Edge Security

Getting Started

Issue 01

Date 2025-11-11

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Quick Access to Edge Security

When you add a domain name in CNAME mode, ESA allocates a CNAME value to the domain name and forwards user requests to edge security nodes through DNS resolution, implementing whole site acceleration and security protection.

Prerequisites

- You have registered a Huawei Cloud account and completed real-name authentication.
- You have enabled CDN.

Purchasing EdgeSec

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

Step 2 Click ☰ in the upper left corner of the page and choose **Content Delivery & Edge** > **CDN and Security**. The Huawei Cloud CDN page is displayed.

Step 3 In the navigation pane on the left, choose **Domains**. Click **Add Domain Name** to configure CDN acceleration for the domain name.

Step 4 On the **Add Domain Names** page, set domain name parameters. The parameters are as follows:

- Service Area: Chinese mainland
- Domain Name: Customize the value.
- Service Type: Website

  NOTE

  If there are dynamic requests, set **Service Type** to **Whole site**.
- Origin Protocol: Select **Same as user**.

Step 5 In the **Origin Server Settings** area, click **Add Origin Server**, enter the origin server address, and add an origin server for the domain name.

Step 6 Click **OK**.

Step 7 Click **OK**. The **View Results** dialog box is displayed. Confirm the information and click **OK**.

Step 8 (Optional) For quick configuration, click **Skip**. You can also select a template and click **Submit**.

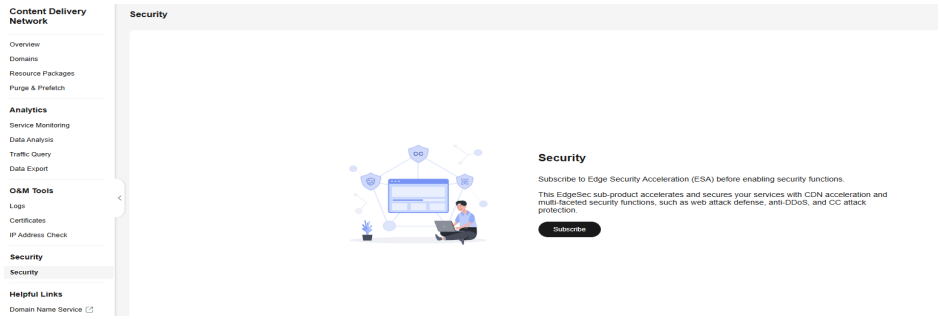
Step 9 Configure the CNAME and click **Skip** in the lower right corner.

Step 10 After the domain name is added, the system automatically allocates a CNAME to the domain name. You can view the CNAME in the CNAME column on the **Domains** page.

NOTE

- The CNAME cannot be accessed directly. You must **add the CNAME** to your domain's DNS records. Then requests for your domain name will be redirected to CDN PoPs for acceleration.
- If your services cover both China and outside China, you need to set **CDN Service** to outside China. Then, add a record that maps the CNAME to both the DNS service in the Chinese mainland and outside China on the DNS platform.
- For details about how to add a domain name, see **Adding a Domain Name**.

Step 11 After the CNAME record is added, your traffic can be scheduled to CDN. You can purchase edge security acceleration in **Security** page to use the security protection service.



Step 12 Click **Subscribe**. The **Buy ESA Package** page is displayed. Set the product parameters.

Step 13 Confirm the order details and click **Pay Now**.

----End

Accessing a Domain Name

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

Step 2 In the upper left corner of the list, click **Add Domain Names**. For details about the parameters, see **Table 1-1**.

Figure 1-1 Adding a website to EdgeSec

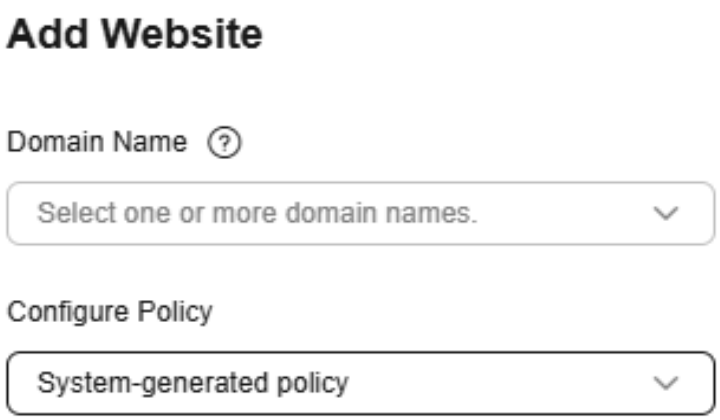


Table 1-1 Parameters for adding a protected website

Name	Description
Protected Domain Name	Select a domain name. You can select a domain name whose **Service Type** is **Website**, **File download**, **On-demand services**, or **Whole site** on the **Domains** page. **NOTE** The protected domain name added here is the domain name added in CDN domain name management.
Configure Policy	The **System-generated policy** is selected by default. You can select a policy you configured before.

Step 3 Click **OK**.

----End

Configuring Protection Policies

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

Step 2 In the upper left corner of the list, click **Add Policy** and set the policy name.

Step 3 Click **OK**.

Step 4 Click the name of the added protection policy. On the displayed page, enable basic web protection and CC attack protection. The recommended parameter settings are as follows:

Table 1-2 Recommended policy configuration

Policy Name	Parameters
Basic Web Protection	• Protection Action: Log only • General Check: enabled • Web Shell Detection: enabled
CC Attack Protection	• Rate Limit Mode: Source IP Address • Trigger: Set **Field** to **Path**, **Logic** to **Include**, and **Content** to **/**. Indicates that all paths containing a slash (/) match the CC rule. • Rate Limit Frequency: 5 times within 1 minute. Indicates that if the source IP address matches the rate limit condition for 5 times within 1 minute, the request will be blocked within the protection duration (response code 418 is returned). If you select Human-machine verification, a verification code is displayed on the page. You need to enter the verification code to continue the access. • Protection Action: Blocked • Protection Duration: 60s

Step 5 Return to the **Protection Policies** page, choose **More** > **Add Domain Name** in the **Operation** column of the policy name, select the domain name to be bound, and click **OK**.

----End

2 Blocking Heavy-Traffic CC Attacks Through CC Attack Protection Rules

You can configure CC attack protection rules to accurately identify and mitigate CC attacks by limiting the access frequency of visitors to resources on the protected website. After you configure CC attack protection rules and enable CC attack protection, the system can defend against CC attacks based on the rules.

Process

Procedure	Description
Preparations	Sign up for a HUAWEI ID, enable Huawei Cloud services, top up your account, and assign EdgeSec permissions to the account.
Step 1: Buy EdgeSec	Buy EdgeSec and select the edition and billing mode.
Step 2: Add Your Website to EdgeSec	Add the website you want to protect to EdgeSec for traffic inspection and forwarding.
Step 3: Configure a CC Attack Protection Rule	Configure and enable CC attack protection rules to mitigate CC attacks against the protected website.
Step 4: Viewing Protection Statistics Events	You can search for CC attacks prevention events to quickly locate attack sources or analyze attack events.

Preparations

1. Before purchasing EdgeSec, create a Huawei account and subscribe to Huawei Cloud.

If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.

2. Ensure that your account has sufficient balance or has a valid payment method configured.
3. Ensure that you have enabled CDN.
4. A domain name has been added on the **Domains** page. For details about domain name management, see **Domain Name Management**.

Step 1: Buy EdgeSec Enterprise Edition

EdgeSec provides the professional and enterprise editions. For details about the differences, see **Edition Differences**.

1. **Log in to the EdgeSec console.**
2. Click **Buy**. The **Buy EdgeSec** page is displayed. Set the product parameters.
3. Confirm the order details and click **Pay Now**.

Step 2: Add Your Website to EdgeSec

1. In the navigation pane on the left, choose **Edge Security** > **Domain Names**. The **Domain Names** page is displayed.
2. In the upper left corner of the list, click **Add Domain Names**. For details about the parameters, see **Table 2-1**.

Figure 2-1 Adding a website to EdgeSec

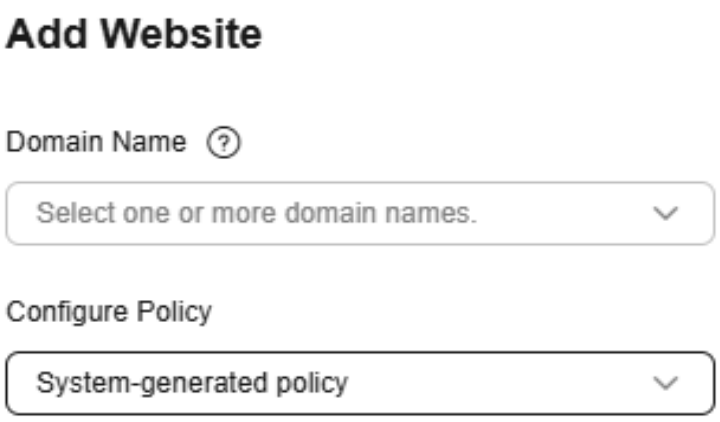


Table 2-1 Parameters for adding a protected website

Name	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 (-_:).
Protected Domain Name	Select a domain name. You can select a domain name whose **Service Type** is **Website**, **File download**, **On-demand services**, or **Whole site** on the **Domains** page. **NOTE** The domain name to be added is the one added on the CDN domain name management page.
Configure Policy	The **System-generated policy** is selected by default. You can select a policy you configured before.

3. Click **OK**.

Step 3: Configure a CC Attack Protection Rule

You can configure such a CC rule to mitigate CC attacks. If an IP address accessed paths under the current domain name more than 1000 times within 30 seconds, this rule will block requests from this IP address for 10 hours. This rule can be used as a preventive configuration for common small and medium-sized websites

1. In the navigation pane on the left, choose **Edge Security** > **Policies**. The **Policies** page is displayed.
2. Click the name of the target policy to go to the protection configuration page.
3. In the **CC Attack Protection** area, enable it.

    : enabled

    : disabled
4. In the upper left corner of the **CC Attack Protection** rule list, click **Add Rule**. In the dialog box displayed, configure the CC attack protection rule by referring to **Figure 2-2**.

   In this example, only some parameters are described. Retain the default values for other parameters. **Table 2-2** describes some parameters.

Figure 2-2 Configuring CC attack protection rules

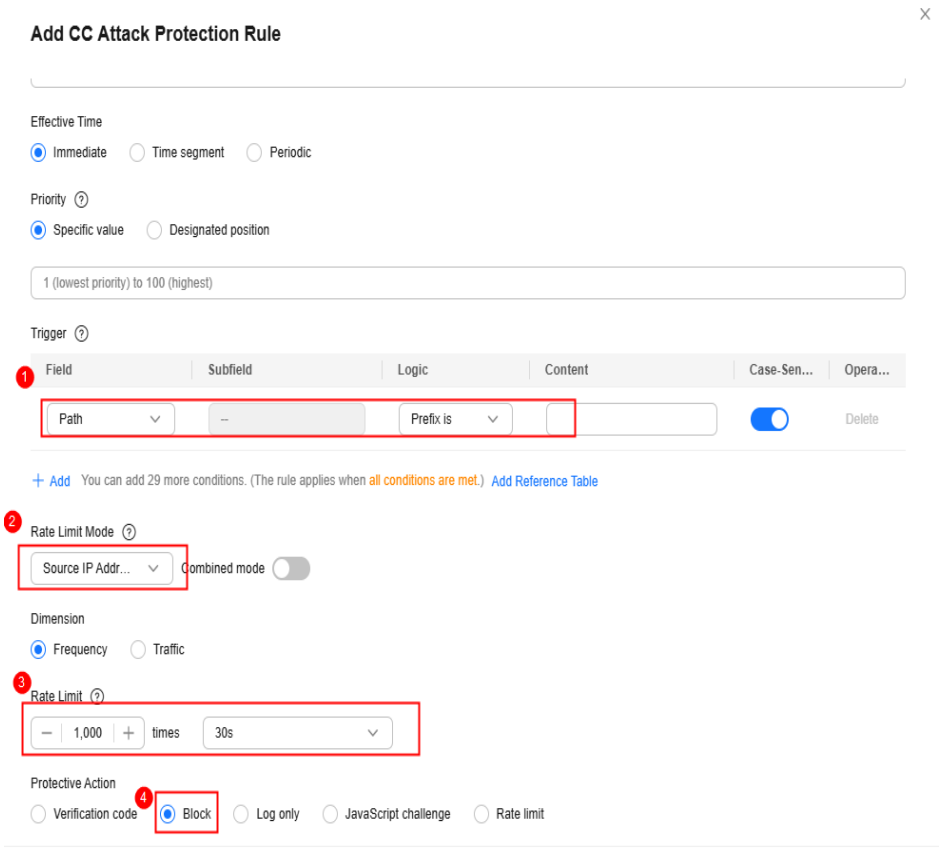


Table 2-2 Mandatory parameters

Parameter	Example Value	Description
Rate Limit Mode	Source IP Address	• Source IP address: A web visitor is identified by the IP address. • Source IP C Segment: Web visitor groups are defined by the source IP C segment. Access frequency is counted, and the rate is limited based on these visitor groups. • Cookie: A web visitor is identified by the cookie. • Header: A web visitor is identified by the customized HTTP header.

Parameter	Example Value	Description
Trigger	• **Field**: **Path** • **Logic**: **Prefix is** • **Content**: /	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 geolocation, path, IPv4, IPv6, cookie, method, header, Params, HTTP code, ASN, and range. **NOTE** If **Field** is set to **Geographical location** or **ASN**, IPv6 address requests cannot be matched. • Subfield: Configure this field only when **Cookie**, **Header**, or **Params** is selected for **Field**. **NOTICE** The length of a subfield cannot exceed 2048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. • Logic: Select the desired logical relationship from the drop-down list. **NOTE** 1. When **Logic** is set to **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is any of them**, **Suffix is any value**, or **Suffix is any of them**, you need to select a reference table. For details about how to create a reference table, see **Creating a Reference Table**. 2. If the condition is length-related logic, the length value cannot be too large. Large requests can be intercepted before reaching the backend engine, preventing them from being processed and making protection rules ineffective. • Content: Enter or select the content that matches the condition.
Rate Limit	**1,000 requests** within **30 seconds**	The maximum requests that a website visitor can initiate within the configured period. If the configured rate limit has been reached, EdgeSec will respond according to the protective action configured.

Parameter	Example Value	Description
Protective Action	**Block**	When the request frequency exceeds the **Rate Limit**, the following actions will be executed for new requests within the protection duration: • **Verification code**: EdgeSec allows requests that trigger the rule as long as your website visitors complete the required verification. Currently, verification code supports English. • Block: EdgeSec blocks requests that trigger the rule. • Log only: EdgeSec only logs requests that trigger the rule. • Rate limiting: When the **Rate Limit** is exceeded, the traffic rate is limited. **NOTE** • The verification code functionality requires JavaScript execution within a complete browser environment. Therefore, it will not function in environments lacking full browser capabilities, such as text-only terminals or devices with incomplete browser support. Incomplete browser environments are unable to execute the JavaScript code necessary for user identity and validity verification, thus preventing the completion of the verification process. • Upon successful verification code validation, the response page must be rendered in a browser environment to ensure proper page restoration. Failure to render the response page may lead to display issues, such as the persistent display of the human-machine verification interface.
Block Duration	**36,000 seconds**	Execution duration of the protection action. You are advised to set the protection duration to a value greater than the rate limiting period. The value ranges from 0 to 65535.

5. Confirm the configuration and click **OK**.

Step 4: Viewing Protection Statistics Events

When your website is under CC attacks, you can search for CC attack events in the event list to quickly locate attack sources or analyze attack events.

1. In the navigation pane on the left, choose **Edge Security** > **Statistics**. The **Statistics** page is displayed.
2. Set the query time to **Custom**. The range cannot exceed one month.

3. In the search box, select the target **Source IP** to query the event.
4. (Optional) In the **Operation** column of the target event, click **More** to handle the event.

   NOTE

   You can use one of the following methods to handle the event:

   - Handling a false alarm
   - Adding to address group
   - Adding to blacklist/whitelist

Related Information

For more information about CC attack protection, see **Configuring CC Attack Protection Rules**.

