Edge Security

API Reference

Issue 03

Date 2024-10-31

HUAWEI

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 Before You Start

1.1 Overview

EdgeSec (Edge Security) is a security protection service built on edge nodes.

ESA (Edge Security Acceleration) is a sub-product of EdgeSec. It provides cache acceleration and application security protection and supports multiple security functions, such as web attack defense, DDoS attack defense, and CC attack defense. ESA comprehensively improves the security protection capability of the acceleration network and ensures high-quality user experience and service security.

This document describes how to use application programming interfaces (APIs) to perform operations on EdgeSec, such as querying and updating.

If you plan to access EdgeSec through an API, ensure that you are familiar with EdgeSec. For more information, see **What Is EdgeSec?**

1.2 API Calling

EdgeSec provides Representational State Transfer (REST) APIs, and allows you to make API calls over HTTPS.

For details about how to call APIs, see **API Calling**.

1.3 Endpoints

An endpoint is the **request address** for calling an API.

Endpoints vary depending on services and endpoints. For the endpoints of all services, see **Regions and Endpoints**.

1.4 Concepts

- Account

An account is created upon successful registration. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used directly to perform routine management. For security purposes, create users and grant them permissions for routine management.

- User

  An IAM user is created by an account in IAM to use cloud services. Each IAM user has its own identity credentials (password and access keys).

- Region

  Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.

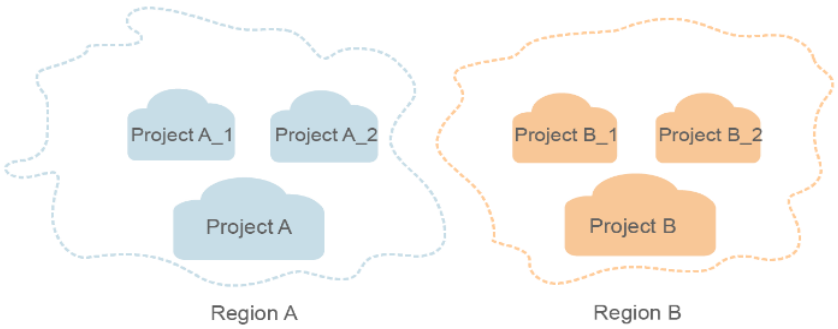
- Availability Zone (AZ)

  An AZ comprises one or multiple physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Compute, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.

- Project

  Projects group and isolate compute, storage, and network resources across physical regions. A default project is provided for each region, and subprojects can be created under each default project. Users can be granted permissions to access all resources in a specific project. For more refined access control, create subprojects under a project and purchase resources in the subprojects. Users can then be assigned permissions to access only specific resources in the subprojects.

Figure 1-1 Project isolation model



2 API Overview

You can use all functions of EdgeSec via APIs.

Type	Description
Anti-DDoS Data Query	Edge anti-DDoS data query APIs, including APIs for querying tenants' attack event data and tenant traffic data.
WAF Domain Name	Edge WAF domain name APIs, including APIs for querying the CDN domain name list, querying the edge WAF domain name list, and creating a protected domain name.
WAF Protection Policy	Edge WAF protection policy APIs, including APIs for creating and modifying protection policies, and querying the protection policy list.
Anti-DDoS Domain Name	Edge anti-DDoS domain name APIs, including adding, querying, and updating protected domain names.
Tenant Subscription Management	APIs used by tenants to query subscription information, including the API for querying purchased edge security products.
WAF Certificate Management	Edge WAF certificate management APIs, including creating, querying, and deleting certificates.

3 API Calling

3.1 Making an API Request

This section describes the structure of a REST API request, and uses the IAM API for **obtaining a user token** as an example to demonstrate how to call an API. The obtained token can then be used to authenticate the calling of other APIs.

Request URI

A request URI is in the following format:

{URI-scheme} :// {Endpoint} / {resource-path} ? {query-string}

Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be transmitted separately.

- **URI-scheme**:

  Protocol used to transmit requests. All APIs use HTTPS.
- **Endpoint**:

  Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**.

  For example, the endpoint of IAM in region **CN-Hong Kong** is **iam.ap-southeast-1.myhuaweicloud.com**.
- **resource-path**:

  Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.
- **query-string**:

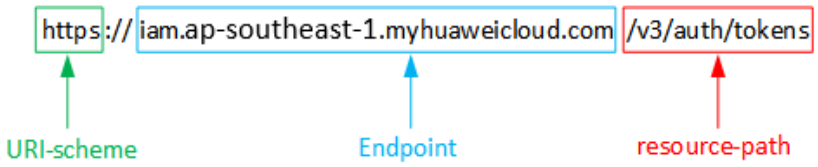
  Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain an IAM token in the **CN-Hong Kong** region, obtain the endpoint of IAM (iam.ap-southeast-1.myhuaweicloud.com)) for this region and

the **resource-path** (**/v3/auth/tokens**) in the URI of the API used to **obtain a user token**. Then, construct the URI as follows:

```
https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

Figure 3-1 Example URI



NOTE

To simplify the URI display in this document, each API is provided only with a **resource-path** and a request method. The **URI-scheme** of all APIs is **HTTPS**, and the endpoints of all APIs in the same region are identical.

Request Methods

The HTTP protocol defines the following request methods that can be used to send a request to the server:

- **GET**: requests the server to return specified resources.
- **PUT**: requests the server to update specified resources.
- **POST**: requests the server to add resources or perform special operations.
- **DELETE**: requests the server to delete specified resources, for example, an object.
- **HEAD**: same as GET except that the server must return only the response header.
- **PATCH**: requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API used to **obtain a user token**, the request method is POST. The request is as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request header fields are as follows:

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**. Other values of this field will be provided for specific APIs if any.
- **X-Auth-Token**: specifies a user token only for token-based API authentication. The user token is a response to the API used to **obtain a user token**. This API is the only one that does not require authentication.

> **NOTE**
>
> In addition to supporting token-based authentication, APIs also support authentication using access key ID/secret access key (AK/SK). During AK/SK-based authentication, an SDK is used to sign the request, and the **Authorization** (signature information) and **X-Sdk-Date** (time when the request is sent) header fields are automatically added to the request.
>
> For more information, see **AK/SK-based Authentication**.

The API used to **obtain a user token** does not require authentication. Therefore, only the **Content-Type** field needs to be added to requests for calling the API. An example of such requests is as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

Request Body

The body of a request is often sent in a structured format as specified in the **Content-Type** header field. The request body transfers content except the request header.

The request body varies between APIs. Some APIs do not require the request body, such as the APIs requested using the GET and DELETE methods.

In the case of the API used to **obtain a user token**, the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Set ***username*** to the name of a user, ***domainname*** to the name of the account that the user belongs to, ********* to the user's login password, and ***xxxxxxxxxxxxxxxxx*** to the project name. You can learn more information about projects from **Regions and Endpoints**. Check the value of the **Region** column.

> **NOTE**
>
> The **scope** parameter specifies where a token takes effect. You can set **scope** to an account or a project under an account. In the following example, the token takes effect only for the resources in a specified project. For more information about this API, see **Obtaining a User Token**.

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "*********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxxxxxxxxxxx"
            }
        }
```



```
    }
}
```

If all data required for the API request is available, you can send the request to call the API through **curl**, **Postman**, or coding. In the response to the API used to obtain a user token, **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

3.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

- Token-based authentication: Requests are authenticated using a token.
- AK/SK-based authentication: Requests are authenticated by encrypting the request body using an AK/SK pair. This method is recommended because it provides higher security than token-based authentication.

Token-based Authentication

NOTE

The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the IAM API used to obtain a user token.

A token specifies temporary permissions in a computer system. During API authentication using a token, the token is added to requests to get permissions for calling the API.

The token can be obtained by calling the required API. For more information, see **Obtaining a User Token**. A project-level token is required for calling this API, that is, **auth.scope** must be set to **project** in the request body. Example:

```
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxx"
            }
        }
    }
}
```

After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when calling other APIs. For example, if the token is **ABCDEFJ....**, **X-Auth-Token: ABCDEFJ....** can be added to a request as follows:


```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK-based Authentication

NOTE

AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.

In AK/SK-based authentication, AK/SK is used to sign requests and the signature is then added to the requests for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests. For details about how to sign requests and use the signing SDK, see **API Signature Guide**.

NOTICE

The signing SDK is only used for signing requests and is different from the SDKs provided by services.

3.3 Returned Values

Status Code

After sending a request, you will receive a response, including a status code, response header, and response body.

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see **Status Code**.

For example, if status code **201** is returned for calling the API used to **obtain a user token**, the request is successful.

Response Header

A response header corresponds to a request header, for example, **Content-Type**.

Figure 3-2 shows the response header for the API of **obtaining a user token**, in which **x-subject-token** is the desired user token. Then, you can use the token to authenticate the calling of other APIs.

Figure 3-2 Header of the response to the request for obtaining a user token

(Optional) Response Body

A response body is generally returned in a structured format, corresponding to the **Content-Type** in the response header, and is used to transfer content other than the response header.

The following shows part of the response body for the API to **obtain a user token**. For the sake of space, only part of the content is displayed here.

```
{
    "token": {
        "expires_at": "2019-02-13T06:52:13.855000Z",
        "methods": [
            "password"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "region_id": "xxxxxxxx",
......
```

If an error occurs during API calling, the system returns an error code and a message to you. The following shows the format of an error response body:

```
{
    "error": {
        "message": "The request you have made requires authentication.",
        "title": "Unauthorized"
    }
}
```

In the preceding information, **error_code** is an error code, and **error_msg** describes the error.

4 API

4.1 Protected Domain Name Management

4.1.1 Querying the Protected Domain Name List

Function

Queries the protection domain name list.

URI

GET /v1/edgesec/configuration/domains

Table 4-1 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Query offset.
limit	No	Integer	Number of records on each page of the query list.
domain_name	No	String	Domain name.
policy_name	No	String	Policy name.
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.

Request Parameters

Table 4-2 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Response Parameters

Status code: 200

Table 4-3 Response body parameters

Parameter	Type	Description
total	Long	Total number of protected domain names.
domain_used_quota	Long	Used domain name quota.
domain_list	Array of **DomainInfo** objects	Details about a protected domain name.

Table 4-4 DomainInfo

Parameter	Type	Description
id	String	Domain name ID.
domain_name	String	Domain name.
enterprise_project_id	String	Enterprise project ID.
dispatch_status	String	• Scheduling status: • Scheduling exception: dispatch_abnormal • Unscheduled: un_dispatch • Scheduling: dispatching • Scheduled: dispatched • Deleting: dispatch_deleting
web_name	String	Website name.
description	String	Description
policy_id	String	Policy ID.

Parameter	Type	Description
protect_status	String	Protection status: • Protected: on • Not protected: off
create_time	Long	Time when the domain name is created.
update_time	Long	Time when the domain name is updated.

Status code: 400

Table 4-5 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-6 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-7 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.1.2 Creating a Domain Name

Function

This API is used to create a protected domain name.

URI

POST /v1/edgesec/configuration/domains

Request Parameters

Table 4-8 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Table 4-9 Request body parameters

Parameter	Mandatory	Type	Description
domain_name	Yes	String	Protected domain name (port allowed).
enterprise_project_id	Yes	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.
policy_id	No	String	ID of the policy associated with the protected domain name.
description	No	String	Domain name description.

Response Parameters

Status code: 400

Table 4-10 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-11 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-12 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Response returned normally.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.1.3 Querying Details About a Protected Domain Name

Function

This API is used to query a protected domain name.

URI

GET /v1/edgesec/configuration/domains/{domain_id}

Table 4-13 Path Parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Protected domain name ID.

Request Parameters

Table 4-14 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

Status code: 200

Table 4-15 Response body parameters

Parameter	Type	Description
id	String	Domain name ID.
domain_name	String	Domain name.
enterprise_project_id	String	Enterprise project ID.
description	String	Domain name description.
policy_id	String	Policy ID.
protect_status	String	Protection status: • Protected: on • Not protected: off
create_time	Long	Time when the domain name is created.
update_time	Long	Time when the domain name is updated.

Status code: 400

Table 4-16 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code

Parameter	Type	Description
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-17 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-18 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.1.4 Updating Protected Domain Names

Function

This API is used to update protected domain names.

URI

PUT /v1/edgesec/configuration/domains/{domain_id}

Table 4-19 Path Parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Domain name.

Request Parameters

Table 4-20 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-21 Request body parameters

Parameter	Mandatory	Type	Description
protect_status	No	String	Protection status. The value can be on (protected) or off (unprotected).

Parameter	Mandatory	Type	Description
description	No	String	Domain name description.

Response Parameters

Status code: 400

Table 4-22 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-23 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-24 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Response returned normally.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.1.5 Deleting a Protected Domain Name

Function

This API is used to delete a protected domain name.

URI

DELETE /v1/edgesec/configuration/domains/{domain_id}

Table 4-25 Path Parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Protected domain name ID.

Table 4-26 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.

Request Parameters

Table 4-27 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-28 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-29 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-30 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	No Content
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.2 HTTP Protection Policy Management

4.2.1 This API is used to query the protection policy list.

Function

This API is used to query the protection policy list.

URI

GET /v1/edgesec/configuration/http/policies

Table 4-31 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project. It can be obtained by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number, which is required for pagination query.
pagesize	No	Integer	Pagination query parameter. The number of records displayed on each page is specified by pagesize.
name	No	String	Policy name used for fuzzy query
hostname	No	String	Domain name used for fuzzy query

Request Parameters

Table 4-32 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

Status code: 200

Table 4-33 Response body parameters

Parameter	Type	Description
total	Integer	Total number of policies.
items	Array of **ShowHttpPolicyResponseBody** objects	Content of the policy.

Table 4-34 ShowHttpPolicyResponseBody

Parameter	Type	Description
id	String	Policy ID.
name	String	Protection policy name.
level	Integer	Protection level.
full_detection	Boolean	Detection mode in the precise protection rule.
action	**HttpPolicyAction** object	Operation.
robot_action	**HttpPolicyAction** object	Operation.
options	**HttpPolicyOption** object	Option.
bind_host	Array of **HttpPolicyBindHost** objects	Basic information about the protected domain.
extend	Map<String,String>	Extended field.
third_bot_options	Map<String,third_bot_options>	Third-party BOT operation.
wap_managed_ruleset_id	String	ID of the hosting rule set for basic web protection.

Table 4-35 HttpPolicyAction

Parameter	Type	Description
category	String	Protection level.
followed_action_id	String	Attack penalty rule ID.

Table 4-36 HttpPolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled.
common	Boolean	Whether general check is enabled.
bot_enable	Boolean	Whether full anti-crawler protection is enabled.

Parameter	Type	Description
crawler	Boolean	Whether anti-crawler protection with feature libraries is enabled.
crawler_engine	Boolean	Whether the search engine is enabled.
crawler_scanner	Boolean	Whether the scanner is enabled.
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled.
crawler_other	Boolean	Whether other crawler check is enabled.
webshell	Boolean	Whether web shell detection is enabled
cc	Boolean	Whether the CC attack protection rule is enabled.
custom	Boolean	Whether precise protection is enabled.
followed_action	Boolean	Whether known attack source detection is enabled.
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled.
geoip	Boolean	Whether the geolocation rule is enabled.
ignore	Boolean	Whether false alarm masking is enabled.
privacy	Boolean	Whether data masking is enabled.
antitamper	Boolean	Whether the web tamper protection is enabled.
antileakage	Boolean	Whether the information leakage prevention is enabled.
anticrawler	Boolean	Whether the JavaScript anti-crawler rule is enabled.
third_bot_river	Boolean	Whether the third-party BOT is enabled

Table 4-37 HttpPolicyBindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-38 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-39 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-40 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.2.2 This API is used to create a protection policy.

Function

This API is used to create a protection policy.

URI

POST /v1/edgesec/configuration/http/policies

Request Parameters

Table 4-41 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Table 4-42 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Protection policy name.

Response Parameters

Status code: 200

Table 4-43 Response body parameters

Parameter	Type	Description
id	String	Policy ID.
name	String	Protection policy name.
level	Integer	Protection level.
full_detection	Boolean	Detection mode in the precise protection rule.
action	**HttpPolicyAction** object	Operation.
robot_action	**HttpPolicyAction** object	Operation.
options	**HttpPolicyOption** object	Option.
bind_host	Array of **HttpPolicyBindHost** objects	Basic information about the protected domain.
extend	Map<String,String>	Extended field.
third_bot_options	Map<String,third_bot_options>	Third-party BOT operation.
wap_managed_ruleset_id	String	ID of the hosting rule set for basic web protection.

Table 4-44 HttpPolicyAction

Parameter	Type	Description
category	String	Protection level.
followed_action_id	String	Attack penalty rule ID.

Table 4-45 HttpPolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled.
common	Boolean	Whether general check is enabled.
bot_enable	Boolean	Whether full anti-crawler protection is enabled.

Parameter	Type	Description
crawler	Boolean	Whether anti-crawler protection with feature libraries is enabled.
crawler_engine	Boolean	Whether the search engine is enabled.
crawler_scanner	Boolean	Whether the scanner is enabled.
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled.
crawler_other	Boolean	Whether other crawler check is enabled.
webshell	Boolean	Whether web shell detection is enabled
cc	Boolean	Whether the CC attack protection rule is enabled.
custom	Boolean	Whether precise protection is enabled.
followed_action	Boolean	Whether known attack source detection is enabled.
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled.
geoip	Boolean	Whether the geolocation rule is enabled.
ignore	Boolean	Whether false alarm masking is enabled.
privacy	Boolean	Whether data masking is enabled.
antitamper	Boolean	Whether the web tamper protection is enabled.
antileakage	Boolean	Whether the information leakage prevention is enabled.
anticrawler	Boolean	Whether the JavaScript anti-crawler rule is enabled.
third_bot_river	Boolean	Whether the third-party BOT is enabled

Table 4-46 HttpPolicyBindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-47 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-48 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-49 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Created
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.2.3 This API is used to query a protection policy.

Function

This API is used to query a protection policy.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}

Table 4-50 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-51 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

Status code: 200

Table 4-52 Response body parameters

Parameter	Type	Description
id	String	Policy ID.
name	String	Protection policy name.
level	Integer	Protection level.
full_detection	Boolean	Detection mode in the precise protection rule.
action	**HttpPolicyAction** object	Operation.
robot_action	**HttpPolicyAction** object	Operation.
options	**HttpPolicyOption** object	Option.
bind_host	Array of **HttpPolicyBindHost** objects	Basic information about the protected domain.
extend	Map<String,String>	Extended field.
third_bot_options	Map<String,third_bot_options>	Third-party BOT operation.
wap_managed_ruleset_id	String	ID of the hosting rule set for basic web protection.

Table 4-53 HttpPolicyAction

Parameter	Type	Description
category	String	Protection level.
followed_action_id	String	Attack penalty rule ID.

Table 4-54 HttpPolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled.
common	Boolean	Whether general check is enabled.
bot_enable	Boolean	Whether full anti-crawler protection is enabled.

Parameter	Type	Description
crawler	Boolean	Whether anti-crawler protection with feature libraries is enabled.
crawler_engine	Boolean	Whether the search engine is enabled.
crawler_scanner	Boolean	Whether the scanner is enabled.
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled.
crawler_other	Boolean	Whether other crawler check is enabled.
webshell	Boolean	Whether web shell detection is enabled
cc	Boolean	Whether the CC attack protection rule is enabled.
custom	Boolean	Whether precise protection is enabled.
followed_action	Boolean	Whether known attack source detection is enabled.
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled.
geoip	Boolean	Whether the geolocation rule is enabled.
ignore	Boolean	Whether false alarm masking is enabled.
privacy	Boolean	Whether data masking is enabled.
antitamper	Boolean	Whether the web tamper protection is enabled.
antileakage	Boolean	Whether the information leakage prevention is enabled.
anticrawler	Boolean	Whether the JavaScript anti-crawler rule is enabled.
third_bot_river	Boolean	Whether the third-party BOT is enabled

Table 4-55 HttpPolicyBindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-56 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-57 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-58 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.2.4 This API is used to update a protection policy.

Function

This API is used to update a protection policy.

URI

PUT /v1/edgesec/configuration/http/policies/{policy_id}

Table 4-59 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-60 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-61 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Protection policy name.

Parameter	Mandatory	Type	Description
action	No	**HttpPolicyAction** object	Operation.
options	No	**HttpPolicyOption** object	Option.
level	No	Integer	Protection level.
full_detection	No	Boolean	Detection mode in the precise protection rule.
robot_action	No	**HttpPolicyAction** object	Operation.
third_bot_options	No	**HttpThirdBotOptions** object	Third-party BOT operation.
extend	No	Map<String,String>	Extended field.

Table 4-62 HttpPolicyOption

Parameter	Mandatory	Type	Description
webattack	No	Boolean	Whether basic web protection is enabled.
common	No	Boolean	Whether general check is enabled.
bot_enable	No	Boolean	Whether full anti-crawler protection is enabled.
crawler	No	Boolean	Whether anti-crawler protection with feature libraries is enabled.
crawler_engine	No	Boolean	Whether the search engine is enabled.
crawler_scanner	No	Boolean	Whether the scanner is enabled.
crawler_script	No	Boolean	Whether the JavaScript anti-crawler is enabled.
crawler_other	No	Boolean	Whether other crawler check is enabled.
webshell	No	Boolean	Whether web shell detection is enabled

Parameter	Mandatory	Type	Description
cc	No	Boolean	Whether the CC attack protection rule is enabled.
custom	No	Boolean	Whether precise protection is enabled.
followed_action	No	Boolean	Whether known attack source detection is enabled.
whiteblackip	No	Boolean	Whether blacklist and whitelist protection is enabled.
geoip	No	Boolean	Whether the geolocation rule is enabled.
ignore	No	Boolean	Whether false alarm masking is enabled.
privacy	No	Boolean	Whether data masking is enabled.
antitamper	No	Boolean	Whether the web tamper protection is enabled.
antileakage	No	Boolean	Whether the information leakage prevention is enabled.
anticrawler	No	Boolean	Whether the JavaScript anti-crawler rule is enabled.
third_bot_river	No	Boolean	Whether the third-party BOT is enabled

Table 4-63 HttpPolicyAction

Parameter	Mandatory	Type	Description
category	No	String	Protection level.
followed_action_id	No	String	Attack penalty rule ID.

Table 4-64 HttpThirdBotOptions

Parameter	Mandatory	Type	Description
river_config	No	**HttpRiverConfig** object	River Security configuration items

Table 4-65 HttpRiverConfig

Parameter	Mandatory	Type	Description
site_id	No	String	River Security site ID.
site_name	No	String	River Security site name.
connect_timeout	No	Integer	Connection timeout (ms).
read_timeout	No	Integer	Read timeout (ms).
send_timeout	No	Integer	Write timeout (ms).

Response Parameters

Status code: 200

Table 4-66 Response body parameters

Parameter	Type	Description
id	String	Policy ID.
name	String	Protection policy name.
level	Integer	Protection level.
full_detection	Boolean	Detection mode in the precise protection rule.
action	**HttpPolicyAction** object	Operation.
robot_action	**HttpPolicyAction** object	Operation.
options	**HttpPolicyOption** object	Option.
bind_host	Array of **HttpPolicyBindHost** objects	Basic information about the protected domain.
extend	Map<String,String>	Extended field.
third_bot_options	Map<String,third_bot_options>	Third-party BOT operation.
wap_managed_ruleset_id	String	ID of the hosting rule set for basic web protection.

Table 4-67 HttpPolicyAction

Parameter	Type	Description
category	String	Protection level.
followed_action_id	String	Attack penalty rule ID.

Table 4-68 HttpPolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled.
common	Boolean	Whether general check is enabled.
bot_enable	Boolean	Whether full anti-crawler protection is enabled.
crawler	Boolean	Whether anti-crawler protection with feature libraries is enabled.
crawler_engine	Boolean	Whether the search engine is enabled.
crawler_scanner	Boolean	Whether the scanner is enabled.
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled.
crawler_other	Boolean	Whether other crawler check is enabled.
webshell	Boolean	Whether web shell detection is enabled
cc	Boolean	Whether the CC attack protection rule is enabled.
custom	Boolean	Whether precise protection is enabled.
followed_action	Boolean	Whether known attack source detection is enabled.
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled.
geoip	Boolean	Whether the geolocation rule is enabled.
ignore	Boolean	Whether false alarm masking is enabled.
privacy	Boolean	Whether data masking is enabled.
antitamper	Boolean	Whether the web tamper protection is enabled.
antileakage	Boolean	Whether the information leakage prevention is enabled.

Parameter	Type	Description
anticrawler	Boolean	Whether the JavaScript anti-crawler rule is enabled.
third_bot_river	Boolean	Whether the third-party BOT is enabled

Table 4-69 HttpPolicyBindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-70 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-71 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-72 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.2.5 This API is used to delete a protection policy.

Function

This API is used to delete a protection policy.

URI

DELETE /v1/edgesec/configuration/http/policies/{policy_id}

Table 4-73 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-74 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-75 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-76 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-77 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	No Content
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.2.6 This API is used to update domain names a policy applies to.

Function

This API is used to update domain names a policy applies to.

URI

POST /v1/edgesec/configuration/http/policies/{policy_id}/hosts

Table 4-78 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-79 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Table 4-80 Request body parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.
hosts	Yes	Array of strings	ID of the domain name to be associated.

Response Parameters

Status code: 200

Table 4-81 Response body parameters

Parameter	Type	Description
id	String	Policy ID.
name	String	Protection policy name.
level	Integer	Protection level.
full_detection	Boolean	Detection mode in the precise protection rule.
action	**HttpPolicyAction** object	Operation.
robot_action	**HttpPolicyAction** object	Operation.

Parameter	Type	Description
options	**HttpPolicyOption** object	Option.
bind_host	Array of **HttpPolicyBindHost** objects	Basic information about the protected domain.
extend	Map<String,String>	Extended field.
third_bot_options	Map<String,third_bot_options>	Third-party BOT operation.
wap_managed_ruleset_id	String	ID of the hosting rule set for basic web protection.

Table 4-82 HttpPolicyAction

Parameter	Type	Description
category	String	Protection level.
followed_action_id	String	Attack penalty rule ID.

Table 4-83 HttpPolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled.
common	Boolean	Whether general check is enabled.
bot_enable	Boolean	Whether full anti-crawler protection is enabled.
crawler	Boolean	Whether anti-crawler protection with feature libraries is enabled.
crawler_engine	Boolean	Whether the search engine is enabled.
crawler_scanner	Boolean	Whether the scanner is enabled.
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled.
crawler_other	Boolean	Whether other crawler check is enabled.
webshell	Boolean	Whether web shell detection is enabled

Parameter	Type	Description
cc	Boolean	Whether the CC attack protection rule is enabled.
custom	Boolean	Whether precise protection is enabled.
followed_action	Boolean	Whether known attack source detection is enabled.
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled.
geoip	Boolean	Whether the geolocation rule is enabled.
ignore	Boolean	Whether false alarm masking is enabled.
privacy	Boolean	Whether data masking is enabled.
antitamper	Boolean	Whether the web tamper protection is enabled.
antileakage	Boolean	Whether the information leakage prevention is enabled.
anticrawler	Boolean	Whether the JavaScript anti-crawler rule is enabled.
third_bot_river	Boolean	Whether the third-party BOT is enabled

Table 4-84 HttpPolicyBindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-85 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-86 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-87 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.2.7 This API is used to update a protection policy rule.

Function

This API is used to update a protection policy rule.

URI

PUT /v1/edgesec/configuration/http/policies/{policy_id}/{rule_type}/{rule_id}/status

Table 4-88 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_type	Yes	String	Protection Rules cc-rule| access-control-rule| blocktrustip-rule|privacy-rule| ignore-rule|geoip-rule| punishment-rule
rule_id	Yes	String	Protection policy ID.

Request Parameters

Table 4-89 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-90 Request body parameters

Parameter	Mandatory	Type	Description
status	Yes	Integer	0: disabled; 1: enabled

Response Parameters

Status code: 200

Table 4-91 Response body parameters

Parameter	Type	Description
category	String	Rule category.
description	String	Description.
id	String	Rule ID.
policyid	String	Policy ID.
status	Integer	Rule status.
timestamp	Number	Time when a rule is added.

Status code: 400

Table 4-92 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-93 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-94 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.3 EdgeSec HTTP Protection Rule Management - CC

4.3.1 This API is used to query the CC attack defense rules.

Function

This API is used to query the CC attack defense rules.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/cc-rule

Table 4-95 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Table 4-96 Query Parameters

Parameter	Mandatory	Type	Description
name	No	String	Rule name
page	No	Integer	Page number, which is required for pagination query.
pagesize	No	Integer	Pagination query parameter. The number of records displayed on each page is specified by pagesize.

Request Parameters

Table 4-97 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-98 Response body parameters

Parameter	Type	Description
total	Integer	Number of CC rules in a policy
items	Array of **ShowHttpCcRuleResponseBody** objects	CC rule list

Table 4-99 ShowHttpCcRuleResponseBody

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
priority	Integer	Priority of a CC rule. A larger value indicates a higher priority. The default value is 1.
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule enabling status
mode	Integer	Rule type (0: standard; 1: advanced)
total_num	Integer	Number of requests of all users in a period
limit_num	Integer	Number of requests of a single user in a period
limit_period	Integer	Rate limit period
lock_time	Integer	Lock duration
tag_type	String	Protection mode
tag_index	String	Protection mode tag
tag_condition	**HttpCcRuleCondition** object	Protection rule condition
unlock_num	Integer	Number of allow actions
domain_aggregation	Boolean	Aggregate domain name
conditions	Array of **HttpCcRuleCondition** objects	The parameters in the condition list are complex and are cascaded. Add a false alarm masking rule on the console. Press F12 to view the request parameters whose path suffix is /cc-rule and method is POST.
action	**HttpRuleAction** object	Action of the protection rule.
producer	Integer	Source
time_mode	String	Effective mode
start	Long	Start time of the customized effective period
terminal	Long	End time of the customized effective period

Parameter	Type	Description
period_type	String	Type of the daily effective time period. Currently, only day is supported.
time_range	Array of **TimeRangeItem** objects	Daily effective time period

Table 4-100 HttpCcRuleCondition

Parameter	Type	Description
category	String	Protection rule field
index	String	Subfield. When category is set to params, cookie, or header, this parameter is mandatory and you need to set this parameter based on the site requirements.
contents	Array of strings	Logical matching content of the condition list. This parameter is mandatory when the value of logic_operation does not end with any or all.
logic_operation	String	Condition matching logic • If the field type category is url, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, or len_not_equal. • If the field type category is ip or ipv6, the matching logic can be equal, not_equal, equal_any, or not_equal_all. • If the field type category is params, cookie, or header, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist, or not_exist.

Parameter	Type	Description
value_list_id	String	ID of the referenced table This parameter is mandatory when the value of logic_operation ends with any or all. In addition, the referenced table type must be the same as the category type.
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	• 1: all subfields • 2: any subfield

Table 4-101 HttpRuleAction

Parameter	Type	Description
category	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.
followed_action_id	String	Attack punishment rule ID. This parameter is available only when category is set to block.
detail	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-102 HttpRuleActionDetail

Parameter	Type	Description
redirect_url	String	URL to which the page is redirected.
response	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-103 HttpRuleActionResponse

Parameter	Type	Description
content_type	String	Content type.
content	String	Content

Table 4-104 TimeRangeItem

Parameter	Type	Description
st	Integer	Start time of the daily effective period
end	Integer	End time of the daily effective period

Status code: 400

Table 4-105 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-106 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-107 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.3.2 This API is used to create a CC attack protection rule.

Function

This API is used to create a CC attack protection rule.

URI

POST /v1/edgesec/configuration/http/policies/{policy_id}/cc-rule

Table 4-108 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-109 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-110 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Rule name
priority	Yes	Integer	Priority of the CC rule. A larger value indicates a higher priority. The default value is 1. This parameter is mandatory during rule creation.
description	No	String	Rule description, which contains a maximum of 512 characters.
mode	Yes	Integer	CC protection rule mode. Currently, only rules of the advanced CC protection mode can be created. • 0: Standard. Only the protection path of a domain name can be restricted. • 1: Advanced. The path, IP address, cookie, header, and params fields can all be restricted.
total_num	No	Integer	Number of requests of all users in a period
limit_num	Yes	Integer	Number of requests of a single user in a period
limit_period	Yes	Integer	Rate limit period
lock_time	No	Integer	Block duration
tag_type	Yes	String	Protection mode
tag_index	No	String	Protection mode tag
tag_condition	No	**HttpCcRuleCondition** object	Protection rule condition
unlock_num	No	Integer	Number of allow actions
domain_aggregation	No	Boolean	Aggregate domain name

Parameter	Mandatory	Type	Description
conditions	No	Array of **HttpCcRuleCondition** objects	Rate limit condition of the CC attack protection rule. This parameter is mandatory when the CC attack protection rule is in advanced mode (mode is set to 1).
action	Yes	**HttpRuleAction** object	Action of the protection rule.
time_mode	Yes	String	Effective mode
start	No	Long	Start time of the customized effective period
terminal	No	Long	End time of the customized effective period
period_type	No	String	Type of the daily effective time period. Currently, only day is supported.
time_range	No	Array of **TimeRangeItem** objects	Daily effective time period

Table 4-111 HttpCcRuleCondition

Parameter	Mandatory	Type	Description
category	Yes	String	Protection rule field
index	No	String	Subfield. When category is set to params, cookie, or header, this parameter is mandatory and you need to set this parameter based on the site requirements.
contents	No	Array of strings	Logical matching content of the condition list. This parameter is mandatory when the value of logic_operation does not end with any or all.

Parameter	Mandatory	Type	Description
logic_operation	Yes	String	Condition matching logic • If the field type category is url, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, or len_not_equal. • If the field type category is ip or ipv6, the matching logic can be equal, not_equal, equal_any, or not_equal_all. • If the field type category is params, cookie, or header, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist, or not_exist.
value_list_id	No	String	ID of the referenced table This parameter is mandatory when the value of logic_operation ends with any or all. In addition, the referenced table type must be the same as the category type.
size	No	Long	This field is used if the protection rule involves a threshold.

Parameter	Mandatory	Type	Description
check_all_indexes_logic	No	Integer	• 1: all subfields • 2: any subfield

Table 4-112 HttpRuleAction

Parameter	Mandatory	Type	Description
category	Yes	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.
followed_action_id	No	String	Attack punishment rule ID. This parameter is available only when category is set to block.
detail	No	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-113 HttpRuleActionDetail

Parameter	Mandatory	Type	Description
redirect_url	No	String	URL to which the page is redirected.
response	No	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-114 HttpRuleActionResponse

Parameter	Mandatory	Type	Description
content_type	No	String	Content type.
content	No	String	Content

Table 4-115 TimeRangeItem

Parameter	Mandatory	Type	Description
st	No	Integer	Start time of the daily effective period
end	No	Integer	End time of the daily effective period

Response Parameters

Status code: 200

Table 4-116 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
priority	Integer	Priority of a CC rule. A larger value indicates a higher priority. The default value is 1.
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule enabling status
mode	Integer	Rule type (0: standard; 1: advanced)
total_num	Integer	Number of requests of all users in a period
limit_num	Integer	Number of requests of a single user in a period
limit_period	Integer	Rate limit period
lock_time	Integer	Lock duration
tag_type	String	Protection mode
tag_index	String	Protection mode tag
tag_condition	**HttpCcRuleCondition** object	Protection rule condition
unlock_num	Integer	Number of allow actions
domain_aggregation	Boolean	Aggregate domain name

Parameter	Type	Description
conditions	Array of **HttpCcRuleCondition** objects	The parameters in the condition list are complex and are cascaded. Add a false alarm masking rule on the console. Press F12 to view the request parameters whose path suffix is /cc-rule and method is POST.
action	**HttpRuleAction** object	Action of the protection rule.
producer	Integer	Source
time_mode	String	Effective mode
start	Long	Start time of the customized effective period
terminal	Long	End time of the customized effective period
period_type	String	Type of the daily effective time period. Currently, only day is supported.
time_range	Array of **TimeRangeItem** objects	Daily effective time period

Table 4-117 HttpCcRuleCondition

Parameter	Type	Description
category	String	Protection rule field
index	String	Subfield. When category is set to params, cookie, or header, this parameter is mandatory and you need to set this parameter based on the site requirements.
contents	Array of strings	Logical matching content of the condition list. This parameter is mandatory when the value of logic_operation does not end with any or all.

Parameter	Type	Description
logic_operation	String	Condition matching logic • If the field type category is url, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, or len_not_equal. • If the field type category is ip or ipv6, the matching logic can be equal, not_equal, equal_any, or not_equal_all. • If the field type category is params, cookie, or header, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist, or not_exist.
value_list_id	String	ID of the referenced table This parameter is mandatory when the value of logic_operation ends with any or all. In addition, the referenced table type must be the same as the category type.
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	• 1: all subfields • 2: any subfield

Table 4-118 HttpRuleAction

Parameter	Type	Description
category	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.
followed_action_id	String	Attack punishment rule ID. This parameter is available only when category is set to block.

Parameter	Type	Description
detail	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-119 HttpRuleActionDetail

Parameter	Type	Description
redirect_url	String	URL to which the page is redirected.
response	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-120 HttpRuleActionResponse

Parameter	Type	Description
content_type	String	Content type.
content	String	Content

Table 4-121 TimeRangeItem

Parameter	Type	Description
st	Integer	Start time of the daily effective period
end	Integer	End time of the daily effective period

Status code: 400

Table 4-122 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-123 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-124 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.3.3 This API is used to query a CC rule.

Function

This API is used to query a CC rule.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/cc-rule/{rule_id}

Table 4-125 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	CC rule ID.

Request Parameters

Table 4-126 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-127 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
priority	Integer	Priority of a CC rule. A larger value indicates a higher priority. The default value is 1.
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created

Parameter	Type	Description
description	String	Rule description
status	Integer	Rule enabling status
mode	Integer	Rule type (0: standard; 1: advanced)
total_num	Integer	Number of requests of all users in a period
limit_num	Integer	Number of requests of a single user in a period
limit_period	Integer	Rate limit period
lock_time	Integer	Lock duration
tag_type	String	Protection mode
tag_index	String	Protection mode tag
tag_condition	**HttpCcRuleCondition** object	Protection rule condition
unlock_num	Integer	Number of allow actions
domain_aggregation	Boolean	Aggregate domain name
conditions	Array of **HttpCcRuleCondition** objects	The parameters in the condition list are complex and are cascaded. Add a false alarm masking rule on the console. Press F12 to view the request parameters whose path suffix is /cc-rule and method is POST.
action	**HttpRuleAction** object	Action of the protection rule.
producer	Integer	Source
time_mode	String	Effective mode
start	Long	Start time of the customized effective period
terminal	Long	End time of the customized effective period
period_type	String	Type of the daily effective time period. Currently, only day is supported.
time_range	Array of **TimeRangeItem** objects	Daily effective time period

Table 4-128 HttpCcRuleCondition

Parameter	Type	Description
category	String	Protection rule field
index	String	Subfield. When category is set to params, cookie, or header, this parameter is mandatory and you need to set this parameter based on the site requirements.
contents	Array of strings	Logical matching content of the condition list. This parameter is mandatory when the value of logic_operation does not end with any or all.
logic_operation	String	Condition matching logic • If the field type category is url, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, or len_not_equal. • If the field type category is ip or ipv6, the matching logic can be equal, not_equal, equal_any, or not_equal_all. • If the field type category is params, cookie, or header, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist, or not_exist.
value_list_id	String	ID of the referenced table This parameter is mandatory when the value of logic_operation ends with any or all. In addition, the referenced table type must be the same as the category type.
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	• 1: all subfields • 2: any subfield

Table 4-129 HttpRuleAction

Parameter	Type	Description
category	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.
followed_action_id	String	Attack punishment rule ID. This parameter is available only when category is set to block.
detail	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-130 HttpRuleActionDetail

Parameter	Type	Description
redirect_url	String	URL to which the page is redirected.
response	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-131 HttpRuleActionResponse

Parameter	Type	Description
content_type	String	Content type.
content	String	Content

Table 4-132 TimeRangeItem

Parameter	Type	Description
st	Integer	Start time of the daily effective period
end	Integer	End time of the daily effective period

Status code: 400

Table 4-133 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-134 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-135 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.3.4 This API is used to update a CC protection rule.

Function

This API is used to update a CC protection rule.

URI

PUT /v1/edgesec/configuration/http/policies/{policy_id}/cc-rule/{rule_id}

Table 4-136 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	CC rule ID.

Request Parameters

Table 4-137 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-138 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Rule name

Parameter	Mandatory	Type	Description
priority	Yes	Integer	Priority of a CC rule. A larger value indicates a higher priority. The default value is 1.
description	No	String	Rule description, which contains a maximum of 512 characters.
status	No	Integer	Rule enabling status
mode	Yes	Integer	CC protection rule mode. Currently, only rules of the advanced CC protection mode can be created. • 0: Standard. Only the protection path of a domain name can be restricted. • 1: Advanced. The path, IP address, cookie, header, and params fields can all be restricted.
total_num	No	Integer	Number of requests of all users in a period
limit_num	Yes	Integer	Number of requests of a single user in a period
limit_period	Yes	Integer	Rate limit period
lock_time	No	Integer	Lock duration
tag_type	Yes	String	Rate limiting mode. • ip: A website visitor is identified by the IP address. • cookie: A website visitor is identified by the cookie key value. • header: A web visitor is identified by the header. • other: A website visitor is identified by the Referer field (user-defined request source). • policy: policy-based rate limiting • domain: domain name-based rate limiting • url: URL rate limiting

Parameter	Mandatory	Type	Description
tag_index	No	String	User ID. This parameter is mandatory when the rate limiting mode is user-based rate limiting (cookie or header). • If cookie is selected, 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. If header is selected, you need to configure the HTTP header that can identify web visitors based on your website requirements.
tag_condition	No	**HttpCcRuleCondition** object	Protection rule condition
unlock_num	No	Integer	Number of allow actions
domain_aggregation	No	Boolean	Aggregate domain name
value_case	No	Boolean	Case-sensitivity. The default value is false, indicating data is stored in lower case letters.
conditions	Yes	Array of **HttpCcRuleCondition** objects	Rate limiting condition
action	Yes	**HttpRuleAction** object	Action of the protection rule.
time_mode	No	String	Effective mode
start	No	Long	Start time of the customized effective period

Parameter	Mandatory	Type	Description
terminal	No	Long	End time of the customized effective period
period_type	No	String	Type of the daily effective time period. Currently, only day is supported.
time_range	No	Array of **TimeRangeItem** objects	Daily effective time period

Table 4-139 HttpCcRuleCondition

Parameter	Mandatory	Type	Description
category	Yes	String	Protection rule field
index	No	String	Subfield. When category is set to params, cookie, or header, this parameter is mandatory and you need to set this parameter based on the site requirements.
contents	No	Array of strings	Logical matching content of the condition list. This parameter is mandatory when the value of logic_operation does not end with any or all.

Parameter	Mandatory	Type	Description
logic_operation	Yes	String	Condition matching logic • If the field type category is url, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, or len_not_equal. • If the field type category is ip or ipv6, the matching logic can be equal, not_equal, equal_any, or not_equal_all. • If the field type category is params, cookie, or header, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist, or not_exist.
value_list_id	No	String	ID of the referenced table This parameter is mandatory when the value of logic_operation ends with any or all. In addition, the referenced table type must be the same as the category type.
size	No	Long	This field is used if the protection rule involves a threshold.

Parameter	Mandatory	Type	Description
check_all_indexes_logic	No	Integer	• 1: all subfields • 2: any subfield

Table 4-140 HttpRuleAction

Parameter	Mandatory	Type	Description
category	Yes	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.
followed_action_id	No	String	Attack punishment rule ID. This parameter is available only when category is set to block.
detail	No	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-141 HttpRuleActionDetail

Parameter	Mandatory	Type	Description
redirect_url	No	String	URL to which the page is redirected.
response	No	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-142 HttpRuleActionResponse

Parameter	Mandatory	Type	Description
content_type	No	String	Content type.
content	No	String	Content

Table 4-143 TimeRangeItem

Parameter	Mandatory	Type	Description
st	No	Integer	Start time of the daily effective period
end	No	Integer	End time of the daily effective period

Response Parameters

Status code: 200

Table 4-144 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
priority	Integer	Priority of a CC rule. A larger value indicates a higher priority. The default value is 1.
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule enabling status
mode	Integer	Rule type (0: standard; 1: advanced)
total_num	Integer	Number of requests of all users in a period
limit_num	Integer	Number of requests of a single user in a period
limit_period	Integer	Rate limit period
lock_time	Integer	Lock duration
tag_type	String	Protection mode
tag_index	String	Protection mode tag
tag_condition	**HttpCcRuleCondition** object	Protection rule condition
unlock_num	Integer	Number of allow actions
domain_aggregation	Boolean	Aggregate domain name

Parameter	Type	Description
conditions	Array of **HttpCcRuleCondition** objects	The parameters in the condition list are complex and are cascaded. Add a false alarm masking rule on the console. Press F12 to view the request parameters whose path suffix is /cc-rule and method is POST.
action	**HttpRuleAction** object	Action of the protection rule.
producer	Integer	Source
time_mode	String	Effective mode
start	Long	Start time of the customized effective period
terminal	Long	End time of the customized effective period
period_type	String	Type of the daily effective time period. Currently, only day is supported.
time_range	Array of **TimeRangeItem** objects	Daily effective time period

Table 4-145 HttpCcRuleCondition

Parameter	Type	Description
category	String	Protection rule field
index	String	Subfield. When category is set to params, cookie, or header, this parameter is mandatory and you need to set this parameter based on the site requirements.
contents	Array of strings	Logical matching content of the condition list. This parameter is mandatory when the value of logic_operation does not end with any or all.

Parameter	Type	Description
logic_operation	String	Condition matching logic • If the field type category is url, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, or len_not_equal. • If the field type category is ip or ipv6, the matching logic can be equal, not_equal, equal_any, or not_equal_all. • If the field type category is params, cookie, or header, the matching logic can be contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist, or not_exist.
value_list_id	String	ID of the referenced table This parameter is mandatory when the value of logic_operation ends with any or all. In addition, the referenced table type must be the same as the category type.
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	• 1: all subfields • 2: any subfield

Table 4-146 HttpRuleAction

Parameter	Type	Description
category	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.
followed_action_id	String	Attack punishment rule ID. This parameter is available only when category is set to block.

Parameter	Type	Description
detail	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-147 HttpRuleActionDetail

Parameter	Type	Description
redirect_url	String	URL to which the page is redirected.
response	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-148 HttpRuleActionResponse

Parameter	Type	Description
content_type	String	Content type.
content	String	Content

Table 4-149 TimeRangeItem

Parameter	Type	Description
st	Integer	Start time of the daily effective period
end	Integer	End time of the daily effective period

Status code: 400

Table 4-150 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-151 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-152 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.3.5 This API is used to delete a CC rule.

Function

This API is used to delete a CC rule.

URI

DELETE /v1/edgesec/configuration/http/policies/{policy_id}/cc-rule/{rule_id}

Table 4-153 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	CC rule ID.

Request Parameters

Table 4-154 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-155 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-156 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-157 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	The rule is deleted.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.4 HTTP Protection Rule Management - Precise Protection

4.4.1 This API is used to query precise protection rules.

Function

This API is used to query precise protection rules.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/access-control-rule

Table 4-158 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Table 4-159 Query Parameters

Parameter	Mandatory	Type	Description
name	No	String	Rule name
page	No	Integer	Page number, which is required for pagination query.
pagesize	No	Integer	Pagination query parameter. The number of records displayed on each page is specified by pagesize.

Request Parameters

Table 4-160 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-161 Response body parameters

Parameter	Type	Description
total	Integer	Number of protection rules in a policy
items	Array of **ShowHttpAccessControlRuleResponseBody** objects	Protection rule list

Table 4-162 ShowHttpAccessControlRuleResponseBody

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.
policy_id	String	ID of the policy to which the rule belongs.
policy_name	String	Name of the policy to which the rule belongs.
timestamp	Long	Time when a rule is created
description	String	Rule description.
status	Integer	Rule enabling status
time	Boolean	Whether to set the effective time
start	Long	Effective time
terminal	Long	Expiration time
priority	Integer	Priority
conditions	Array of **HttpAccessControlRuleCondition** objects	Hit condition.
action	**HttpRuleAction** object	Action of the protection rule.
producer	Integer	Source

Table 4-163 HttpAccessControlRuleCondition

Parameter	Type	Description
category	String	Field type. The options are url, custom_asn, custom_geoip, robot, user-agent, ip, params, cookie, referer, header, method, request_line, request, response_code, response_length, response_time, response_header and response_body.
index	String	Subfield: • If the field type is url, custom_asn, custom_geoip, robot, user-agent, referer, request_line, method, request, response_code, response_length, response_time or response_body, the index parameter does not need to be passed in. • If the field type is params, cookie, header, or response_header and the subfield is customized, the index field is a customized subfield.
contents	Array of strings	Content list
logic_operation	String	Processing logic
value_list_id	String	ID of the reference table
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	1. All subfields/2. Any subfield

Table 4-164 HttpRuleAction

Parameter	Type	Description
category	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.
followed_action_id	String	Attack punishment rule ID. This parameter is available only when category is set to block.
detail	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-165 HttpRuleActionDetail

Parameter	Type	Description
redirect_url	String	URL to which the page is redirected.
response	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-166 HttpRuleActionResponse

Parameter	Type	Description
content_type	String	Content type.
content	String	Content

Status code: 400

Table 4-167 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-168 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-169 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.4.2 This API is used to create a precise protection rule.

Function

This API is used to create a precise protection rule.

URI

POST /v1/edgesec/configuration/http/policies/{policy_id}/access-control-rule

Table 4-170 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-171 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-172 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Rule name
description	No	String	Rule description, which contains a maximum of 512 characters.
time	Yes	Boolean	Time when the precise protection rule takes effect. • false: The rule takes effect immediately. • true: The effective time is customized.
start	No	Long	Timestamp (s) when the precise protection rule takes effect. This parameter needs to be set only when time is set to true.
terminal	No	Long	Timestamp (s) when the precise protection rule expires. This parameter needs to be set only when time is set to true.
priority	Yes	Integer	Priority of a rule. A small value indicates a high priority. If two rules are assigned with the same priority, the rule added earlier has higher priority. Value range: 0 to 1000.

Parameter	Mandatory	Type	Description
conditions	Yes	Array of **HttpAccessControlRuleCondition** objects	Hit condition.
action	Yes	**HttpRuleAction** object	Action of the protection rule.

Table 4-173 HttpAccessControlRuleCondition

Parameter	Mandatory	Type	Description
category	No	String	Field type. The options are url, custom_asn, custom_geoip, robot, user-agent, ip, params, cookie, referer, header, method, request_line, request, response_code, response_length, response_time, response_header and response_body.
index	No	String	Subfield: • If the field type is url, custom_asn, custom_geoip, robot, user-agent, referer, request_line, method, request, response_code, response_length, response_time or response_body, the index parameter does not need to be passed in. • If the field type is params, cookie, header, or response_header and the subfield is customized, the index field is a customized subfield.
contents	No	Array of strings	Content list
logic_operation	No	String	Processing logic
value_list_id	No	String	ID of the reference table

Parameter	Mandatory	Type	Description
size	No	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	No	Integer	1. All subfields/2. Any subfield

Table 4-174 HttpRuleAction

Parameter	Mandatory	Type	Description
category	Yes	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.
followed_action_id	No	String	Attack punishment rule ID. This parameter is available only when category is set to block.
detail	No	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-175 HttpRuleActionDetail

Parameter	Mandatory	Type	Description
redirect_url	No	String	URL to which the page is redirected.
response	No	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-176 HttpRuleActionResponse

Parameter	Mandatory	Type	Description
content_type	No	String	Content type.
content	No	String	Content

Response Parameters

Status code: 200

Table 4-177 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.
policy_id	String	ID of the policy to which the rule belongs.
policy_name	String	Name of the policy to which the rule belongs.
timestamp	Long	Time when a rule is created
description	String	Rule description.
status	Integer	Rule enabling status
time	Boolean	Whether to set the effective time
start	Long	Effective time
terminal	Long	Expiration time
priority	Integer	Priority
conditions	Array of **HttpAccessControlRuleCondition** objects	Hit condition.
action	**HttpRuleAction** object	Action of the protection rule.
producer	Integer	Source

Table 4-178 HttpAccessControlRuleCondition

Parameter	Type	Description
category	String	Field type. The options are url, custom_asn, custom_geoip, robot, user-agent, ip, params, cookie, referer, header, method, request_line, request, response_code, response_length, response_time, response_header and response_body.

Parameter	Type	Description
index	String	Subfield: • If the field type is url, custom_asn, custom_geoip, robot, user-agent, referer, request_line, method, request, response_code, response_length, response_time or response_body, the index parameter does not need to be passed in. • If the field type is params, cookie, header, or response_header and the subfield is customized, the index field is a customized subfield.
contents	Array of strings	Content list
logic_operation	String	Processing logic
value_list_id	String	ID of the reference table
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	1. All subfields/2. Any subfield

Table 4-179 HttpRuleAction

Parameter	Type	Description
category	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.
followed_action_id	String	Attack punishment rule ID. This parameter is available only when category is set to block.
detail	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-180 HttpRuleActionDetail

Parameter	Type	Description
redirect_url	String	URL to which the page is redirected.

Parameter	Type	Description
response	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-181 HttpRuleActionResponse

Parameter	Type	Description
content_type	String	Content type.
content	String	Content

Status code: 400

Table 4-182 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-183 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-184 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.4.3 This API is used to query a precise protection rule.

Function

This API is used to query a precise protection rule.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/access-control-rule/{rule_id}

Table 4-185 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-186 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-187 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.
policy_id	String	ID of the policy to which the rule belongs.
policy_name	String	Name of the policy to which the rule belongs.
timestamp	Long	Time when a rule is created
description	String	Rule description.
status	Integer	Rule enabling status
time	Boolean	Whether to set the effective time
start	Long	Effective time
terminal	Long	Expiration time
priority	Integer	Priority
conditions	Array of **HttpAccessControlRuleCondition** objects	Hit condition.
action	**HttpRuleAction** object	Action of the protection rule.

Parameter	Type	Description
producer	Integer	Source

Table 4-188 HttpAccessControlRuleCondition

Parameter	Type	Description
category	String	Field type. The options are url, custom_asn, custom_geoip, robot, user-agent, ip, params, cookie, referer, header, method, request_line, request, response_code, response_length, response_time, response_header and response_body.
index	String	Subfield: • If the field type is url, custom_asn, custom_geoip, robot, user-agent, referer, request_line, method, request, response_code, response_length, response_time or response_body, the index parameter does not need to be passed in. • If the field type is params, cookie, header, or response_header and the subfield is customized, the index field is a customized subfield.
contents	Array of strings	Content list
logic_operation	String	Processing logic
value_list_id	String	ID of the reference table
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	1. All subfields/2. Any subfield

Table 4-189 HttpRuleAction

Parameter	Type	Description
category	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.

Parameter	Type	Description
followed_action_id	String	Attack punishment rule ID. This parameter is available only when category is set to block.
detail	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-190 HttpRuleActionDetail

Parameter	Type	Description
redirect_url	String	URL to which the page is redirected.
response	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-191 HttpRuleActionResponse

Parameter	Type	Description
content_type	String	Content type.
content	String	Content

Status code: 400

Table 4-192 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-193 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-194 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.4.4 This API is used to update a precise protection rule.

Function

This API is used to update a precise protection rule.

URI

PUT /v1/edgesec/configuration/http/policies/{policy_id}/access-control-rule/{rule_id}

Table 4-195 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-196 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-197 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Rule name.
description	No	String	Rule description, which contains a maximum of 512 characters.
status	No	Integer	Rule enabling status
time	Yes	Boolean	Whether to set the effective time
start	No	Long	Effective time
terminal	No	Long	Expiration time
priority	Yes	Integer	Priority

Parameter	Mandatory	Type	Description
conditions	Yes	Array of **HttpAccessControlRuleCondition** objects	Hit condition
action	Yes	**HttpRuleAction** object	Action of the protection rule.

Table 4-198 HttpAccessControlRuleCondition

Parameter	Mandatory	Type	Description
category	No	String	Field type. The options are url, custom_asn, custom_geoip, robot, user-agent, ip, params, cookie, referer, header, method, request_line, request, response_code, response_length, response_time, response_header and response_body.
index	No	String	Subfield: • If the field type is url, custom_asn, custom_geoip, robot, user-agent, referer, request_line, method, request, response_code, response_length, response_time or response_body, the index parameter does not need to be passed in. • If the field type is params, cookie, header, or response_header and the subfield is customized, the index field is a customized subfield.
contents	No	Array of strings	Content list
logic_operation	No	String	Processing logic
value_list_id	No	String	ID of the reference table

Parameter	Mandatory	Type	Description
size	No	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	No	Integer	1. All subfields/2. Any subfield

Table 4-199 HttpRuleAction

Parameter	Mandatory	Type	Description
category	Yes	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.
followed_action_id	No	String	Attack punishment rule ID. This parameter is available only when category is set to block.
detail	No	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-200 HttpRuleActionDetail

Parameter	Mandatory	Type	Description
redirect_url	No	String	URL to which the page is redirected.
response	No	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-201 HttpRuleActionResponse

Parameter	Mandatory	Type	Description
content_type	No	String	Content type.
content	No	String	Content

Response Parameters

Status code: 200

Table 4-202 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.
policy_id	String	ID of the policy to which the rule belongs.
policy_name	String	Name of the policy to which the rule belongs.
timestamp	Long	Time when a rule is created
description	String	Rule description.
status	Integer	Rule enabling status
time	Boolean	Whether to set the effective time
start	Long	Effective time
terminal	Long	Expiration time
priority	Integer	Priority
conditions	Array of **HttpAccessControlRuleCondition** objects	Hit condition.
action	**HttpRuleAction** object	Action of the protection rule.
producer	Integer	Source

Table 4-203 HttpAccessControlRuleCondition

Parameter	Type	Description
category	String	Field type. The options are url, custom_asn, custom_geoip, robot, user-agent, ip, params, cookie, referer, header, method, request_line, request, response_code, response_length, response_time, response_header and response_body.

Parameter	Type	Description
index	String	Subfield: • If the field type is url, custom_asn, custom_geoip, robot, user-agent, referer, request_line, method, request, response_code, response_length, response_time or response_body, the index parameter does not need to be passed in. • If the field type is params, cookie, header, or response_header and the subfield is customized, the index field is a customized subfield.
contents	Array of strings	Content list
logic_operation	String	Processing logic
value_list_id	String	ID of the reference table
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	1. All subfields/2. Any subfield

Table 4-204 HttpRuleAction

Parameter	Type	Description
category	String	Operation type, • block: block. • pass: allow. • log: Only log detected attacks.
followed_action_id	String	Attack punishment rule ID. This parameter is available only when category is set to block.
detail	**HttpRuleActionDetail** object	Action of the protection rule.

Table 4-205 HttpRuleActionDetail

Parameter	Type	Description
redirect_url	String	URL to which the page is redirected.

Parameter	Type	Description
response	**HttpRuleActionResponse** object	Return page of the protection rule

Table 4-206 HttpRuleActionResponse

Parameter	Type	Description
content_type	String	Content type.
content	String	Content

Status code: 400

Table 4-207 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-208 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-209 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.4.5 This API is used to delete a precise protection rule.

Function

This API is used to delete a precise protection rule.

URI

DELETE /v1/edgesec/configuration/http/policies/{policy_id}/access-control-rule/{rule_id}

Table 4-210 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-211 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-212 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-213 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-214 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	The rule is deleted.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.5 HTTP Protection Rule Management - IP Address Blacklist and Whitelist

4.5.1 This API is used to query IP address blacklist and whitelist rules.

Function

This API is used to query IP address blacklist and whitelist rules.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/blocktrustip-rule

Table 4-215 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Table 4-216 Query Parameters

Parameter	Mandatory	Type	Description
name	No	String	Rule name
addr	No	String	IP address/IP address segment.
page	No	Integer	Page number, which is required for pagination query.
pagesize	No	Integer	Pagination query parameter. The number of records displayed on each page is specified by pagesize.

Request Parameters

Table 4-217 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-218 Response body parameters

Parameter	Type	Description
total	Integer	Number of protection rules in a policy
items	Array of **ShowHttpBlockTrustIpRuleResponseBody** objects	Protection rule list

Parameter	Type	Description
size	Long	Number of IP addresses or IP address segments in a protection rule

Table 4-219 ShowHttpBlockTrustIpRuleResponseBody

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule status: • 0: disabled • 1: enabled
addr	String	IP address/address segment
white	Integer	• 0: Block • 1: Allow • 2: Record only
followed_action_id	String	Attack penalty rule ID
ip_group	**HttpIpGroup** object	IP address group

Table 4-220 HttpIpGroup

Parameter	Type	Description
id	String	IP address group ID
name	String	IP address group name
ips	Array of strings	IP address/address segment list
size	Integer	IP address/address segment size
description	String	IP address group description

Parameter	Type	Description
create_time	Long	Timestamp when an IP address group is created

Status code: 400

Table 4-221 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-222 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-223 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.5.2 This API is used to create an IP address blacklist or whitelist rule.

Function

This API is used to create an IP address blacklist or whitelist rule.

URI

POST /v1/edgesec/configuration/http/policies/{policy_id}/blocktrustip-rule

Table 4-224 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-225 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-226 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Rule name
description	No	String	Rule description, which contains a maximum of 512 characters.
addr	No	String	IP address/address segment. At least one IP address/ address segment or IP address group ID must be specified.
white	Yes	Integer	• 0: Block • 1: Allow • 2: Record only
followed_action_id	No	String	Attack penalty rule ID
ip_group_id	No	String	IP address group ID. At least one IP address/address segment or IP address group ID must be specified.

Response Parameters

Status code: 200

Table 4-227 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule status: • 0: disabled • 1: enabled

Parameter	Type	Description
addr	String	IP address/address segment
white	Integer	• 0: Block • 1: Allow • 2: Record only
followed_action_id	String	Attack penalty rule ID
ip_group	HttpIpGroup object	IP address group

Table 4-228 HttpIpGroup

Parameter	Type	Description
id	String	IP address group ID
name	String	IP address group name
ips	Array of strings	IP address/address segment list
size	Integer	IP address/address segment size
description	String	IP address group description
create_time	Long	Timestamp when an IP address group is created

Status code: 400

Table 4-229 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-230 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-231 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.5.3 This API is used to query an IP address blacklist or whitelist rule.

Function

This API is used to query an IP address blacklist or whitelist rule.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/blocktrustip-rule/{rule_id}

Table 4-232 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-233 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-234 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description

Parameter	Type	Description
status	Integer	Rule status: • 0: disabled • 1: enabled
addr	String	IP address/address segment
white	Integer	• 0: Block • 1: Allow • 2: Record only
followed_action_id	String	Attack penalty rule ID
ip_group	**HttpIpGroup** object	IP address group

Table 4-235 HttpIpGroup

Parameter	Type	Description
id	String	IP address group ID
name	String	IP address group name
ips	Array of strings	IP address/address segment list
size	Integer	IP address/address segment size
description	String	IP address group description
create_time	Long	Timestamp when an IP address group is created

Status code: 400

Table 4-236 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-237 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-238 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.5.4 This API is used to update an IP address blacklist or whitelist rule.

Function

This API is used to update an IP address blacklist or whitelist rule.

URI

PUT /v1/edgesec/configuration/http/policies/{policy_id}/blocktrustip-rule/{rule_id}

Table 4-239 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-240 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-241 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Rule name
description	No	String	Rule description, which contains a maximum of 512 characters.
status	No	Integer	Rule status: • 0: disabled • 1: enabled
addr	No	String	IP address/address segment. At least one IP address/ address segment or IP address group ID must be specified.

Parameter	Mandatory	Type	Description
white	Yes	Integer	• 0: Block • 1: Allow • 2: Record only
followed_action_id	No	String	Attack penalty rule ID
ip_group_id	No	String	IP address group ID. At least one IP address/address segment or IP address group ID must be specified.

Response Parameters

Status code: 200

Table 4-242 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule status: • 0: disabled • 1: enabled
addr	String	IP address/address segment
white	Integer	• 0: Block • 1: Allow • 2: Record only
followed_action_id	String	Attack penalty rule ID
ip_group	**HttpIpGroup** object	IP address group

Table 4-243 HttpIpGroup

Parameter	Type	Description
id	String	IP address group ID
name	String	IP address group name
ips	Array of strings	IP address/address segment list
size	Integer	IP address/address segment size
description	String	IP address group description
create_time	Long	Timestamp when an IP address group is created

Status code: 400

Table 4-244 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-245 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-246 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.5.5 This API is used to delete a blacklist or whitelist rule.

Function

This API is used to delete a blacklist or whitelist rule.

URI

DELETE /v1/edgesec/configuration/http/policies/{policy_id}/blocktrustip-rule/{rule_id}

Table 4-247 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-248 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-249 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-250 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-251 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	The rule is deleted.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.6 HTTP Protection Rule Management - Geographical Location

4.6.1 This API is used to query the geolocation access control rules.

Function

This API is used to query the geolocation access control rules.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/geoip-rule

Table 4-252 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Table 4-253 Query Parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number, which is required for pagination query.
pagesize	No	Integer	Pagination query parameter. The number of records displayed on each page is specified by pagesize.

Request Parameters

Table 4-254 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-255 Response body parameters

Parameter	Type	Description
total	Integer	Number of protection rules in a policy
items	Array of **ShowHttpGeoIpRuleResponseBody** objects	Protection rule list

Table 4-256 ShowHttpGeoIpRuleResponseBody

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
policyid	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule enabling status
geo_ip	String	Geo-location
geo_tag_list	Array of strings	Geographical location list
white	Integer	Block/Allow/Record only

Status code: 400

Table 4-257 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-258 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-259 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.6.2 This API is used to create a geolocation access control rule.

Function

This API is used to create a geolocation access control rule.

URI

POST /v1/edgesec/configuration/http/policies/{policy_id}/geoip-rule

Table 4-260 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-261 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-262 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Rule name
description	No	String	Rule description, which contains a maximum of 512 characters.

Parameter	Mandatory	Type	Description
geo_ip	Yes	String	Select the region code and separate them with a vertical bar (|):\n(Beijing: CN_BJ, Shanghai: CN_SH, Tianjin: CN_TJ, Chongqing: CN_CQ, Guangdong: CN_GD, Zhejiang: CN_ZJ, Jiangsu: CN_JS, Fujian: CN_FJ, Jilin: CN_JL, Liaoning: CN_LN, Taiwan: CN_TW, Guizhou: CN_GZ, Anhui: CN_AH, Heilongjiang: CN_HL, Henan: CN_HA, Sichuan: CN_SC, Hebei: CN_HE, Yunnan: CN_YN, Hubei: CN_HB, Hainan: CN_HI, Qinghai: CN_QH, Hunan: CN_HN, Jiangxi: CN_JX, Shanxi: CN_SX, Shaanxi: CN_SN, Gansu: CN_GS, Shandong: CN_SD, Macao: CN_MO, Hong Kong: CN_HK, Ningxia: CN_NX, Guangxi: CN_GX, Xinjiang: CN_XJ, Tibet: CN_XZ, Inner Mongolia: CN_NM, India: IN, United States: US, Indonesia: ID, Pakistan: PK, Brazil: BR, Nigeria: NG, Bangladesh: BD, Russian Federation: RU, Japan: JP, Mexico: MX, Ethiopia: ET, Philippines: PH, Egypt: EG, Viet Nam: VN, Germany: DE, Turkey: TR, Thailand: TH, France: FR, United Kingdom: GB, Italy: IT, South Africa: ZA, Myanmar: MM, Kenya: KE, United Republic of Tanzania: TZ, Colombia: CO, Spain: ES, Ukraine: UA, Iraq: IQ, Poland: PL, Saudi Arabia: SA, Peru: PE, Uganda: UG, Malaysia: MY, Sudan: SD, Romania: RO, Afghanistan: AF, Canada: CA, Morocco: MA, Chile: CL, Democratic Republic of the Congo: CD, Iran, Islamic Republic of: IR, Korea, Republic of: KR, Angola: AO, Ghana: GH, Mozambique: MZ, Argentina: AR, Algeria: DZ, Nepal: NP, Madagascar: MG,

Parameter	Mandatory	Type	Description
			Korea, Democratic People's Republic of: KP, Cameroon: CM, Cote d'Ivoire: CI, Australia: AU, Netherlands: NL, Niger: NE, Sri Lanka: LK, Burkina Faso: BF, Uzbekistan: UZ, Mali: ML, Venezuela: VE, Kazakhstan: KZ, Malawi: MW, Zambia: ZM, Yemen: YE, Belgium: BE, Guatemala: GT, Syrian Arab Republic: SY, Ecuador: EC, Senegal: SN, Chad: TD, Somalia: SO, Zimbabwe: ZW, Guinea: GN, Rwanda: RW, Tunisia: TN, Benin: BJ, Czech Republic: CZ, Bolivia: BO, Cuba: CU, Burundi: BI, Haiti: HT, Cambodia: KH, Greece: GR, Dominican Republic: DO, Sweden: SE, Portugal: PT, Jordan: JO, South Sudan: SS, Azerbaijan: AZ, Hungary: HU, United Arab Emirates: AE, Honduras: HN, Belarus: BY, Tajikistan: TJ, Israel: IL, Austria: AT, Papua New Guinea: PG, Switzerland: CH, Togo: TG, Sierra Leone: SL, Lao People's Democratic Republic: LA, Bulgaria: BG, Serbia: RS, Paraguay: PY, Lebanon: LB, Libya: LY, Nicaragua: NI, El Salvador: SV, Kyrgyzstan: KG, Turkmenistan: TM, Denmark: DK, Singapore: SG, Finland: FI, Slovakia: SK, Norway: NO, Congo: CG, Costa Rica: CR, New Zealand: NZ, Ireland: IE, Oman: OM, Liberia: LR, Central African Republic: CF, Palestine, State of: PS, Mauritania: MR, Panama: PA, Kuwait: KW, Croatia: HR, Georgia: GE, Moldova, Republic of: MD, Uruguay: UY, Bosnia and Herzegovina: BA, Puerto Rico: PR, Mongolia: MN, Armenia: AM, Jamaica: JM, Albania: AL, Lithuania: LT, Qatar: QA, Namibia: NA,

Parameter	Mandatory	Type	Description
			Gambia: GM, Botswana: BW, Gabon: GA, Lesotho: LS, Macedonia, the Former Yugoslav Republic of: MK, Slovenia: SI, Latvia: LV, Guinea-Bissau: GW, Kosovo: XK, Bahrain: BH, Trinidad and Tobago: TT, Estonia: EE, Equatorial Guinea: GQ, Timor-Leste: TL, Mauritius: MU, Cyprus: CY, Eswatini: SZ, Djibouti: DJ, Fiji: FJ, Reunion: RE, Comoros: KM, Guyana: GY, Bhutan: BT, Solomon Islands: SB, Montenegro: ME, Luxembourg: LU, Suriname: SR, Cape Verde: CV, Maldives: MV, Western Sahara: EH, Malta: MT, Brunei Darussalam: BN, Guadeloupe: GP, Bahamas: BS, Belize: BZ, Martinique: MQ, Iceland: IS, French Guiana: GF, Vanuatu: VU, Barbados: BB, New Caledonia: NC, French Polynesia: PF, Mayotte: YT, Netherlands Antilles: AN, Sao Tome and Principe: ST, Samoa: WS, Saint Lucia: LC, Guam: GU, Curacao: CW, Kiribati: KI, Micronesia, Federated States of: FM, Grenada: GD, Saint Vincent and the Grenadines: VC, US Virgin Islands: VI, Jersey: JE, Aruba: AW, Tonga: TO, Seychelles: SC, Antigua and Barbuda: AG, Isle of Man: IM, Andorra: AD, Dominica: DM, Cayman Islands: KY, Bermuda: BM, Guernsey: GG, Marshall Islands: MH, Northern Mariana Islands: MP, Greenland: GL, American Samoa: AS, Saint Kitts and Nevis: KN, Faroe Islands: FO, Sint Maarten (Dutch part): SX, Monaco: MC, Liechtenstein: LI, Turks and Caicos Islands: TC, Saint Martin (French part): MF, San Marino: SM, Gibraltar:

Parameter	Mandatory	Type	Description
			GI, British Virgin Islands: VG, Åland Islands: AX, Bonaire: BQ, Palau: PW, Cook Islands: CK, Anguilla: AI, Nauru: NR, Wallis and Futuna: WF, Tuvalu: TV, Saint Barthelemy: BL, Saint Pierre and Miquelon: PM, Montserrat: MS, Saint Helena: SH, Falkland Islands (Malvinas): FK, Norfolk Island: NF, Niue: NU, Tokelau: TK, Christmas Island: CX, Holy See (Vatican City State): VA, Cocos (Keeling) Islands: CC, United States Minor Outlying Islands: UM, Pitcairn: PN, South Georgia and the South Sandwich Islands: GS, Antarctica: AQ, Bouvet Island: BV, Eritrea: ER, Heard Island and McDonald Islands: HM, British Indian Ocean Territory: IO, French Southern Territories: TF, Svalbard and Jan Mayen: SJ)
white	Yes	Integer	Protection action: • 0: Block • 1: Allow • 2: Record only

Response Parameters

Status code: 200

Table 4-263 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
policyid	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description

Parameter	Type	Description
status	Integer	Rule enabling status
geo_ip	String	Geo-location
geo_tag_list	Array of strings	Geographical location list
white	Integer	Block/Allow/Record only

Status code: 400

Table 4-264 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-265 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-266 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.6.3 This API is used to query a geolocation access control rule.

Function

This API is used to query a geolocation access control rule.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/geoip-rule/{rule_id}

Table 4-267 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-268 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-269 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
policyid	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule enabling status
geo_ip	String	Geo-location
geo_tag_list	Array of strings	Geographical location list
white	Integer	Block/Allow/Record only

Status code: 400

Table 4-270 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-271 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-272 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.6.4 This API is used to update a geolocation access control rule.

Function

This API is used to update a geolocation access control rule.

URI

PUT /v1/edgesec/configuration/http/policies/{policy_id}/geoip-rule/{rule_id}

Table 4-273 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-274 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-275 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Rule name
description	No	String	Rule description, which contains a maximum of 512 characters.
status	No	Integer	Rule enabling status

Parameter	Mandatory	Type	Description
geo_ip	Yes	String	Select the region code and separate them with a vertical bar (|):\n(Beijing: CN_BJ, Shanghai: CN_SH, Tianjin: CN_TJ, Chongqing: CN_CQ, Guangdong: CN_GD, Zhejiang: CN_ZJ, Jiangsu: CN_JS, Fujian: CN_FJ, Jilin: CN_JL, Liaoning: CN_LN, Taiwan: CN_TW, Guizhou: CN_GZ, Anhui: CN_AH, Heilongjiang: CN_HL, Henan: CN_HA, Sichuan: CN_SC, Hebei: CN_HE, Yunnan: CN_YN, Hubei: CN_HB, Hainan: CN_HI, Qinghai: CN_QH, Hunan: CN_HN, Jiangxi: CN_JX, Shanxi: CN_SX, Shaanxi: CN_SN, Gansu: CN_GS, Shandong: CN_SD, Macao: CN_MO, Hong Kong: CN_HK, Ningxia: CN_NX, Guangxi: CN_GX, Xinjiang: CN_XJ, Tibet: CN_XZ, Inner Mongolia: CN_NM, India: IN, United States: US, Indonesia: ID, Pakistan: PK, Brazil: BR, Nigeria: NG, Bangladesh: BD, Russian Federation: RU, Japan: JP, Mexico: MX, Ethiopia: ET, Philippines: PH, Egypt: EG, Viet Nam: VN, Germany: DE, Turkey: TR, Thailand: TH, France: FR, United Kingdom: GB, Italy: IT, South Africa: ZA, Myanmar: MM, Kenya: KE, United Republic of Tanzania: TZ, Colombia: CO, Spain: ES, Ukraine: UA, Iraq: IQ, Poland: PL, Saudi Arabia: SA, Peru: PE, Uganda: UG, Malaysia: MY, Sudan: SD, Romania: RO, Afghanistan: AF, Canada: CA, Morocco: MA, Chile: CL, Democratic Republic of the Congo: CD, Iran, Islamic Republic of: IR, Korea, Republic of: KR, Angola: AO, Ghana: GH, Mozambique: MZ, Argentina: AR, Algeria: DZ, Nepal: NP, Madagascar: MG,

Parameter	Mandatory	Type	Description
			Korea, Democratic People's Republic of: KP, Cameroon: CM, Cote d'Ivoire: CI, Australia: AU, Netherlands: NL, Niger: NE, Sri Lanka: LK, Burkina Faso: BF, Uzbekistan: UZ, Mali: ML, Venezuela: VE, Kazakhstan: KZ, Malawi: MW, Zambia: ZM, Yemen: YE, Belgium: BE, Guatemala: GT, Syrian Arab Republic: SY, Ecuador: EC, Senegal: SN, Chad: TD, Somalia: SO, Zimbabwe: ZW, Guinea: GN, Rwanda: RW, Tunisia: TN, Benin: BJ, Czech Republic: CZ, Bolivia: BO, Cuba: CU, Burundi: BI, Haiti: HT, Cambodia: KH, Greece: GR, Dominican Republic: DO, Sweden: SE, Portugal: PT, Jordan: JO, South Sudan: SS, Azerbaijan: AZ, Hungary: HU, United Arab Emirates: AE, Honduras: HN, Belarus: BY, Tajikistan: TJ, Israel: IL, Austria: AT, Papua New Guinea: PG, Switzerland: CH, Togo: TG, Sierra Leone: SL, Lao People's Democratic Republic: LA, Bulgaria: BG, Serbia: RS, Paraguay: PY, Lebanon: LB, Libya: LY, Nicaragua: NI, El Salvador: SV, Kyrgyzstan: KG, Turkmenistan: TM, Denmark: DK, Singapore: SG, Finland: FI, Slovakia: SK, Norway: NO, Congo: CG, Costa Rica: CR, New Zealand: NZ, Ireland: IE, Oman: OM, Liberia: LR, Central African Republic: CF, Palestine, State of: PS, Mauritania: MR, Panama: PA, Kuwait: KW, Croatia: HR, Georgia: GE, Moldova, Republic of: MD, Uruguay: UY, Bosnia and Herzegovina: BA, Puerto Rico: PR, Mongolia: MN, Armenia: AM, Jamaica: JM, Albania: AL, Lithuania: LT, Qatar: QA, Namibia: NA,

Parameter	Mandatory	Type	Description
			Gambia: GM, Botswana: BW, Gabon: GA, Lesotho: LS, Macedonia, the Former Yugoslav Republic of: MK, Slovenia: SI, Latvia: LV, Guinea-Bissau: GW, Kosovo: XK, Bahrain: BH, Trinidad and Tobago: TT, Estonia: EE, Equatorial Guinea: GQ, Timor-Leste: TL, Mauritius: MU, Cyprus: CY, Eswatini: SZ, Djibouti: DJ, Fiji: FJ, Reunion: RE, Comoros: KM, Guyana: GY, Bhutan: BT, Solomon Islands: SB, Montenegro: ME, Luxembourg: LU, Suriname: SR, Cape Verde: CV, Maldives: MV, Western Sahara: EH, Malta: MT, Brunei Darussalam: BN, Guadeloupe: GP, Bahamas: BS, Belize: BZ, Martinique: MQ, Iceland: IS, French Guiana: GF, Vanuatu: VU, Barbados: BB, New Caledonia: NC, French Polynesia: PF, Mayotte: YT, Netherlands Antilles: AN, Sao Tome and Principe: ST, Samoa: WS, Saint Lucia: LC, Guam: GU, Curacao: CW, Kiribati: KI, Micronesia, Federated States of: FM, Grenada: GD, Saint Vincent and the Grenadines: VC, US Virgin Islands: VI, Jersey: JE, Aruba: AW, Tonga: TO, Seychelles: SC, Antigua and Barbuda: AG, Isle of Man: IM, Andorra: AD, Dominica: DM, Cayman Islands: KY, Bermuda: BM, Guernsey: GG, Marshall Islands: MH, Northern Mariana Islands: MP, Greenland: GL, American Samoa: AS, Saint Kitts and Nevis: KN, Faroe Islands: FO, Sint Maarten (Dutch part): SX, Monaco: MC, Liechtenstein: LI, Turks and Caicos Islands: TC, Saint Martin (French part): MF, San Marino: SM, Gibraltar:

Parameter	Mandatory	Type	Description
			GI, British Virgin Islands: VG, Åland Islands: AX, Bonaire: BQ, Palau: PW, Cook Islands: CK, Anguilla: AI, Nauru: NR, Wallis and Futuna: WF, Tuvalu: TV, Saint Barthelemy: BL, Saint Pierre and Miquelon: PM, Montserrat: MS, Saint Helena: SH, Falkland Islands (Malvinas): FK, Norfolk Island: NF, Niue: NU, Tokelau: TK, Christmas Island: CX, Holy See (Vatican City State): VA, Cocos (Keeling) Islands: CC, United States Minor Outlying Islands: UM, Pitcairn: PN, South Georgia and the South Sandwich Islands: GS, Antarctica: AQ, Bouvet Island: BV, Eritrea: ER, Heard Island and McDonald Islands: HM, British Indian Ocean Territory: IO, French Southern Territories: TF, Svalbard and Jan Mayen: SJ)
white	Yes	Integer	Protection action: • 0: Block • 1: Allow • 2: Record only

Response Parameters

Status code: 200

Table 4-276 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
policyid	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description

Parameter	Type	Description
status	Integer	Rule enabling status
geo_ip	String	Geo-location
geo_tag_list	Array of strings	Geographical location list
white	Integer	Block/Allow/Record only

Status code: 400

Table 4-277 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-278 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-279 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.6.5 This API is used to delete a geolocation access control rule.

Function

This API is used to delete a geolocation access control rule.

URI

DELETE /v1/edgesec/configuration/http/policies/{policy_id}/geoip-rule/{rule_id}

Table 4-280 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-281 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-282 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-283 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-284 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	The rule is deleted.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.7 HTTP Protection Rule Management - False Alarm Masking

4.7.1 This API is used to query false alarm masking rules.

Function

This API is used to query false alarm masking rules.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/ignore-rule

Table 4-285 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Table 4-286 Query Parameters

Parameter	Mandatory	Type	Description
status	No	Integer	Rule enabling status
page	No	Integer	Page number, which is required for pagination query.
pagesize	No	Integer	Pagination query parameter. The number of records displayed on each page is specified by pagesize.
rule	No	String	Undetected module type

Request Parameters

Table 4-287 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-288 Response body parameters

Parameter	Type	Description
total	Integer	Number of protection rules in a policy
items	Array of **ShowHttpIgnoreRuleResponseBody** objects	Protection rule list

Table 4-289 ShowHttpIgnoreRuleResponseBody

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule enabling status
url	String	URL of the false alarm
rule	String	Rule No.
mode	Integer	False alarm masking mode. The default value is 0, indicating the old mode.
domains	Array of strings	Domain name list
url_logic	String	URL type of the masking rule (prefix or equal)
advanced	**HttpIgnoreRuleCondition** object	The parameters in the condition list are complex and are cascaded. Add a false alarm masking rule on the console. Press F12 to view the request parameters whose path suffix is /ignore-rule and method is POST.
conditions	Array of **HttpIgnoreRuleCondition** objects	Hit condition
hit_num	Integer	Hit count
update_time	Long	Timestamp for the last update
clear_time	Long	Timestamp for clearing the last hit count

Table 4-290 HttpIgnoreRuleCondition

Parameter	Type	Description
category	String	Field type. The value can be ip, url, params, cookie, or header.

Parameter	Type	Description
index	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield.
contents	Array of strings	Content list
logic_operation	String	Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported.
value_list_id	String	ID of the referenced table
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	1. All subfields/2. Any subfield

Status code: 400

Table 4-291 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-292 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code

Parameter	Type	Description
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-293 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.7.2 This API is used to add a false alarm masking rule.

Function

This API is used to add a false alarm masking rule.

URI

POST /v1/edgesec/configuration/http/policies/{policy_id}/ignore-rule

Table 4-294 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-295 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-296 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Rule name
description	No	String	Rule description, which contains a maximum of 512 characters.
url	No	String	URL of the false alarm
rule	Yes	String	Rule No.
mode	Yes	Integer	False alarm masking mode. The default value is 0, indicating the old mode.
domains	Yes	Array of strings	Domain name list
url_logic	No	String	URL type of the masking rule (prefix or equal)

Parameter	Mandatory	Type	Description
advanced	No	**HttpIgnoreRuleCondition** object	The parameters in the condition list are complex and are cascaded. Add a false alarm masking rule on the console. Press F12 to view the request parameters whose path suffix is /ignore-rule and method is POST.
conditions	Yes	Array of **HttpIgnoreRuleCondition** objects	Hit condition

Table 4-297 HttpIgnoreRuleCondition

Parameter	Mandatory	Type	Description
category	Yes	String	Field type. The value can be ip, url, params, cookie, or header.
index	No	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield.
contents	Yes	Array of strings	Content list
logic_operation	Yes	String	Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported.
value_list_id	No	String	ID of the referenced table

Parameter	Mandatory	Type	Description
size	No	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	No	Integer	1. All subfields/2. Any subfield

Response Parameters

Status code: 200

Table 4-298 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule enabling status
url	String	URL of the false alarm
rule	String	Rule No.
mode	Integer	False alarm masking mode. The default value is 0, indicating the old mode.
domains	Array of strings	Domain name list
url_logic	String	URL type of the masking rule (prefix or equal)
advanced	**HttpIgnoreRuleCondition** object	The parameters in the condition list are complex and are cascaded. Add a false alarm masking rule on the console. Press F12 to view the request parameters whose path suffix is /ignore-rule and method is POST.
conditions	Array of **HttpIgnoreRuleCondition** objects	Hit condition
hit_num	Integer	Hit count

Parameter	Type	Description
update_time	Long	Timestamp for the last update
clear_time	Long	Timestamp for clearing the last hit count

Table 4-299 HttpIgnoreRuleCondition

Parameter	Type	Description
category	String	Field type. The value can be ip, url, params, cookie, or header.
index	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield.
contents	Array of strings	Content list
logic_operation	String	Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported.
value_list_id	String	ID of the referenced table
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	1. All subfields/2. Any subfield

Status code: 400

Table 4-300 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-301 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-302 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK

Status Code	Description
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.7.3 This API is used to query a false alarm masking rule.

Function

This API is used to query a false alarm masking rule.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/ignore-rule/{rule_id}

Table 4-303 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-304 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-305 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule enabling status
url	String	URL of the false alarm
rule	String	Rule No.
mode	Integer	False alarm masking mode. The default value is 0, indicating the old mode.
domains	Array of strings	Domain name list
url_logic	String	URL type of the masking rule (prefix or equal)
advanced	**HttpIgnoreRuleCondition** object	The parameters in the condition list are complex and are cascaded. Add a false alarm masking rule on the console. Press F12 to view the request parameters whose path suffix is /ignore-rule and method is POST.
conditions	Array of **HttpIgnoreRuleCondition** objects	Hit condition
hit_num	Integer	Hit count
update_time	Long	Timestamp for the last update
clear_time	Long	Timestamp for clearing the last hit count

Table 4-306 HttpIgnoreRuleCondition

Parameter	Type	Description
category	String	Field type. The value can be ip, url, params, cookie, or header.

Parameter	Type	Description
index	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield.
contents	Array of strings	Content list
logic_operation	String	Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported.
value_list_id	String	ID of the referenced table
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	1. All subfields/2. Any subfield

Status code: 400

Table 4-307 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-308 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code

Parameter	Type	Description
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-309 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.7.4 This API is used to update a false alarm masking rule.

Function

This API is used to update a false alarm masking rule.

URI

PUT /v1/edgesec/configuration/http/policies/{policy_id}/ignore-rule/{rule_id}

Table 4-310 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-311 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-312 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Rule name
description	No	String	Rule description, which contains a maximum of 512 characters.
status	No	Integer	Rule enabling status
url	No	String	URL of the false alarm

Parameter	Mandatory	Type	Description
rule	Yes	String	Rule to be masked. One or more rules can be masked. Use semicolons (;) to separate multiple rules. • To mask a built-in tule, set the parameter to the rule ID. You can query the rule ID by navigating to Policies > Policy Name > Basic Web Protection > Advanced Settings > Protection Rules on the WAF console. The rule ID is also available in event details. • To mask a type of basic web protection rule needs, set this parameter to the name of the rule. xss: XSS attack; webshell: website Trojan; vuln: other types of attack; sqli: SQL injection attack; robot: malicious crawler; rfi: remote file inclusion; lfi: local file inclusion; cmdi: command injection attack • To mask the entire basic web protection module, set the parameter to all. • To mask all detection modules, set the parameter to bypass.
mode	Yes	Integer	False alarm masking mode. The default value is 0, indicating the old mode.
domains	Yes	Array of strings	Domain name or website to e protect. If the array length is 0, the rule takes effect for all domain names or websites.
url_logic	No	String	URL type of the masking rule (prefix or equal)

Parameter	Mandatory	Type	Description
advanced	No	**HttpIgnoreRuleCondition** object	The parameters in the condition list are complex and are cascaded. Add a false alarm masking rule on the console. Press F12 to view the request parameters whose path suffix is /ignore-rule and method is POST.
conditions	Yes	Array of **HttpIgnoreRuleCondition** objects	Hit condition

Table 4-313 HttpIgnoreRuleCondition

Parameter	Mandatory	Type	Description
category	Yes	String	Field type. The value can be ip, url, params, cookie, or header.
index	No	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield.
contents	Yes	Array of strings	Content list
logic_operation	Yes	String	Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported.
value_list_id	No	String	ID of the referenced table

Parameter	Mandatory	Type	Description
size	No	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	No	Integer	1. All subfields/2. Any subfield

Response Parameters

Status code: 200

Table 4-314 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule enabling status
url	String	URL of the false alarm
rule	String	Rule No.
mode	Integer	False alarm masking mode. The default value is 0, indicating the old mode.
domains	Array of strings	Domain name list
url_logic	String	URL type of the masking rule (prefix or equal)
advanced	**HttpIgnoreRuleCondition** object	The parameters in the condition list are complex and are cascaded. Add a false alarm masking rule on the console. Press F12 to view the request parameters whose path suffix is /ignore-rule and method is POST.
conditions	Array of **HttpIgnoreRuleCondition** objects	Hit condition
hit_num	Integer	Hit count

Parameter	Type	Description
update_time	Long	Timestamp for the last update
clear_time	Long	Timestamp for clearing the last hit count

Table 4-315 HttpIgnoreRuleCondition

Parameter	Type	Description
category	String	Field type. The value can be ip, url, params, cookie, or header.
index	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield.
contents	Array of strings	Content list
logic_operation	String	Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported.
value_list_id	String	ID of the referenced table
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	1. All subfields/2. Any subfield

Status code: 400

Table 4-316 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-317 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-318 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.

Status Code	Description
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.7.5 This API is used to delete a false alarm masking rule.

Function

This API is used to delete a false alarm masking rule.

URI

DELETE /v1/edgesec/configuration/http/policies/{policy_id}/ignore-rule/{rule_id}

Table 4-319 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-320 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-321 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-322 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-323 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	The rule is deleted.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.7.6 This API is used to reset a false alarm masking rule.

Function

This API is used to reset a false alarm masking rule.

URI

POST /v1/edgesec/configuration/http/policies/{policy_id}/ignore-rule/{rule_id}/recount

Table 4-324 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-325 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-326 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Rule name
policy_id	String	ID of the policy to which the rule belongs
policy_name	String	Name of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
status	Integer	Rule enabling status
url	String	URL of the false alarm
rule	String	Rule No.
mode	Integer	False alarm masking mode. The default value is 0, indicating the old mode.
domains	Array of strings	Domain name list
url_logic	String	URL type of the masking rule (prefix or equal)
advanced	**HttpIgnoreRuleCondition** object	The parameters in the condition list are complex and are cascaded. Add a false alarm masking rule on the console. Press F12 to view the request parameters whose path suffix is /ignore-rule and method is POST.
conditions	Array of **HttpIgnoreRuleCondition** objects	Hit condition
hit_num	Integer	Hit count
update_time	Long	Timestamp for the last update
clear_time	Long	Timestamp for clearing the last hit count

Table 4-327 HttpIgnoreRuleCondition

Parameter	Type	Description
category	String	Field type. The value can be ip, url, params, cookie, or header.

Parameter	Type	Description
index	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield.
contents	Array of strings	Content list
logic_operation	String	Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported.
value_list_id	String	ID of the referenced table
size	Long	This field is used if the protection rule involves a threshold.
check_all_indexes_logic	Integer	1. All subfields/2. Any subfield

Status code: 400

Table 4-328 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-329 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code

Parameter	Type	Description
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-330 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.8 HTTP Protection Rule Management - Attack Penalty

4.8.1 Querying Known Attack Source Rules

Function

This API is used to query known attack source rules.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/punishment-rule

Table 4-331 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Table 4-332 Query Parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number, which is required for pagination query.
pagesize	No	Integer	Pagination query parameter. The number of records displayed on each page is specified by pagesize.

Request Parameters

Table 4-333 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-334 Response body parameters

Parameter	Type	Description
total	Integer	Number of protection rules in a policy
items	Array of **ShowHttpPunishmentRuleResponseBody** objects	Protection rule list

Table 4-335 ShowHttpPunishmentRuleResponseBody

Parameter	Type	Description
id	String	Rule ID
policy_id	String	ID of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
category	String	Blocking type. The options are as follows: long_ip_block (long-time IP address blocking), long_cookie_block (long-time cookie blocking), long_params_block (long-time parameter blocking), and short_ip_block (short-time IP address blocking). short_cookie_block (short-time cookie blocking) and short_params_block (short-time parameter blocking)
block_time	Integer	Blocking duration.

Status code: 400

Table 4-336 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-337 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-338 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.8.2 Creating a Known Attack Source Rule.

Function

This API is used to create a known attack source rule.

URI

POST /v1/edgesec/configuration/http/policies/{policy_id}/punishment-rule

Table 4-339 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-340 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-341 Request body parameters

Parameter	Mandatory	Type	Description
description	No	String	Rule description, which contains a maximum of 512 characters.
category	Yes	String	Blocking type. The options are as follows: long_ip_block (long-time IP address blocking), long_cookie_block (long-time cookie blocking), long_params_block (long-time parameter blocking), and short_ip_block (short-time IP address blocking). short_cookie_block (short-time cookie blocking) and short_params_block (short-time parameter blocking)

Parameter	Mandatory	Type	Description
block_time	Yes	Integer	Blocking duration. If the prefix of the attack penalty type is long, the value range of block_time is 301-1800. If the prefix of the attack penalty type is short, the value range of block_time is 0-300.

Response Parameters

Status code: 200

Table 4-342 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policy_id	String	ID of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
category	String	Blocking type. The options are as follows: long_ip_block (long-time IP address blocking), long_cookie_block (long-time cookie blocking), long_params_block (long-time parameter blocking), and short_ip_block (short-time IP address blocking). short_cookie_block (short-time cookie blocking) and short_params_block (short-time parameter blocking)
block_time	Integer	Blocking duration.

Status code: 400

Table 4-343 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-344 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-345 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.8.3 Querying a Penalty Rule

Function

This API is used to query a penalty rule.

URI

GET /v1/edgesec/configuration/http/policies/{policy_id}/punishment-rule/{rule_id}

Table 4-346 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-347 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-348 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policy_id	String	ID of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description

Parameter	Type	Description
category	String	Blocking type. The options are as follows: long_ip_block (long-time IP address blocking), long_cookie_block (long-time cookie blocking), long_params_block (long-time parameter blocking), and short_ip_block (short-time IP address blocking). short_cookie_block (short-time cookie blocking) and short_params_block (short-time parameter blocking)
block_time	Integer	Blocking duration.

Status code: 400

Table 4-349 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-350 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-351 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code

Parameter	Type	Description
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.8.4 Updating a Known Attack Source Rule

Function

This API is used to update a known attack source rule.

URI

PUT /v1/edgesec/configuration/http/policies/{policy_id}/punishment-rule/{rule_id}

Table 4-352 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-353 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-354 Request body parameters

Parameter	Mandatory	Type	Description
description	No	String	Rule description, which contains a maximum of 512 characters.
block_time	Yes	Integer	Blocking duration. If the prefix of the attack penalty type is long, the value range of block_time is 301-1800. If the prefix of the attack penalty type is short, the value range of block_time is 1-300.

Response Parameters

Status code: 200

Table 4-355 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policy_id	String	ID of the policy to which the rule belongs
timestamp	Long	Time when a rule is created
description	String	Rule description
category	String	Blocking type. The options are as follows: long_ip_block (long-time IP address blocking), long_cookie_block (long-time cookie blocking), long_params_block (long-time parameter blocking), and short_ip_block (short-time IP address blocking). short_cookie_block (short-time cookie blocking) and short_params_block (short-time parameter blocking)

Parameter	Type	Description
block_time	Integer	Blocking duration.

Status code: 400

Table 4-356 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-357 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-358 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.8.5 Deleting a Known Attack Source Rule

Function

This API is used to delete a known attack source rule.

URI

DELETE /v1/edgesec/configuration/http/policies/{policy_id}/punishment-rule/{rule_id}

Table 4-359 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID.
rule_id	Yes	String	Protection rule ID.

Request Parameters

Table 4-360 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-361 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-362 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-363 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	The rule is deleted.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.9 IP Address Group Management

4.9.1 Querying IP Address Groups

Function

This API is used to query IP address groups.

URI

GET /v1/edgesec/configuration/http/ip-groups

Table 4-364 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.
page	No	Integer	Page number, which is required for pagination query.
pagesize	No	Integer	Pagination query parameter. The number of records displayed on each page is specified by pagesize.
name	No	String	IP address group name
ip	No	String	IP address/range

Request Parameters

Table 4-365 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

Status code: 200

Table 4-366 Response body parameters

Parameter	Type	Description
total	Integer	Total number of IP address groups
items	Array of **ShowHttpIpGroupResponseBody** objects	Detailed information about the IP address group.

Table 4-367 ShowHttpIpGroupResponseBody

Parameter	Type	Description
id	String	IP address group ID.
name	String	IP address group name
ips	String	IP address/range.
size	String	IP address/address segment size
description	String	IP address group remarks
timestamp	Long	Time when the IP address group was created.
rules	Array of **HttpRuleInfo** objects	List of policies and rules that use the IP address group.

Table 4-368 HttpRuleInfo

Parameter	Type	Description
rule_id	String	Rule ID in the policy.
rule_name	String	Rule name in the policy.
policy_id	String	Policy ID.
policy_name	String	Policy name.

Status code: 400

Table 4-369 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-370 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-371 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.9.2 Creating an IP Address Group

Function

This API is used to create an IP address group.

URI

POST /v1/edgesec/configuration/http/ip-groups

Request Parameters

Table 4-372 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Table 4-373 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	IP address group name
ips	Yes	String	IP address or IP address segment. Use commas (,) to separate multiple IP addresses or IP address segments. A maximum of 200 IP addresses or IP address segments can be configured.
description	No	String	Remarks of the IP address group. The value contains a maximum of 512 characters.

Response Parameters

Status code: 200

Table 4-374 Response body parameters

Parameter	Type	Description
id	String	IP address group ID.
name	String	IP address group name
ips	String	IP address/range.

Parameter	Type	Description
size	String	IP address/address segment size
description	String	IP address group remarks
timestamp	Long	Time when the IP address group was created.
rules	Array of HttpRuleInfo objects	List of policies and rules that use the IP address group.

Table 4-375 HttpRuleInfo

Parameter	Type	Description
rule_id	String	Rule ID in the policy.
rule_name	String	Rule name in the policy.
policy_id	String	Policy ID.
policy_name	String	Policy name.

Status code: 400

Table 4-376 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-377 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-378 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Created
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.9.3 Querying an IP Address Group

Function

This API is used to query an IP address group.

URI

GET /v1/edgesec/configuration/http/ip-groups/{ip_group_id}

Table 4-379 Path Parameters

Parameter	Mandatory	Type	Description
ip_group_id	Yes	String	IP address group ID

Request Parameters

Table 4-380 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

Status code: 200

Table 4-381 Response body parameters

Parameter	Type	Description
id	String	IP address group ID.
name	String	IP address group name
ips	String	IP address/range.
size	String	IP address/address segment size
description	String	IP address group remarks
timestamp	Long	Time when the IP address group was created.
rules	Array of **HttpRuleInfo** objects	List of policies and rules that use the IP address group.

Table 4-382 HttpRuleInfo

Parameter	Type	Description
rule_id	String	Rule ID in the policy.
rule_name	String	Rule name in the policy.
policy_id	String	Policy ID.
policy_name	String	Policy name.

Status code: 400

Table 4-383 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-384 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-385 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.9.4 Updating an IP Address Group

Function

This API is used to update an IP address group.

URI

PUT /v1/edgesec/configuration/http/ip-groups/{ip_group_id}

Table 4-386 Path Parameters

Parameter	Mandatory	Type	Description
ip_group_id	Yes	String	IP address group ID

Request Parameters

Table 4-387 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-388 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	IP address group name
ips	Yes	String	IP address/range
description	No	String	Remarks of the IP address group. The value contains a maximum of 512 characters.

Response Parameters

Status code: 200

Table 4-389 Response body parameters

Parameter	Type	Description
id	String	IP address group ID.
name	String	IP address group name
ips	String	IP address/range.
size	String	IP address/address segment size
description	String	IP address group remarks
timestamp	Long	Time when the IP address group was created.
rules	Array of **HttpRuleInfo** objects	List of policies and rules that use the IP address group.

Table 4-390 HttpRuleInfo

Parameter	Type	Description
rule_id	String	Rule ID in the policy.

Parameter	Type	Description
rule_name	String	Rule name in the policy.
policy_id	String	Policy ID.
policy_name	String	Policy name.

Status code: 400

Table 4-391 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-392 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-393 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.9.5 Deleting an IP Address Group

Function

This API is used to delete an IP address group.

URI

DELETE /v1/edgesec/configuration/http/ip-groups/{ip_group_id}

Table 4-394 Path Parameters

Parameter	Mandatory	Type	Description
ip_group_id	Yes	String	IP address group ID

Request Parameters

Table 4-395 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-396 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-397 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-398 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	No Content
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.10 Security Overview

4.10.1 Querying Website Request Statistics

Function

This API is used to query website request statistics.

URI

GET /v1/edgesec/stat/http/overviews/statistics

Table 4-399 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.
from	Yes	Long	Start time
to	Yes	Long	End time
domain_name	No	String	Domain name.

Request Parameters

Table 4-400 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

Status code: 200

Table 4-401 Response body parameters

Parameter	Type	Description
[items]	Array of **HttpStatisticsItem** objects	Security statistics

Table 4-402 HttpStatisticsItem

Parameter	Type	Description
attack_category	String	Attack type.
stat_num	Long	Statistical quantity.

Status code: 400

Table 4-403 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-404 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-405 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Security statistics
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.10.2 Querying Attack Domain Names

Function

This API is used to query top security information, including the attack domain name, attack source IP address, attack URL, attack source region, and protection type.

URI

GET /v1/edgesec/stat/http/overviews/classification

Table 4-406 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.
from	Yes	Long	Start time
to	Yes	Long	End time
top	No	Integer	The first several results to query
domain_name	No	String	Domain name.

Request Parameters

Table 4-407 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

Status code: 200

Table 4-408 Response body parameters

Parameter	Type	Description
domain	**DomainClassificationItem** object	-
attack_type	**AttackTypeClassificationItem** object	-
ip	**IpClassificationItem** object	-
url	**UrlClassificationItem** object	-
geo	**GeoClassificationItem** object	-

Table 4-409 DomainClassificationItem

Parameter	Type	Description
total	Integer	Total number of DomainItem
items	Array of **DomainItem** objects	DomainItem details

Table 4-410 DomainItem

Parameter	Type	Description
key	String	Domain name.
num	Integer	Quantity
web_tag	String	Website name.

Table 4-411 AttackTypeClassificationItem

Parameter	Type	Description
total	Integer	Total number of AttackTypeItem

Parameter	Type	Description
items	Array of **AttackTypeItem** objects	AttackTypeItem details

Table 4-412 AttackTypeItem

Parameter	Type	Description
key	String	Attack type.
num	Integer	Quantity

Table 4-413 IpClassificationItem

Parameter	Type	Description
total	Integer	Total number of IpItem
items	Array of **IpItem** objects	IpItem details

Table 4-414 IpItem

Parameter	Type	Description
key	String	IP address
num	Integer	Quantity

Table 4-415 UrlClassificationItem

Parameter	Type	Description
total	Integer	Total number of UrlItem
items	Array of **UrlItem** objects	UrlItem details

Table 4-416 UrlItem

Parameter	Type	Description
key	String	URL path
num	Integer	Quantity
host	String	Domain name.

Table 4-417 GeoClassificationItem

Parameter	Type	Description
total	Integer	Total number of GeoItem
items	Array of **GeoItem** objects	GeoItem details

Table 4-418 GeoItem

Parameter	Type	Description
key	String	Attack source location.
num	Integer	Quantity

Status code: 400

Table 4-419 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-420 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-421 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.11 Reference Table Management

4.11.1 Querying the Reference Table List

Function

This API is used to query the reference table list.

URI

GET /v1/edgesec/configuration/http/reference-table

Table 4-422 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project. It can be obtained by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number, which is required for pagination query.
pagesize	No	Integer	Number of records on each page, which is required for pagination query
name	No	String	Fuzzy query of the reference table name

Request Parameters

Table 4-423 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-424 Response body parameters

Parameter	Type	Description
total	Integer	Number of referenced tables
items	Array of **ShowHttpReferenceTableResponseBody** objects	Reference table list

Table 4-425 ShowHttpReferenceTableResponseBody

Parameter	Type	Description
id	String	ID of the referenced table
name	String	Reference table name
type	String	Reference table type
description	String	Reference table description
timestamp	Long	Reference table timestamp
values	Array of strings	Value of the reference table
producer	Integer	Source

Status code: 400

Table 4-426 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-427 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-428 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.11.2 Creating a Reference Table

Function

This API is used to create a reference table.

URI

POST /v1/edgesec/configuration/http/reference-table

Request Parameters

Table 4-429 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-430 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Reference table name
type	Yes	String	Reference table type. The value can be url, params, ip, cookie, referer, user-agent, header, response_code, response_header or response_body.
values	Yes	Array of strings	Value of the reference table
description	No	String	Reference table description. The value contains a maximum of 128 characters.

Response Parameters

Status code: 200

Table 4-431 Response body parameters

Parameter	Type	Description
id	String	ID of the referenced table
name	String	Reference table name

Parameter	Type	Description
type	String	Reference table type
description	String	Reference table description
timestamp	Long	Reference table timestamp
values	Array of strings	Value of the reference table
producer	Integer	Source

Status code: 400

Table 4-432 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-433 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-434 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.11.3 Updating a Reference Table

Function

This API is used to update a reference table.

URI

PUT /v1/edgesec/configuration/http/reference-table/{table_id}

Table 4-435 Path Parameters

Parameter	Mandatory	Type	Description
table_id	Yes	String	ID of the referenced table

Request Parameters

Table 4-436 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-437 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Reference table name
type	Yes	String	Reference table type. The value can be url, params, ip, cookie, referer, user-agent, header, response_code, response_header or response_body.
values	Yes	Array of strings	Value of the reference table
description	No	String	Reference table description. The value contains a maximum of 128 characters.

Response Parameters

Status code: 200

Table 4-438 Response body parameters

Parameter	Type	Description
id	String	ID of the referenced table
name	String	Reference table name
type	String	Reference table type
description	String	Reference table description
timestamp	Long	Reference table timestamp
values	Array of strings	Value of the reference table
producer	Integer	Source

Status code: 400

Table 4-439 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-440 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-441 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.11.4 Deleting a Reference Table

Function

This API is used to delete a reference table.

URI

DELETE /v1/edgesec/configuration/http/reference-table/{table_id}

Table 4-442 Path Parameters

Parameter	Mandatory	Type	Description
table_id	Yes	String	ID of the referenced table

Request Parameters

Table 4-443 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-444 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-445 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-446 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	The rule is deleted.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.12 DDoS Statistics

4.12.1 Querying the Timeline Data of DDoS Attack Statistics

Function

This API is used to query the timeline data of DDoS attack statistics.

URI

GET /v1/edgesec/stat/ddos-attack-timelines

Table 4-447 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.
stat_type	Yes	String	Type of the security statistics metric. Currently, bw and pps are supported.
group_by	Yes	String	bw corresponds to max_bps and avg_bps, and pps corresponds to max_pps and avg_pps.
start_time	Yes	Long	Start time

Parameter	Mandatory	Type	Description
end_time	Yes	Long	End time

Request Parameters

Table 4-448 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Response Parameters

Status code: 200

Table 4-449 Response body parameters

Parameter	Type	Description
stat_type	String	Metric type
group_by	String	Group type
interval	Integer	Time granularity (s)
values	Array of **TimeStatItem** objects	Value array

Table 4-450 TimeStatItem

Parameter	Type	Description
key	Long	Timestamp, which is left aligned with the time granularity. For example, if the time granularity is 5 minutes and the time range is [19:10,19:15), the timestamp is 19:10.
value	Long	Number of attack requests

Status code: 400

Table 4-451 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error description

Status code: 401

Table 4-452 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error description

Status code: 500

Table 4-453 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error description

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.13 HTTP Statistics

4.13.1 Querying HTTP Attack Distribution Data

Function

This API is used to query HTTP attack distribution data.

URI

GET /v1/edgesec/stat/http-attack-distribution

Table 4-454 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.
domain_name	No	String	Domain name.
stat_type	Yes	String	Type of a security statistic metric. For example, req_num (number of requests) and bw (bandwidth). Currently, only req_num is supported.
group_by	Yes	String	Currently, the value can be action (protection action) or attack_type (attack type).
start_time	Yes	Long	Start time, which is a timestamp in seconds.
end_time	Yes	Long	End time, which is a timestamp in seconds.

Request Parameters

Table 4-455 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

Status code: 200

Table 4-456 Response body parameters

Parameter	Type	Description
stat_type	String	Security statistics metric type
group_by	String	Statistics grouping dimension
stat_num	Long	Statistical quantity
values	Array of **CommonStatItem** objects	Statistics array
start_time	Long	Start time
end_time	Long	End time

Table 4-457 CommonStatItem

Parameter	Type	Description
key	String	Subcategory corresponding to the request parameter group_by. For example, in the API for querying the HTTP attack distribution statistics, if group_by is action, the key can be log, block, captcha, or js_challenge. In the API for querying top HTTP attack statistics, if group_by is url, the key can be the requested URL, for example, /abc.
value	Long	Number of attack requests

Status code: 400

Table 4-458 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error description

Status code: 401

Table 4-459 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error description

Status code: 500

Table 4-460 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error description

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request successful.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.13.2 Querying the Timeline Data of HTTP Attack Statistics

Function

This API is used to query the timeline data of HTTP attack statistics.

URI

GET /v1/edgesec/stat/http-attack-timelines

Table 4-461 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.
domain_name	No	String	Domain name.
stat_type	Yes	String	Metric type. Currently, only req_num is supported.
group_by	Yes	String	Group type. Currently, only action and attack_category are supported.
group_by_value	No	String	Value corresponding to the group type. (If this parameter is not passed, the total value is used by default.) For example, the action metric type can be log, block, captcha, or js_challenge, and the attack_category metric type can be cc, access_control, bot, or web_app_attack.

Parameter	Mandatory	Type	Description
interval	Yes	Integer	Time granularity (unit: second). Different time ranges have different time granularities. For the time rage of [0,1H], the available time granularities are 1M and 5M. For the time range of (1H,1D], the available time granularities are 1M, 5M, and 1H. For the time range of (1D,3D], the available time granularities are 1M, 5M, 1H, and 1D. For the time range of (3D,7D], the available time granularities are 5M, 1H, and 1D. For the time range of (7D,30D], the available time granularities are 1H and 1D. M indicates minute, H indicates hour, and D indicates day.
start_time	Yes	Long	Start time
end_time	Yes	Long	End time

Request Parameters

Table 4-462 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

Status code: 200

Table 4-463 Response body parameters

Parameter	Type	Description
stat_type	String	Metric type
group_by	String	Group type
group_by_value	String	Value corresponding to the group type

Parameter	Type	Description
interval	Integer	Time granularity (s)
values	Array of TimeStatItem objects	Value array

Table 4-464 TimeStatItem

Parameter	Type	Description
key	Long	Timestamp, which is left aligned with the time granularity. For example, if the time granularity is 5 minutes and the time range is [19:10,19:15), the timestamp is 19:10.
value	Long	Number of attack requests

Status code: 400

Table 4-465 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error description

Status code: 401

Table 4-466 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error description

Status code: 500

Table 4-467 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error description

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.13.3 Querying Top HTTP Attacks

Function

This API is used to query top HTTP attacks.

URI

GET /v1/edgesec/stat/http-attack-top

Table 4-468 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.

Parameter	Mandatory	Type	Description
domain_name	No	String	Domain name.
stat_type	Yes	String	Metric type. For example, req_num (number of requests) and bw (bandwidth). Currently, only req_num is supported.
group_by	Yes	String	Group type. Response values are collected by group type. The group type can be host (requested server domain name), sip (requested client IP address), url (requested URL), rule (customized policy type description), user-agent (user agent), method (request method), or country (location)
limit	No	Integer	This API is ued to limit the number of top users. The value cannot exceed 100. The default value is 10.
time_type	Yes	String	Time enumeration. The options are: LATEST (last 30 minutes), TODAY (today), CUSTOMIZE (customized, any integer from 1 to 30)
start_time	No	Long	Start time
end_time	No	Long	End time

Request Parameters

Table 4-469 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

Status code: 200

Table 4-470 Response body parameters

Parameter	Type	Description
stat_type	String	Metric type
group_by	String	Group type
values	Array of **CommonStatItem** objects	Single statistical model
start_time	Long	Start time
end_time	Long	End time

Table 4-471 CommonStatItem

Parameter	Type	Description
key	String	Subcategory corresponding to the request parameter group_by. For example, in the API for querying the HTTP attack distribution statistics, if group_by is action, the key can be log, block, captcha, or js_challenge. In the API for querying top HTTP attack statistics, if group_by is url, the key can be the requested URL, for example, /abc.
value	Long	Number of attack requests

Status code: 400

Table 4-472 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error description

Status code: 401

Table 4-473 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error description

Status code: 500

Table 4-474 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error description

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.14 DDoS Attack Logs

4.14.1 Querying DDoS Attack Logs

Function

This API is used to query DDoS attack logs.

URI

GET /v1/edgesec/log/ddos-attack-logs

Table 4-475 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.
start_time	Yes	Long	Start time, which is a 13-digit timestamp
end_time	Yes	Long	End time, which is a 13-digit timestamp
offset	No	Integer	Query offset.
limit	No	Integer	Number of records on each page of the query list.

Request Parameters

Table 4-476 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

Status code: 200

Table 4-477 Response body parameters

Parameter	Type	Description
total	Long	Number of attack logs
items	Array of **DdosAttackLog** objects	Attack log details

Table 4-478 DdosAttackLog

Parameter	Type	Description
attack_time	Long	DDoS attack time

Parameter	Type	Description
avg_bps	Long	Average attack traffic bandwidth
avg_pps	Long	Peak attack traffic bandwidth
max_bps	Long	Average packet forwarding rate
max_pps	Long	Peak packet forwarding rate

Status code: 400

Table 4-479 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 401

Table 4-480 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Status code: 500

Table 4-481 Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorization_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

4.14.2 Downloading DDoS Attack Logs

Function

This API is used to download DDoS attack logs.

URI

POST /v1/edgesec/log/ddos-attack-logs/download

Table 4-482 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS). The default value is 0.
start_time	Yes	Long	Start time, which is a 13-digit timestamp
end_time	Yes	Long	End time, which is a 13-digit timestamp
offset	No	Integer	Query offset.
limit	No	Integer	Number of records on each page of the query list.

Request Parameters

Table 4-483 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token

Response Parameters

None

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	document file
400	Request failed.

Status Code	Description
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See **Error Codes**.

A Appendix

A.1 Status Code

- Normal

Status Code	Description	Description
200	OK	The request is successfully processed.

- Abnormal

Status Code	Description	Description
400	Bad Request	It is a bad request.
401	Unauthorized	You do not have permissions to perform this action.
403	Forbidden	Access is denied.
404	Not Found	The page is not found.
500	Internal Server Error	There is an internal server error.

A.2 Error Codes

If an error code starting with APIGW is returned after you call an API, rectify the fault by referring to the instructions provided in **API Gateway Error Codes**.

Status Code	Error Codes	Error Message	Description	Solution
400	EdgeSec.00000007	Invalid Domain dispatch status.	Invalid domain name scheduling status.	Contact technical support.
400	EdgeSec.00000009	Invalid domain.	Invalid domain name.	Check the domain name.
400	EdgeSec.00000012	Invalid area type.	Invalid service region.	Check the domain name and the service region of the purchased product.
400	EdgeSec.00000014	Not support operation in this enterprise project.	Operation not supported for the current enterprise project.	Check the permissions for the current enterprise project.
400	EdgeSec.00000015	All enterprise projects do not support write operations.	Write operation not supported for "All project".	Check the permissions for "All project".
400	EdgeSec.00000016	Tms Illegal Request.	Invalid request for the tag management system.	Check the request input parameters or contact Huawei technical support.
400	EdgeSec.00000017	Duplicate resource id.	Duplicate resource IDs.	Check the resource ID in the request input parameters or contact technical support.
400	EdgeSec.00000018	This version only supports default enterprise project.	The current version only supports resource management using the default enterprise project.	Use the default enterprise project to manage resources.

Status Code	Error Codes	Error Message	Description	Solution
400	EdgeSec.00000019	Frozen can not create eps tag.	EdgeSec resources are frozen and tags cannot be managed.	Unfreeze EdgeSec resources.
400	EdgeSec.00010003	Domain name ineligible for this feature.	The domain name does not support this function.	Check the domain name.
400	EdgeSec.00010004	Domain Already Exists.	The domain name already exists.	Check the domain name.
400	EdgeSec.00010006	Blacklist and whitelist rules of an edge WAF policy exceed the quota.	Blacklist and Whitelist Rules of Edge WAF Exceed the Quota	1.Delete unnecessary blacklist and whitelist rules so that the number of blacklist and whitelist rules in each policy does not exceed the current quota;Blacklist and whitelist rule quota = Edition quota + Number of rule expansion packages x 10. For example, if you use the professional edition of edge WAF and have two rule expansion packages, you can create 120 blacklist and whitelist rules (100 + 2 x 10 = 120).

Status Code	Error Codes	Error Message	Description	Solution
400	EdgeSec.00010007	The IP address group quota of edge WAF is insufficient.	Insufficient IP Address Group Quota of Edge WAF	For details about how to view the IP address group quota, see https://support.huaweicloud.com/en-us/usermanual-edgesec/edgesec_01_0058.html#section1. If the IP address group quota is insufficient, contact technical support.
400	EdgeSec.00010008	The edge WAF certificate quota is insufficient.	Insufficient Edge WAF Certificate Quota	The certificate quota is the same as the domain name quota. Purchase the domain name expansion package of the edge WAF.
400	EdgeSec.00020001	Must enable waf protection first.	To enable anti-DDoS protection for a domain name, enable WAF first.	Enable WAF for the domain name.
400	EdgeSec.00020002	Domain Already Exists.	The anti-DDoS domain name already exists.	Check the domain name.
400	EdgeSec.00030001	Illegal ElasticSearch Request.	An error occurred when querying protection data.	Check the query parameters.
400	EdgeSec.00030002	Search Error.	An error occurred when querying protection data.	Check the query parameters.

Status Code	Error Codes	Error Message	Description	Solution
400	EdgeSec.00030003	Statistic Type Error.	An error occurred when querying the protected data type.	Check the protected data type.
400	EdgeSec.00040004	The customer has purchased this product.	You have purchased the product.	Cancel purchase or contact technical support.
400	EdgeSec.00040007	No Permission To Operate.	EdgeSec has been unsubscribed from or frozen. You do not have the permission to perform this operation.	Purchase EdgeSec or contact technical support.
400	EdgeSec.00040008	The customer has not purchased this main resource.	You have not purchased EdgeSec.	Purchase EdgeSec or contact technical support.
400	EdgeSec.00040009	The domain name scope does not match the service scope.	The domain name is not in the region you purchased EdgeSec.	Check the region of the domain name or purchase EdgeSec in the correct region.
400	EdgeSec.00040010	The remaining resources are insufficient.	Insufficient resources.	Expand resources or delete unnecessary resources.
400	EdgeSec.00040011	Please wait until the release is complete.	Resources are being released.	Please wait.

Status Code	Error Codes	Error Message	Description	Solution
400	EdgeSec.00040012	Due to security reasons, your account has been restricted from purchasing certain pay-per-use cloud service resources according to the HUAWEI CLOUD Customer Agreement. If you have any questions, contact customer service.	Account restricted. The current product cannot be purchased.	Contact customer service.
400	EdgeSec.00050001	Domain is in processing, please wait it.	The domain name is being scheduled.	Please wait.
400	WAF.00011001	bad.request	Bad request	Check param
400	WAF.00011002	url.param.illegal	The URL format is incorrect	Check URL format
400	WAF.00011003	request.body.illegal	Request body format error: missing parameter and illegal value in body	Check request body
400	WAF.00011004	id.illegal	Illegal ID	Check ID
400	WAF.00011005	name.illegal	Illegal name	Check name
400	WAF.00011006	host.illegal	Illegal domain name	Check domain name
400	WAF.00011007	port.illegal	Illegal port	Check port

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00011008	protect.status.illegal	Illegal protection status	Check whether the protection state is in the range of enumeration value
400	WAF.00011009	access.status.illegal	Illegal access status	Check whether the access status is in the range of enumeration value
400	WAF.00011010	offsetOrLimit.illegal	Illegal offset or limit number	Check whether the starting line or limit number is within the range
400	WAF.00011011	pageOrPageSize.illegal	Illegal page number or number of entries per page	Check if page number or number of items per page are in range
400	WAF.00011012	standard.violated	Invalid parameter	Check the parameters
400	WAF.00011013	description.illegal	Illegal description format	Check description format
400	WAF.00011014	request.header.illegal	Request header format error: missing parameter and illegal value in header	Check header required parameters
400	WAF.00012001	invalid.token	Illegal token	Check whether the token is correct
400	WAF.00012002	invalid.project	Inconsistency between project_id and token	Check Consistency of project_id and token

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00012003	permission.denied	No permission	Assign WAF required permissions to account
400	WAF.00012004	account.frozen	Account freezing	Account unfreezing
400	WAF.00012005	not.subscribe	Unsubscribed	Subscribe to WAF service first
400	WAF.00012006	pdp.permission.denied	No permission	Check the PDP authority of the account
400	WAF.00012007	jwt.authentication.disabled	JWT certification off	Open JWT certification
400	WAF.00012008	jwt.authentication.invalid.token	Illegal JWT token	Check whether the account has JWT permission
400	WAF.00012009	jwt.authentication.failed	JWT authentication failed	Give the account authorization first
400	WAF.00012010	eps.all.not.support	eps.all.not.support	Open the write permission of enterprise project
400	WAF.00013001	insufficient.quota	Insufficient function quota	Purchase function quota upgrade package
400	WAF.00013002	feature.not.support	Function not supported	nothing
400	WAF.00013003	port.not.support	Port not supported	Port conversion via ELB
400	WAF.00013004	protocol.not.support	Protocol not supported	Through ELB conversion protocol
400	WAF.00013005	wildcard.domain.not.support	Pan domain name not supported	Use specific domain names
400	WAF.00013006	ipv6.not.support	IPv6 is not supported	The current version does not support IPv6

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00013007	insufficient.tenant.quota	insufficient.tenant.quota	Purchase quota upgrade package
400	WAF.00014001	resource.not.found	Resource not found	The resource has been deleted or does not exist
400	WAF.00014002	resource.already.exists	Resource already exists	Resource already exists
400	WAF.00014003	open.protect.failed	Failed to open protection	Check domain name protection status
400	WAF.00014004	access.failed	Failed to access WAF	Modify DNS resolution
400	WAF.00014005	bypass.failed	Bypasswaf failed	Check the protection status and try again
400	WAF.00014006	proxy.config.error	Agent configuration error	Reconfigure the agent correctly and try again
400	WAF.00014007	host.conflict	Domain name conflict	Check that the domain name already exists in the website configuration
400	WAF.00014008	cert.inconsistent	The same domain name, but the certificate is inconsistent	Use the same certificate
400	WAF.00014009	api.not.found	The interface does not exist	Check interface URL
400	WAF.00014010	port.protocol.mismatch	Port and protocol mismatch	Select the matching protocol and port
400	WAF.00014011	host.blacklist	It is forbidden to add the protection website, and the domain name is blacklisted	

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00014012	insufficient.tenant.quota	Insufficient tenant quota	Purchase quota upgrade package
400	WAF.00014013	exclusive.ip.config.error	Exclusive IP configuration error	Check exclusive IP configuration
400	WAF.00014014	exclusive.ip.config.error	exclusive.ip.config.error	Check exclusive IP configuration
400	WAF.00021002	url.param.illegal	The URL format is incorrect	It is recommended to modify the URL in the request body parameter to the standard URL and debug again
400	WAF.00021003	request.body.illegal	The request body parameter is incorrect	It is recommended that you verify the parameters according to the document before initiating debugging
400	WAF.00021004	id.illegal	The unique identifier ID format is incorrect	It is recommended to follow the correct instructions in the documentation to obtain the ID
400	WAF.00021005	name.illegal	The name parameter format is incorrect	Check the format of name, which can only be composed of letters, numbers, -_ And. Cannot exceed 64 characters in length
400	WAF.00021006	host.illegal	The domain name format is incorrect	Domain name can only be composed of letters, numbers, -_ And. Cannot exceed 64 characters in length

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00021007	protocol.illegal	The back-end protocol format is incorrect	The back-end protocol can only be configured as HTTP or HTTPS and must be capitalized
400	WAF.00021008	port.illegal	The source port format is incorrect	Check whether the configured port is empty and whether the target port is in the range of 0-65535
400	WAF.00021009	ip.illegal	Incorrect IP format	Check whether the IP format meets the standard format of IPv4 or IPv6
400	WAF.00021010	server.address.illegal	Server configuration exception	Check whether the server configuration is empty and whether the quantity is in the range of 1-80
400	WAF.00021012	path.illegal	The URL format in the rule configuration is incorrect	It is recommended to modify the URL in the request body parameter to the standard URL and debug again
400	WAF.00021013	cert.illegal	The HTTPS certificate has expired	It is recommended to upload the unexpired certificate again
400	WAF.00021014	action.illegal	Illegal protective action	It is recommended to configure protection actions according to the enumerated values in the document

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00021015	rule.status.illegal	Illegal rule status	It is recommended to modify the rule status according to the rule status enumeration value in the document
400	WAF.00021016	description.illegal	Description exception	It is recommended to use standard English grammar for description
400	WAF.00021017	incorrect.rule.config	Incorrect rule configuration	It is recommended to configure protection rules according to the documentation in the help center
400	WAF.00021018	incorrect.reference.table.config	Incorrect reference table configuration	It is recommended to configure the reference table according to the documentation in the help center
400	WAF.00021019	incorrect.route.config	Incorrect line configuration	It is recommended to configure the line according to the documentation in the help center
400	WAF.00021020	offsetOrLimit.illegal	Paging parameter error	It is recommended to fill in pagination parameters according to the documents in the help center

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00021021	param.exceed.limit	Parameter exceeds limit	It is recommended to view the parameter limits according to the documentation in the help center
400	WAF.00022002	resource.already.exists	Resource already exists	It is recommended to check whether the created resource already exists in the console
400	WAF.00022003	resource.is.being.used	The resource is in use	Remove the relationship between the resource and the user before deleting the resource
400	WAF.00022004	rule.conflict	Rule conflict	Check whether the target rule conflicts with the existing rule
401	EdgeSec.00000002	Get Request Attributes Error.	An error occurred when obtaining IAM system parameters.	Contact technical support.
401	EdgeSec.00000003	Get IAM Context Error.	Failed to obtain the IAM context.	Contact technical support.
401	EdgeSec.00000004	Get Token Result Error.	Failed to obtain the IAM token.	Contact technical support.
401	EdgeSec.00000005	Invalid parameters.	Invalid parameter.	Check parameters or contact technical support.
401	EdgeSec.00000020	The project id does not match the token.	The project ID and x-auth-token do not match.	Check the Project ID and x-auth-token.

Status Code	Error Codes	Error Message	Description	Solution
401	EdgeSec.00010001	Failed to get IAM projects.	Failed to obtain the IAM project.	Use the current account to log in to Huawei Cloud and check whether the project exists in IAM. If it does not exist, contact technical support.
401	EdgeSec.00010002	IAM project not ready for WAF.	The current project does not support WAF functions.	Contact technical support.
403	WAF.00022005	insufficient.quota	Insufficient resources	It is recommended to purchase the upgrade package of corresponding resources
404	WAF.00022001	resource.not.found	Resource does not exist	It is recommended to check the resource status on the console or ask for technical support
500	EdgeSec.00000001	An internal error occurs in the system.	Internal service error.	Contact technical support.
500	EdgeSec.00000006	send request fail.	Failed to send the request.	Try again later or contact technical support.
500	EdgeSec.00000010	Service returned nothing.	The returned result is empty.	Try again later or contact technical support.
500	EdgeSec.00000013	Please try again.	Please try again.	Please try again.
500	WAF.00010001	internal.error	Internal error	Contact technical support
500	WAF.00010002	system.busy	Internal error	Contact technical support

Status Code	Error Codes	Error Message	Description	Solution
500	WAF.00010003	cname.failed	Failed to create or modify CNAME	Contact technical support
500	WAF.00010004	cname.failed	Failed to get OBS file download link	Contact technical support
500	WAF.00020001	internal.error	Service internal exception	It is recommended to try again in five minutes
500	WAF.00020002	system.busy	System busy	It is recommended to try again in five minutes

A.3 Troubleshooting

A.3.1 EdgeSec.00000005 Invalid Parameter

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

- The page is not refreshed for a long time.
- Invalid input

Solution

Step 1 Refresh the page. Then, select a proper time range and try again.

Step 2 Enter information about the edge WAF policy or rule as prompted.

----End

A.3.2 EdgeSec.00000013 Concurrent Modification Exception

Root Cause

This error code is triggered when too many concurrent access requests are performed on APIs.

Troubleshooting and Solution

<table>
<tr><th colspan="2">Event Scenario</th><th>Cause</th><th>Check Items</th><th>Solution</th></tr>
<tr><td rowspan="8">Creating an edge WAF policy rule</td><td>Adding a CC attack protection rule</td><td rowspan="10">This error code is triggered when there are a large number of concurrent requests performed on APIs.</td><td rowspan="8">Whether concurrent requests are performed on the console.</td><td rowspan="8">Retry on the console.</td></tr>
<tr><td>Adding a precise protection rule</td></tr>
<tr><td>Creating a geolocation access control rule</td></tr>
<tr><td>Creating a global whitelist rule</td></tr>
<tr><td>Adding a data masking rule</td><td rowspan="2">Check whether users concurrently invoke related APIs.</td><td rowspan="2">Reduce the concurrency of invoking related APIs.</td></tr>
<tr><td>Adding an IP address blacklist or whitelist rule</td></tr>
<tr><td>Creating a reference table rule</td></tr>
<tr><td colspan="2">Creating an edge WAF certificate</td></tr>
<tr><td colspan="2">Creating an edge WAF address group</td></tr>
</table>

A.3.3 EdgeSec.00000014 Only Default Enterprise Project Supported (Not support operation in this enterprise project)

Root Cause

Currently, EdgeSec can be purchased only in the default enterprise project. If you add a domain name to edge WAF or edge DDoS in other enterprise projects, this error will be reported.

Solution

- Console: Switch to the default enterprise project and add a domain name again.

- API: When calling the API for adding a domain name to WAF, change the value of **enterprise_project_id** to **0** (default enterprise project).

A.3.4 EdgeSec.00000015 Write Operation Not Supported When All Enterprise Projects Are Selected (All enterprise projects do not support the write operation)

Root Cause

This error is reported when a user selected **All projects** for **Enterprise Project** and attempted to add a domain name to edge WAF or edge Anti-DDoS. When **All projects** is selected for **Enterprise Project**, only query is supported.

Solution

- Console: Switch to the default enterprise project and add a domain name again.
- API: When calling the API for adding a domain name to WAF, change the value of **enterprise_project_id** to **0** (default enterprise project).

A.3.5 EdgeSec.00000018 Migration of Resources to Non-Default Enterprise Project Not Supported (This version only supports default enterprise project)

Root Cause

Currently, EdgeSec can be purchased only in the default enterprise project. Resources cannot be migrated to a non-default enterprise project.

Troubleshooting and Solution

Event Scenario	Cause	Solution
An error was reported when a user attempted to migrate resources to a non-default enterprise project on the EPS console.	The current edition of EdgeSec does not support non-default enterprise projects.	The current edition does not support this operation. You can upgrade your edition and try again.

A.3.6 EdgeSec.00000019 Frozen Resources Cannot Be Migrated to or from an Enterprise Project (frozen cannot create eps tag)

Root Cause

Frozen resources cannot be added to or removed from an enterprise project.

Troubleshooting Methods

Check whether the resource is frozen.

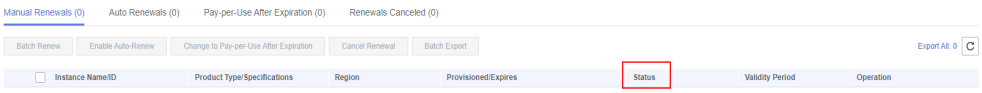
Procedure

Step 1 Log in to the management console.

Step 2 In the upper right corner of the page, choose **Billing & Costs** > **Renewal**. The **Renewals** page is displayed.

Step 3 Check the status of the resource.

Figure A-1 Resource status



----End

Solution

The current version supports only default enterprise project. Migrations to or from other enterprise projects are not supported.

NOTE

Note: The later version will support custom enterprise projects. You can migrate renewed resources between enterprise projects then.

A.3.7 EdgeSec.00000023 Operation Not Supported by the Current Specifications

Root Cause

This error is reported when the specifications in-use do not support some operations.

Troubleshooting Methods

Check the operation permissions of each edition.

Solution

Upgrade the service to the edition that supports the operation.

A.3.8 EdgeSec.00000025 Invalid Block Time (Invalid block time)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

When adding or modifying a protection rule for an edge WAF, enter the block time as instructed.

Solution

Refresh the page and enter a valid block time for the edge WAF protection rule.

A.3.9 EdgeSec.00000026 Invalid Whitelist Rule Type (Invalid rule type)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

Check the condition length.

Solution

Refresh the page and enter the whitelist rule type as instructed.

A.3.10 EdgeSec.00000027 Invalid CC Rule Condition Length (Invalid cc condition length value)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

Check the condition length.

Solution

Refresh the page and enter the length as prompted.

A.3.11 EdgeSec.00010001 Invalid IAM Service Project (Failed to get IAM projects)

Root Cause

This error was reported when an IAM project is abnormal.

Troubleshooting Methods

Check the IAM projects.

Solution

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

Step 2 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Identity Access and Management**.

Step 3 In the navigation pane on the left, choose **Projects** and view the region to which the project belongs.

- If you have registered with the Huawei Cloud International website, there should be a project in the **AP-Singapore** region.
- If you have registered with the Huawei Cloud Chinese Mainland website, there should be a project in the **CN North-Beijing4** region.

NOTE

If there is no such a project, **Submit a Service Ticket** enables the project in the region.

----End

A.3.12 EdgeSec.00010005 Insufficient WAF Policy Rule Quota

Root Cause

The edge WAF policy rule quota is insufficient.

Troubleshooting Methods

Check the policy rule quota of each edition.

Solution

Scenario	Solution
The edition with the largest quota can meet the requirements.	Upgrade the service edition to the required edition.
	If the quota of IP address blacklist and whitelist rules is insufficient, you can upgrade the service edition, or purchase the rule expansion package of edge WAF.

Scenario	Solution
The edition with the largest quota still fails to meet the requirements.	**Submit a service ticket**.

A.3.13 EdgeSec.00010006 Blacklist and Whitelist Rules of Edge WAF Exceed the Quota

Root Cause

Blacklist and whitelist rules of an edge WAF policy exceed the quota.

Troubleshooting Methods

Step 1 **Viewing Blacklist and Whitelist Rule Quotas**

Step 2 Check whether there are protection policies in which the number of blacklist and whitelist rules exceeds the current quota.

----End

Viewing Blacklist and Whitelist Rule Quotas

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

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

Step 3 Click **Edge WAF** in the upper right corner of the page to view the current rule quota.

Figure A-2 Rule Quota

NOTE

Rule quota shows an example. If the rule quota is 1010, the blacklist and whitelist rule quota for a single protection policy is 1010.

----End

Solution

Scenario	Solution
Some blacklist and whitelist rules can be deleted.	Delete unnecessary blacklist and whitelist rules so that the number of blacklist and whitelist rules in each policy does not exceed the current quota.
Existing blacklist and whitelist rules cannot be deleted.	Upgrade the edition or purchase a rule expansion package to ensure that the number of blacklist and whitelist rules in each policy does not exceed the new quota. Blacklist and whitelist rule quota = Edition quota + Number of rule expansion packages x 10. For example, if you use the professional edition of edge WAF and have two rule expansion packages, you can create 120 blacklist and whitelist rules (100 + 2 x 10 = 120). **NOTE** A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules.

A.3.14 EdgeSec.00010007 Insufficient IP Address Group Quota of Edge WAF

Root Cause

The IP address group quota of edge WAF is insufficient.

Troubleshooting Methods

For details about how to view the IP address group quota, see **Specifications Restrictions**

Solution

If the IP address group quota is insufficient, contact technical support.

A.3.15 EdgeSec.00010008 Insufficient Edge WAF Certificate Quota

Root Cause

The edge WAF certificate quota is insufficient.

Troubleshooting Methods

View the domain name quota of edge WAF.

NOTE

The certificate quota is the same as the domain name quota.

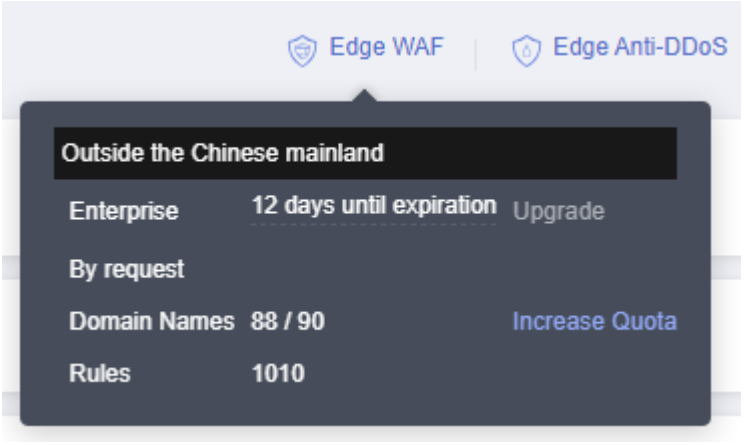
Viewing Domain Quotas

Step 1 Log in to the management console.

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

Step 3 Click **Edge WAF** in the upper right corner of the page to view the current domain name quota.

Figure A-3 Domain name quota



NOTE

Certificate quota = Domain name quota. For example, if the domain name quota is 90, the certificate quota is 90, as shown in **Domain name quota**.

----End

Solution

Purchase the domain name expansion package of the edge WAF.

A.3.16 EdgeSec.00030001 Invalid DDoS Overview Parameters (Illegal Elasticsearch Request)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

Check the parameters on the query page.

Solution

Refresh the page. Then, select a proper time range, specify other parameters, and try again.

A.3.17 EdgeSec.00030003 DDoS Overview Query Type Exception (Statistic Type Error)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

Check the parameters on the query page.

Solution

Refresh the page. Then, select a proper time range, specify other parameters, and try again.

A.3.18 EdgeSec.00030002 DDoS Overview Query Type Exception (Search Error)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

Check the parameters on the query page.

Solution

Refresh the page. Then, select a proper time range, specify other parameters, and try again.

A.3.19 EdgeSec.00040007 No Permission To Operate

Root Cause

This error was reported when the operation permission is insufficient.

Troubleshooting and Solution

Event Scenario	Sub-Scenario	Cause	Solution
Adding, modifying, and deleting operations	Edge WAF	Edge WAF resources are frozen.	Renew the affected resources.
	Edge Anti-DDoS	• No edge Anti-DDoS resources are purchased. • Edge Anti-DDoS resources are frozen.	Buy or renew edge Anti-DDoS resources.
Viewing operation	Edge Anti-DDoS	No edge Anti-DDoS resources are purchased.	Buy edge Anti-DDoS.

A.3.20 EdgeSec.00040013 Insufficient Top-Level Domain Name Quota

Root Cause

This error was reported when the top-level domain name quota in edge WAF was insufficient.

Troubleshooting Methods

1. Learn the top-level domain name quota specified in each EdgeSec edition. For details, see **Specification Limitations**.
2. **Viewing Top-Level Domain Name Quotas**

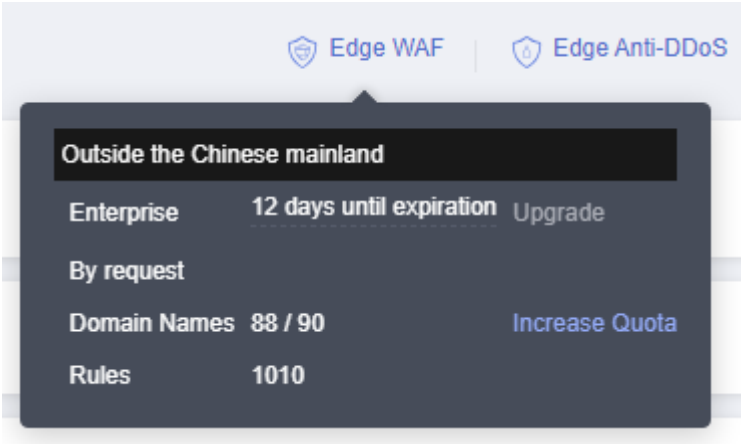
Viewing Top-Level Domain Name Quotas

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

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

Step 3 Click **Edge WAF** in the upper right corner of the page to view the current domain name quota.

Figure A-4 Domain name quota



NOTE

First-level domain name quota = Domain name quota/10. For example, if the domain name quota is 90, as shown in **Figure A-4**, the top-level domain name quota is 9.

----End

Solution

Scenario	Method
The enterprise edition edge WAF is in use.	Buy a domain name expansion package. **NOTE** Each domain name expansion package contains a top-level domain name.
The basic or professional edition edge WAF is in use.	Upgrade the edition or buy a domain name expansion package. **NOTE** Each domain name expansion package contains a top-level domain name.

A.3.21 EdgeSec.00040014 Expansion Resource Quota Has Been Used

Root Cause

This error was generated when expansion resource quotas were in use while the user attempt to unsubscribe from expansion packages they have.

Troubleshooting and Solution

Event Scenario	Cause	Solution
A user attempts to unsubscribe from an edge WAF domain name expansion package.	The number of domain names or rules used by the user has exceeded the quota provided by the edition.	Check the used edge WAF domain names or rules, delete the ones not in use, and keep their quantity within the specifications supported by the service edition in use.
A user attempts to unsubscribe from an edge WAF rule expansion package.		

A.3.22 WAF.00022002 Resource Already Exists (Domain Already Exists)

Root Cause

This error was reported when there are edge WAF resources in the system while a user attempted to create the same ones.

Troubleshooting Methods

Scenario	Cause
Adding or modifying an edge WAF blacklist/ whitelist rule	There is a blacklist or whitelist rule with the same name.
	There is a blacklist or whitelist rule with the same IP addresses listed.
Adding or modifying an edge WAF data masking rule	Duplicate combination of the path, masked fields, and masked field name.

Solution

A rule cannot be added repeatedly. Modify the rule parameters.

A.3.23 WAF.00014002 Resource Already Exists

Root Cause

This error was reported when there are edge WAF resources in the system while a user attempted to create the same ones.

Troubleshooting Methods

Scenario	Cause
Adding an address group	There is already an address group with the same name.

Solution

Do not use an existing address group name when adding an address group.

A.3.24 common.01010003 No Purchase Permission

Root Cause

The current account does not have the purchase permission.

Solution

Event Scenario	Solution
• An IAM user attempts to purchase resources. • An IAM user attempts to change resources.	• Add the IAM user to the admin user group. • Add the IAM user to the group having the EdgeSec_FullAccess Permission. • Use the account that is used to create the IAM user.

A.4 Obtaining a Project ID

Obtaining a Project ID by Calling an API

You can obtain the project ID by calling the API for **Querying Project Information Based on Specified Criteria**.

The API used to obtain a project ID is GET https://{Endpoint}/v3/projects. **{Endpoint}** is the IAM endpoint and can be obtained from **Regions and Endpoints**. For details about API authentication, see **Authentication**.

In the following example, **id** indicates the project ID.

```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180d14e684b",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "xxxxxxxx",
            "description": "",
            "links": {
                "next": null,
```



```
            "previous": null,
            "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
        },
        "id": "a4a5d4098fb4474fa22cd05f897d6b99",
        "enabled": true
    }
  ],
  "links": {
    "next": null,
    "previous": null,
    "self": "https://www.example.com/v3/projects"
  }
}
```


Obtaining a Project ID from the Console

A project ID is required for some URLs when an API is called. To obtain a project ID, perform the following operations:

1. Log in to the management console.
2. Click the username and choose **My Credentials** from the drop-down list.
3. On the page, view the project ID in the project list.

Figure A-5 Viewing project IDs