: Configure this field only when **Cookie**, **Header**, or **Params** is selected for **Field**. NOTICE The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. ● **Logic**: Select a logical relationship from the drop-down list. NOTE If you set **Logic** to **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**, select an existing reference table. For details, see **Adding a Reference Table**. ● **Content**: Enter or select the content that matches the condition.	**Path Include / admin**
Rate Limit	The maximum requests that a website visitor can initiate within the configured period. If the configured rate limit has been reached, Edge WAF will respond according to the protective action configured.	**10** requests allowed in **60** seconds

Parameter	Description	Example Value
Protective Action	The action that WAF will take if the number of requests exceeds **Rate Limit** you configured. The options are as follows: ● **Verification code**: WAF allows requests that trigger the rule as long as your website visitors complete the required verification. ● **Block**: WAF blocks requests that trigger the rule. ● **Block dynamically**: WAF blocks requests that trigger the rule based on **Allowable Frequency**, which you configure after the first rate limit period is over. ● **Log only**: WAF only logs requests that trigger the rule.	Block
Allowable Frequency	This parameter can be set if you select **Block dynamically** for **Protective Action**. WAF blocks requests that trigger the rule based on **Rate Limit** first. Then, in the following rate limit period, WAF blocks requests that trigger the rule based on **Allowable Frequency** you configure. **Allowable Frequency** cannot be larger than **Rate Limit**. **NOTE** If you set **Allowable Frequency** to **0**, WAF blocks all requests that trigger the rule in the next rate limit period.	**8** requests allowed in **60** seconds
Block Duration	Period of time for which to block the item when you set **Protective Action** to **Block**.	**600** seconds
Block Page	The page displayed if the maximum number of requests has been reached. This parameter is configured only when **Protective Action** is set to **Block**. ● If you select **Default settings**, the default block page is displayed. ● If you select **Custom**, a custom error message is displayed.	Custom
Block Page Type	If you select **Custom** for **Block Page**, select a type of the block page among options **application/json**, **text/html**, and **text/xml**.	text/html

Parameter	Description	Example Value
Page Content	If you select **Custom** for **Block Page**, configure the content to be returned.	Page content styles corresponding to different page types are as follows: ● **text/html**: <html><body>Forbidden</body></html> ● **application/json**: {"msg": "Forbidden"} ● **text/xml**: <?xml version="1.0" encoding="utf-8"?><error><msg>Forbidden</msg></error>

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.

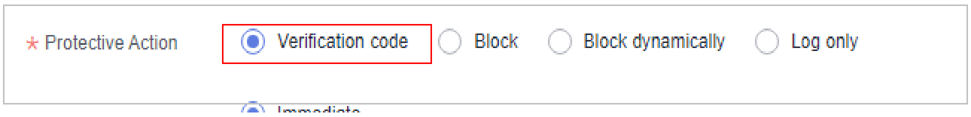
----End

Configuration Example - Verification Code

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

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

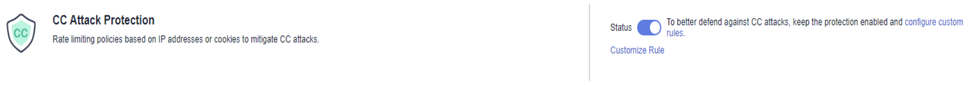
Figure 2-24 Verification code



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

Step 2 Enable CC attack protection.

Figure 2-25 CC Attack Protection configuration area



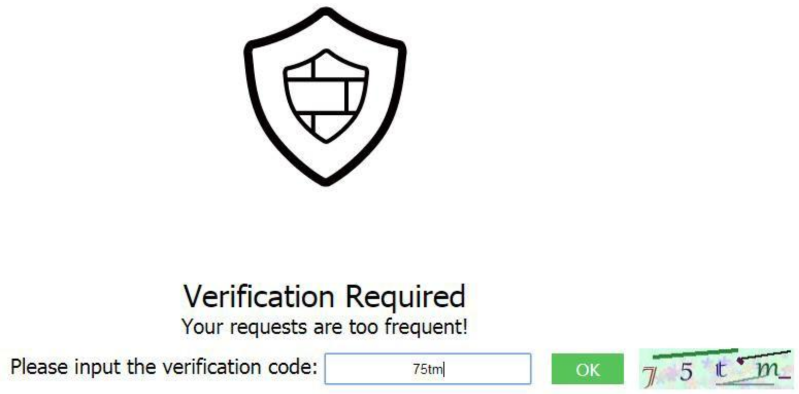
CC Attack Protection
Rate limiting policies based on IP addresses or cookies to mitigate CC attacks.

Status ● To better defend against CC attacks, keep the protection enabled and configure custom rules.

Customize Rule

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.



Verification Required

Your requests are too frequent!

Please input the verification code: 75tm

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

----End

2.4.4 Configuring a Precise Protection Rule

WAF 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 WAF allow, 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 Edge WAF**.

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**. Edge WAF 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

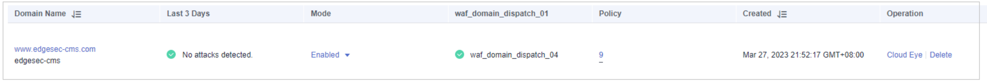
Step 1 Log in to the management console.

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 **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

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

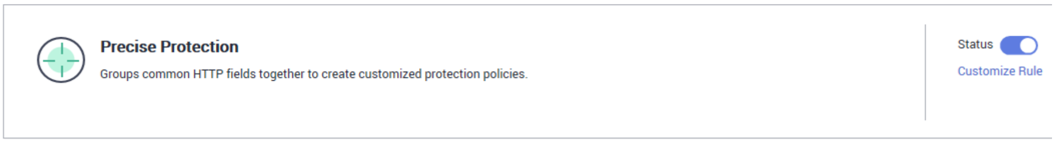
Figure 2-26 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	✓ No attacks detected.	Enabled ▾	✓ waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | 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 2-27 Precise Protection configuration area



Precise Protection

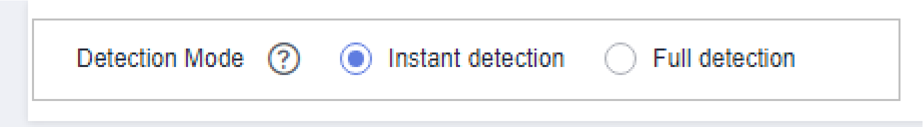
Groups common HTTP fields together to create customized protection policies.

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

Figure 2-28 Setting Detection Mode



Detection Mode ● Instant detection ○ Full detection

Step 7 Click **Add Rule**.

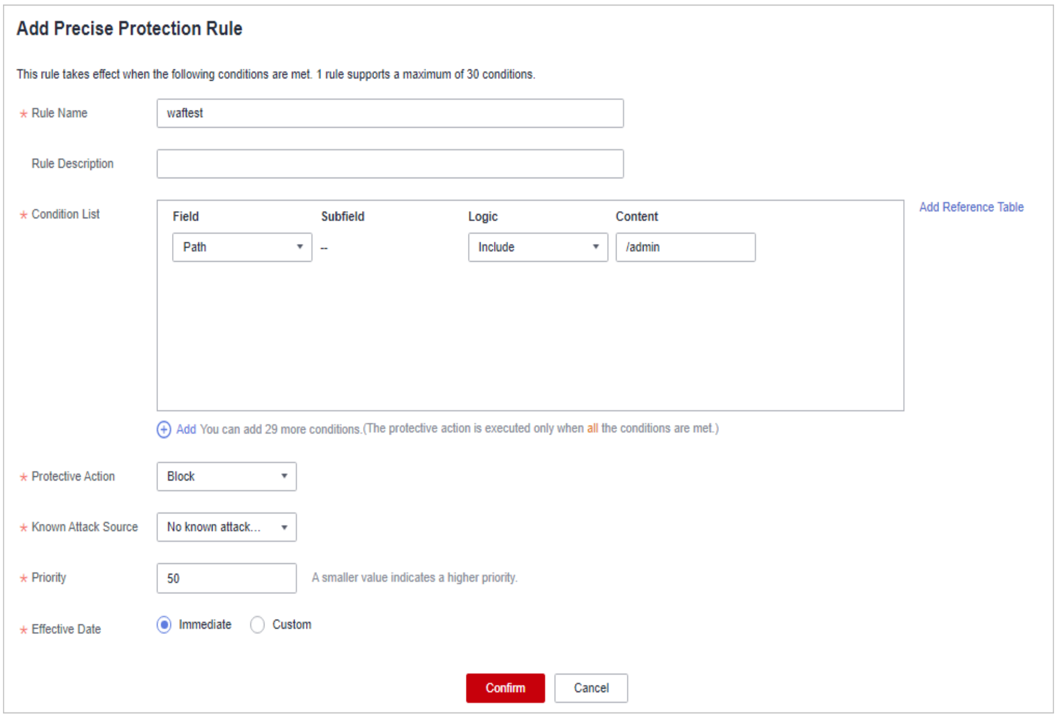
Step 8 In the displayed dialog box, add a rule by referring to **Table 2-12** and **Table 2-13**.

The settings shown in **Figure 2-29** are used as an example. If a visitor tries to access a URL containing **/admin**, Edge WAF will block the request.

NOTICE

To ensure that Edge WAF 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 2-29 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: waftest

Rule Description:

* Condition List:

Field	Subfield	Logic	Content
Path	--	Include	/admin

Add Reference Table

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

* Protective Action: Block

* Known Attack Source: No known attack...

* Priority: 50 A smaller value indicates a higher priority.

* Effective Date: ● Immediate ○ Custom

Table 2-12 Rule parameters

Parameter	Description	Example Value
Condition List	Click **Add** 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: Parameters for configuring a condition are described as follows: ● **Field** ● **Subfield**: Configure this field only when **IP**, **Params**, **Cookie**, or **Header** is selected for **Field**. NOTICE The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. ● **Logic**: Select a logical relationship from the drop-down list. NOTE – If **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** is selected, select an existing reference table in the **Content** drop-down list. For details, see **Adding a Reference Table**. – **Exclude any value**, **Not equal to any value**, **Prefix is not any of them**, and **Suffix is not any of them** indicates, respectively, that WAF performs the protection action (block, allow, 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 **Path** field is set to **Exclude any value** and the **test** reference table is selected. If *test1*, *test2*, and *test3* are set in the **test** reference table, WAF performs the protection action when the path of the access request does not contain *test1*, *test2*, or *test3*. ● **Content**: Enter or select the content of condition matching.	● **Path Include /admin** ● **User Agent Prefix is not mozilla/5.0** ● **IP Equal to 192.168.2.3** ● **Cookie key1 Prefix is not jsessionid**

Parameter	Description	Example Value
	NOTE For more details about the configurations in general, see **Table 2-13**.	
Protective Action	You can select **Block**, **Allow**, **Record only**, or **JS Challenge** (Edge WAF returns JavaScript code).	**Block**
Known Attack Source	If you set **Protective Action** to **Block**, you can select a blocking type for a known attack source rule. Edge WAF 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**
Priority	Rule priority. If you have added multiple rules, rules are matched by priority. The smaller the value you set, the higher the priority. **NOTICE** If multiple precise access control rules have the same priority, WAF matches the rules in the sequence of time the rules are added.	**5**
Effective Date	Select **Immediate** to enable the rule immediately, or select **Custom** to configure when you wish the rule to be enabled.	**Immediate**

Table 2-13 Condition list configurations

Field	Subfield	Logic	Example Content
Path: 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 **/admin**, **Path** must be set to **/admin**.	None	Select a logical relationship from the drop-down list.	**/buy/phone/** **NOTICE** If **Path** is set to **/**, all paths of the website are protected.
User Agent: A user agent of the scanner to be checked.	None		**Mozilla/5.0 (Windows NT 6.1)**

Field	Subfield	Logic	Example Content
IP: An IP address of the visitor for the protection.	- Client IP Address - X-Forwarded-For		XXX.XXX.1.1
Params: A request parameter.	--		**201901150929**
Cookie: A small piece of data to identify web visitors	- All fields - Any subfield - Custom		jsessionid
Referer: A user-defined request resource. For example, if the protected path is **/admin/xxx** and you do not want visitors to access the page from **www.test.com**, set **Content** to **http://www.test.com**.	None		http://www.test.com
Header: A user-defined HTTP header.	- All fields - Any subfield - Custom		**text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8**
Method: the user-defined request method.	None		**GET**, **POST**, **PUT**, **DELETE**, and **PATCH**
Request Line: Length of a user-defined request line.	None		**50**
Request: Length of a user-defined request. It includes the request header, request line, and request body.	None		None

Field	Subfield	Logic	Example Content
Protocol: the protocol of the request.	None		http
Response Code: Status code returned to the request.	None		404
Response Length: the length of the response to the request.	None		None
Response Time: time to respond the request.	None		None
Response Header: response header.	● All fields ● Any subfield ● Custom		None
Response Body: response message body	None		None
Request message body.	None		None

NOTICE

The professional and enterprise editions support **Response Code**, **Response Length**, **Response Time**, **Response Header**, and **Response Body**.

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

Protection Effect

If you have configured a precise protection rule as shown in **Figure 2-29** for your domain name, to verify WAF 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 Edge WAF by following the instructions in **Adding a Website to Edge WAF**.
- If the website is accessible, go to **2**.

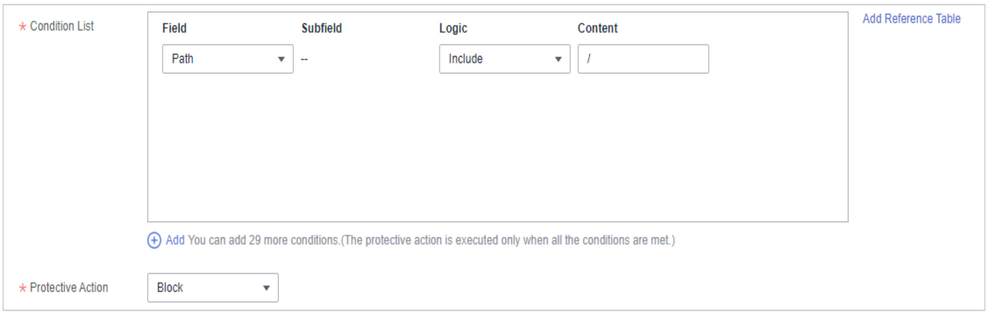
Step 2 Clear the browser cache and enter **http://www.example.com/admin** (or any page containing **/admin**) in the address bar. Normally, Edge WAF blocks the requests that meet the conditions and returns the block page.

----End

Configuration Example - Allowing a Specified IP Address to Access Your Website

You can configure two precise protection rules, one to block all requests, as shown in **Figure 2-30**, but then another one to allow the access from a specific IP address, as shown in **Figure 2-31**.

Figure 2-30 Blocking all requests



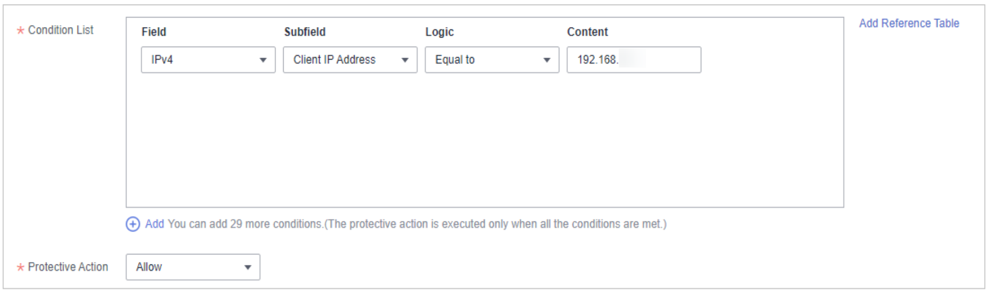
* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/

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

* Protective Action: Block

Figure 2-31 Allowing the access of a specified IP address



* Condition List

Field	Subfield	Logic	Content
IPv4	Client IP Address	Equal to	192.168.

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

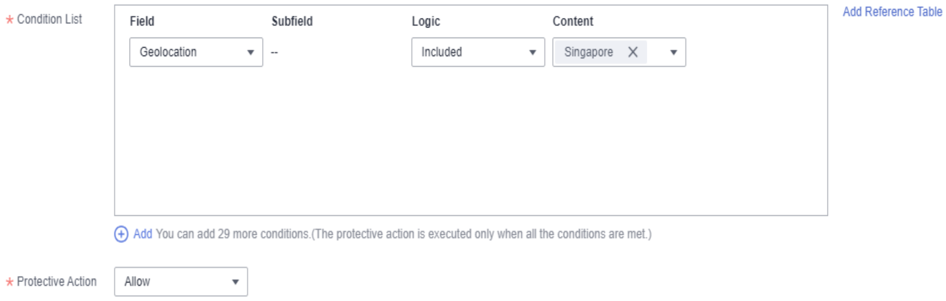
* Protective Action: Allow

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

Assume that domain name *www.example.com* has been connected to Edge WAF and you want to allow only IP addresses in **Singapore**, to access the domain name. Perform the following steps:

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

Figure 2-32 Adding a geolocation access control rule



* Condition List

Field	Subfield	Logic	Content
Geolocation	--	Included	Singapore

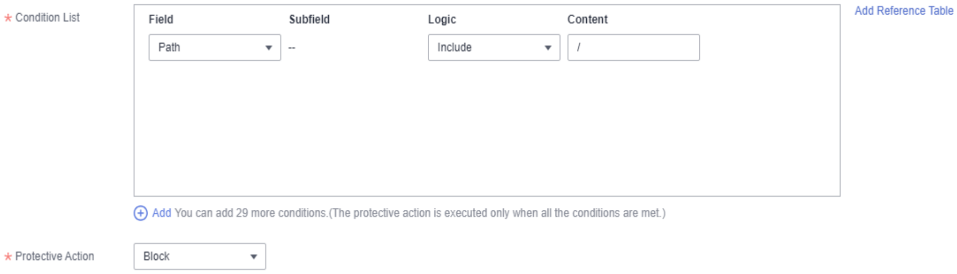
Add Reference Table

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

* Protective Action: Allow

Step 2 Configure a precise protection rule to block all requests.

Figure 2-33 Blocking all access requests



* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/

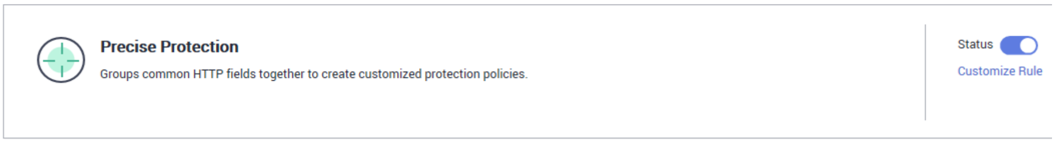
Add Reference Table

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

* Protective Action: Block

Step 3 Enable the precise protection rule.

Figure 2-34 Precise Protection configuration area



Precise Protection

Groups common HTTP fields together to create customized protection policies.

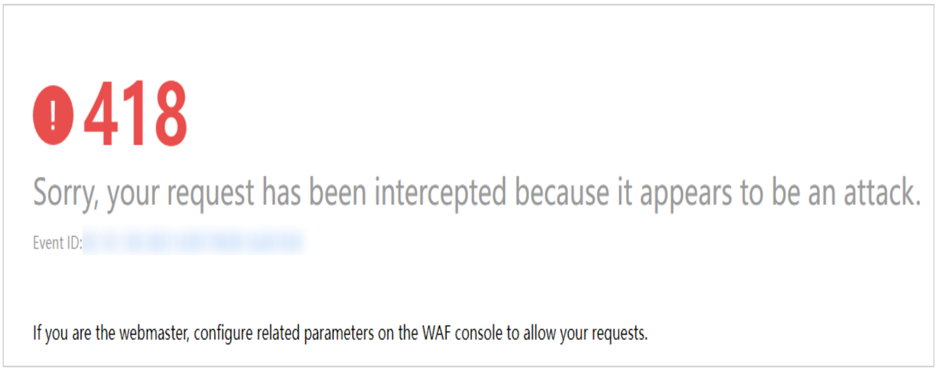
Status

Customize Rule

Step 4 Clear the browser cache and access http://www.example.com.

When an access request from IP addresses outside **Singapore** accesses a page, Edge WAF blocks the access request, as shown in **Figure 2-35**.

Figure 2-35 Block page



418

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

Event ID: [redacted]

If you are the webmaster, configure related parameters on the WAF console to allow your requests.

Step 5 Go to the Edge WAF console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page. You will see that all requests not from **Singapore** have been blocked.

----End

2.4.5 Adding a Reference Table

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 Edge WAF**.

Constraints

The basic edition does not support this function.

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

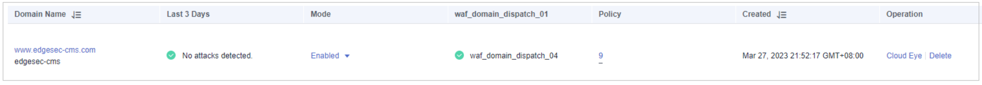
Step 1 **Log in to the management console.**

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 **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

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

Figure 2-36 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	✓ No attacks detected.	Enabled ▾	✓ waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | Delete

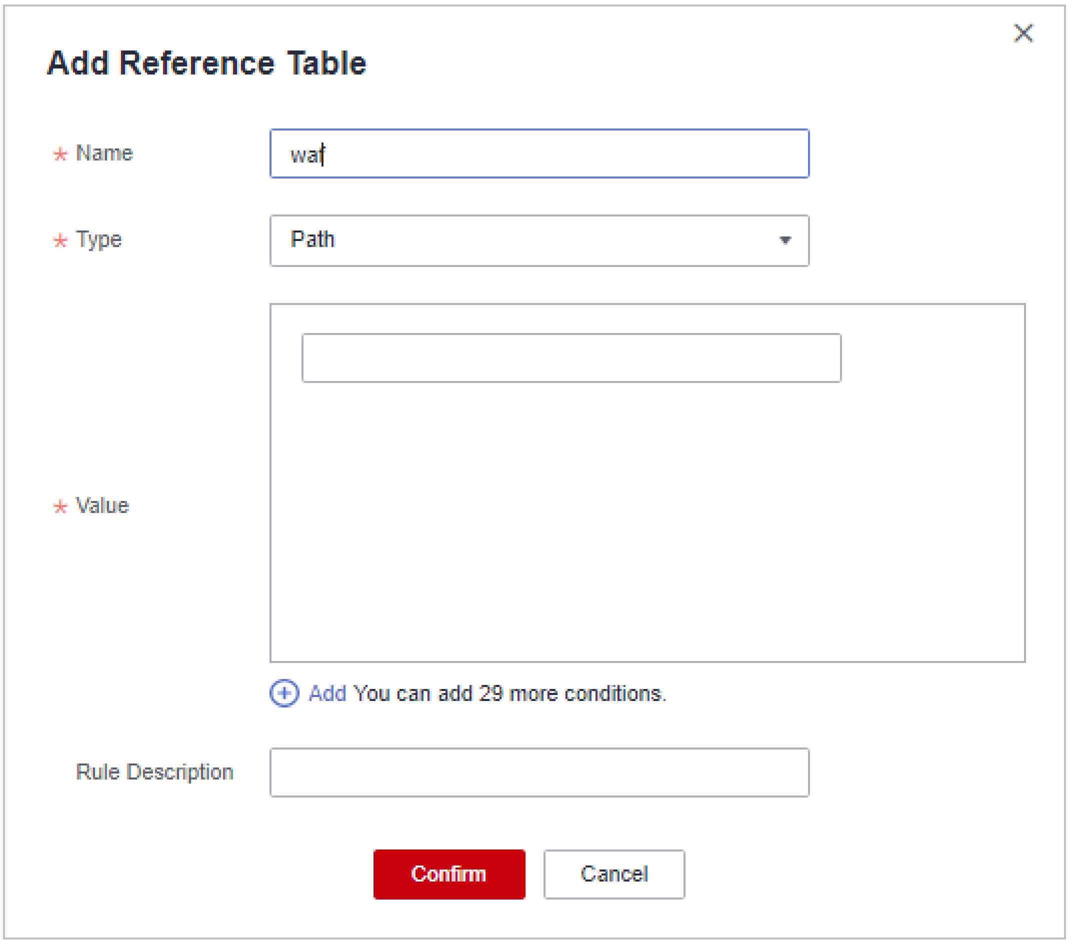
Step 5 In the **CC Attack Protection** or **Precise Protection** area, click **Customize Rule**.

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 2-14**.

Figure 2-37 Adding a reference table



Add Reference Table

* Name: waf
* Type: Path
* Value

Add You can add 29 more conditions.

Rule Description

Table 2-14 Parameter description

Parameter	Description	Example Value
Name	Table name you entered	test

Parameter	Description	Example Value
Type	● **Path**: A URL to be protected, excluding a domain name ● **User Agent**: A user agent of the scanner to be protected ● **IP**: An IP address of the visitor to be protected. ● **Params**: A request parameter to be protected ● **Cookie**: A small piece of data to identify web visitors ● **Referer**: A user-defined request resource For example, if the protected path is **/admin/xxx** and you do not want visitors to be able to access it from *www.test.com*, set **Value** to **http://www.test.com**. ● **Header**: A user-defined HTTP header	**Path**
Value	Value of the corresponding **Type**. Wildcards are not allowed. **NOTE** Click **Add** to add more than one value.	**/buy/phone/**

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.

2.4.6 Configuring an IP Address Blacklist or Whitelist Rule

By default, all IP addresses are allowed to access your website. You can configure blacklist and whitelist rules to block, log only, or allow access requests from specific 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 Edge WAF**.

Constraints

- Edge WAF 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, and if a whitelist conflicts with a blacklist, the whitelist rule takes priority. If you want to allow only a specific IP address within a range of blocked addresses, add a blacklist rule to block the range and then add a whitelist rule to allow the individual address you wish to allow.
- 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**. Edge WAF will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.

Specification Limitations

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) or upgrade your EdgeSec instance edition to increase such quota.

Impact on the System

If an IP address is added to a blacklist or whitelist, Edge WAF blocks or allows requests from that IP address without checking whether the requests are malicious.

Procedure

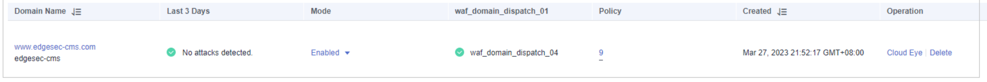
Step 1 **Log in to the management console.**

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 WAF** > **Website Settings**. The **Website Settings** page is displayed.

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

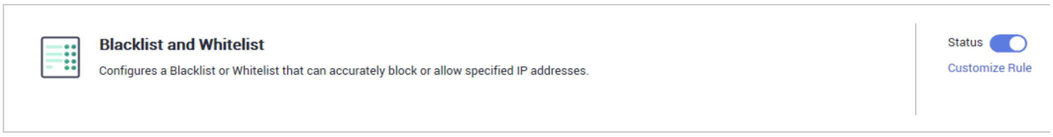
Figure 2-38 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	No attacks detected.	Enabled	waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | Delete

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

Figure 2-39 Blacklist and Whitelist configuration area



Blacklist and Whitelist

Configures a Blacklist or Whitelist that can accurately block or allow specified IP addresses.

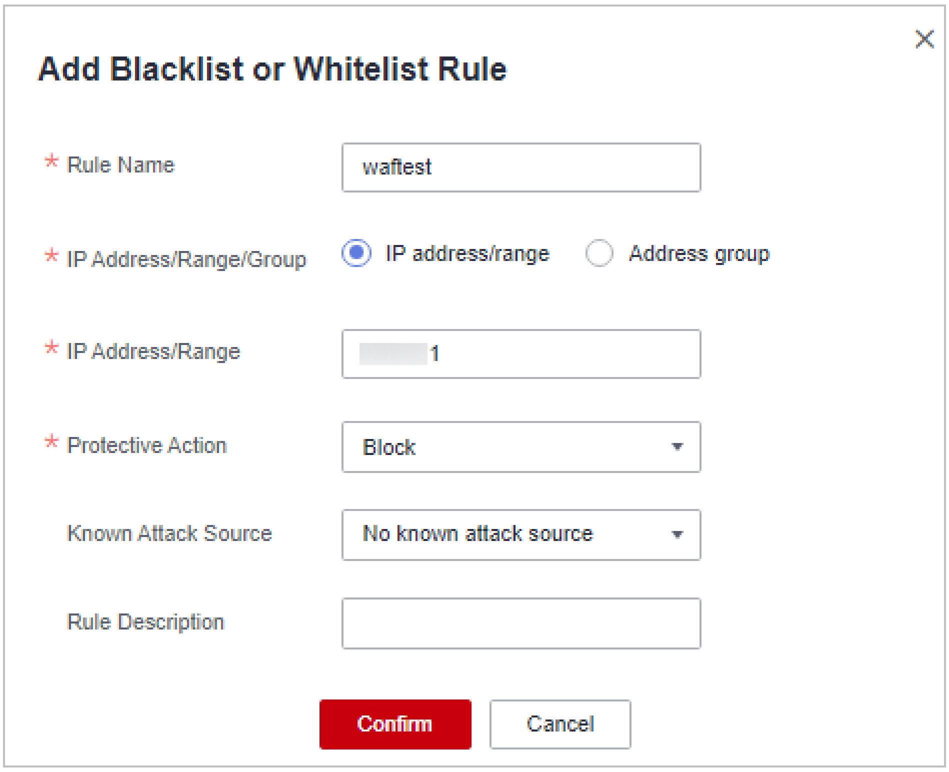
Step 6 In the upper left corner of the **Blacklist and Whitelist** page, click **Add Rule**.

Step 7 In the displayed dialog box, add a blacklist or whitelist rule, as shown in **Figure 2-40**.

NOTE

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

Figure 2-40 Adding a blacklist or whitelist rule



Add Blacklist or Whitelist Rule

* Rule Name: waftest

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

* IP Address/Range: [redacted]1

* Protective Action: Block

Known Attack Source: No known attack source

Rule Description:

Table 2-15 Rule parameters

Parameter	Description	Example Value
Rule Name	Rule name you entered.	waftest
IP Address/ Range/Group	You can select **IP address/ Range** or **Address Group** to add IP addresses a blacklist or whitelist rule.	IP Address/Range
IP Address/ Range	This parameter is mandatory if you select **IP address/range** for **IP Address/Range/Group**. The value can be an IP address or an IP address range. ● IP address: IP address to be added to the blacklist or whitelist ● IP address range: IP address and subnet mask defining a network segment	XXX.XXX.2.3
Select Address Group	This parameter is mandatory if you select **Address group** for IP **Address/Range/Group**. Select an IP address group from the drop-down list. You can also click **Add Address Group** to create an address group. For details, see **Adding a Blacklist or Whitelist IP Address Group**.	-
Protective Action	● **Block**: Select **Block** if you want to blacklist an IP address or IP address range. ● **Allow**: Select **Allow** if you want to whitelist an IP address or IP address range. ● **Log only**: Select **Log only** if you want to observe an IP address or IP address range.	Block
Known Attack Source	If you select **Block** for **Protective Action**, you can select a blocking type of a known attack source rule. Edge WAF 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

Parameter	Description	Example Value
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.

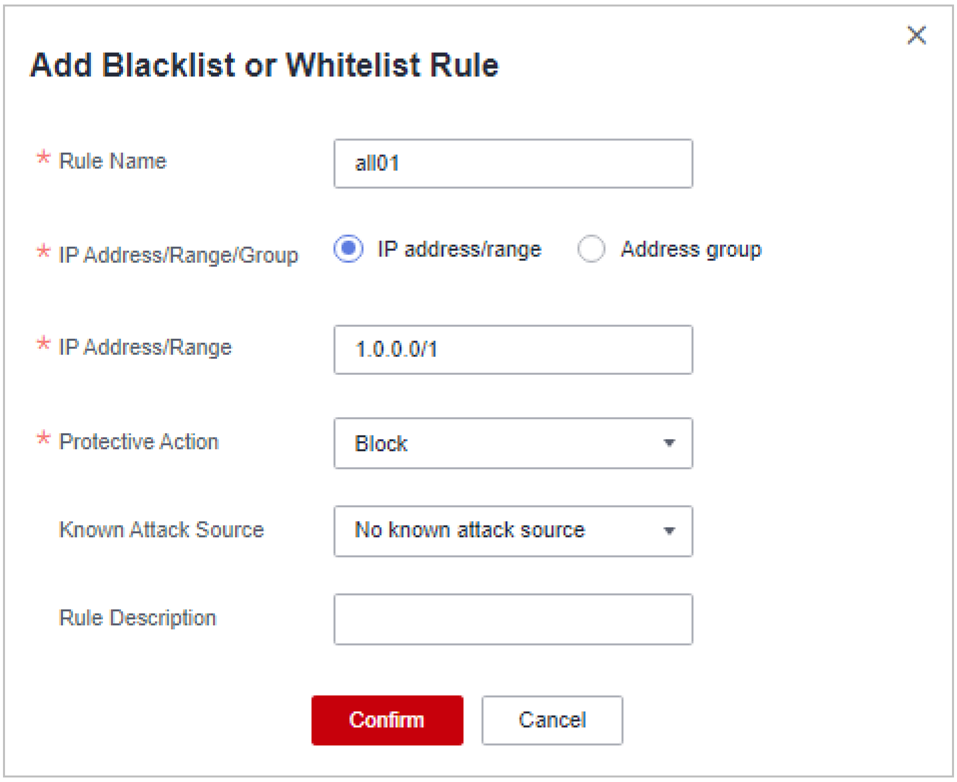
----End

Example Configuration - Allowing a Specified IP Addresses

If domain name *www.example.com* has been connected to Edge WAF, you can perform the following steps to verify the rule takes effect:

Step 1 Add the following two blacklist and whitelist rules to block all IP addresses:

Figure 2-41 Blocking IP address range 1.0.0.0/1



Add Blacklist or Whitelist Rule

* Rule Name: all01

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

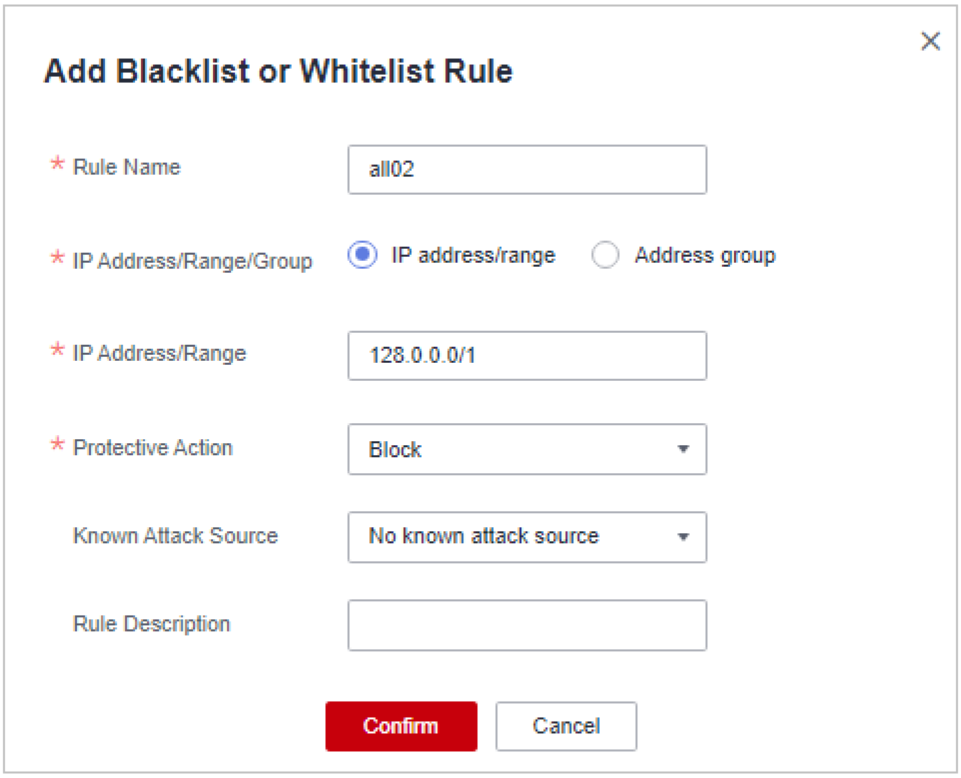
* IP Address/Range: 1.0.0.0/1

* Protective Action: Block

Known Attack Source: No known attack source

Rule Description:

Figure 2-42 Blocking IP address range 128.0.0.0/1



Add Blacklist or Whitelist Rule

* Rule Name: all02

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

* IP Address/Range: 128.0.0.0/1

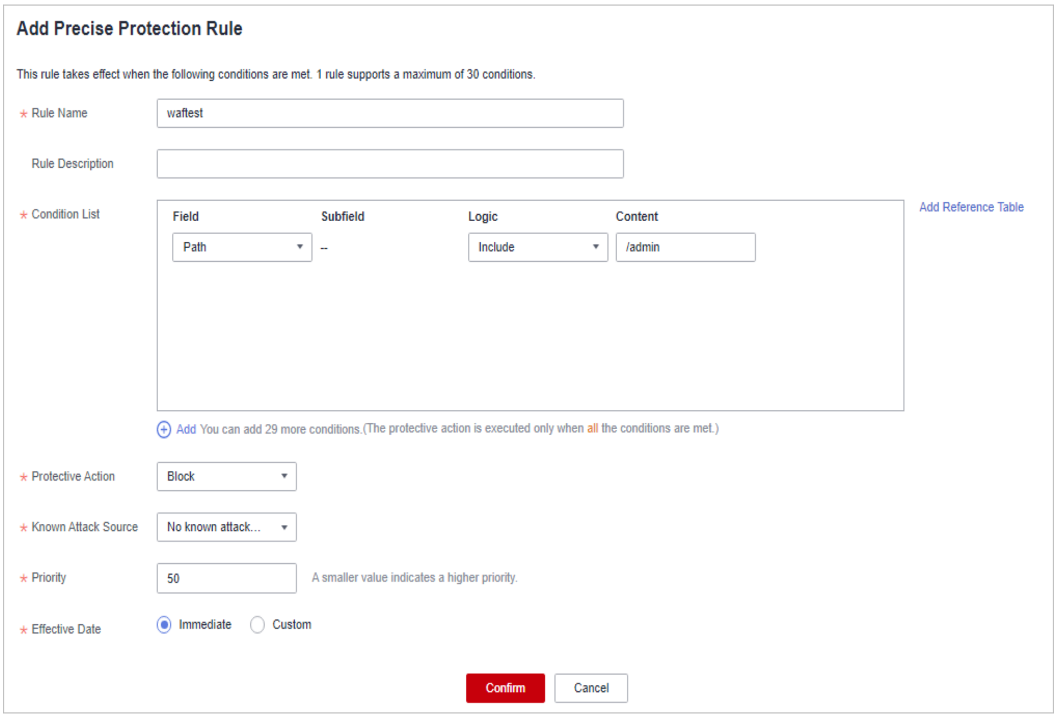
* Protective Action: Block

Known Attack Source: No known attack source

Rule Description:

You can also add a precise protection rule to block all access requests, as shown in **Figure 2-43**.

Figure 2-43 Blocking all access requests



Add Precise Protection Rule

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

* Rule Name: waftest

Rule Description:

* Condition List:

Field	Subfield	Logic	Content
Path	--	Include	/admin

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

* Protective Action: Block

* Known Attack Source: No known attack...

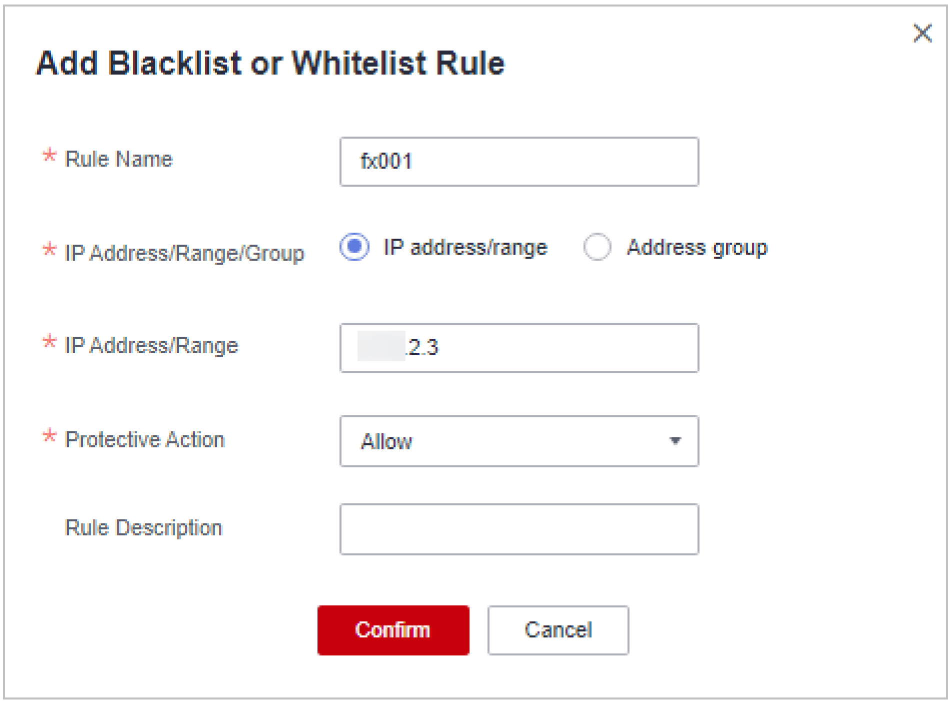
* Priority: 50 A smaller value indicates a higher priority.

* Effective Date: ● Immediate ○ Custom

For details, see **Configuring a Precise Protection Rule**.

Step 2 Refer to **Figure 2-44** and add a whitelist rule to allow a specified IP address, for example, *XXX.XXX.2.3*.

Figure 2-44 Allowing the access of a specified IP address



Add Blacklist or Whitelist Rule

* Rule Name: fx001

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

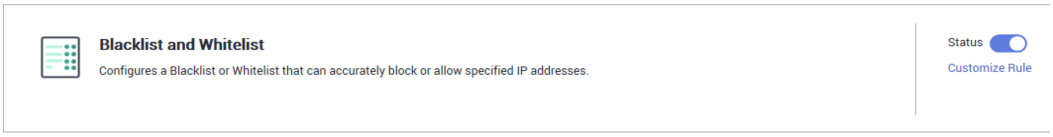
* IP Address/Range: [redacted].2.3

* Protective Action: Allow

Rule Description:

Step 3 Enable the white and blacklist protection.

Figure 2-45 Blacklist and Whitelist configuration area



Blacklist and Whitelist

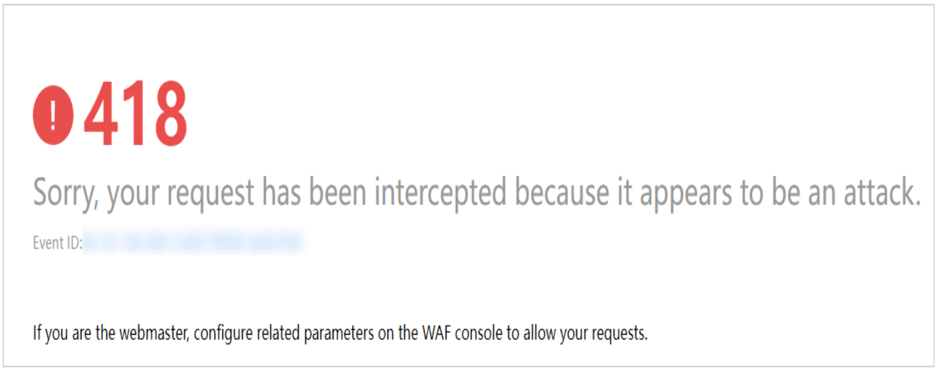
Configures a Blacklist or Whitelist that can accurately block or allow specified IP addresses.

Status: enabled

Step 4 Clear the browser cache and access http://www.example.com.

If the IP address of a visitor is not the one specified in **Step 2**, Edge WAF blocks the access request. **Figure 2-46** shows an example of the block page.

Figure 2-46 Block page



418

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

Event ID: [redacted]

If you are the webmaster, configure related parameters on the WAF console to allow your requests.

Step 5 Go to the EdgeSec console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page.

----End

2.4.7 Configuring a Known Attack Source Rule

If Edge WAF blocks a malicious request by IP address, Cookie, or Params, you can configure a known attack source rule to let Edge WAF 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, Edge WAF 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 Edge WAF**.

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

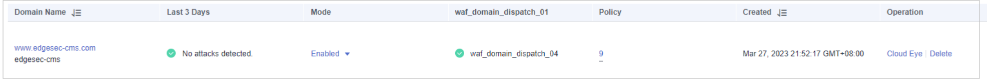
Step 1 **Log in to the management console.**

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 **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

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

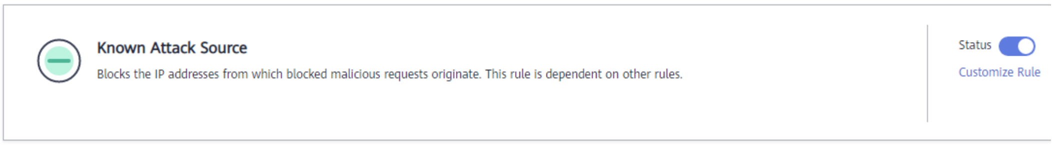
Figure 2-47 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	No attacks detected.	Enabled	waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | 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 2-48 Known Attack Source configuration



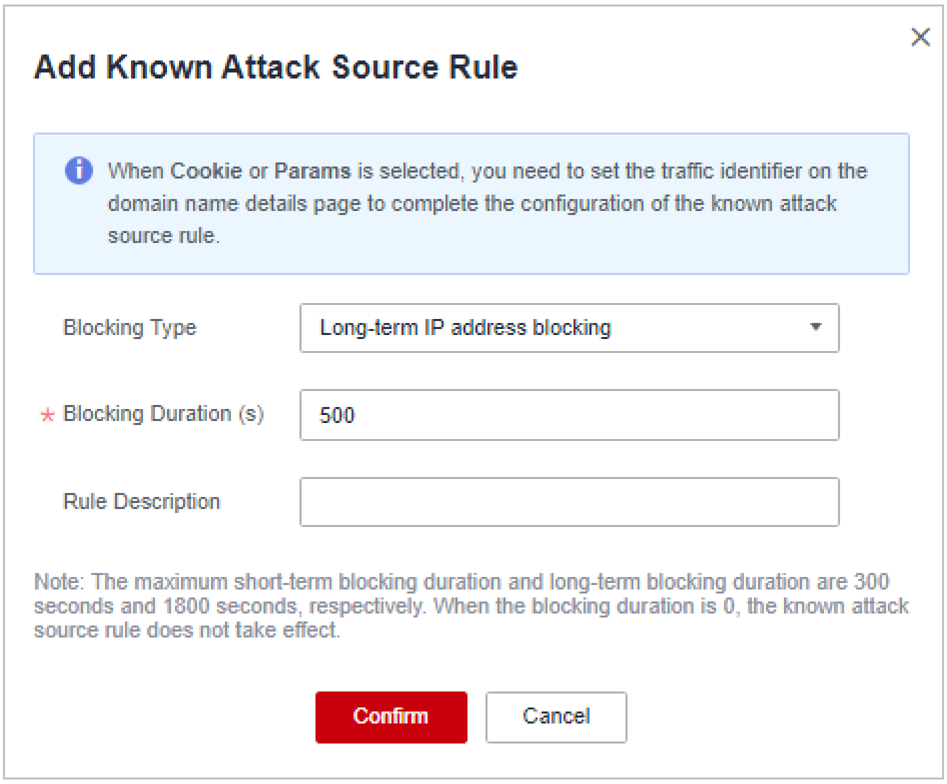
Known Attack Source

Blocks the IP addresses from which blocked malicious requests originate. This rule is dependent on other rules.

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 2-16**.

Figure 2-49 Add Known Attack Source Rule



Add Known Attack Source Rule

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): 500

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.

Table 2-16 Known attack source parameters

Parameter	Description	Example Value
Blocking Type	Specifies the blocking type. The options are: ● **Long-term IP address blocking** ● **Short-term IP address blocking** ● **Long-term Cookie blocking** ● **Short-term Cookie blocking** ● **Long-term Params blocking** ● **Short-term Params blocking**	**Long-term IP address blocking**
Blocking Duration (s)	The blocking duration must be an integer and range from: ● (300, 1800] for long-term blocking ● (0, 300] for short-term blocking	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 row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

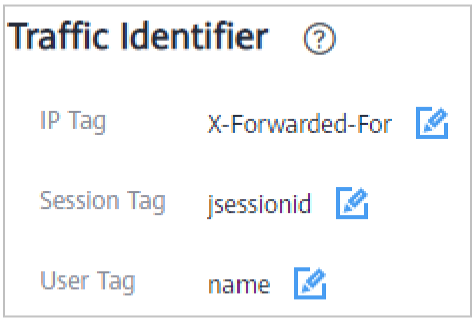
Configuration Example - Blocking Known Attack Source Identified by Cookie

Assume that domain name *www.example.com* has been connected to Edge WAF 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 2-50 Traffic Identifier

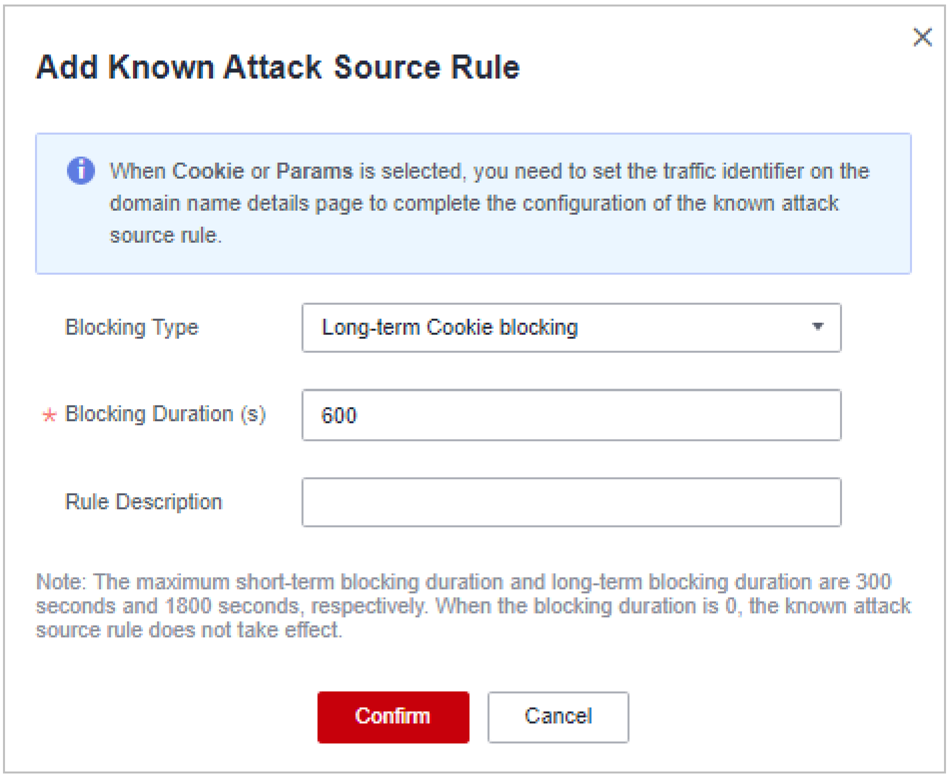


Traffic Identifier

IP Tag	X-Forwarded-For
Session Tag	jsessionid
User Tag	name

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

Figure 2-51 Adding a Cookie-based known attack source rule



Add Known Attack Source Rule

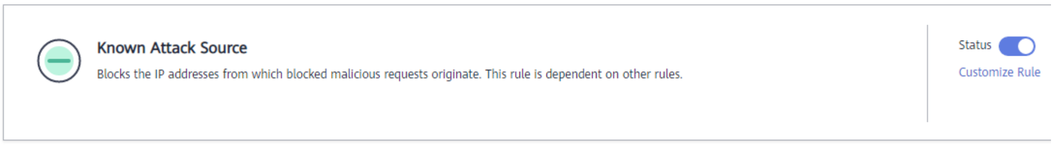
When Cookie or Params is selected, you need to set the traffic identifier on the domain name details page to complete the configuration of the known attack source rule.

Blocking Type	Long-term Cookie blocking
* Blocking Duration (s)	600
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.

Step 4 Enable the known attack source protection.

Figure 2-52 Known Attack Source configuration

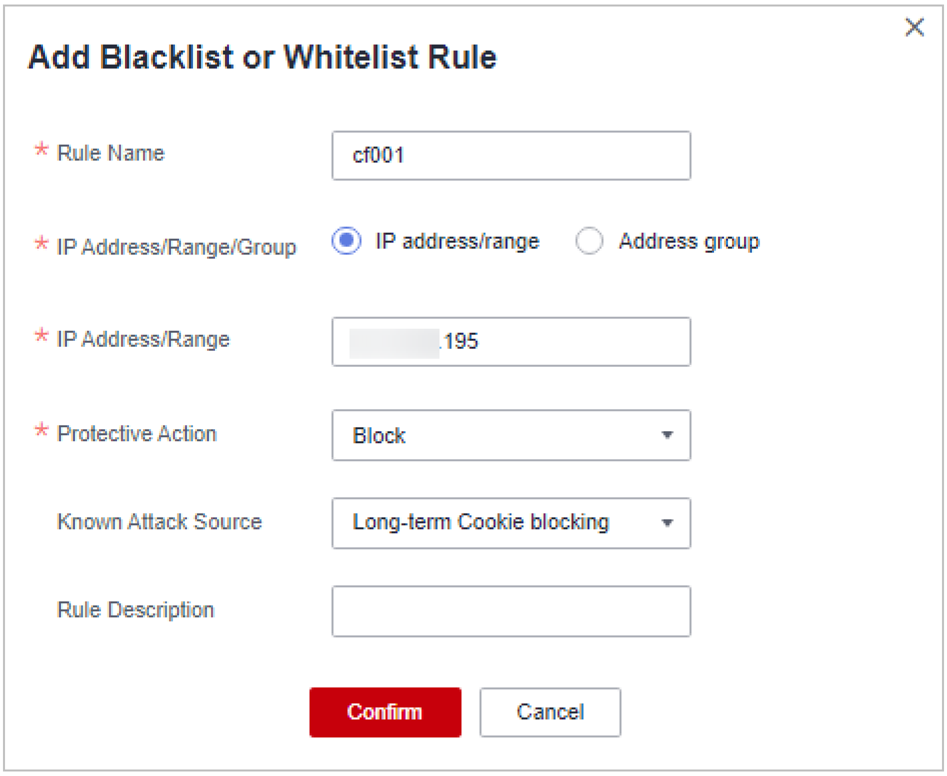


Known Attack Source

Blocks the IP addresses from which blocked malicious requests originate. This rule is dependent on other rules.

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

Figure 2-53 Specifying a known attack source rule



Add Blacklist or Whitelist Rule

* Rule Name: cf001

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

* IP Address/Range: [redacted].195

* Protective Action: Block

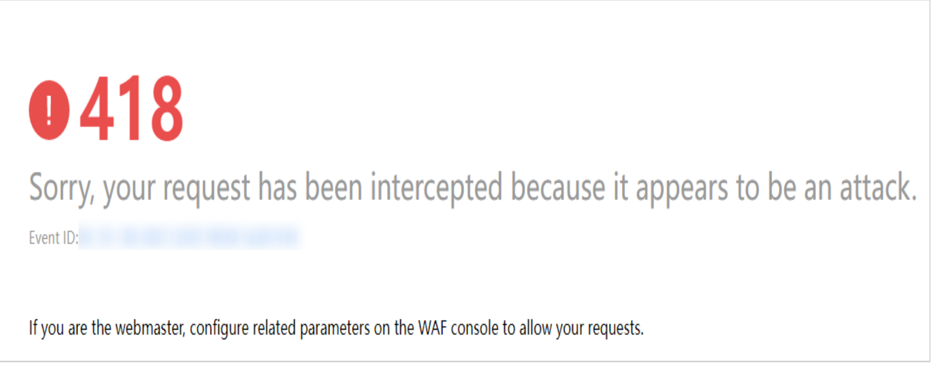
Known Attack Source: Long-term Cookie blocking

Rule Description:

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

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

Figure 2-54 Block page



418

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

Event ID: [redacted]

If you are the webmaster, configure related parameters on the WAF console to allow your requests.

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

----End

2.4.8 Configuring a Geolocation Access Control Rule

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.

To allow only the IP addresses in a certain region to access the protected website, configure a rule by referring to **Configuration Example - Allowing Access Requests from IP Addresses in a Specified Region**.

Prerequisites

A protected website has been added. For details, see **Adding a Website to Edge WAF**.

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.

Procedure

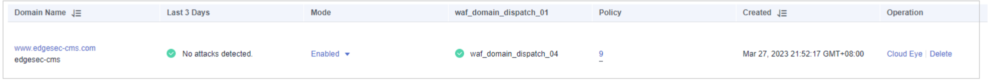
Step 1 **Log in to the management console.**

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 WAF** > **Website Settings**. The **Website Settings** page is displayed.

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

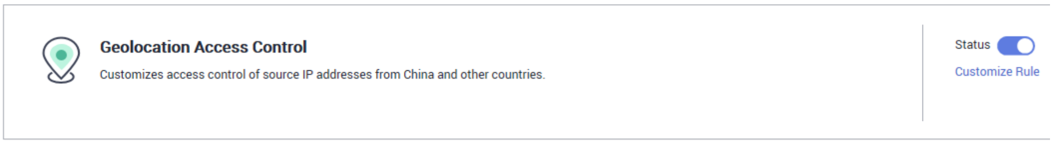
Figure 2-55 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	✓ No attacks detected.	Enabled ▾	✓ waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | Delete

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

Figure 2-56 Geolocation Access Control configuration area



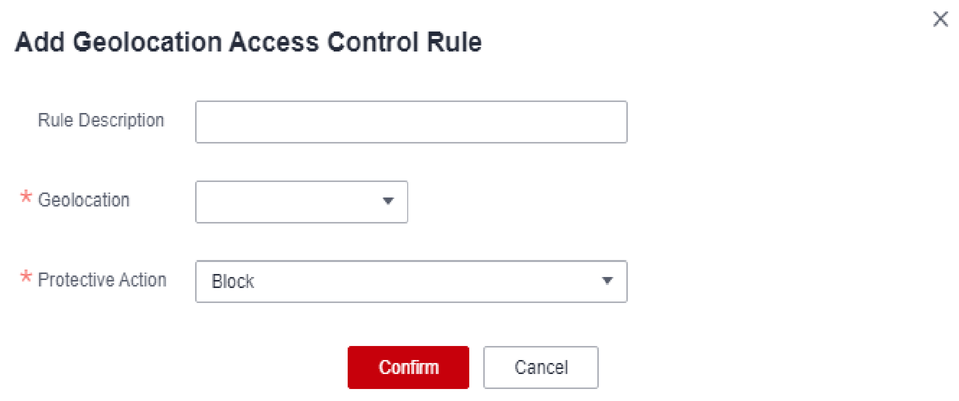
Geolocation Access Control

Customizes access control of source IP addresses from China and other countries.

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 2-17**.

Figure 2-57 Adding a geolocation access control rule



Add Geolocation Access Control Rule

Rule Description

* Geolocation

* Protective Action: Block

Table 2-17 Rule parameters

Parameter	Description	Example Value
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 WAF will take if the rule is hit. You can select **Block**, **Allow**, or **Log only**.	**Block**

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

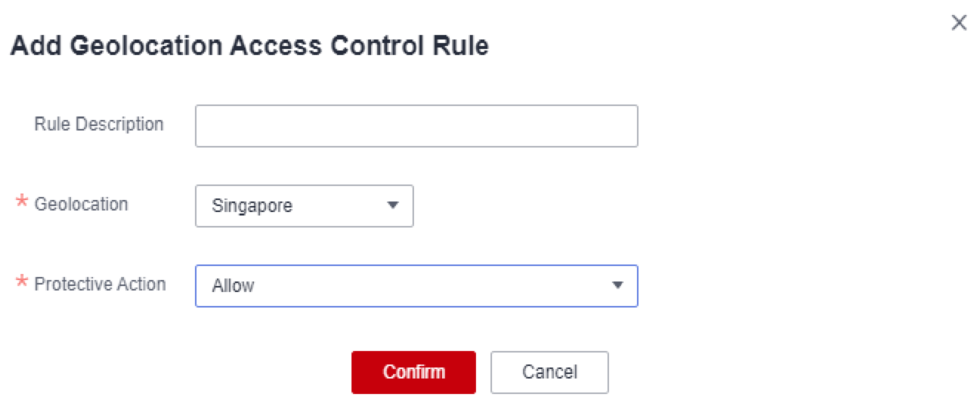
----End

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

Assume that domain name *www.example.com* has been connected to Edge WAF and you want to allow only IP addresses in Singapore, to access the domain name. Perform the following steps:

Step 1 Add a geolocation access control rule: Select **Singapore** for **Geolocation** and select **Allow** for **Protective Action**.

Figure 2-58 Add Geolocation Access Control Rule



Add Geolocation Access Control Rule

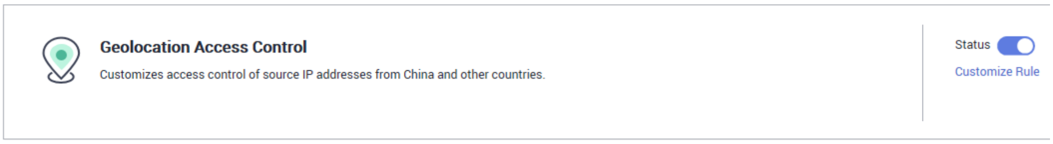
Rule Description

* Geolocation: Singapore

* Protective Action: Allow

Step 2 Enable geolocation access control.

Figure 2-59 Geolocation Access Control configuration area

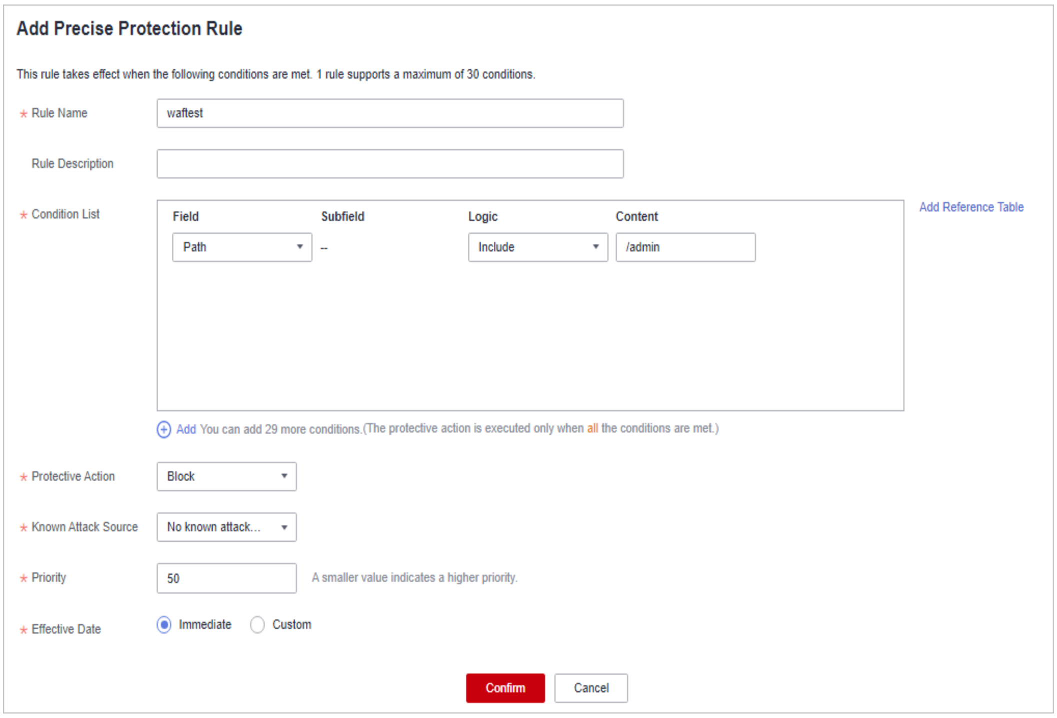


Geolocation Access Control

Customizes access control of source IP addresses from China and other countries.

Step 3 Configure a precise protection rule to block all requests.

Figure 2-60 Blocking all access requests



Add Precise Protection Rule

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

* Rule Name: waftest

Rule Description

* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/admin

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

* Protective Action: Block

* Known Attack Source: No known attack...

* Priority: 50 A smaller value indicates a higher priority.

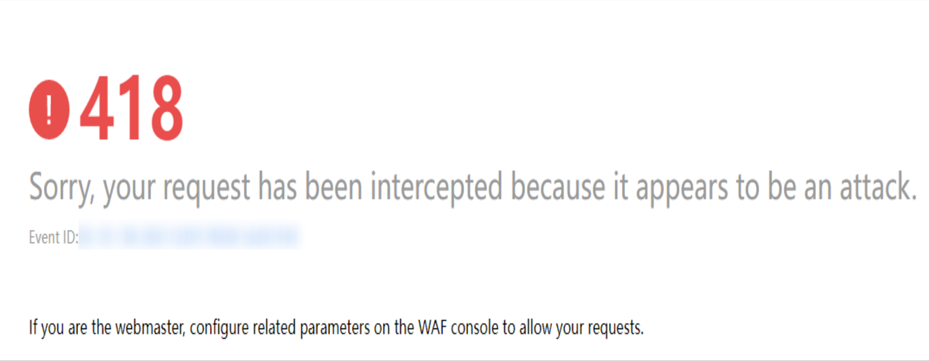
* Effective Date: ● Immediate ○ Custom

For details, see **Configuring a Precise Protection Rule**.

Step 4 Clear the browser cache and access http://www.example.com.

When an access request from IP addresses outside Singapore accesses the page, Edge WAF blocks the access request. **Figure 2-61** shows an example block page.

Figure 2-61 Block page



418

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

Event ID: [redacted]

If you are the webmaster, configure related parameters on the WAF console to allow your requests.

Step 5 Go to the Edge WAF console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page. You will see that all requests not from Shanghai have been blocked.

----End

Protection Effect

To verify WAF 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 Edge WAF by following the instructions in **Adding a Website to Edge WAF**.
- 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, WAF blocks such requests and returns the block page.

----End

2.4.9 Configuring an Anti-Crawler Rule

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 Edge WAF**.

Constraints

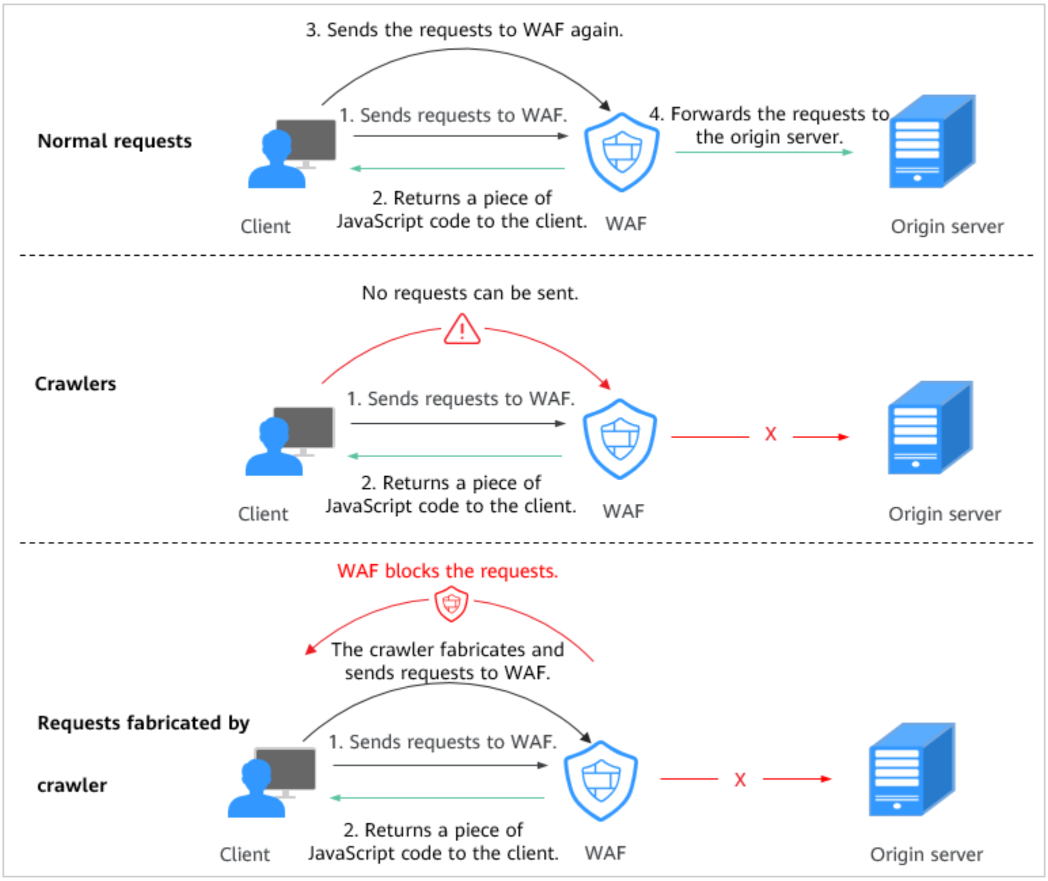
- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.

- 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 2-62 shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

Figure 2-62 JavaScript Anti-Crawler protection process

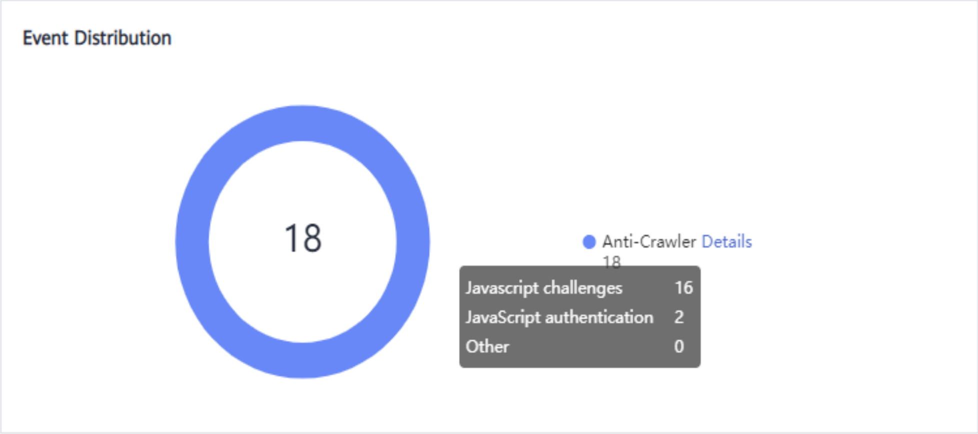

3. Sends the requests to WAF again.
Normal requests
1. Sends requests to WAF.
4. Forwards the requests to the origin server.
2. Returns a piece of JavaScript code to the client.
Client
WAF
Origin server
No requests can be sent.
Crawlers
1. Sends requests to WAF.
X
2. Returns a piece of JavaScript code to the client.
Client
WAF
Origin server
WAF blocks the requests.
The crawler fabricates and sends requests to WAF.
Requests fabricated by crawler
1. Sends requests to WAF.
X
2. Returns a piece of JavaScript code to the client.
Client
WAF
Origin server

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

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

By collecting statistics on the number of JavaScript challenges and authentication responses, the system calculates how many requests the JavaScript anti-crawler defends. In **Figure 2-63**, 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 WAF authentication requests fabricated by the crawler.

Figure 2-63 Parameters of a JavaScript anti-crawler protection rule



NOTICE

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

Procedure

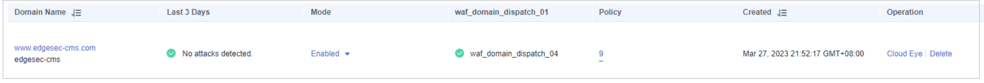
Step 1 Log in to the management console.

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 **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

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

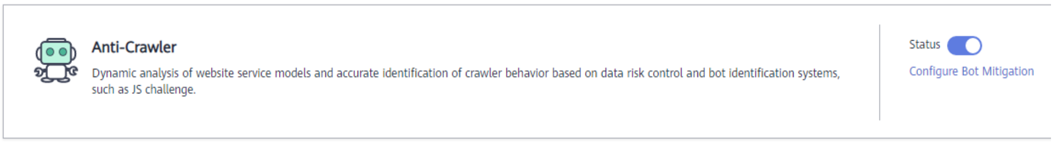
Figure 2-64 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	No attacks detected.	Enabled	waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | 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 2-65 Anti-Crawler configuration area



Anti-Crawler

Dynamic analysis of website service models and accurate identification of crawler behavior based on data risk control and bot identification systems, such as JS challenge.

Status ●

Configure Bot Mitigation

Step 6 Select the **Feature Library** tab and enable the protection by referring to **Figure 2-66**.

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

- **Block**

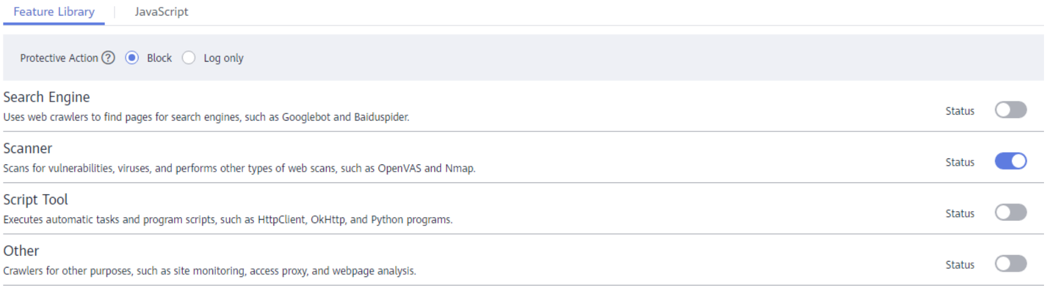
  WAF blocks and logs detected attacks.

- **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 2-66 Feature Library



Feature Library | JavaScript

Protective Action ⓘ ● Block ○ Log only

Search Engine
Uses web crawlers to find pages for search engines, such as Googlebot and Baiduspider. Status ○

Scanner
Scans for vulnerabilities, viruses, and performs other types of web scans, such as OpenVAS and Nmap. Status ●

Script Tool
Executes automatic tasks and program scripts, such as HttpClient, OkHttp, and Python programs. Status ○

Other
Crawlers for other purposes, such as site monitoring, access proxy, and webpage analysis. Status ○

Table 2-18 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, WAF detects and blocks search engine crawlers. **NOTE** If **Search Engine** is not enabled, Edge WAF does not block POST requests from Googlebot or Baiduspider. If you want to block POST requests from Baiduspider, use the configuration described in **Configuration Example - Search Engine**.
Scanner	This rule is used to block scanners, such as OpenVAS and Nmap. A scanner scans for vulnerabilities, viruses, and other jobs.	After you enable this rule, WAF detects and blocks scanner crawlers.

Type	Description	Remarks
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, WAF detects and blocks the execution of automatic tasks and program scripts. **NOTE** If your application uses scripts such as HttpClient, OkHttp, and Python, disable **Script Tool**. Otherwise, WAF will identify such script tools as crawlers and block the application.
Other	This rule is used to block crawlers used for other purposes, such as site monitoring, using access proxies, and web page analysis. **NOTE** To avoid being blocked by WAF, crawlers may use a large number of IP address proxies.	If you enable this rule, WAF 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.

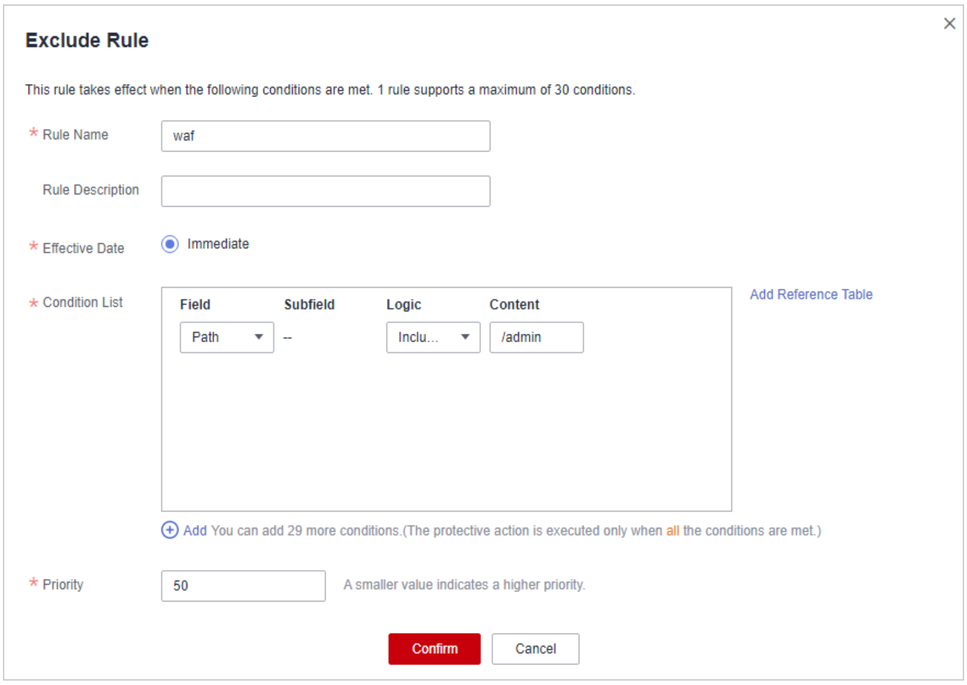
Step 8 Configure a JavaScript-based anti-crawler rule by referring to **Table 2-19**.

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 2-67 Exclude Path



Exclude Rule

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

* Rule Name: waf

Rule Description:

* Effective Date: ● Immediate

* Condition List

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

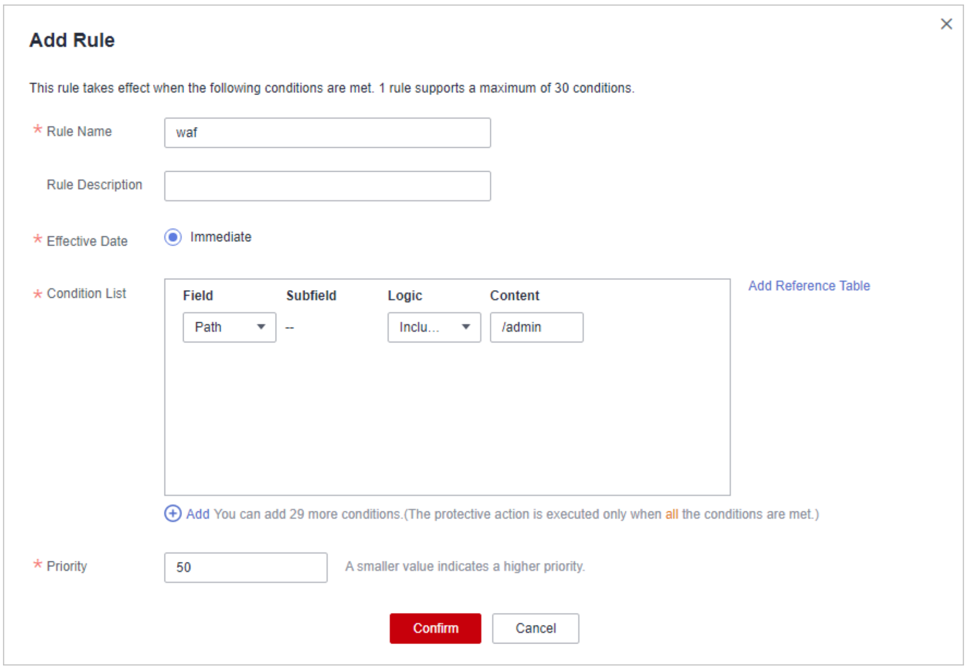
Add Reference Table
⊕ Add You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)

* Priority: 50 A smaller value indicates a higher priority.

- To protect a specified request only

  Set **Protection Mode** to **Protect specified requests**, click **Add Rule**, configure the request rule, and click **Confirm**.

Figure 2-68 Add Rule



Add Rule

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

* Rule Name: waf

Rule Description:

* Effective Date: ● Immediate

* Condition List

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

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

* Priority: 50 A smaller value indicates a higher priority.

Table 2-19 Parameters of a JavaScript-based anti-crawler protection rule

Parameter	Description	Example Value
Rule Name	Name of the rule	waf
Rule Description	A brief description of the rule. This parameter is optional.	-
Effective Date	Time the rule takes effect.	Immediate
Condition List	Parameters for configuring a condition are as follows: ● **Field**: Select the field you want to protect from the drop-down list. Currently, only **Path** and **User Agent** are included. ● **Subfield** ● **Logic**: Select a logical relationship from the drop-down list. **NOTE** If you select **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**, a reference table must be selected for **Content**. For details about reference tables, see **Creating a Reference Table**. ● **Content**: Enter or select the content that matches the condition.	**Path Include /admin**
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 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.

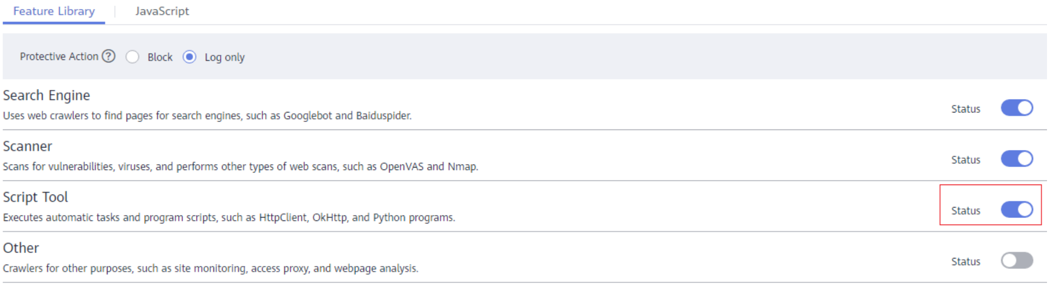
Configuration Example - Logging Script Crawlers Only

To verify that WAF 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 WAF detects an attack, it logs the attack only.)

Figure 2-69 Enabling Script Tool



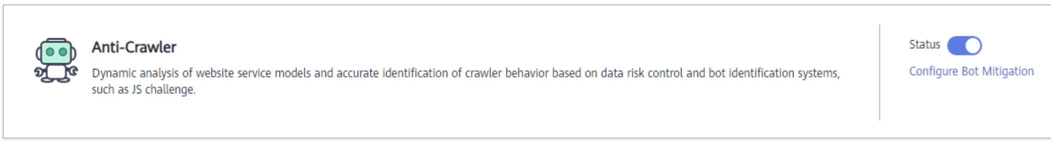
Feature Library | JavaScript

Protective Action ? ○ Block ● Log only

Search Engine Uses web crawlers to find pages for search engines, such as Googlebot and Baiduspider.	Status ●
Scanner Scans for vulnerabilities, viruses, and performs other types of web scans, such as OpenVAS and Nmap.	Status ●
Script Tool Executes automatic tasks and program scripts, such as HttpClient, OkHttp, and Python programs.	Status ●
Other Crawlers for other purposes, such as site monitoring, access proxy, and webpage analysis.	Status ○

Step 3 Enable anti-crawler protection.

Figure 2-70 Anti-Crawler configuration area



Anti-Crawler

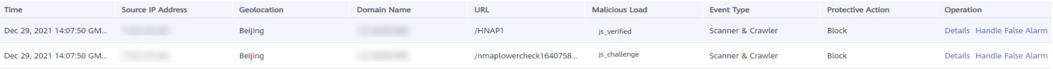
Dynamic analysis of website service models and accurate identification of crawler behavior based on data risk control and bot identification systems, such as JS challenge.

Status ●

Configure Bot Mitigation

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

Figure 2-71 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 GM...	[redacted]	Beijing	[redacted]	/HNAP1	js_verified	Scanner & Crawler	Block	Details Handle False Alarm
Dec 29, 2021 14:07:50 GM...	[redacted]	Beijing	[redacted]	/nmaplowercheck1640758...	js_challenge	Scanner & Crawler	Block	Details Handle False Alarm

----End

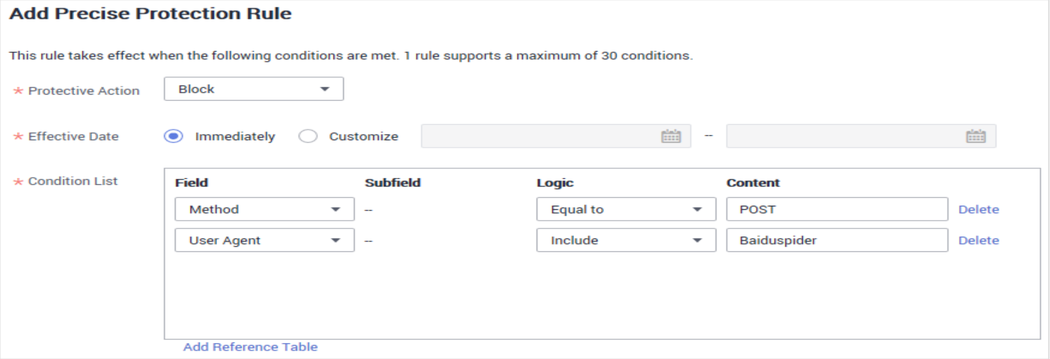
Configuration Example - Search Engine

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 2-72 Blocking POST requests



Add Precise Protection Rule

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

* Protective Action: Block

* Effective Date: ● Immediately ○ Customize

* Condition List

Field	Subfield	Logic	Content	
Method	--	Equal to	POST	Delete
User Agent	--	Include	Baiduspider	Delete

Add Reference Table

----End

2.4.10 Configuring a Global Protection Whitelist (Formerly False Alarm Masking) Rule

When WAF 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 WAF ignore certain rule IDs or event types (for example, skip XSS checks for a specific URL).

- If you select **All protection** for **Ignore WAF Protection**, all WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule.
- If you select **Basic Web Protection** for **Ignore WAF 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 Edge WAF**.

Constraints

- If you select **All protection** for **Ignore WAF Protection**, all WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule.
- If you select **Basic web protection** for **Ignore WAF Protection**, global protection whitelist (formerly false alarm masking) rules take effect only for events triggered against WAF 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 (formerly false alarm masking) rule by referring to **Handling False Alarms**. After handling a false alarm, you can view the rule in the global protection whitelist (formerly false alarm masking) rule list.

Procedure

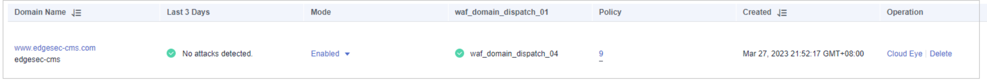
Step 1 **Log in to the management console.**

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 **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

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

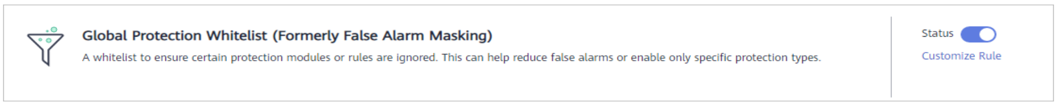
Figure 2-73 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	No attacks detected.	Enabled	waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | Delete

Step 5 In the **Global Protection Whitelist (Formerly False Alarm Masking)** configuration area, change **Status** as required and click **Customize Rule**.

Figure 2-74 Global Protection Whitelist configuration area



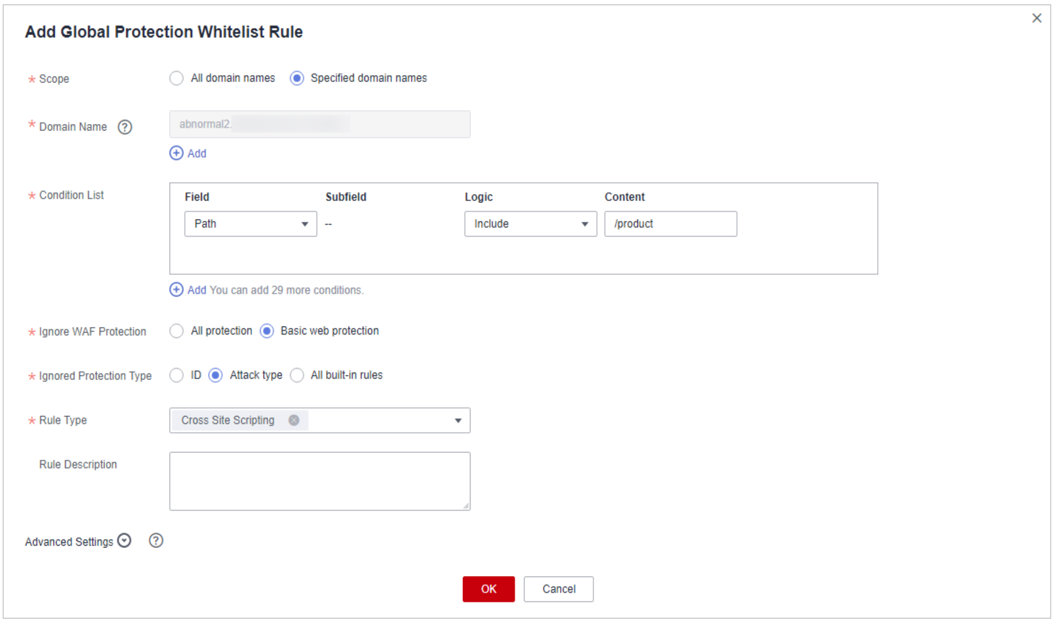
Global Protection Whitelist (Formerly False Alarm Masking)

A whitelist to ensure certain protection modules or rules are ignored. This can help reduce false alarms or enable only specific protection types.

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 2-20**.

Figure 2-75 Add Global Protection Whitelist Rule



Add Global Protection Whitelist Rule

* Scope: ○ All domain names ● Specified domain names

* Domain Name: abnormal2[redacted]

⊕ Add

* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/product

⊕ Add You can add 29 more conditions.

* Ignore WAF Protection: ○ All protection ● Basic web protection

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

* Rule Type: Cross Site Scripting

Rule Description:

Advanced Settings

Table 2-20 Parameters

Parameter	Description	Example Value
Scope	- **All domain names**: By default, this rule will be used to all domain names that are protected by the current policy. - **Specified domain names**: This rule will be used to the specified domain names that match the wildcard domain name being protected by the current policy.	Specified domain names
Domain Name	This parameter is mandatory when you select **Specified domain names** for **Scope**. Enter a single domain name that matches the wildcard domain name being protected by the current policy.	www.example.com

Parameter	Description	Example Value
Condition List	Click **Add** 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: Parameters for configuring a condition are described as follows: ● Field ● **Subfield**: Configure this field only when **Params**, **Cookie**, or **Header** is selected for **Field**. **NOTICE** The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. ● **Logic**: Select a logical relationship from the drop-down list. ● **Content**: Enter or select the content that matches the condition.	Path, Include, / product
Ignore WAF Protection	● **All protection**: All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule. ● **Basic Web 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.	Basic Web Protection
Ignored Protection Type	If you select **Basic web protection** for **Ignored Protection Type**, specify the following parameters: ● **Attack type**: Configure the rule by attack type, such as XSS and SQL injection. One type contains one or more rule IDs. ● **All built-in rules**: all checks enabled in **Basic Web Protection**.	Attack type

Parameter	Description	Example Value
Attack type	This parameter is mandatory when you select **Attack type** for **Ignored Protection Type**. Select an attack type from the drop-down list box. WAF can defend against XSS attacks, web shells, SQL injection attacks, malicious crawlers, remote file inclusions, local file inclusions, command injection attacks, and other attacks.	SQL injection
Rule Description	A brief description of the rule. This parameter is optional.	SQL injection attacks are not intercepted.
Advanced Settings	To ignore attacks of a specific field, specify the field in the **Advanced Settings** area. After you add the rule, WAF will stop blocking attack events of the specified field. Select a target field from the first drop-down list box on the left. The following fields are supported: **Params**, **Cookie**, **Header**, **Body**, and **Multipart**. ● If you select **Params**, **Cookie**, or **Header**, you can select **All** or **Specified field** to configure a subfield. ● If you select **Body** or **Multipart**, you can select **All**. ● If you select **Cookie**, the **Domain Name** and **Path** can be empty. **NOTE** If **All** is selected, WAF will not block all attack events of the selected field.	Params All

Step 8 Click **OK**.

----End

Other Operations

- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a global protection whitelist (formerly false alarm masking) rule, click **Modify** in the row containing the rule.
- To delete a global protection whitelist (formerly false alarm masking) rule, click **Delete** in the row containing the rule.

2.4.11 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.

Prerequisites

A protected website has been added. For details, see **Adding a Website to Edge WAF**.

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

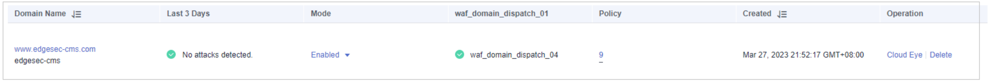
Step 1 **Log in to the management console.**

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 **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

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

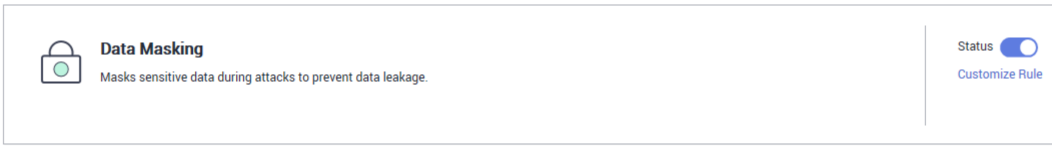
Figure 2-76 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	✓ No attacks detected.	Enabled ▾	✓ waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | Delete

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

Figure 2-77 Data Masking configuration area



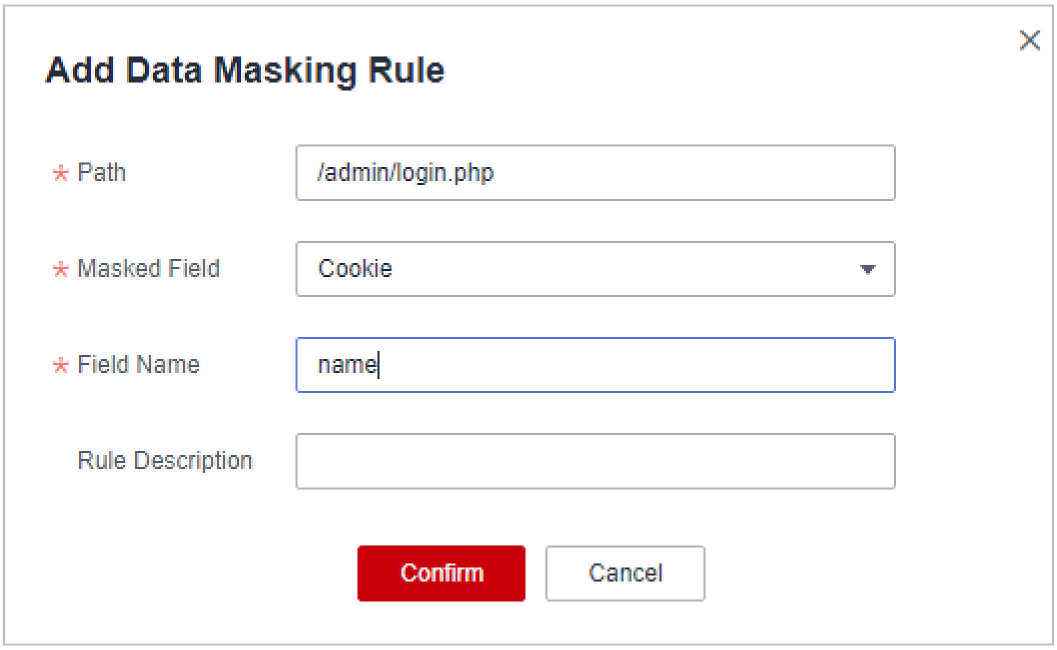
Data Masking

Masks sensitive data during attacks to prevent data leakage.

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 described in **Table 2-21**.

Figure 2-78 Adding a data masking rule



Add Data Masking Rule

* Path: /admin/login.php

* Masked Field: Cookie

* Field Name: name

Rule Description:

Table 2-21 Rule parameters

Parameter	Description	Example Value
Path	Part of the URL that does not include the domain name. ● Prefix match: The path ending with * indicates that the path is used as a prefix. For example, if the path to be protected is **/admin/test.php** or **/adminabc**, set **Path** to **/admin***. ● Exact match: The path to be entered must match the path to be protected. If the path to be protected is **/admin**, set **Path** to **/admin**. NOTE ● The path supports prefix and exact matches only and does not support regular expressions. ● The path cannot contain two or more consecutive slashes. For example, **///admin**. If you enter **///admin**, WAF converts **///** to **/**.	**/admin/login.php** For example, if the URL to be protected is **http://www.example.com/admin/login.php**, set **Path** to **/admin/login.php**.

Parameter	Description	Example Value
Masked Field	A field set to be masked ● **Params**: A request parameter ● **Cookie**: A small piece of data to identify web visitors ● **Header**: A user-defined HTTP header ● **Form**: A form parameter	● If **Masked Field** is **Params** and **Field Name** is **id**, content that matches **id** is masked. ● If **Masked Field** is **Cookie** and **Field Name** is **name**, content that matches **name** is masked.
Field Name	Set the parameter based on **Masked Field**. The masked field will not be displayed in logs. **NOTICE** The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.	
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

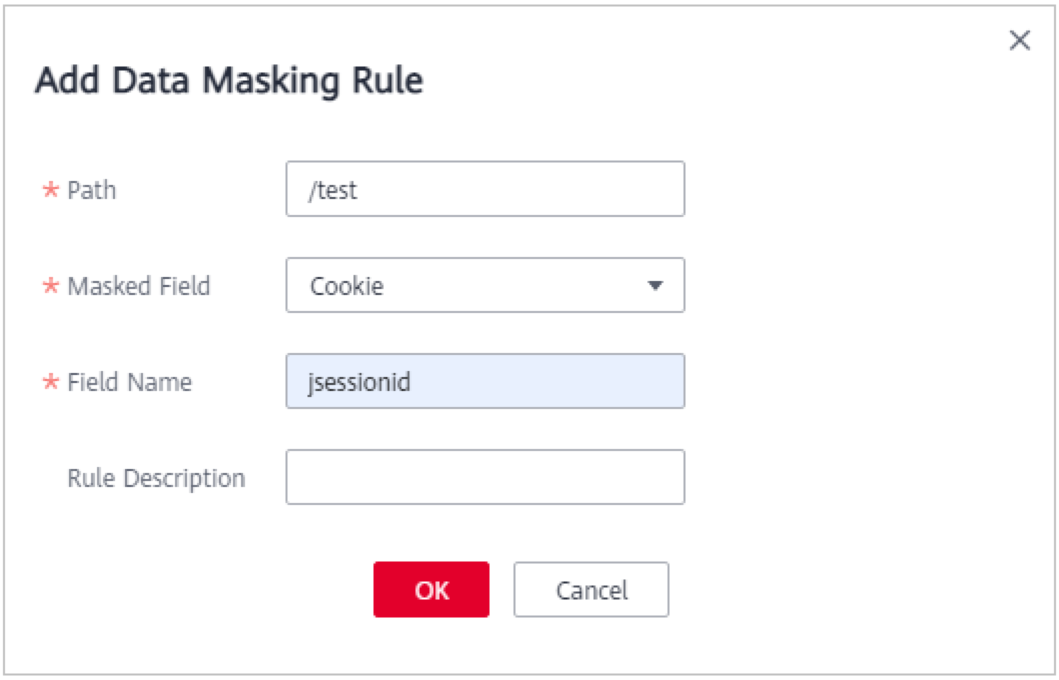
- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

Configuration Example - Masking the Cookie Field

To verify that WAF 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 2-79 Select **Cookie** for **Masked Field** and enter **jsessionid** in **Field Name**.



Add Data Masking Rule

* Path: /test

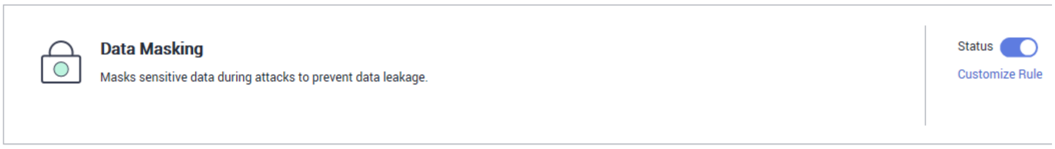
* Masked Field: Cookie

* Field Name: jsessionid

Rule Description:

Step 2 Enable data masking.

Figure 2-80 Data Masking configuration area



Data Masking

Masks sensitive data during attacks to prevent data leakage.

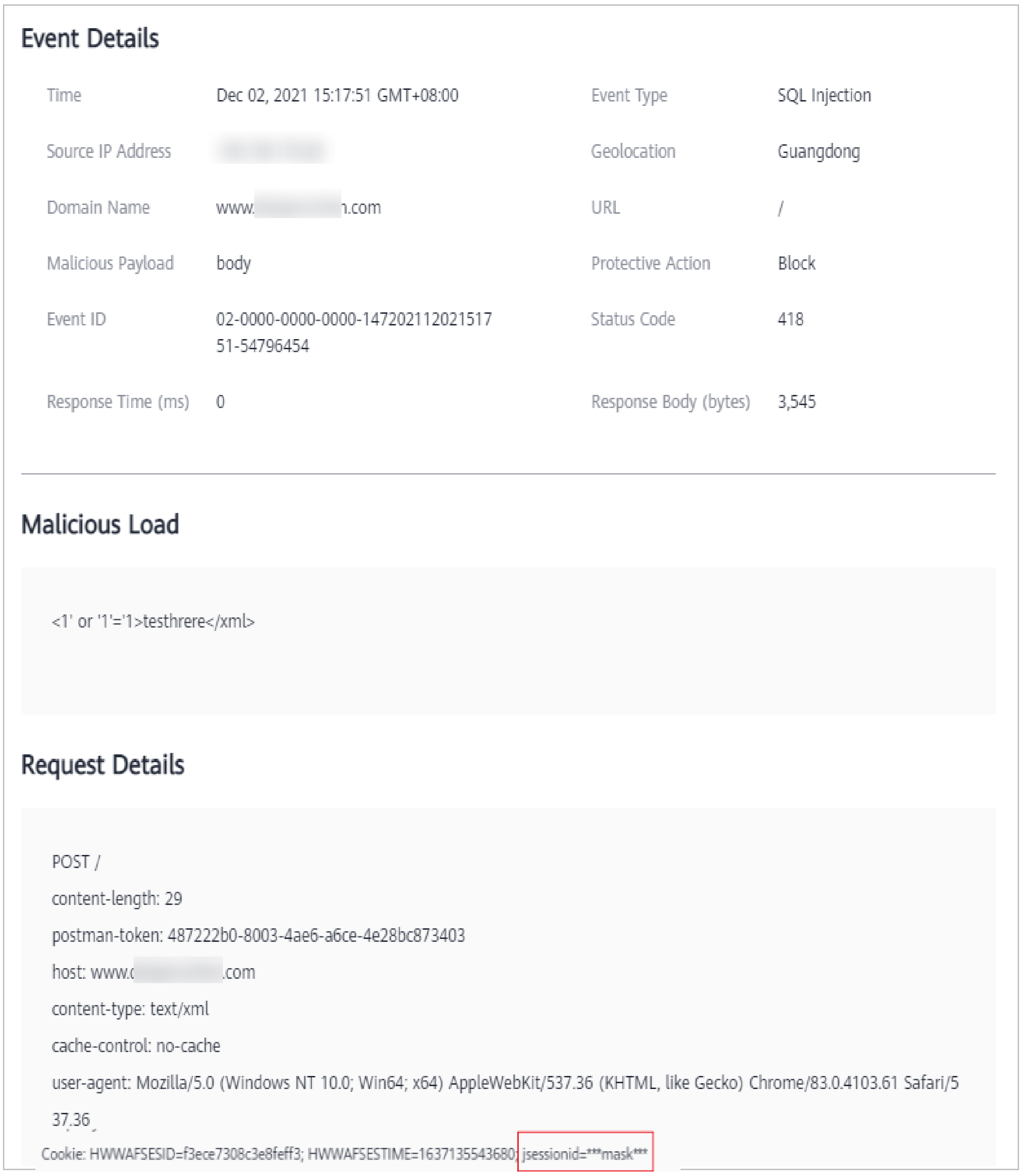
Status: on

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 2-81 Viewing events - privacy data masking



Event Details

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 51-54796454	Status Code	418
Response Time (ms)	0	Response Body (bytes)	3,545

Malicious Load

```
<1' or '1'='1>testhrere</xml>
```

Request Details

```
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/5
37.36
Cookie: HWWAFSESID=f3ece7308c3e8feff3; HWWAFSESTIME=1637135543680; jsessionid=***mask***
```

----End

2.5 Website Settings

2.5.1 Adding a Website to Edge WAF

This section describes how to add a domain name to Edge WAF so that the website traffic can pass through Edge WAF. After you connect a domain name to Edge WAF, Edge WAF works as a reverse proxy between the client and the server. The real IP address of the server is hidden and only the IP address of Edge WAF is visible to web visitors.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and add domain names of websites to be protected in the project.

Prerequisites

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

Constraints

- Only website domain names on the **Domains** page on the CDN console can be added. For details about the service types, see **Adding a Domain Name**.
- A protected domain name can only be added to Edge WAF once.

Specification Limitations

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

Procedure

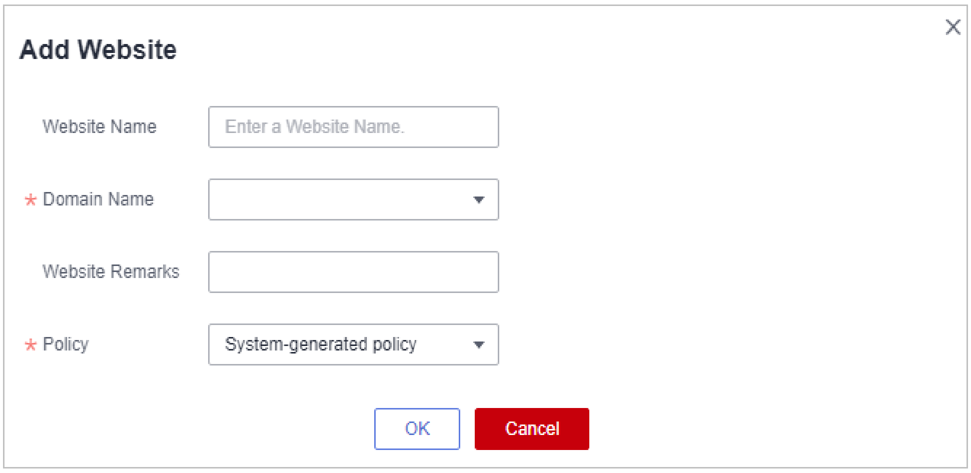
Step 1 **Log in to the management console.**

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 **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

Step 4 In the upper left corner of the list, click **Add Website**. For details about the parameters, see **Table 2-22**.

Figure 2-82 Adding a website



Add Website

Website Name: Enter a Website Name.

* Domain Name:

Website Remarks:

* Policy: System-generated policy

Table 2-22 Parameters for adding a protected website

Parameter	Description
Website Name	Name of the website you want to protect. It must meet the following requirements: ● The name must be unique. ● The name must start with a letter. ● The length cannot exceed 128 characters. ● The value can contain uppercase letters, lowercase letters, digits, and special characters (-_:).
Domain Name	Select a domain name to be protected. You can only select a domain name whose **Service Type** is **Website** on the **Domains** page of CDN.
Website Remarks	A brief description of the website
Policy	The **System-generated policy** is selected by default. You can select a policy you configured before.
Certificate Name	If a domain name using the HTTPS protocol is selected for **Domain Name**, you are required to configure a certificate on Edge WAF and associate the certificate with the domain name. For details about how to manage certificates, see **Certificate Management**.

Step 5 Click **OK**.

----End

2.5.2 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.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and view domain names in the project.

Prerequisites

A protected website has been added. For details, see **Adding a Website to Edge WAF**.

Procedure

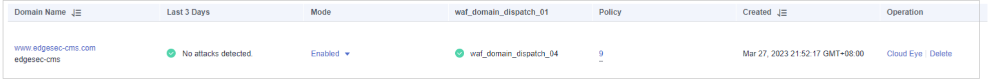
Step 1 **Log in to the management console.**

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 WAF** > **Website Settings**. The **Website Settings** page is displayed.

Step 4 View the protected website information, as shown in **Figure 2-83**. For details about the parameters, see **Table 2-23**.

Figure 2-83 Website list



Domain Name	Last 3 Days	Mode	waf_domain_dispatch_01	Policy	Created	Operation
www.edgesec-cms.com edgesec-cms	✓ No attacks detected.	Enabled ▾	✓ waf_domain_dispatch_04	9	Mar 27, 2023 21:52:17 GMT+08:00	Cloud Eye | Delete

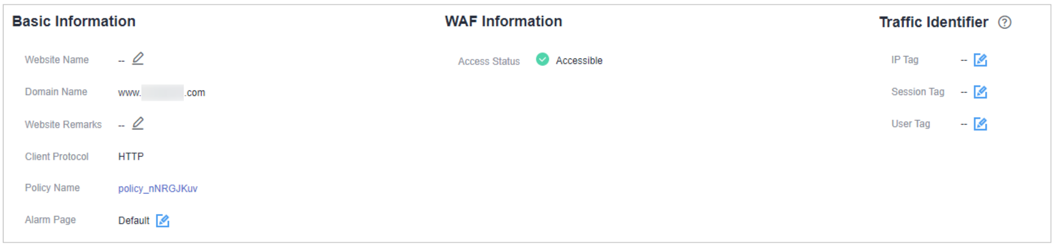
Table 2-23 Website list parameters

Parameter	Description
Domain Name	Protected domain name
Last 3 Days	Protection status of the domain name over the past three days
Mode	Edge WAF mode of the protected domain name Click ▾ to select one of the following protection modes: ● **Enabled** ● **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 Edge WAF only forwards requests. It does not scan for attacks. This mode is risky. You are advised to reduce false alarms by **Configuring a Global Whitelist (Originally False Alarm Masking) Rule**.
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 **Configuring Protection Rules**.
Created	Time the website was added
Operation	● Click **Cloud Eye** to switch to Cloud Eye and view the monitoring information about the protected website. ● To remove a protected website from Edge WAF, click **Delete**.

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 2-84**.

Figure 2-84 Viewing the basic information



Basic Information

Website Name --

Domain Name www.[redacted].com

Website Remarks --

Client Protocol HTTP

Policy Name policy_nNRGJKuv

Alarm Page Default

WAF Information

Access Status ✓ Accessible

Traffic Identifier ?

IP Tag --

Session Tag --

User Tag --

- 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

2.5.3 Switching Working Mode

You can switch the working mode of Edge WAF.

> **NOTE**
>
> If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your Edge WAF instance locates. Then, you can select the enterprise project from the **Enterprise Project** drop-down list and switch Edge WAF working mode for a specific domain name.

Prerequisites

A protected website has been added. For details, see **Adding a Website to Edge WAF**.

Application Scenarios

- **Enabled**: In this mode, WAF 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 WAF only forwards requests. It does not scan for or log attacks. This mode is risky. You are advised to use the global protection whitelist (formerly false alarm masking) rules to reduce false alarms.

Impact on the System

In the Suspended mode, your website is not protected because WAF 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

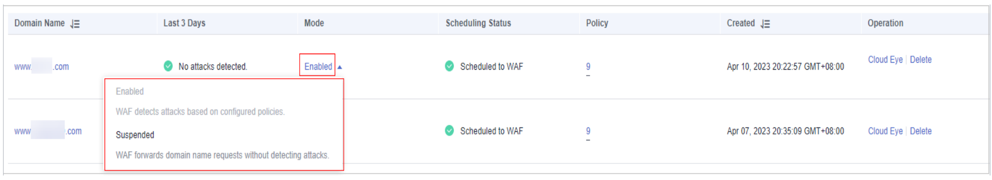
Step 1 **Log in to the management console.**

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 **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

Step 4 In the row containing the target domain name, click ▼ in the **Mode** column and select a mode you want.

Figure 2-85 Switching working mode



Domain Name	Last 3 Days	Mode	Scheduling Status	Policy	Created	Operation
www.[redacted].com	No attacks detected.	Enabled ▲	Scheduled to WAF	9	Apr 10, 2023 20:22:57 GMT+08:00	Cloud Eye | Delete
www[redacted].com			Scheduled to WAF	9	Apr 07, 2023 20:35:09 GMT+08:00	Cloud Eye | Delete

Enabled
WAF detects attacks based on configured policies.
Suspended
WAF forwards domain name requests without detecting attacks.

- **Enabled**: In this mode, WAF 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 WAF only forwards requests. It does not scan for or log attacks. This mode is risky. You are advised to use the global protection whitelist (formerly false alarm masking) rules to reduce false alarms.

----End

Other Operations

- **Handling False Alarms**

2.5.4 Configuring a Traffic Identifier for a Known Attack Source

Edge WAF 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**.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your Edge WAF instance locates. Then, you can select the project from the **Enterprise Project** drop-down list and configure known attack source traffic identifiers for the domain names.

Prerequisites

A protected website has been added. For details, see **Adding a Website to Edge WAF**.

Constraints

- If the IP address tag is not configured, Edge WAF identifies the client IP address by default.
- 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.

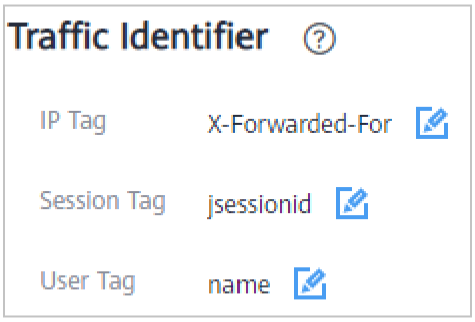
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

Step 3 In the navigation pane on the left, choose **Edge WAF** > **Website Settings**. The **Website Settings** page is displayed.

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 **IP Tag**, **Session Tag**, or **User Tag** to configure a traffic identifier by referring to **Table 2-24**.

Figure 2-86 Traffic Identifier



Traffic Identifier ⓘ

IP Tag X-Forwarded-For ✎

Session Tag jsessionid ✎

User Tag name ✎

Table 2-24 Traffic identifier parameters

Identifier	Description	Example Value
IP Tag	HTTP request header field of the original client IP address. If there are multiple field names separated by commas (,), WAF reads the fields from left to right to obtain the client IP address. For example, for **X-Forwarded-For,CDN-Src-IP,X-real-IP**, WAF obtains the client IP address from the **X-Forwarded-For** field first. If this field has no value, WAF then obtains the value from other fields in sequence. If there is no field configured by the customer, WAF obtains the source IP address in the TCP connection by default.	X-Forwarded-For
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.	jssessionid
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

2.6 Certificate Management

2.6.1 Uploading a Certificate

You can upload a certificate to Edge WAF. Then you can directly select the uploaded certificate for the protected website.

Prerequisites

You have obtained the certificate file and certificate private key.

Specification Limitations

You can upload as many certificates in Edge WAF as the number of domain names that can be protected by your Edge WAF instances in the same account. For example, if you purchase a basic edition Edge WAF instance, which can protect 10 domain names, and a domain name expansion package, which can protect 20 domain names, your Edge WAF instance can protect 30 domain names total. In this case, you can upload 30 certificates.

Constraints

If you import a new certificate when adding a protected website or updating a certificate, the certificate is added to the certificate list on the **Certificates** page, and the imported certificate is also counted towards your total certificate quota.

Procedure

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

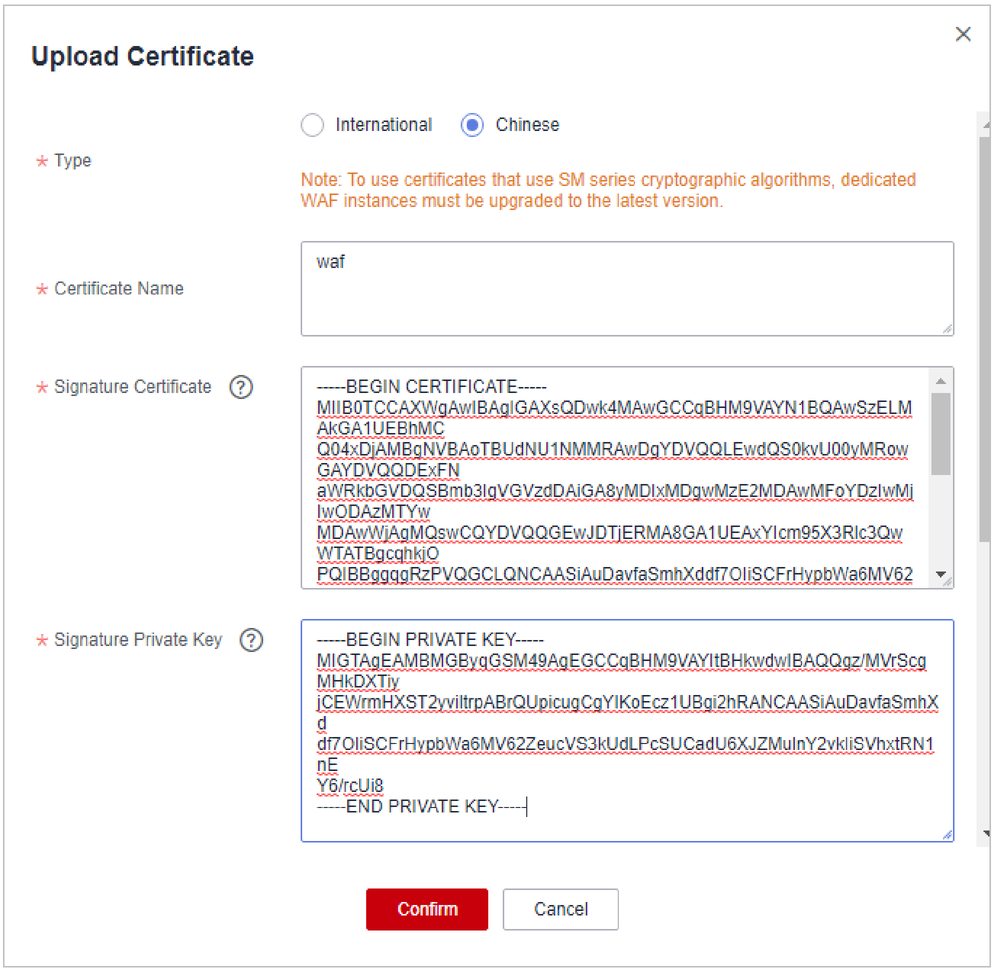
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

Step 3 In the navigation pane on the left, choose **Edge WAF** > **Certificates**.

Step 4 Click **Upload Certificate** in the upper left corner.

Step 5 In the **Upload Certificate** dialog box, enter a certificate name, and copy the certificate file and private key into the corresponding text boxes.

Figure 2-87 Uploading a certificate



Upload Certificate

* Type: ○ International ● Chinese

Note: To use certificates that use SM series cryptographic algorithms, dedicated WAF instances must be upgraded to the latest version.

* Certificate Name: waf

* Signature Certificate

```
-----BEGIN CERTIFICATE-----
MIIB0TCCAXWgAwIBAgIGAXsQDwk4MAwGCCqBHM9VAYN1BQAwSzELM
AkGA1UEBhMC
Q04xDjAMBgNVBAoTBUdNU1NMMRAwDgYDVQQLEwdQS0kvU00yMRow
GAYDVQQDExFN
aWRkbGVDQSBmb3IgVGVzdDAiGA8yMDIxMDgwMzE2MDAwMFoYDzIwMj
IwODAzMTYw
MDAwWjAgMQswCQYDVQQGEwJDTjERMA8GA1UEAxYIcm95X3Rlc3Qw
WTATBgcqhkjO
PQIBBggqgRzPVQGCLQNCAASiAuDavfaSmhXddf7OliSCFrHypbWa6MV62
```

* Signature Private Key

```
-----BEGIN PRIVATE KEY-----
MIGTAgEAMBMGByqGSM49AgEGCCqBHM9VAYItBHkwdwIBAQQgz/MVrScg
MHkDXTiy
jCEWrmHXST2yviltrpABrQUpicugCgYIKoEcz1UBgi2hRANCAASiAuDavfaSmhX
d
df7OliSCFrHypbWa6MV62ZeucVS3kUdLPcSUCadU6XJZMulnY2vkliSVhxtRN1
nE
Y6/rcUi8
-----END PRIVATE KEY-----
```

Currently, only .pem certificates are supported. If the certificate is not in .pem format, convert it into .pem locally by referring to **Table 2-25** before uploading it.

Table 2-25 Certificate conversion commands

Format	Conversion Method
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.
PFX	- Obtain a private key. For example, run the following command to convert **cert.pfx** into **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** - Obtain a certificate. For example, run the following command to convert **cert.pfx** into **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. Convert a certificate. For example, run the following command to convert **cert.p7b** into **cert.cer**: **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. Rename obtained certificate file **cert.cer** to **cert.pem**.

Format	Conversion Method
DER	● Obtain a private key. For example, run the following command to convert **privatekey.der** into **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** ● Obtain a certificate. For example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTE

- Before running an OpenSSL command, ensure that the **OpenSSL** tool has been installed on the local host.
- If your local PC runs a Windows operating system, go to the command line interface (CLI) and then run the certificate conversion command.

Step 6 Click **Confirm**.

----End

Other Operations

- To change the certificate name, move the cursor over the name of the certificate, click ✎, and enter a certificate name.

  NOTICE

  If the certificate is in use, unbind the certificate from the domain name first. Otherwise, the certificate name cannot be changed.

- To view details about a certificate, locate the row of the certificate and **View** in the **Operation** column of the certificate.
- To delete a certificate, locate the row of the certificate and click **Delete** in the **Operation** column.

2.6.2 Deleting a Certificate

This section describes how to delete an expired or invalid certificate.

Prerequisites

The certificate you want to delete is not bound to a protected website.

Constraints

If a certificate to be deleted is bound to a website, unbind it from the website before deletion.

Impact on the System

- Deleting certificates does not affect services.
- Deleted certificates cannot be recovered. Exercise caution when performing this operation.

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 WAF** > **Certificates**.

Step 4 In the row containing the certificate you want to delete, click **Delete** in the **Operation** column.

Step 5 In the dialog box that is displayed, click **Confirm** to delete the certificate.

----End

2.6.3 Viewing Certificate Information

This section describes how to view certificate details, including the certificate name, domain name a certificate is used for, and expiration time.

Prerequisites

A certificate has been created.

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 WAF** > **Certificates**.

Step 4 View the certificate information. For details about related parameters, see Table 2-26.

Table 2-26 Certificate parameters

Parameter	Description
Name	Certificate name

Parameter	Description
Expires	Certificate expiration time. It is recommended that you update the certificate before it expires. Otherwise, all EdgeSec protection rules will be unable to take effect, and there can be massive impacts on the origin server, even more severe than a crashed host or website access failures.
Domain Name	The domain names protected by the certificate. Each domain name must be bound to a certificate. One certificate can be used for multiple domain names.
Enterprise Project	The enterprise project to which a certificate belongs.

----End

Other Operations

- To change the certificate name, move the cursor over the name of the certificate, click ✎, and enter a certificate name.

  NOTICE

  If the certificate is in use, unbind the certificate from the domain name first. Otherwise, the certificate name cannot be changed.

- To view details about a certificate, locate the row of the certificate and **View** in the **Operation** column of the certificate.
- To delete a certificate, locate the row of the certificate and click **Delete** in the **Operation** column.

2.7 Address Group Management

2.7.1 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.

Specifications Restrictions

- 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 an IP Address Blacklist or Whitelist Rule**.
  - If the quota of IP address whitelist and blacklist rules of your cloud WAF instance cannot meet your requirements, you can purchase rule expansion packages under the current WAF instance edition or upgrade your WAF 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.**

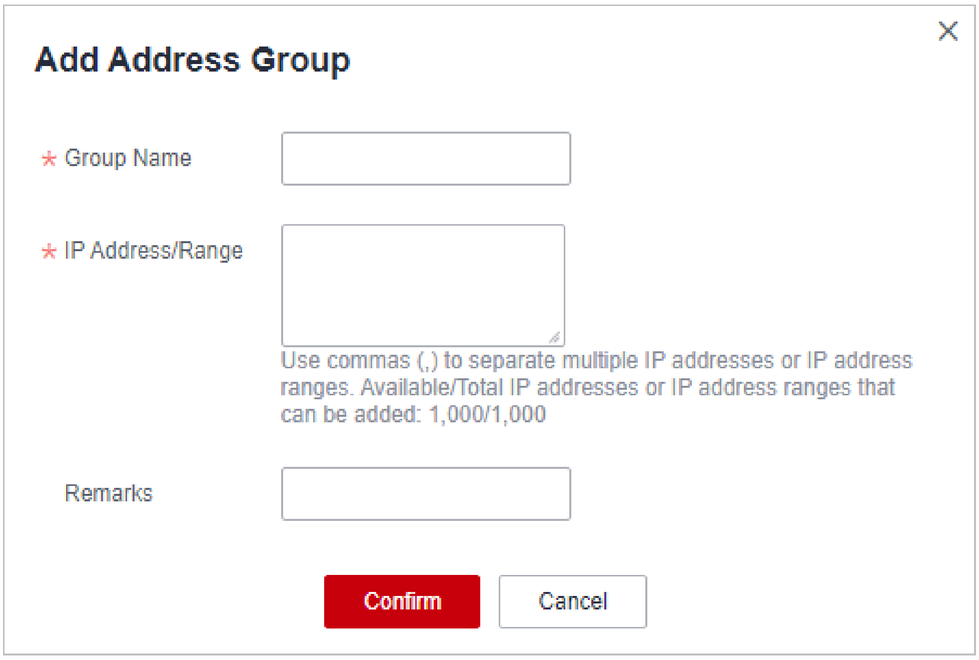
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

Step 3 In the navigation pane on the left, choose **Edge WAF** > **Address Groups**.

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 2-88 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: 1,000/1,000

Remarks

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

2.7.2 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 WAF** > **Address Groups**.

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

Table 2-27 Parameter description

Parameter	Description
Group Name	Address group name you configured
IP Address/ 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 Edge Anti-DDoS Management

3.1 Viewing the Protection Information

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

📖 NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and view the protection information of the project.

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 Anti-DDoS** > **Overview**.

Step 4 In the upper part of the page, select a project from the **Enterprise Project** drop-down list. For details about the parameters, see **Table 3-1**.

- The query time can be **Last 24 hours**, **Last 3 days**, **Last 7 days**, **Last 30 days**, or **Customize**. You can customize the query time to view protection logs generated in the last 90 days.

Figure 3-1 DDoS attack protection logs

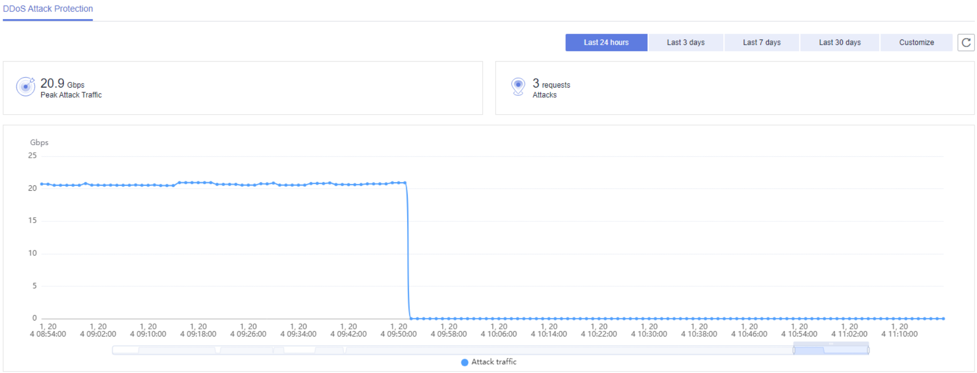


Table 3-1 DDoS attack protection parameters

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

3.2 Protecting Domain Names Using Policies

This section describes how to add domain names of websites so that they can be protected by policies of Edge Anti-DDoS.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and view the protection policies of the project.

Specifications Restrictions

Each Edge Anti-DDoS instance can protect a maximum of 50 domain names. Domain names that need to be protected cannot be added in batches.

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 Anti-DDoS** > **Policies**.

Step 4 On the displayed page, click **Add Domain Name**.

Step 5 Select the domain name to protect and click **OK**. The selected domain name is displayed in the domain name list.

Step 6 Locate the added domain name and click in the **Security Protection** column to enable protection of the domain name.

----End

Other Operations

To cancel protection of a domain name, click in the **Security Protection** column or click **Delete** in the **Operation** column.

4 Managing Logs

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

LTS analyzes and processes a large number of logs. It enables you to process logs in real-time, efficiently, and securely. Logs can be stored in LTS for seven days by default but you can configure LTS for up to 30 days if needed. Logs earlier than 30 days are automatically deleted. However, you can configure LTS to dump those logs to an Object Storage Service (OBS) bucket or enable Data Ingestion Service (DIS) for long-term storage.

> NOTE
>
> - On the LTS console, you can view logs for the last 30 days and download logs for the last five days.
> - LTS is billed by traffic and is billed separately from Edge WAF. For details about LTS pricing, see **Price Calculator**.
> - If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your Edge WAF instance locates. Then, you can select the project from the **Enterprise Project** drop-down list and configure Edge WAF logging.

- For details about how to configure protection logs, see **Enabling LTS for Edge WAF Protection Event Logging**.
- For details about how to view logs on the LTS console, see **Viewing Protection Logs on LTS**.
- Edge WAF provides access logs and attack logs.
  - For details about access logs, see **Description of the Edge WAF access_log Field**.
  - For details about attack logs, see **Description of the Edge WAF attack_log Field**.

Prerequisites

A protected website has been added. For details, see **Adding a Website to Edge WAF**.

Enabling LTS for Edge WAF Protection Event Logging

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 Select the configuration path as required.

Configure Edge WAF logs. In the navigation pane on the left, choose **Edge WAF** > **Events**. On the **Events** page that is displayed, click the **Configure Logs** tab.

Step 4 Toggle on ● to use LTS to collect attack logs. Select a log group region, log group, and log stream, or click **LTS** to go to the LTS console to create a log group and log stream. For details, see **Creating Log Groups and Log Streams**.

Step 5 Click **OK**.

----End

Viewing Protection Logs on LTS

Step 1 Log in to the management console.

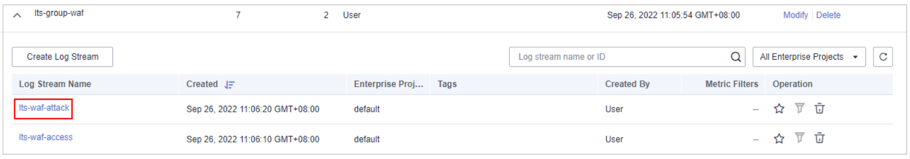
Step 2 Click ☰ in the upper left corner of the page and choose **Management & Deployment** > **Log Tank Service**.

Step 3 In the log group list, click ⌄ to expand the log group (for example, **lts-group-waf**).

Step 4 View protection logs.

- View attack logs.
  a. In the log stream list, click the name of the configured attack log stream.

Figure 4-1 Log stream name configured for attack logs

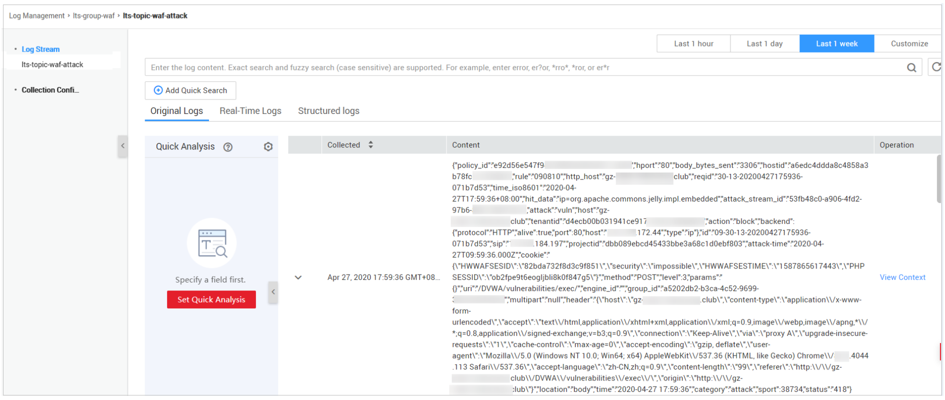


lts-group-waf 7 2 User Sep 26, 2022 11:05:54 GMT+08:00

Log Stream Name	Created	Enterprise Proj...	Tags	Created By	Metric Filters	Operation
lts-waf-attack	Sep 26, 2022 11:06:20 GMT+08:00	default		User	--	☆ ▽ 🗑
lts-waf-access	Sep 26, 2022 11:06:10 GMT+08:00	default		User	--	☆ ▽ 🗑

  b. View attack logs. **Figure 4-2** shows an example.

Figure 4-2 View attack logs.



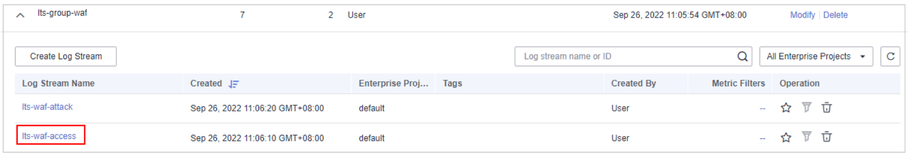
Apr 27, 2020 17:59:36 GMT+08...

```
{"policy_id":"e92d56e547f9[redacted]","hport":"80","body_bytes_sent":"3306","hostid":"a6edc4ddda8c4858a3
b78fc[redacted],"rule":"090810","http_host":"gz-[redacted]club","reqid":"30-13-20200427175936-
071b7d53","time_iso8601":"2020-04-
27T17:59:36+08:00","hit_data":"ip=org.apache.commons.jelly.impl.embedded","attack_stream_id":"53fb48c0-a906-4fd2-
97b6-[redacted]","attack":"vuln","host":"gz-
[redacted]club","tenantid":"d4ecb00b031941ce917[redacted]","action":"block","backend":
{"protocol":"HTTP","alive":true,"port":80,"host":"[redacted].172.44","type":"ip"},"id":"09-30-13-20200427175936-
071b7d53","sip":"[redacted].184.197","projectid":"dbb089ebcd45433bbe3a68c1d0ebf803","attack-time":"2020-04-
27T09:59:36.000Z","cookie":"
{\"HWWAFSESID\":\"82bda732f8d3c9f851\",\"security\":\"impossible\",\"HWWAFSESTIME\":\"1587865617443\",\"PHP
SESSID\":\"ob2fpe9t6eogljbli8k0f847g5\"}","method":"POST","level":3,"params":"
{}","uri":"/DVWA/vulnerabilities/exec/","engine_id":"","group_id":"a5202db2-b3ca-4c52-9699-
[redacted]","multipart":"null","header":"{\"host\":\"gz-[redacted].club\",\"content-type\":\"application\\/x-www-
form-
urlencoded\",\"accept\":\"text\\/html,application\\/xhtml+xml,application\\/xml;q=0.9,image\\/webp,image\\/apng,*\\/
*;q=0.8,application\\/signed-exchange;v=b3;q=0.9\",\"connection\":\"Keep-Alive\",\"via\":\"proxy A\",\"upgrade-insecure-
requests\":\"1\",\"cache-control\":\"max-age=0\",\"accept-encoding\":\"gzip, deflate\",\"user-
agent\":\"Mozilla\\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\\/537.36 (KHTML, like Gecko) Chrome\\/[redacted].4044
.113 Safari\\/537.36\",\"accept-language\":\"zh-CN,zh;q=0.9\",\"content-length\":\"99\",\"referer\":\"http:\\/\\/gz-
[redacted]club\\/DVWA\\/vulnerabilities\\/exec\\/\",\"origin\":\"http:\\/\\/gz-
[redacted]club\"}","location":"body","time":"2020-04-27 17:59:36","category":"attack","sport":38734,"status":"418"}
```

- View access logs.

a. In the log stream list, click the name of the configured access log stream.

Figure 4-3 Log stream name configured for access logs

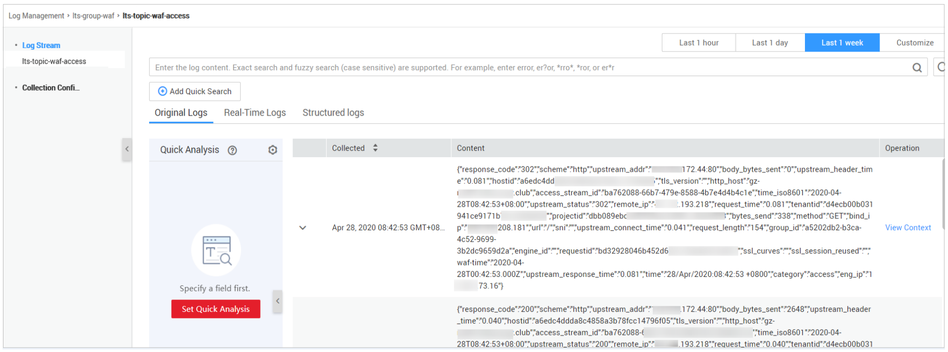


lts-group-waf 7 2 User Sep 26, 2022 11:05:54 GMT+08:00 Modify | Delete

Log Stream Name	Created	Enterprise Proj...	Tags	Created By	Metric Filters	Operation
lts-waf-attack	Sep 26, 2022 11:06:20 GMT+08:00	default		User	--	☆ ▽ 🗑
lts-waf-access	Sep 26, 2022 11:06:10 GMT+08:00	default		User	--	☆ ▽ 🗑

b. View access logs. **Figure 4-4** shows an example.

Figure 4-4 View access logs.



Apr 28, 2020 08:42:53 GMT+08...

```
{"response_code":"302","scheme":"http","upstream_addr":"[redacted]172.44:80","body_bytes_sent":"0","upstream_header_time":"0.081","hostid":"a6edc4dd[redacted]","tls_version":"","http_host":"gz-[redacted].club","access_stream_id":"ba762088-66b7-479e-8588-4b7e4d4b4c1e","time_iso8601":"2020-04-28T08:42:53+08:00","upstream_status":"302","remote_ip":"[redacted].193.218","request_time":"0.081","tenantid":"d4ecb00b031941ce9171b[redacted]","projectid":"dbb089ebc[redacted]","bytes_send":"338","method":"GET","bind_ip":"[redacted]208.181","url":"/","sni":"","upstream_connect_time":"0.041","request_length":"154","group_id":"a5202db2-b3ca-4c52-9699-3b2dc9659d2a","engine_id":"","requestid":"bd32928046b452d6[redacted]","ssl_curves":"","ssl_session_reused":"","waf-time":"2020-04-28T00:42:53.000Z","upstream_response_time":"0.081","time":"28/Apr/2020:08:42:53 +0800","category":"access","eng_ip":"1[redacted]73.16"}
{"response_code":"200","scheme":"http","upstream_addr":"[redacted].172.44:80","body_bytes_sent":"2648","upstream_header_time":"0.040","hostid":"a6edc4ddda8c4858a3b78fcc14796f05","tls_version":"","http_host":"gz-[redacted].club","access_stream_id":"ba762088-[redacted]","time_iso8601":"2020-04-28T08:42:53+08:00","upstream_status":"200","remote_ip":"[redacted].193.218","request_time":"0.040","tenantid":"d4ecb00b031
```

----End

Description of the Edge WAF access_log Field

Field	Type	Field Description	Description
access_log.requestid	string	Random ID	The value is the same as the last eight characters of the **req_id** field in the attack log.
access_log.time	string	Access time	GMT time a log is generated.
access_log.connection_requests	string	Sequence number of the request over the connection	-
access_log.eng_ip	string	IP address of the engine	-
access_log.pid	string	The engine that processes the request	Engine (worker PID).
access_log.hostid	string	Domain name identifier of the access request.	Protected domain name ID (upstream_id).

Field	Type	Field Description	Description
access_log.tenantid	string	Account ID	Each Huawei Cloud account corresponds to one tenant ID.
access_log.projectid	string	ID of the project the protected domain name belongs to	Project ID of a user in a specific region.
access_log.remote_ip	string	Remote IP address of the request at layer 4	IP address from which a client request originates. **NOTICE** If a layer-7 proxy is deployed in front of Edge WAF, this field indicates the IP address of the proxy node closest to Edge WAF. The real IP address of the visitor is specified by the **x-forwarded-for** and **x_real_ip** fields.
access_log.remote_port	string	Remote port of the request at layer 4	Port used by the IP address from which a client request originates
access_log.sip	string	IP address of the client that sends the request	For example, XFF.
access_log.scheme	string	Request protocol	Protocols that can be used in the request: ● HTTP ● HTTPS
access_log.response_code	string	Response code	Response status code returned by the origin server to Edge WAF
access_log.method	string	Request method.	Request type in a request line. Generally, the value is **GET** or **POST**.
access_log.http_host	string	Domain name of the requested server	Address, domain name, or IP address entered in the address box of a browser.
access_log.url	string	Request URL.	Path in a URL (excluding the domain name).
access_log.request_length	string	Request length.	The request length includes the access request address, HTTP request header, and number of bytes in the request body.

Field	Type	Field Description	Description
access_log.bytes_send	string	Total number of bytes sent to the client.	Number of bytes sent by Edge WAF to the client
access_log.body_bytes_sent	string	Total number of bytes of the response body sent to the client	Number of bytes of the response body sent by Edge WAF to the client
access_log.upstream_addr	string	Address of the backend server.	IP address of the origin server for which a request is destined. For example, if Edge WAF forwards requests to an ECS, the IP address of the ECS is returned to this parameter.
access_log.request_time	string	Request processing time	Processing time starts when the first byte of the client is read (unit: s).
access_log.upstream_response_time	string	Backend server response time	Time the backend server responds to the Edge WAF request (unit: s).
access_log.upstream_status	string	Backend server response code	Response status code returned by the backend server to Edge WAF.
access_log.upstream_connect_time	string	Time elapsed for origin servers to connect to backend servers	Time for the origin server to establish a connection to its backend servers. If the backend service uses an encryption protocol, this parameter includes the handshake time (unit: s).
access_log.upstream_header_time	string	Time used by the backend server to receive the first byte of the response header.	-
access_log.bind_ip	string	Edge WAF engine back-to-source IP address	Back-to-source IP address used by the Edge WAF engine
access_log.group_id	string	LTS log group ID	ID of the log group for interconnecting Edge WAF with LTS
access_log.access_stream_id	string	Log stream ID	ID of **access_stream** of the user in the log group identified by the **group_id** field.

Field	Type	Field Description	Description
access_log.engine_id	string	Edge WAF engine ID	Unique ID of the Edge WAF engine
access_log.time_iso8601	string	ISO 8601 time format of logs.	-
access_log.sni	string	Domain name requested through SNI.	-
access_log.tls_version	string	Protocol version for establishing an SSL connection.	TLS version used in the request.
access_log.ssl_curves	string	Curve group list supported by the client.	-
access_log.ssl_session_reused	string	SSL session reuse	Whether the SSL session can be reused **r**: Yes **.**: No
access_log.process_time	string	Engine attack detection duration (unit: ms)	-
access_log.args	string	The parameter data in the URL	-
access_log.x_forwarded_for	string	A string of IP addresses for a proxy when the proxy is deployed in front of Edge WAF	The sting includes one or more IP addresses. The leftmost IP address is the originating IP address of the client. Each time the proxy server receives a request, it adds the source IP address of the request to the right of the originating IP address.
access_log.cdn_src_ip	string	Client IP address identified by CDN when CDN is deployed in front of Edge WAF	This field specifies the real IP address of the client if CDN is deployed in front of Edge WAF. **NOTICE** Some CDN vendors may use other fields. Edge WAF records only the most common fields.

Field	Type	Field Description	Description
access_log.x_real_ip	string	Real IP address of the client when a proxy is deployed in front of Edge WAF.	Real IP address of the client, which is identified by the proxy.
access_log.intel_crawler	string	Used for intelligence anti-crawler analysis.	-
access_log.ssl_ciphers_md5	string	MD5 value of the SSL cipher (ssl_ciphers).	-
access_log.ssl_cipher	string	SSL cipher used.	-
access_log.web_tag	string	Website name.	-
access_log.user_agent	string	User agent in the request header.	-
access_log.upstream_response_length	string	Backend server response size	-
access_log.region_id	string	Region where the request is received.	-
access_log.enterprise_project_id	string	ID of the enterprise project that the requested domain name belongs to.	-
access_log.referer	string	Referer content in the request header.	The value can contain a maximum of 128 characters. Characters over 128 characters will be truncated.
access_log.rule	string	Protection rule that the request matched.	If multiple rules are matched, only one rule is displayed.

Description of the Edge WAF attack_log Field

Field	Type	Field Description	Description
attack_log.category	string	Log category	The value is **attack**.
attack_log.time	string	Log time	-
attack_log.time_iso8601	string	ISO 8601 time format of logs	-
attack_log.policy_id	string	Policy ID	-
attack_log.level	string	Protection level	Protection level of a built-in rule in basic web protection ● **1**: Low ● **2**: Medium ● **3**: High

Field	Type	Field Description	Description
attack_log.attack	string	Type of attack	Attack type. This parameter is listed in attack logs only. - **default**: default attacks - **sqli**: SQL injections - **xss**: cross-site scripting (XSS) attacks - **webshell**: web shells - **robot**: malicious crawlers - **cmdi**: command injections - **rfi**: remote file inclusion attacks - **lfi**: local file inclusion attacks - **illegal**: unauthorized requests - **vuln**: exploits - **cc**: attacks that hit the CC protection rules - **custom_custom**: attacks that hit a precise protection rule - **custom_whiteblackip**: attacks that hit an IP address blacklist or whitelist rule - **custom_geoip**: attacks that hit a geolocation access control rule - **antitamper**: attacks that hit a web tamper protection rule - **anticrawler**: attacks that hit the JS challenge anti-crawler rule - **leakage**: vulnerabilities that hit an information leakage prevention rule - **antiscan_high_freq_scan**: Attacks that hit malicious scanning rules. - **followed_action**: The source is marked as a known attack source. For details, see **Configuring a Known Attack Source Rule**.
attack_log.action	string	Protective action	Edge WAF defense action. - **block**: WAF blocks attacks. - **log**: WAF only logs detected attacks. - **captcha**: Verification code

Field	Type	Field Description	Description
attack_log.sub_type	string	Crawler types	When **attack** is set to **robot**, this parameter cannot be left blank. ● **script_tool**: Script tools ● **search_engine**: Search engines ● **scanner:** Scanning tools ● **uncategorized**: Other crawlers
attack_log.rule	string	ID of the triggered rule or the description of the custom policy type.	-
attack_log.rule_name	string	Description of a custom rule type	This field is empty when a basic protection rule is matched
attack_log.location	string	Location triggering the malicious load	-
attack_log.req_body	sting	Request body	-
attack_log.resp_headers	string	Response header	-
attack_log.hit_data	string	String triggering the malicious load	-
attack_log.resp_body	string	Response body	-
attack_log.backend.protocol	string	Backend protocol	-
attack_log.backend.alive	string	Backend server status	-
attack_log.backend.port	string	Backend server port	-
attack_log.backend.host	string	Backend server host value	-
attack_log.backend.type	string	Backend server type	IP address or domain name

Field	Type	Field Description	Description
attack_log.backend.weight	number	Backend server weight	-
attack_log.status	string	Response status code	-
attack_log.upstream_status	string	Origin server response code	-
attack_log.reqid	string	Random ID	The value consists of the engine IP address suffix, request timestamp, and request ID allocated by Nginx.
attack_log.requestid	string	Unique ID of the request	Request ID allocated by Nginx
attack_log.id	string	Attack ID	ID of the attack
attack_log.method	string	Request method	-
attack_log.sip	string	Client request IP address	-
attack_log.sport	string	Client request port	-
attack_log.host	string	Requested domain name	-
attack_log.http_host	string	Domain name of the requested server	-
attack_log.hport	string	Port of the requested server	-
attack_log.uri	string	Request URL	The domain is excluded.

Field	Type	Field Description	Description
attack_log.header	A JSON string. A JSON table is obtained after the string is decoded.	Request header	-
attack_log.mutipart	A JSON string. A JSON table is obtained after the string is decoded.	Request multipart header	This parameter is used to upload files.
attack_log.cookie	A JSON string. A JSON table is obtained after the string is decoded.	Cookie of the request	-

Field	Type	Field Description	Description
attack_log.params	A JSON string. A JSON table is obtained after the string is decoded.	Params value following the request URI	-
attack_log.body_bytes_sent	string	Total number of bytes of the response body sent to the client	Total number of bytes of the response body sent by Edge WAF to the client
attack_log.upstream_response_time	string	Backend server response time	-
attack_log.engine_id	string	Unique ID of the engine	-
attack_log.region_id	string	ID of the region where the engine is located	-
attack_log.engine_ip	string	Engine IP address	-
attack_log.process_time	string	Detection duration	-
attack_log.remote_ip	string	Layer-4 IP address of the client that sends the request	-
attack_log.x_forwarded_for	string	Content of **X-Forwarded-For** in the request header	-

Field	Type	Field Description	Description
attack_log.cdn_src_ip	string	Content of **Cdn-Src-Ip** in the request header	-
attack_log.x_real_ip	string	Content of **X-Real-IP** in the request header	-
attack_log.group_id	string	Log group ID	LTS log group ID
attack_log.attack_stream_id	string	Log stream ID	ID of **access_stream** of the user in the log group identified by the **group_id** field.
attack_log.hostid	string	Protected domain name ID (upstream_id)	-
attack_log.tenantid	string	Account ID	-
attack_log.projectid	string	ID of the project the protected domain name belongs to	-
attack_log.enterprise_project_id	string	ID of the enterprise project that the requested domain name belongs to	-
attack_log.web_tag	string	Website name	-
attack_log.req_body	string	Request body. (If the request body larger than 1 KB, it will be truncated.)	-

5 Permissions Management

5.1 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 5-1** shows the procedure.

Prerequisites

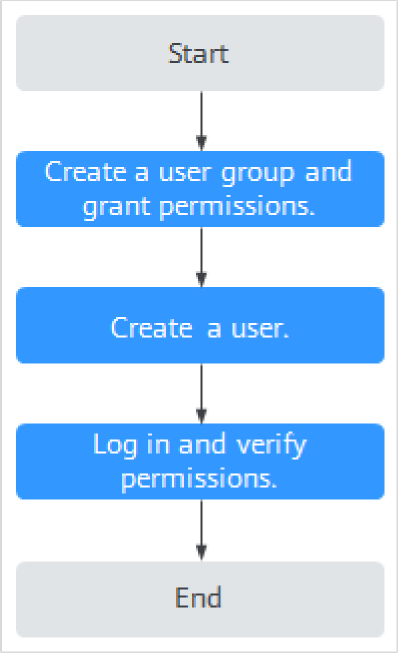
Before granting permissions to a user group, you need to learn about the permissions supported by EdgeSec in **Table 5-1** and choose policies or roles based on your requirements.

Table 5-1 EdgeSec system roles

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

Permission Granting Process

Figure 5-1 Process for granting permissions


Start
Create a user group and grant permissions.
Create a user.
Log in and verify permissions.
End

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.

6 Key Operations Recorded by CTS

6.1 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 6-1 lists the EdgeSec operations recorded by CTS.

Table 6-1 EdgeSec operations recorded by CTS

Operation	Resource Type	Trace
Adding a CDN domain name scheduling task	cdnDomainScheduleTask	addCdnDomainScheduleTask
Add 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	wafAntiCrawlerRule	createWafAntiCrawlerRule
Deleting a script anti-crawler rule	wafAntiCrawlerRule	deleteWafAntiCrawlerRule
Changing the script anti-crawler mode	wafAntiCrawlerRule	switchWafAntiCrawlerRule
Updating a script anti-crawler rule	wafAntiCrawlerRule	updateWafAntiCrawlerRule
Creating a CC attack protection rule	wafCcRule	createWafCcRule
Deleting a CC attack protection rule	wafCcRule	deleteWafCcRule
Updating a CC attack protection rule	wafCcRule	updateWafCcRule
Creating a certificate	wafCertificate	createWafCertificate
Deleting a certificate	wafCertificate	deleteWafCertificate
Updating a certificate	wafCertificate	updateWafCertificate
Creating a precise protection rule	wafCustomRule	createWafCustomRule
Deleting a precise protection rule	wafCustomRule	deleteWafCustomRule
Updating a precise protection rule	wafCustomRule	updateWafCustomRule
Creating a domain name to be protected	wafDomain	createWafDomain
Deleting a protected domain name	wafDomain	deleteWafDomain
Updating a protected domain name	wafDomain	updateWafDomain
Creating a geolocation access control rule	wafGeoIpRule	createWafGeoIpRule
Deleting a geolocation access control rule	wafGeoIpRule	deleteWafGeoIpRule

Operation	Resource Type	Trace
Updating a geolocation access control rule	wafGeoIpRule	updateWafGeoIpRule
Creating a false alarm masking rule	wafIgnoreRule	createWafIgnoreRule
Deleting a false alarm masking rule	wafIgnoreRule	deleteWafIgnoreRule
Resetting a false alarm masking rule	wafIgnoreRule	recountWafIgnoreRule
Updating a false alarm masking rule	wafIgnoreRule	updateWafIgnoreRule
Creating an IP address group	wafIpGroup	CreateWafIpGroup
Deleting an IP address group	wafIpGroup	DeleteWafIpGroup
Updating an IP address group	wafIpGroup	UpdateWafIpGroup
Updating the domain names to which a protection policy applies	wafPolicy	applyWafPolicy
Creating a protection policy	wafPolicy	createWafPolicy
Deleting a protection policy	wafPolicy	deleteWafPolicy
Updating a protection policy	wafPolicy	updateWafPolicy
Creating a privacy masking rule	wafPrivacyMaskRule	createWafPrivacyMaskRule
Deleting a privacy masking rule	wafPrivacyMaskRule	deleteWafPrivacyMaskRule
Updating a privacy masking rule	wafPrivacyMaskRule	updateWafPrivacyMaskRule
Creating a known attack source rule	wafPunishmentRule	createWafPunishmentRule
Deleting a known attack source rule	wafPunishmentRule	deleteWafPunishmentRule
Updating a known attack source rule	wafPunishmentRule	updateWafPunishmentRule

Operation	Resource Type	Trace
Creating a reference table	wafValueList	createWafValueList
Deleting a reference table	wafValueList	deleteWafValueList
Updating a reference table	wafValueList	updateWafValueList
Adding an IP address blacklist or whitelist rule	wafWhiteBlackIpRule	createWafWhiteBlackIpRule
Deleting an IP address blacklist or whitelist rule	wafWhiteBlackIpRule	deleteWafWhiteBlackIpRule
Updating an IP address blacklist or whitelist rule	wafWhiteBlackIpRule	updateWafWhiteBlackIpRule

6.2 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)**.

7 Monitoring

7.1 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 7-1 EdgeSec metrics

ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
requests	Number of Requests	Number of requests returned by WAF in the last 5 minutes Unit: count Collection method: Collect the number of requests for accessing the protected domain name.	≥ 0 Value type: Float	Protected domain dame	5 minutes
waf_http_2xx	WAF Status Code (2XX)	Number of 2XX status codes returned by WAF in the last 5 minutes Unit: count Collection method: Collect the number of 2XX status codes returned.	≥ 0 Value type: Float	Protected domain dame	5 minutes
waf_http_3xx	WAF Status Code (3XX)	Number of 3XX status codes returned by WAF in the last 5 minutes Unit: count Collection method: Collect the number of 3XX status codes returned	≥ 0 Value type: Float	Protected domain dame	5 minutes

ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
waf_http_4xx	WAF Status Code (4XX)	Number of 4XX status codes returned by WAF in the last 5 minutes Unit: count Collection method: Collect the number of 4XX status codes returned.	≥ 0 Value type: Float	Protected domain dame	5 minutes
waf_http_5xx	WAF Status Code (5XX)	Number of 5XX status codes returned by WAF in the last 5 minutes Unit: count Collection method: Collect the number of 5XX status codes returned.	≥ 0 Value type: Float	Protected domain dame	5 minutes
waf_fused_counts	WAF Traffic Threshold	Number of requests destined for the protected domain name in the last 5 minutes during breakdown protection duration Unit: count Collection method: Collect the number of requests destined for the protected domain name in the last 5 minutes during breakdown protection duration.	≥ 0 Value type: Float	Protected domain dame	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 Unit: Mbit/s Collection method: Collect the total inbound traffic in the last 5 minutes.	≥ 0 Mbit/s Value type: Float	Protected domain dame	5 minutes
outbound_traffic	Total Outbound Traffic	Total outbound traffic in the last 5 minutes Unit: Mbit/s Collection method: Collect the total outbound traffic in the last 5 minutes.	≥ 0 Mbit/s Value type: Float	Protected domain dame	5 minutes
waf_process_time_0	WAF Latency [0, 10) ms	Number of requests processed by WAF at a latency from 0 ms (included) to 10 ms (excluded) in the last 5 minutes Unit: count Collection method: Collect the number of requests processed by WAF at a latency from 0 ms (included) to 10 ms (excluded) in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes

ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
waf_process_time_10	WAF Latency [10, 20) ms	Number of requests processed by WAF at a latency from 10 ms (included) to 20 ms (excluded) in the last 5 minutes Unit: count Collection method: Collect the number of requests processed by WAF at a latency from 10 ms (included) to 20 ms (excluded) in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes
waf_process_time_20	WAF Latency [20, 50) ms	Number of requests processed by WAF at a latency from 20 ms (included) to 50 ms (excluded) in the last 5 minutes Unit: count Collection method: Collect the number of requests processed by WAF at a latency from 20 ms (included) to 50 ms (excluded) in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes

ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
waf_process_time_50	WAF Latency [50, 100) ms	Number of requests processed by WAF at a latency from 50 ms (included) to 100 ms (excluded) in the last 5 minutes Unit: count Collection method: Collect the number of requests processed by WAF at a latency from 50 ms (included) to 100 ms (excluded) in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes
waf_process_time_100	WAF Latency [100, 1,000) ms	Number of requests processed by WAF at a latency from 100 ms (included) to 1,000 ms (excluded) in the last 5 minutes Unit: count Collection method: Collect the number of requests processed by WAF at a latency from 100 ms (included) to 1,000 ms (excluded) in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes

ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
waf_process_time_1000	WAF Latency [1,000, above) ms	Number of requests processed by WAF at a latency greater than or equal to 1,000 ms in the last 5 minutes Unit: count Collection method: Collect the number of requests processed by WAF at a latency greater than or equal to 1,000 ms in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes
qps_peak	Peak QPS	Peak QPS of the protected domain name in the last 5 minutes Unit: count Collection method: Collect the peak QPS of the protected domain name in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes
qps_mean	Average QPS	Average QPS of the protected domain name in the last 5 minutes Unit: count Collection method: Collect the average QPS of the protected domain name in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes

ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
waf_http_0	No WAF Status Code	Number of requests with no status code returned by WAF in the last 5 minutes Unit: count Collection method: Collect the number of requests with no status code returned by WAF in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	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 Unit: count Collection method: Collect the number of requests with a *2XX* status code returned by the origin server in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	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 Unit: count Collection method: Collect the number of requests with a *3XX* status code returned by the origin server in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	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 Unit: count Collection method: Collect the number of requests with a *4XX* status code returned by the origin server in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	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 Unit: count Collection method: Collect the number of requests with a *5XX* status code returned by the origin server in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes
upstream_code_0	No Origin Server Status Code	Number of requests with no status code returned in the last 5 minutes Unit: count Collection method: Collect the number of requests with no status code returned in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes
inbound_traffic_peak	Peak Inbound Traffic	Peak inbound traffic to the domain name in the last 5 minutes Unit: Mbit/s Collection method: Collect the peak inbound traffic to the domain name in the last 5 minutes.	≥ 0 Mbit/s Value type: Float	Protected domain dame	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 Unit: Mbit/s Collection method: Collect the average inbound traffic to the domain name in the last 5 minutes.	≥ 0 Mbit/s Value type: Float	Protected domain dame	5 minutes
outbound_traffic_peak	Peak Outbound Traffic	Peak outbound traffic to the domain name in the last 5 minutes Unit: Mbit/s Collection method: Collect the peak outbound traffic to the domain name in the last 5 minutes.	≥ 0 Mbit/s Value type: Float	Protected domain dame	5 minutes
outbound_traffic_mean	Average Outbound Traffic	Average outbound traffic to the domain name in the last 5 minutes Unit: Mbit/s Collection method: Collect the average outbound traffic to the domain name in the last 5 minutes.	≥ 0 Mbit/s Value type: Float	Protected domain dame	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 Unit: count Collection method: Collect the number of attacks against the domain name in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes
crawlers	Number of Crawler Attacks	Number of crawler attacks against the domain name in the last 5 minutes Unit: count Collection method: Collect the number of crawler attacks against the domain name in the last 5 minutes.	≥ 0 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 Unit: count Collection method: Collect the number of attacks blocked by basic web protection rules over the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	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 Unit: count Collection method: Collect the number of attacks blocked by precise protection rules over the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	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 Unit: count Collection method: Collect the number of attacks blocked by CC protection rules over the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes

Dimensions

Key	Value
instance_id	ID of the dedicated WAF instance
waf_instance_id	ID of the website protected with WAF

Example of Raw Data Format of Monitored Metrics

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

```
          // Dimension name, for example, protected website
          "name": "waf_instance_id",
          // ID of the monitored object in this dimension, for example, ID of the protected website
          "value": "082db2f542e0438aa520035b3e99cd99"
        }
      ],
     // Metric ID
      "metric_name": "waf_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
  }
]
```

7.2 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**.

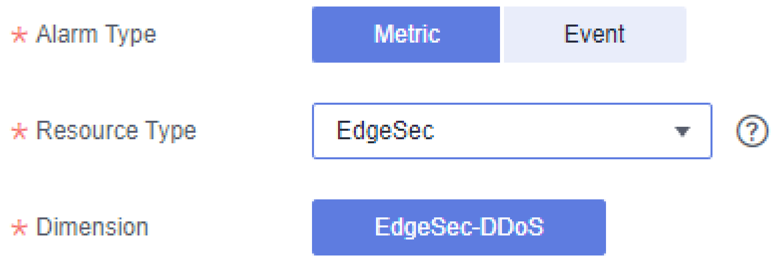
Step 2 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

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**: **Metric**
- **Resource Type**: **EdgeSec**
- **Dimension**: **EdgeSec-DDoS**

Figure 7-1 EdgeSec monitoring alarm rule



* Alarm Type: Metric | Event

* Resource Type: EdgeSec

* Dimension: EdgeSec-DDoS

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

----End

7.3 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 more 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** > **Edge WAF**.

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

----End

8 Managing Projects and Enterprise Projects

Selections are available only if you have enabled the enterprise project function, or your account is an enterprise account. An enterprise project provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.

Creating a Project and Assigning Permissions

- Creating a project

  Log in to the management console, click the username in the upper right corner, and select **Identity and Access Management**. In the navigation pane on the left, choose **Projects**. In the right pane, click **Create Project**. On the displayed **Create Project** page, select a region and enter a project name.

- Granting permissions

  You can assign permissions (of resources and operations) to user groups to associate projects with user groups. You can add users to a user group to control which projects they can access and what resources they can perform operations on. To do so, perform the following operations:

  a. On the **User Groups** page, locate the target user group and click **Configure Permission** in the **Operation** column. The **User Group Permissions** page is displayed. Locate the row that contains the target project, click **Configure Policy**, and select the required policies for the project.

  b. On the **Users** page, locate the target user and click **Modify** in the **Operation** column. In the **User Groups** area, add a user group for the user.

Creating an Enterprise Project and Assigning Permissions

- Creating an enterprise project

  On the management console, click **Enterprise** in the upper right corner. The **Enterprise Management** page is displayed. In the navigation pane on the left, choose **Enterprise Project Management**. In the right pane, click **Create Enterprise Project** and enter a name.

NOTE

Enterprise is available on the management console only if you have enabled the enterprise project, or you have an enterprise account. To enable this function, contact customer service.

- Granting permissions

  You can add a user group to an enterprise project and configure a policy to associate the enterprise project with the user group. You can add users to a user group to control which projects they can access and what resources they can perform operations on. To do so, perform the following operations:

  a. Locate the row that contains the target enterprise project, click **More** in the **Operation** column, and select **View User Group**. On the displayed **User Groups** page, click **Add User Group**. In the displayed **Add User Group** dialog box, select the user groups you want to add and move them to the right pane. Click **Next** and select the policies.

  b. In the navigation pane on the left, choose **Personnel Management** > **User Management**. Locate the row that contains the target user, click **More** in the **Operation** column, and select **Add to User Group**. In the displayed **Add to User Group** dialog box, select the user groups for which policies have been configured and click **OK**.

- Associating HSS with enterprise projects

  You can use enterprise projects to manage cloud resources.

  - Select an enterprise project when purchasing EdgeSec.

    On the page for buying HSS, select an enterprise project from the **Enterprise Project** drop-down list.

  - Adding resources

    On the **Enterprise Project Management** page, you can add existing resources to an enterprise project.

    Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.

  For more information, see **Creating an Enterprise Project**.

9 Change History

Date	Description
2024-01-25	This issue is the fifth official release. Added: Configuration example of allowing access requests from the source IP addresses in a specified region in section **Configuring a Precise Protection Rule**. Optimized: ● Parameters and descriptions in section **Viewing the Protection Information**. ● Configuration procedure and parameters in section **Configuring a Monitoring Alarm Rule**. Deleted: Region parameter in **Purchasing EdgeSec**.
2023-12-05	This issue is the fourth official release. Deleted: ● Anti-DDoS overview page section. ● Description about the DDoS log field in section **Managing Logs**.
2023-10-31	This issue is the third official release. Optimized: **Purchasing EdgeSec**.
2023-08-08	This issue is the second official release. Added: ● Added enterprise project information to **Managing Edge WAF** and **Edge Anti-DDoS Management**. ● **Managing Logs** ● **Managing Projects and Enterprise Projects**
2023-03-30	This issue is the first official release.