Cloud Firewall (CFW)

API Reference

Issue	01
Date	2023-07-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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 Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to "Vul. Response Process". For details about the policy, see the following website:https://www.huawei.com/en/psirt/vul-response-process For enterprise customers who need to obtain vulnerability information, visit:https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Before You Start

1.1 Overview

Cloud Firewall (CFW) is a next-generation cloud-native firewall. It protects Internet on the cloud by real-time intrusion detection and prevention, global unified access control, full traffic analysis, log audit, and tracing. It employs AI for intelligent defense, and can be elastically scaled to meet changing business needs, helping you easily handle security threats. CFW is a basic service that provides network security protection for user services on the cloud.

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

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

1.2 API Calling

CFW provides Representational State Transfer (REST) APIs, allowing you to use HTTPS requests to call them. For details, see **API Calling**.

1.3 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), 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.

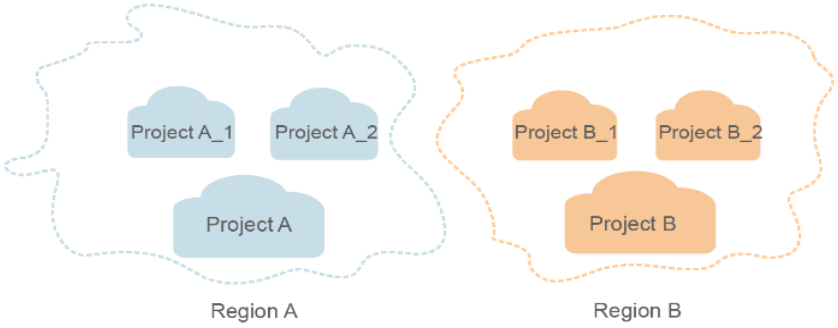
- Availability Zone (AZ)

  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

  A region corresponds to a project. Default projects are defined to group and physically isolate resources (including computing, storage, and network resources) across regions. You can grant users permissions in a default project to access all resources in the region associated with the 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 CFW through its APIs.

Type	Description
CFW Information	This API is used to query CFW information, including querying a CFW instance and the CFW instance list.
ACL Rule	This API is used to create, update, and delete ACL rules.
Blacklist/Whitelist Management	This API is used to manage blacklists and whitelists, including creating, updating, and deleting items in blacklists and whitelists.
IPS Feature Switch	This API is used to manage the IPS feature switch, including querying the status and enabling or disabling the IPS feature.
Elastic IP Address (EIP)	This API is used to manage EIPs, including enabling, disabling, and querying EIPs.
Domain Name Management	This API is used to manage domain names, including querying and updating the DNS server list.
Address Group Management	This API is used to manage address groups, including adding, querying, and updating address groups.
Service Group Management	This API is used to manage service groups, including adding, querying, and modifying service groups.
East-West Protection	This API is used to create, obtain, and modify east-west protection rules.

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 the administrator.

- **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.

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 ***xxxxxxxxxxxxxxxxxx*** to the project name. You can learn more information about projects from the administrator.

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": "xxxxxxxxxxxxxxxxxx"
            }
        }
    }
}
```

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.

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 3-1 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 3-1 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 Domain Name Management

4.1.1 Querying the DNS Server List

Function

This API is used to query the DNS server list.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/dns/servers

Table 4-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-2 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Request Parameters

Table 4-3 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-4 Response body parameters

Parameter	Type	Description
data	Array of DnsServersResponseDTO objects	dns server list
total	Integer	dns server total

Table 4-5 DnsServersResponseDTO

Parameter	Type	Description
id	Integer	id
is_applied	Integer	Indicates whether to apply. 0: no; 1: yes
is_customized	Integer	Indicates whether the DNS server is user-defined. 0: no; 1: yes
server_ip	String	DNS server IP address

Example Requests

Obtain the DNS server list of the project whose ID is 2349ba469daf4b7daf268bb0261d18b0.

```
https://{Endpoint}/cfw/v1/2349ba469daf4b7daf268bb0261d18b0/dns/servers
```

Example Responses

Status code: 200

Response to the request for obtaining DNS servers

```
{
  "data" : [ {
    "id" : 2380,
    "is_applied" : 1,
    "is_customized" : 0,
    "server_ip" : "100.79.1.240"
  }, {
    "id" : 2377,
    "is_applied" : 0,
    "is_customized" : 0,
    "server_ip" : "114.114.114.114"
  } ],
  "total" : 2
}
```

Status Codes

Status Code	Description
200	Response to the request for obtaining DNS servers
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.1.2 Updating the DNS Server List

Function

This API is used to update the DNS server list.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

PUT /v1/{project_id}/dns/servers

Table 4-6 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-7 Query Parameters

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Request Parameters

Table 4-8 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-9 Request body parameters

Parameter	Mandatory	Type	Description
dns_server	No	Array of **dns_server** objects	DNS server

Table 4-10 dns_server

Parameter	Mandatory	Type	Description
server_ip	No	String	DNS server IP address
is_customized	No	Integer	Indicates whether the DNS server is user-defined. 0: no; 1: yes
is_applied	No	Integer	Indicates whether to apply. 0: no; 1: yes

Response Parameters

Status code: 200

Table 4-11 Response body parameters

Parameter	Type	Description
data	Array of strings	Domain name server list

Status code: 400

Table 4-12 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Update the settings of the DNS resolver whose project ID is 2349ba469daf4b7daf268bb0261d18b0. Set server 8.8.8.8 to the default server and put it in use. Set server IP address 192.168.0.2 to a user-defined server and do not put it in use.

```
https://{Endpoint}/v1/2349ba469daf4b7daf268bb0261d18b0/dns/servers

{
  "dns_server" : [ {
    "server_ip" : "8.8.8.8",
    "is_customized" : 0,
    "is_applied" : 1
  }, {
    "server_ip" : "192.168.0.2",
    "is_customized" : 1,
    "is_applied" : 0
  } ]
}
```

Example Responses

Status code: 200

Response to the request for updating the DNS server list

```
{
  "data" : [ "100.95.150.83", "114.114.114.114", "223.5.5.5", "223.6.6.6", "119.29.29.29", "8.8.8.8",
"100.79.1.250", "100.79.1.240" ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.01000001",
  "error_msg" : "Duplicate DNS server IP address"
}
```

Status Codes

Status Code	Description
200	Response to the request for updating the DNS server list
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.1.3 Querying the IP Address for Domain Name Resolution

Function

This API is used to test the validity of a domain name.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/domain/parse/{domain_name}

Table 4-13 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
domain_name	Yes	String	Domain name

Table 4-14 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-15 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-16 Response body parameters

Parameter	Type	Description
data	Array of strings	Domain name ID list

Status code: 400

Table 4-17 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Check whether the ceshi.com domain name in the project whose ID is 5c69cf330cda42369cbd726ee1bc5e76 is valid.

```
https://{Endpoint}/cfw/v1/5c69cf330cda42369cbd726ee1bc5e76/domain/parse/ceshi.com
```

Example Responses

Status code: 200

Return value of a domain name validity query

```
{
  "data" : [ "192.168.88.85", "192.168.88.50", "192.168.88.22", "192.168.88.87", "192.168.88.86",
"192.168.5.1", "192.168.88.88", "192.168.88.90", "192.168.88.83", "192.168.88.84" ]
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00109004",
  "error_msg" : "http to external service error"
}
```

Status Codes

Status Code	Description
200	Return value of a domain name validity query
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

Status Code	Description
500	Internal Server Error

Error Codes

See **Error Codes**.

4.2 VPC Protection

4.2.1 Querying the Number of Protected VPCs

Function

This API is used to query protected VPCs.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/vpcs/protection

Table 4-18 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-19 Query Parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-20 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-21 Response body parameters

Parameter	Type	Description
trace_id	String	Call chain ID
data	**VPCProtectsVo** object	Return value of VPC protection

Table 4-22 VPCProtectsVo

Parameter	Type	Description
total	Integer	Total number of VPCs
self_total	Integer	Total number of self VPCs
other_total	Integer	Total number of other VPCs
protect_vpcs	Array of **VpcAttachmentDetail** objects	Protect VPC
self_protect_vpcs	Array of **VpcAttachmentDetail** objects	Self Protect VPC
other_protect_vpcs	Array of **VpcAttachmentDetail** objects	Other Protect VPC

Table 4-23 VpcAttachmentDetail

Parameter	Type	Description
id	String	id
name	String	name
vpc_id	String	vpc id
virsubnet_id	String	subnet id
state	String	state
created_at	String	create time
updated_at	String	update time
tags	Array of **Tag** objects	tag
description	String	description
project_id	String	project id
vpc_project_id	String	vpc project id
enterprise_project_id	String	enterprise project id

Table 4-24 Tag

Parameter	Type	Description
key	String	key
value	String	value

Status code: 500

Table 4-25 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query the east-west firewall protection information about the projected object with the ID 8839526e-b804-4a15-a082-a2c797dce633 in project 0b2179bbe180d3762fb0c01a2d5725c7.

```
https://{ENDPOINT}/v1/0b2179bbe180d3762fb0c01a2d5725c7/vpcs/protection?object_id=8839526e-b804-4a15-a082-a2c797dce633
```

Example Responses

Status code: 200

Return value of east-west protection query

```
{
  "data" : {
    "protect_vpcs" : [ {
      "created_at" : "2022-09-30T02:27:06.33Z",
      "description" : "",
      "id" : "cd7d7f62-0b04-42e8-a859-671dfce75cc1",
      "name" : "er-attach-c4ab",
      "project_id" : "09bb24e6fe80d23d2fa2c010b53b418c",
      "state" : "available",
      "tags" : [ ],
      "updated_at" : "2022-09-30T02:35:35.332Z",
      "virsubnet_id" : "81fda592-b1e9-4437-8078-7fcf786f4e80",
      "vpc_id" : "122c2907-eada-4df4-8ffe-6088cf33d425"
    } ],
    "self_protect_vpcs" : [ ],
    "other_protect_vpcs" : [ ],
    "total" : 1,
    "self_total" : 0,
    "other_total" : 0
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00109004",
  "error_msg" : "http to external service error"
}
```

Status Codes

Status Code	Description
200	Return value of east-west protection query
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.3 Rule Hit Count

4.3.1 Obtaining the Rule Hit Count

Function

This API is used to obtain the rule hit count.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

POST /v1/{project_id}/acl-rule/count

Table 4-26 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-27 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-28 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-29 Request body parameters

Parameter	Mandatory	Type	Description
rule_ids	Yes	Array of strings	Rule ID list

Response Parameters

Status code: 200

Table 4-30 Response body parameters

Parameter	Type	Description
data	**RuleHitCountRecords** object	Rule hit count

Table 4-31 RuleHitCountRecords

Parameter	Type	Description
limit	Integer	Number of records displayed on each page
offset	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
total	Integer	Total
records	Array of **RuleHitCountObject** objects	Rule hit count list

Table 4-32 RuleHitCountObject

Parameter	Type	Description
rule_id	String	Rule ID
rule_hit_count	Integer	Rule Hit Count

Example Requests

Query the ACL rule hit count.

```
https://{Endpoint}/v1/0b2179bbe180d3762fb0c01a2d5725c7/acl_rule/count

{
  "rule_ids" : [ "59ff6bd9-0a76-41ec-9650-380086069965" ]
}
```

Example Responses

Status code: 200

Response to the request for obtaining the number of rule hits

```
{
  "data" : {
    "limit" : 1,
    "offset" : 1,
```

```
  "records" : [ {
    "rule_hit_count" : 0,
    "rule_id" : "59ff6bd9-0a76-41ec-9650-380086069965"
  } ],
  "total" : 1
 }
}
```

Status Codes

Status Code	Description
200	Response to the request for obtaining the number of rule hits
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.3.2 Deleting the Rule Hit Count

Function

This API is used to delete the rule hit count.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

DELETE /v1/{project_id}/acl-rule/count

Table 4-33 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	project id

Table 4-34 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-35 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-36 Request body parameters

Parameter	Mandatory	Type	Description
rule_ids	Yes	Array of strings	Rule ID list

Response Parameters

Status code: 400

Table 4-37 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Delete the ACL rule hit count.

```
https://{Endpoint}/v1/0b2179bbe180d3762fb0c01a2d5725c7/acl_rule/count

{
  "rule_ids" : [ "59ff6bd9-0a76-41ec-9650-380086069965" ]
}
```

Example Responses

Status code: 200

OK

```
{ }
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00400006",
  "error_msg" : "clear rule hit count param error."
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.4 IPS Switch Management

4.4.1 Querying the IPS Switch Status

Function

This API is used to query the IPS switch status.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/ips/switch

Table 4-38 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	project_id

Table 4-39 Query Parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-40 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-41 Response body parameters

Parameter	Type	Description
data	**IpsSwitchResponseDTO** object	ips switch response

Table 4-42 IpsSwitchResponseDTO

Parameter	Type	Description
id	String	Ips switch id
basic_defense_status	Integer	Basic defense status
virtual_patches_status	Integer	Virtual patch status

Example Requests

Query the patch status of the current user based on the received user ID and load the virtual patch status on the intrusion prevention page.

```
https://{Endpoint}/v1/14181c1245cf4fd786824efe1e2b9388/ips/switch
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
```

```
    "basic_defense_status" : 1,
    "id" : "cefe80aa-83e4-4308-99aa-f9b6c816de00",
    "virtual_patches_status" : 0
  }
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.4.2 Enabling or Disabling IPS

Function

This API is used to enable or disable the feature.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

POST /v1/{project_id}/ips/switch

Table 4-43 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	project_id

Table 4-44 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-45 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-46 Request body parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
ips_type	Yes	Integer	Patch type. Only virtual patch is supported. The value is 2.
status	Yes	Integer	IPS switch status

Response Parameters

Status code: 200

Table 4-47 Response body parameters

Parameter	Type	Description
trace_id	String	trace_id
data	**data** object	object

Table 4-48 data

Parameter	Type	Description
id	String	Protected object ID

Example Requests

Enable or disable the basic patch and virtual patch of the engine on the user portal. The patch is enabled or disabled based on the received protected object ID, user ID, patch type ID, and status.

```
https://{Endpoint}/v1/14181c1245cf4fd786824efe1e2b9388/ips/switch
```

```
{
  "ips_type" : 1,
  "object_id" : "1530de8a-522d-4771-9067-9fa4e2f53b48",
  "status" : 1
}
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "id" : "1530de8a-522d-4771-9067-9fa4e2f53b48"
  },
  "trace_id" : "358144a9885ff55100aa63cb0d0e1039"
}
```

Status Codes

Status Code	Description
200	OK
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.5 East-west Protection

4.5.1 Obtaining East-West Firewall Information

Function

This API is used to obtain east-west firewall information.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/firewall/east-west

Table 4-49 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-50 Query Parameters

Parameter	Mandatory	Type	Description
limit	Yes	Integer	Number of records displayed on each page
offset	Yes	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-51 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-52 Response body parameters

Parameter	Type	Description
data	**GetEastWestFirewallResponseBody** object	Get east west firewall data response

Table 4-53 GetEastWestFirewallResponseBody

Parameter	Type	Description
object_id	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
project_id	String	Project ID
status	Integer	Protection status. The value can be 0 (protection enabled) or 1 (protection disabled).
er_associated_subnet	**SubnetInfo** object	Information about the subnet associated with ER

Parameter	Type	Description
firewall_associated_subnets	Array of **SubnetInfo** objects	Subnet associated with CFW
er	**ErInstance** object	Information about the associated outbound enterprise router
inspection_vpc	**VpcDetail** object	Monitoring VPC information
protect_infos	Array of **EwProtectResourceInfo** objects	East-west protection resource information
total	Integer	Total number of protected VPCs
offset	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	Integer	Number of records displayed on each page

Table 4-54 SubnetInfo

Parameter	Type	Description
availability_zone	String	Subnet ID
cidr	String	vpc cidr
name	String	Subnet name
id	String	Subnet ID
gateway_ip	String	Subnet gateway IP address
vpc_id	String	vpc id
status	String	Subnet status

Table 4-55 ErInstance

Parameter	Type	Description
id	String	ER instance ID
name	String	ER name
state	String	ER status

Parameter	Type	Description
enterprise_project_id	String	Enterprise user ID
project_id	String	User ID
enable_ipv6	String	Whether to enable IPv6

Table 4-56 VpcDetail

Parameter	Type	Description
id	String	id
name	String	Name
cidr	String	vpc cidr
status	String	Status

Table 4-57 EwProtectResourceInfo

Parameter	Type	Description
protected_resource_type	Integer	Protection resource type. The value can be 0 (VPC) or 1 (VGW).
protected_resource_name	String	Protected resource name
protected_resource_id	String	Protected resource ID
protected_resource_nat_name	String	Name of the NAT gateway of the protected resource
protected_resource_nat_id	String	ID of the NAT gateway of the protected resource
protected_resource_project_id	String	Tenant ID of the protected resource

Status code: 500

Table 4-58 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Obtaining East-West Firewall Information

```
https://{Endpoint}/v1/09bb24e6f280d23d0f9fc0104b901480/firewall/east-west?limit=10&offset=0
```

Example Responses

Status code: 200

Response to the request for querying east-west firewall information

```
{
  "data" : {
    "er" : {
      "id" : "91fcda9e-2ac7-49a0-89f1-ebee2710347f",
      "name" : "er-test2"
    },
    "er_associated_subnet" : {
      "cidr" : "192.168.0.0/28",
      "id" : "f4467981-2271-4330-b403-cc9f024ab913",
      "name" : "aafdsfas"
    },
    "firewall_associated_subnets" : [ {
      "cidr" : "192.168.0.16/28",
      "id" : "b7cc2358-ede7-4be2-88d0-cfa20fcd4fe9",
      "name" : "aaa"
    }, {
      "cidr" : "192.168.0.32/28",
      "id" : "357a9cca-fd98-4b76-b4e4-ef40954c061a",
      "name" : "asdf"
    } ],
    "inspection_vpc" : {
      "cidr" : "192.168.0.0/24",
      "id" : "9a11350a-3ca5-46b6-a33f-d82c263bc7d8",
      "name" : "ws-01"
    },
    "limit" : 10,
    "object_id" : "8839526e-b804-4a15-a082-a2c797dce633",
    "offset" : 0,
    "project_id" : "0b2179bbe180d3762fb0c01a2d5725c7",
    "protect_infos" : [ ],
    "status" : 3,
    "total" : 0
  }
}
```


Status Codes

Status Code	Description
200	Response to the request for querying east-west firewall information
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.5.2 Changing the East-West Firewall Protection Status

Function

This API is used to enable or disable east-west protection.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

POST /v1/{project_id}/firewall/east-west/protect

Table 4-59 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-60 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-61 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-62 Request body parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
status	Yes	Integer	Protection status. The value can be 0 (enabled) or 1 (disabled). Enumeration values: • **0** • **1**

Response Parameters

Status code: 200

Table 4-63 Response body parameters

Parameter	Type	Description
data	**data** object	Response body
trace_id	String	trace id

Table 4-64 data

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-65 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

In the project with the ID 09bb24e6fe80d23d2fa2c010b53b418c, enable protection for the object with the ID 74820b38-1cc0-4f0b-8cce-32490fa840a3.

```
https://{Endpoint}/v1/09bb24e6fe80d23d2fa2c010b53b418c/firewall/east-west/protect

{
  "object_id" : "74820b38-1cc0-4f0b-8cce-32490fa840a3",
  "status" : 1
}
```

Example Responses

Status code: 200

Response body for updating the east-west protection status

```
{
  "data" : {
    "id" : "5c539816-7a94-4833-9df0-944b362f0797"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	Response body for updating the east-west protection status
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.6 ACL Rule Management

4.6.1 Creating an ACL Rule

Function

This API is used to create an ACL rule.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

POST /v1/{project_id}/acl-rule

Table 4-66 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-67 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-68 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-69 Request body parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
type	Yes	Integer	Rule type. The value can be 0 (Internet rule), 1 (VPC rule), or 2 (NAT rule). Enumeration values: • **0** • **1** • **2**
rules	Yes	Array of **rules** objects	rules

Table 4-70 rules

Parameter	Mandatory	Type	Description
name	Yes	String	Rule name
sequence	Yes	**OrderRuleAclDto** object	Rule sequence
address_type	Yes	Integer	Address type. The value can be 0 (IPv4), 1 (IPv6), or 2 (domain). Enumeration values: • **0** • **1** • **2**
action_type	Yes	Integer	Action. 0: allow; 1: deny

Parameter	Mandatory	Type	Description
status	Yes	Integer	Rule delivery status. 0: disabled; 1: enabled. Enumeration values: • **0** • **1**
long_connect_time	No	Long	Persistent connection duration
long_connect_time_hour	No	Long	Persistent connection duration (hour)
long_connect_time_minute	No	Long	Persistent connection duration (minute)
long_connect_time_second	No	Long	Persistent Connection Duration (second)
long_connect_enable	Yes	Integer	Whether to support persistent connections. 0: not supported; 1: supported. Enumeration values: • **0** • **1**
description	No	String	Description
direction	No	Integer	direction:0 outToin,1 inToout Enumeration values: • **0** • **1**
source	Yes	**RuleAddressDto** object	Source address transmission object
destination	Yes	**RuleAddressDto** object	Destination address transmission object
service	Yes	**RuleServiceDto** object	Service object

Table 4-71 OrderRuleAclDto

Parameter	Mandatory	Type	Description
dest_rule_id	No	String	ID of the rule that the added rule will follow. This parameter cannot be left blank if the rule is not pinned on top, and is empty when the added rule is pinned on top.
top	No	Integer	Whether to pin on top. The options are as follows: 0: no; 1: yes.

Table 4-72 RuleAddressDto

Parameter	Mandatory	Type	Description
type	Yes	Integer	Source type. 0: manual input; 1: associated IP address group; 2: domain name
address_type	No	Integer	Source type. 0: IPv4; 1: IPv6
address	No	String	Source IP address. The value cannot be empty for the manual type, and cannot be empty for the automatic or domain type.
address_set_id	No	String	ID of the associated IP address group. The value cannot be empty for the automatic type or for the manual or domain type.
address_set_name	No	String	IP address group name
domain_address_name	No	String	Name of the domain name address. This parameter cannot be left empty for the domain name type, and is empty for the manual or automatic type.

Table 4-73 RuleServiceDto

Parameter	Mandatory	Type	Description
type	Yes	Integer	Service input type. The value 0 indicates manual input, and the value 1 indicates automatic input.
protocol	No	Integer	Protocol type. The value 6 indicates TCP, 17 indicates UDP, 1 indicates ICMP, 58 indicates ICMPv6, and -1 indicates any protocol. Regarding the addition type, a null value indicates it is automatically added.
source_port	No	String	Source port
dest_port	No	String	Destination port
service_set_id	No	String	Service group ID. This parameter is left blank for the manual type and cannot be left blank for the automatic type.
service_set_name	No	String	Service group name

Response Parameters

Status code: 200

Table 4-74 Response body parameters

Parameter	Type	Description
data	**RuleIdList** object	Rule ID list

Table 4-75 RuleIdList

Parameter	Type	Description
rules	Array of **RuleId** objects	Rule ID list

Table 4-76 RuleId

Parameter	Type	Description
id	String	id

Status code: 400

Table 4-77 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

The following example shows how to add an IPv4 inbound rule. The rule name is TestRule, the source is the IP address 1.1.1.1, the destination is the IP address 2.2.2.2, the service type is service, the protocol type is TCP, the source port is 0, and the destination port is 0. Persistent connections are not supported. The action is to allow. The status is enabled.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/acl-rule

{
  "object_id" : "e12bd2cd-ebfc-4af7-ad6f-ebe6da398029",
  "rules" : [ {
    "name" : "TestRule",
    "status" : 1,
    "action_type" : 0,
    "description" : "",
    "source" : {
      "type" : 0,
      "address" : "1.1.1.1"
    },
    "destination" : {
      "type" : 0,
      "address" : "2.2.2.2"
    },
    "service" : {
      "type" : 0,
      "protocol" : 6,
      "source_port" : "0",
      "dest_port" : "0"
    },
    "address_type" : 0,
    "long_connect_enable" : 0,
    "direction" : 0,
    "sequence" : {
      "top" : 1
```

```
    }
  } ],
  "type" : 0
}
```

Example Responses

Status code: 200

Response to the request for adding an ACL

```
{
  "data" : {
    "rules" : [ {
      "id" : "ceaa0407-b9c8-4dfd-9eca-b6ead2dfd031"
    } ]
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00900016",
  "error_msg" : "The import task is in progress. Please operate after the task is completed"
}
```

Status Codes

Status Code	Description
200	Response to the request for adding an ACL
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.6.2 Updating an ACL Rule

Function

This API is used to update an ACL rule.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

PUT /v1/{project_id}/acl-rule/{acl_rule_id}

Table 4-78 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
acl_rule_id	Yes	String	Rule ID

Table 4-79 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-80 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-81 Request body parameters

Parameter	Mandatory	Type	Description
address_type	No	Integer	Address type. The value can be 0 (IPv4) or 1 (IPv6). Enumeration values: • **0** • **1**
name	No	String	Rule name
sequence	No	**OrderRuleAclDto** object	UpdateRuleAclDto
direction	No	Integer	Rule direction Enumeration values: • **0** • **1**
action_type	No	Integer	Action. 0: allow; 1: deny Enumeration values: • **0** • **1**
status	No	Integer	Rule delivery status. 0: disabled; 1: enabled.
description	No	String	Description
long_connect_time_hour	No	Long	Persistent connection duration (hour)
long_connect_time_minute	No	Long	Persistent connection duration (hour)
long_connect_time_second	No	Long	Persistent connection duration (minute)

Parameter	Mandatory	Type	Description
long_connect_time	No	Long	Persistent connection duration
long_connect_enable	No	Integer	Whether to support persistent connections. 0: not supported; 1: supported. Enumeration values: • **0** • **1**
source	No	**RuleAddressDto** object	Rule address DTO
destination	No	**RuleAddressDto** object	Rule address DTO
service	No	**RuleServiceDto** object	RuleServiceDto
type	No	Integer	Rule type. The value can be 0 (Internet rule), 1 (VPC rule), or 2 (NAT rule). Enumeration values: • **0** • **1** • **2**

Table 4-82 OrderRuleAclDto

Parameter	Mandatory	Type	Description
dest_rule_id	No	String	ID of the rule that the added rule will follow. This parameter cannot be left blank if the rule is not pinned on top, and is empty when the added rule is pinned on top.
top	No	Integer	Whether to pin on top. The options are as follows: 0: no; 1: yes.

Table 4-83 RuleAddressDto

Parameter	Mandatory	Type	Description
type	Yes	Integer	Source type. 0: manual input; 1: associated IP address group; 2: domain name
address_type	No	Integer	Source type. 0: IPv4; 1: IPv6
address	No	String	Source IP address. The value cannot be empty for the manual type, and cannot be empty for the automatic or domain type.
address_set_id	No	String	ID of the associated IP address group. The value cannot be empty for the automatic type or for the manual or domain type.
address_set_name	No	String	IP address group name
domain_address_name	No	String	Name of the domain name address. This parameter cannot be left empty for the domain name type, and is empty for the manual or automatic type.

Table 4-84 RuleServiceDto

Parameter	Mandatory	Type	Description
type	Yes	Integer	Service input type. The value 0 indicates manual input, and the value 1 indicates automatic input.
protocol	No	Integer	Protocol type. The value 6 indicates TCP, 17 indicates UDP, 1 indicates ICMP, 58 indicates ICMPv6, and -1 indicates any protocol. Regarding the addition type, a null value indicates it is automatically added.
source_port	No	String	Source port
dest_port	No	String	Destination port

Parameter	Mandatory	Type	Description
service_set_id	No	String	Service group ID. This parameter is left blank for the manual type and cannot be left blank for the automatic type.
service_set_name	No	String	Service group name

Response Parameters

Status code: 200

Table 4-85 Response body parameters

Parameter	Type	Description
data	**RuleId** object	Rule ID

Table 4-86 RuleId

Parameter	Type	Description
id	String	id

Status code: 400

Table 4-87 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

The following example shows how to update an IPv4 inbound rule. The rule name is TestRule, the source is the IP address 1.1.1.1, the destination is the IP address 2.2.2.2, the service type is service, the protocol type is TCP, the source port is 0,

and the destination port is 0. Persistent connections are not supported. The action is to allow. The status is enabled.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/acl-rule/ceaa0407-b9c8-4dfd-9eca-b6ead2dfd031

{
  "name" : "TestRule",
  "status" : 1,
  "action_type" : 0,
  "description" : "",
  "source" : {
    "type" : 0,
    "address" : "1.1.1.1"
  },
  "destination" : {
    "type" : 0,
    "address" : "2.2.2.2"
  },
  "service" : {
    "type" : 0,
    "protocol" : 6,
    "source_port" : "0",
    "dest_port" : "0"
  },
  "type" : 0,
  "address_type" : 0,
  "long_connect_enable" : 0,
  "direction" : 0
}
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "id" : "ceaa0407-b9c8-4dfd-9eca-b6ead2dfd031"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.6.3 Deleting an ACL Rule Group

Function

This API is used to delete an ACL rule group.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

DELETE /v1/{project_id}/acl-rule/{acl_rule_id}

Table 4-88 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
acl_rule_id	Yes	String	Rule ID

Table 4-89 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-90 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-91 Response body parameters

Parameter	Type	Description
data	**RuleId** object	

Table 4-92 RuleId

Parameter	Type	Description
id	String	id

Status code: 400

Table 4-93 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Delete the rule whose project ID is 9d80d070b6d44942af73c9c3d38e0429 and rule ID is ceaa0407-b9c8-4dfd-9eca-b6ead2dfd031.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/acl-rule/ceaa0407-b9c8-4dfd-9eca-b6ead2dfd031
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "id" : "ceaa0407-b9c8-4dfd-9eca-b6ead2dfd031"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00900016",
  "error_msg" : "The import task is in progress. Please operate after the task is completed"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.6.4 Querying a Protection Rule

Function

This API is used to query a protection rule.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/acl-rules

Table 4-94 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-95 Query Parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
type	No	Integer	Specifies the rule type. The value can be 0 (Internet rule), 1 (VPC rule), or 2 (NAT rule). Enumeration values: • **0** • **1** • **2**
protocol	No	Integer	Protocol type. The value is 6 for TCP, 17 for UDP, 1 for ICMP, 58 for ICMPv6, and -1 for any protocol. Enumeration values: • **6** • **17** • **1** • **58**
ip	No	String	IP address
name	No	String	Name
direction	No	Integer	Direction. 0: inbound; 1: outbound
status	No	Integer	Indicates the rule delivery status. 0: disabled; 1: enabled. Enumeration values: • **0** • **1**

Parameter	Mandatory	Type	Description
action_type	No	Integer	Action. 0: allow; 1: deny Enumeration values: • **0** • **1**
address_type	No	Integer	Address type. The value can be 0 (IPv4), 1 (IPv6), or 2 (domain). Enumeration values: • **0** • **1** • **2**
limit	Yes	Integer	Number of records displayed on each page
offset	Yes	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-96 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-97 Response body parameters

Parameter	Type	Description
data	**data** object	data

Table 4-98 data

Parameter	Type	Description
offset	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	Integer	Number of records displayed on each page
total	Integer	Total number of queried records
object_id	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
records	Array of **records** objects	records

Table 4-99 records

Parameter	Type	Description
rule_id	String	Rule ID
address_type	Integer	Address type. The value can be 0 (IPv4) or 1 (IPv6).
name	String	Rule name
sequence	**OrderRuleAclDto** object	UpdateRuleAclDto
direction	Integer	Rule direction. 0: inbound; 1: outbound Enumeration values: • **0** • **1**
action_type	Integer	Action. 0: allow; 1: deny
status	Integer	Rule delivery status. 0: disabled; 1: enabled.
description	String	Description
long_connect_time_hour	Long	Persistent connection duration (hour)
long_connect_time_minute	Long	Persistent connection duration (hour)
long_connect_time_second	Long	Persistent connection duration (hour)
long_connect_time	Long	Persistent connection duration
long_connect_enable	Integer	Persistent connection support
source	**RuleAddressDto** object	Source address transmission object
destination	**RuleAddressDto** object	destination
service	**RuleServiceDto** object	service
type	Integer	Rule type. The value can be 0 (Internet rule), 1 (VPC rule), or 2 (NAT rule). Enumeration values: • **0** • **1** • **2**

Table 4-100 OrderRuleAclDto

Parameter	Type	Description
dest_rule_id	String	ID of the rule that the added rule will follow. This parameter cannot be left blank if the rule is not pinned on top, and is empty when the added rule is pinned on top.
top	Integer	Whether to pin on top. The options are as follows: 0: no; 1: yes.

Table 4-101 RuleAddressDto

Parameter	Type	Description
type	Integer	Source type. 0: manual input; 1: associated IP address group; 2: domain name
address_type	Integer	Source type. 0: IPv4; 1: IPv6
address	String	Source IP address. The value cannot be empty for the manual type, and cannot be empty for the automatic or domain type.
address_set_id	String	ID of the associated IP address group. The value cannot be empty for the automatic type or for the manual or domain type.
address_set_name	String	IP address group name
domain_address_name	String	Name of the domain name address. This parameter cannot be left empty for the domain name type, and is empty for the manual or automatic type.

Table 4-102 RuleServiceDto

Parameter	Type	Description
type	Integer	Service input type. The value 0 indicates manual input, and the value 1 indicates automatic input.
protocol	Integer	Protocol type. The value 6 indicates TCP, 17 indicates UDP, 1 indicates ICMP, 58 indicates ICMPv6, and -1 indicates any protocol. Regarding the addition type, a null value indicates it is automatically added.
source_port	String	Source port

Parameter	Type	Description
dest_port	String	Destination port
service_set_id	String	Service group ID. This parameter is left blank for the manual type and cannot be left blank for the automatic type.
service_set_name	String	Service group name

Status code: 400

Table 4-103 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query the data whose project ID is 9d80d070b6d44942af73c9c3d38e0429, project ID is e12bd2cd-ebfc-4af7-ad6f-ebe6da398029, and size is 10.

```
https://{Endpoint}/cfw/v1/9d80d070b6d44942af73c9c3d38e0429/acl-rules?object_id=e12bd2cd-ebfc-4af7-ad6f-ebe6da398029&limit=10&offset=0
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "limit" : 10,
    "object_id" : "cfebd347-b655-4b84-b938-3c54317599b2",
    "offset" : 0,
    "records" : [ {
      "action_type" : 0,
      "address_type" : 0,
      "destination" : {
        "address" : "0.0.0.0/0",
        "address_type" : 0,
        "type" : 0
      },
      "direction" : 1,
      "long_connect_enable" : 0,
```



```
    "name" : "eip_ipv4_n_w_allow",
    "rule_id" : "ffe9af47-d893-483b-86e3-ee5242e8cb15",
    "service" : {
      "dest_port" : "0",
      "protocol" : -1,
      "source_port" : "0",
      "type" : 0
    },
    "source" : {
      "address_set_id" : "48bfb09b-6f3a-4371-8ddb-05d5d7148bcc",
      "address_set_name" : "ip_group",
      "address_type" : 0,
      "type" : 1
    },
    "status" : 1,
    "type" : "0"
   } ],
   "total" : 1
 }
}
```


Status code: 400

Bad Request


```
{
  "error_code" : "CFW.0020016",
  "error_msg" : "instance status error"
}
```


Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.6.5 Setting the Priority of an ACL Protection Rule

Function

This API is used to set the priority of an ACL protection rule.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

PUT /v1/{project_id}/acl-rule/order/{acl_rule_id}

Table 4-104 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
acl_rule_id	Yes	String	Rule ID

Table 4-105 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-106 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-107 Request body parameters

Parameter	Mandatory	Type	Description
dest_rule_id	No	String	ID of the rule that the added rule will follow. This parameter cannot be left blank if the rule is not pinned on top, and is empty when the added rule is pinned on top.
top	No	Integer	Whether to pin on top. The options are as follows: 0: no; 1: yes.

Response Parameters

Status code: 200

Table 4-108 Response body parameters

Parameter	Type	Description
data	**RuleId** object	Rule ID list

Table 4-109 RuleId

Parameter	Type	Description
id	String	id

Status code: 400

Table 4-110 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Set the project ID and rule ID. 9d80d070b6d44942af73c9c3d38e0429 indicates the ID of the ffe9af47-d893-483b-86e3-ee5242e8cb15 rule after it is moved behind the rule whose ID is 69c32dc5-f801-4294-98ee-978b51f97d35.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/acl-rule/order/ffe9af47-d893-483b-86e3-ee5242e8cb15

{
  "top" : 0,
  "dest_rule_id" : "69c32dc5-f801-4294-98ee-978b51f97d35"
}
```

Example Responses

Status code: 200

Rule sorting response

```
{
  "data" : {
    "id" : "ffe9af47-d893-483b-86e3-ee5242e8cb15"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	Rule sorting response
400	Bad Request
401	Unauthorized

Status Code	Description
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.7 Blacklist and Whitelist Management

4.7.1 Creating a Blacklist or Whitelist Rule

Function

This API is used for creating a blacklist or whitelist rule.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

POST /v1/{project_id}/black-white-list

Table 4-111 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-112 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-113 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-114 Request body parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
list_type	Yes	Integer	Blacklist/Whitelist type. The options are 4 (blacklist) and 5 (whitelist).
direction	Yes	Integer	Indicates the address direction. 0: source address 1: destination address
address_type	Yes	Integer	IP address type. 0: ipv4; 1: ipv6; 2: domain
address	Yes	String	Address type
protocol	Yes	Integer	Protocol type. The value 6 indicates TCP, 17 indicates UDP, 1 indicates ICMP, 58 indicates ICMPv6, and -1 indicates any protocol. Regarding the addition type, a null value indicates it is automatically added.
port	Yes	String	Destination port

Response Parameters

Status code: 200

Table 4-115 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Response to the request for adding a blacklist or whitelist

Table 4-116 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-117 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Add an IPv4 TCP whitelist to object cfebd347-b655-4b84-b938-3c54317599b2 of project 9d80d070b6d44942af73c9c3d38e0429. Direction: source address; IP address: 1.1.1.1; protocol type: TCP; port number: 1

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/black-white-list

{
  "object_id" : "cfebd347-b655-4b84-b938-3c54317599b2",
  "list_type" : 5,
  "direction" : 0,
  "address" : "1.1.1.1",
  "protocol" : 6,
  "port" : "1",
  "address_type" : 0
}
```

Example Responses

Status code: 200

Response to the request for adding a blacklist or whitelist

```
{
  "data" : {
    "id" : "2eee3fe8-0b9b-49ac-8e7f-eaafa321e99a"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.0020016",
  "error_msg" : "instance status error"
}
```

Status Codes

Status Code	Description
200	Response to the request for adding a blacklist or whitelist
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.7.2 Updating the Blacklist or Whitelist

Function

This API is used to update the blacklist or whitelist.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

PUT /v1/{project_id}/black-white-list/{list_id}

Table 4-118 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
list_id	Yes	String	Blacklist/Whitelist ID

Table 4-119 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-120 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-121 Request body parameters

Parameter	Mandatory	Type	Description
direction	No	Integer	Indicates the address direction. 0: source address 1: destination address
address_type	No	Integer	Address type. 0: ipv4; 1: ipv6; 2: domain
address	No	String	IP address
protocol	No	Integer	Protocol type. The value is 6 for TCP, 17 for UDP, 1 for ICMP, 58 for ICMPv6, and -1 for any protocol.
port	No	String	Port
list_type	No	Integer	Blacklist/Whitelist type. The options are 4 (blacklist) and 5 (whitelist). Enumeration values: • **4** • **5**

Parameter	Mandatory	Type	Description
object_id	No	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.

Response Parameters

Status code: 200

Table 4-122 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Response to the request for updating a blacklist or whitelist

Table 4-123 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-124 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**

Parameter	Type	Description
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Add an IPv4 TCP whitelist to object cfebd347-b655-4b84-b938-3c54317599b2 of project 9d80d070b6d44942af73c9c3d38e0429. Whitelist direction: source address; IP address: 1.1.1.1; protocol type: TCP; port number: 1

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/black-white-list/
9d80d070b6d44942af73c9c3d38e042b

{
  "object_id" : "cfebd347-b655-4b84-b938-3c54317599b2",
  "list_type" : 5,
  "direction" : 0,
  "address" : "1.1.1.1",
  "protocol" : 6,
  "port" : "1",
  "address_type" : 0
}
```

Example Responses

Status code: 200

Blacklist/Whitelist update response

```
{
  "data" : {
    "id" : "2eee3fe8-0b9b-49ac-8e7f-eaafa321e99a"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	Blacklist/Whitelist update response
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.7.3 Deleting a Blacklist or Whitelist Rule

Function

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

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

DELETE /v1/{project_id}/black-white-list/{list_id}

Table 4-125 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
list_id	Yes	String	Blacklist/Whitelist ID

Table 4-126 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-127 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-128 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Response to the request for deleting a blacklist or whitelist

Table 4-129 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-130 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Delete the blacklist and whitelist whose ID is 2eee3fe8-0b9b-49ac-8e7f-eaafa321e99a from the project whose ID is 9d80d070b6d44942af73c9c3d38e0429.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/black-white-list/2eee3fe8-0b9b-49ac-8e7f-eaafa321e99a
```

Example Responses

Status code: 200

Blacklist/Whitelist deletion response

```
{
  "data" : {
    "id" : "2eee3fe8-0b9b-49ac-8e7f-eaafa321e99a"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	Blacklist/Whitelist deletion response
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.7.4 Querying a Blacklist or Whitelist

Function

This API is used to query a blacklist or whitelist.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/black-white-lists

Table 4-131 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-132 Query Parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
list_type	Yes	Integer	Blacklist/Whitelist type. The options are 4 (blacklist) and 5 (whitelist). Enumeration values: • **4** • **5**
address_type	No	Integer	Specifies the IP address type. The value can be 0 (IPv4), 1 (IPv6), or 2 (domain). Enumeration values: • **0** • **1** • **2**
address	No	String	IP address
port	No	String	Port
limit	Yes	Integer	Number of records displayed on each page
offset	Yes	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-133 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-134 Response body parameters

Parameter	Type	Description
data	**data** object	Return value for querying the blacklist or whitelist

Table 4-135 data

Parameter	Type	Description
object_id	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
offset	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	Integer	Number of records displayed on each page
total	Integer	Total number of queried records
records	Array of **records** objects	Blacklist and whitelist records

Table 4-136 records

Parameter	Type	Description
list_id	String	Blacklist/Whitelist ID
direction	Integer	Direction of a black or white address. 0: source address; 1: destination address.
address_type	Integer	IP address type. 0: ipv4; 1: ipv6; 2: domain
address	String	IP address
protocol	Integer	Protocol type. The value 6 indicates TCP, 17 indicates UDP, 1 indicates ICMP, 58 indicates ICMPv6, and -1 indicates any protocol. Regarding the addition type, a null value indicates it is automatically added.
port	String	Port

Status code: 400

Table 4-137 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query five whitelist records on the first page of object cfebd347-b655-4b84-b938-3c54317599b2 in project 9d80d070b6d44942af73c9c3d38e0429.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/black-white-lists?object_id=cfebd347-b655-4b84-b938-3c54317599b2&limit=10&offset=0&list_type=5
```

Example Responses

Status code: 200

Return value of a blacklist or whitelist query

```
{
  "data" : {
    "limit" : 10,
    "offset" : 0,
    "records" : [ {
      "address" : "1.1.1.1",
      "address_type" : 0,
      "direction" : 0,
      "list_id" : "1310d401-daf5-44f2-8276-f79e1643984d",
      "port" : "1",
      "protocol" : 6
    } ],
    "total" : 1
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.0020016",
  "error_msg" : "instance status error"
}
```

Status Codes

Status Code	Description
200	Return value of a blacklist or whitelist query

Status Code	Description
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.8 Log Query Management

4.8.1 Querying Flow Logs

Function

This API is used to query flow logs.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/cfw/logs/flow

Table 4-138 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-139 Query Parameters

Parameter	Mandatory	Type	Description
fw_instance_id	Yes	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.
direction	No	String	Direction
log_type	No	String	Log type Enumeration values: • **internet** • **vpc** • **nat**
start_time	Yes	Long	Start time
end_time	Yes	Long	End time
src_ip	No	String	Source IP address
src_port	No	Integer	Source port Minimum: **0** Maximum: **65535**
dst_ip	No	String	Destination IP address
dst_port	No	Integer	Destination port Minimum: **0** Maximum: **65535**
protocol	No	String	Protocol type. The value 6 indicates TCP, 17 indicates UDP, 1 indicates ICMP, 58 indicates ICMPv6, and -1 indicates any protocol. Regarding the addition type, a null value indicates it is automatically added. Enumeration values: • **6** • **17** • **1** • **58**
app	No	String	Application protocol

Parameter	Mandatory	Type	Description
log_id	No	String	Document ID. The value is null for the first page and not null for the rest of the pages.
next_date	No	Long	Date. The value is null for the first page and not null for the rest of the pages.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	Yes	Integer	Number of records displayed on each page Minimum: **1** Maximum: **1024**
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Request Parameters

Table 4-140 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-141 Response body parameters

Parameter	Type	Description
data	**data** object	Value returned for flow log query

Table 4-142 data

Parameter	Type	Description
total	Integer	Returned quantity
limit	Integer	Number of records displayed on each page
records	Array of **records** objects	Record

Table 4-143 records

Parameter	Type	Description
bytes	Integer	Byte
direction	String	Direction, which can be inbound or outbound Enumeration values: • **out2in** • **in2out**
packets	Integer	Packet
start_time	Integer	Start time
end_time	Integer	End time
log_id	String	Document ID
src_ip	String	Source IP address
src_port	String	Source port
dst_ip	String	Destination IP address
app	String	Application protocol
dst_port	String	Destination port
protocol	String	Protocol type. The value 6 indicates TCP, 17 indicates UDP, 1 indicates ICMP, 58 indicates ICMPv6, and -1 indicates any protocol. Regarding the addition type, a null value indicates it is automatically added.

Status code: 400

Table 4-144 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query the flow logs on the first page of the firewall with the ID 2af58b7c-893c-4453-a984-bdd9b1bd6318 in the project 9d80d070b6d44942af73c9c3d38e0429. The query time range is 1663555012000 to 1664159798000.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/cfw/logs/flow?
fw_instance_id=2af58b7c-893c-4453-a984-
bdd9b1bd6318&start_time=1663555012000&end_time=1664159798000&limit=10
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "limit" : 10,
    "records" : [ {
      "app" : "SSH",
      "bytes" : 34.5,
      "direction" : "out2in",
      "dst_ip" : "100.95.148.49",
      "dst_port" : 22,
      "end_time" : 1664155493000,
      "log_id" : "76354",
      "packets" : 25,
      "protocol" : "TCP",
      "src_ip" : "100.93.27.17",
      "src_port" : 49634,
      "start_time" : 1664155428000
    } ],
    "total" : 1
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00500002",
  "error_msg" : "time range error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.8.2 Querying Access Control Logs

Function

This API is used to query access control logs.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/cfw/logs/access-control

Table 4-145 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-146 Query Parameters

Parameter	Mandatory	Type	Description
fw_instance_id	Yes	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.
rule_id	No	String	Rule ID
start_time	Yes	Long	Start time
end_time	Yes	Long	End time
src_ip	No	String	Source IP address
src_port	No	Integer	Source port
dst_ip	No	String	Destination IP address
dst_port	No	Integer	Destination port
protocol	No	String	Protocol
app	No	String	Application protocol
log_id	No	String	Document ID. The value is null for the first page and not null for the rest of the pages.
next_date	No	Integer	Date. The value is null for the first page and not null for the rest of the pages.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	Yes	Integer	Number of records displayed on each page
log_type	No	String	Log type Enumeration values: • **internet** • **nat** • **vpc**

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Request Parameters

Table 4-147 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-148 Response body parameters

Parameter	Type	Description
data	**data** object	Data returned for querying access control logs

Table 4-149 data

Parameter	Type	Description
total	Integer	Returned quantity
limit	Integer	Number of records displayed on each page
records	Array of **records** objects	Record

Table 4-150 records

Parameter	Type	Description
action	String	Action. 0: allow; 1: deny

Parameter	Type	Description
rule_name	String	Rule name
rule_id	String	Rule ID
hit_time	Integer	Hit time
log_id	String	Document ID
src_ip	String	Source IP address
src_port	String	Source port
dst_ip	String	Destination IP address
dst_port	String	Destination port
protocol	String	Protocol type. The value 6 indicates TCP, 17 indicates UDP, 1 indicates ICMP, 58 indicates ICMPv6, and -1 indicates any protocol. Regarding the addition type, a null value indicates it is automatically added.
app	String	Application protocol

Status code: 400

Table 4-151 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query the records whose initial position is 0 on the first page of the firewall with the ID 2af58b7c-893c-4453-a984-bdd9b1bd6318 in the project 9d80d070b6d44942af73c9c3d38e0429. The query time range is 1664159069544 to 1664162669544.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/cfw/logs/access-control?
fw_instance_id=2af58b7c-893c-4453-a984-
bdd9b1bd6318&start_time=1664159069544&end_time=1664162669544&limit=10
```

Example Responses

Status code: 200

OK


```
{
  "data" : {
    "limit" : 10,
    "records" : [ {
      "action" : "deny",
      "app" : "PING",
      "dst_ip" : "100.85.216.211",
      "dst_port" : 59,
      "hit_time" : 1664164255000,
      "log_id" : "46032",
      "protocol" : "ICMP: ECHO_REQUEST",
      "rule_id" : "c755be1c-4b92-4ae7-a15e-c2d02b152538",
      "rule_name" : "eip_ipv4_w_n_default_deny",
      "src_ip" : "100.95.148.49",
      "src_port" : 24954
    } ],
    "total" : 1
  }
}
```


Status code: 400

Bad Request


```
{
  "error_code" : "CFW.00500002",
  "error_msg" : "time range error"
}
```


Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.8.3 Querying Attack Logs

Function

This API is used to query attack logs.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/cfw/logs/attack

Table 4-152 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-153 Query Parameters

Parameter	Mandatory	Type	Description
start_time	Yes	Long	Start time
end_time	Yes	Long	End time
src_ip	No	String	Source IP address
src_port	No	Integer	Source port number Minimum: **0** Maximum: **65535**
dst_ip	No	String	Destination IP address
dst_port	No	Integer	Destination port number Minimum: **0** Maximum: **65535**

Parameter	Mandatory	Type	Description
protocol	No	String	Protocol type. The value 6 indicates TCP, 17 indicates UDP, 1 indicates ICMP, 58 indicates ICMPv6, and -1 indicates any protocol. Regarding the addition type, a null value indicates it is automatically added. Enumeration values: • **6** • **17** • **1** • **58**
app	No	String	Application protocol
log_id	No	String	Log ID. The value is null for the first page and not null for the rest of the pages.
next_date	No	Long	Next date. The value is null for the first page and not null for the rest of the pages.
offset	No	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	Yes	Integer	Number of records displayed on each page
fw_instance_id	Yes	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.
action	No	String	Action. 0: allow; 1: deny Enumeration values: • **0** • **1**

Parameter	Mandatory	Type	Description
direction	No	String	Direction. 0: inbound; 1: outbound Enumeration values: • **0** • **1**
attack_type	No	String	Intrusion event type
attack_rule	No	String	Intrusion event rule
level	No	String	Threat level
source	No	String	Source
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Request Parameters

Table 4-154 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-155 Response body parameters

Parameter	Type	Description
data	**data** object	Return value of attack log query

Table 4-156 data

Parameter	Type	Description
total	Integer	Returned quantity

Parameter	Type	Description
limit	Integer	Number of records displayed on each page
records	Array of **records** objects	Record

Table 4-157 records

Parameter	Type	Description
direction	String	Direction, which can be inbound or outbound Enumeration values: • **out2in** • **in2out**
action	String	Action
event_time	String	Event time
attack_type	String	Attack type
attack_rule	String	Attack rule
level	String	Threat level
source	String	Source
packet_length	Long	Packet length
attack_rule_id	Integer	Attack rule ID
hit_time	Integer	Hit time
log_id	String	Log ID
src_ip	String	Source IP address
src_port	Integer	Source port Minimum: **0** Maximum: **65535**
dst_ip	String	Destination IP address
dst_port	Integer	Destination port Minimum: **0** Maximum: **65535**
protocol	String	Protocol
packet	**Packet** object	Attack log packet
app	String	Application protocol

Parameter	Type	Description
packetMessages	Array of PacketMessage objects	packet message

Table 4-158 Packet

Parameter	Type	Description
hex_index	String	Hexadecimal code
utf8_string	String	UTF-8 string
hexs	Array of strings	Hexadecimal single bytecode array

Table 4-159 PacketMessage

Parameter	Type	Description
hex_index	String	hex index
hexs	Array of strings	hexs
utf8_String	String	utf8 string

Status code: 400

Table 4-160 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query 10 records on the first page of the firewall with the ID 2af58b7c-893c-4453-a984-bdd9b1bd6318 in the project 9d80d070b6d44942af73c9c3d38e0429. The query time range is 1663567058000 to 1664171765000.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/cfw/logs/access-control?
fw_instance_id=2af58b7c-893c-4453-a984-
bdd9b1bd6318&start_time=1663567058000&end_time=1664171765000&limit=10
```

Example Responses

Status code: 200

OK


```
{
  "data" : {
    "limit" : 10,
    "records" : [ {
      "action" : "deny",
      "app" : "HTTP",
      "attack_rule" : "Tool Nmap Web Server Probe Detected",
      "attack_rule_id" : "336154",
      "attack_type" : "Web Attack",
      "direction" : "out2in",
      "dst_ip" : "100.95.148.49",
      "dst_port" : 8080,
      "event_time" : 1664146216000,
      "level" : "MEDIUM",
      "log_id" : "15591",
      "packet" : "+hZUZMhV+hY/AaHMCABFKABpXPNAADAGof1kVe6QZF
+UMcTQH5B0wdaz888+uoAYAOVyNQAAAQEICjrmikVb9JLCR0VUIC9uaWNlJTIwcG9ydHMlMkMvVHJpJTZFaX
R5LnR4dCUyZWJhayBIVFRQLzEuMA0KDQo=",
      "packetMessages" : [ {
        "hex_index" : "00000000",
        "hexs" : [ "fa", "16", "54", "64", "c8", "55", "fa", "16", "3f", "01", "a1", "cc", "08", "00", "45", "28" ],
        "utf8_String" : ".\u0016Td.U.\u0016?.....E("
      }, {
        "hex_index" : "00000010",
        "hexs" : [ "00", "69", "5c", "f3", "40", "00", "30", "06", "a1", "fd", "64", "55", "ee", "90", "64", "5f" ],
        "utf8_String" : ".i\\.@.0...dU.d_"
      }, {
        "hex_index" : "00000020",
        "hexs" : [ "94", "31", "c4", "d0", "1f", "90", "74", "c1", "d6", "b3", "f3", "cf", "3e", "ba", "80", "18" ],
        "utf8_String" : ".1..\u001Ft.,,>..."
      }, {
        "hex_index" : "00000030",
        "hexs" : [ "00", "e5", "72", "35", "00", "00", "01", "01", "08", "0a", "3a", "e6", "8a", "45", "5b", "f4" ],
        "utf8_String" : "..r5.....:.E[."
      }, {
        "hex_index" : "00000040",
        "hexs" : [ "92", "c2", "47", "45", "54", "20", "2f", "6e", "69", "63", "65", "25", "32", "30", "70", "6f" ],
        "utf8_String" : "..GET /nice%20po"
      }, {
        "hex_index" : "00000050",
        "hexs" : [ "72", "74", "73", "25", "32", "43", "2f", "54", "72", "69", "25", "36", "45", "69", "74", "79" ],
        "utf8_String" : "rts%2C/Tri%6Eity"
      }, {
        "hex_index" : "00000060",
        "hexs" : [ "2e", "74", "78", "74", "25", "32", "65", "62", "61", "6b", "20", "48", "54", "54", "50", "2f" ],
        "utf8_String" : ".txt%2ebak HTTP/"
      }, {
        "hex_index" : "00000070",
        "hexs" : [ "31", "2e", "30", "0d", "0a", "0d", "0a" ],
        "utf8_String" : "1.0\r.\r."
      } ],
      "packet_length" : 119,
      "protocol" : "TCP",
      "source" : "0",
      "src_ip" : "100.85.238.144",
      "src_port" : 50384
    } ],
    "total" : 1
```



```
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "00500002",
  "error_msg" : "time range error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.9 Protection Mode Management

4.9.1 Querying the Protection Mode

Function

This API is used to query the protection mode.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/ips/protect

Table 4-161 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-162 Query Parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-163 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-164 Response body parameters

Parameter	Type	Description
data	**IpsProtectModeObject** object	IpsProtectModeObject

Table 4-165 IpsProtectModeObject

Parameter	Type	Description
id	String	ips protect mode id
mode	String	IPS protection mode. 0: observation mode; 1: strict mode; 2: medium mode; 3: loose mode

Status code: 400

Table 4-166 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query the IPS protection mode of the project whose ID is 9d80d070b6d44942af73c9c3d38e0429.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/ips/protect
```

Example Responses

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.0020016",
  "error_msg" : "instance status error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.9.2 Switching the Protection Mode

Function

This API is used to switch the protection mode.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

POST /v1/{project_id}/ips/protect

Table 4-167 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-168 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-169 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-170 Request body parameters

Parameter	Mandatory	Type	Description
object_id	No	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
mode	No	Integer	IPS protection mode. 0: observation mode; 1: strict mode; 2: medium mode; 3: loose mode

Response Parameters

Status code: 200

Table 4-171 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Update the IPS protection mode

Table 4-172 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-173 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Deliver the strict protection mode to object cfebd347-b655-4b84-b938-3c54317599b2 in project 9d80d070b6d44942af73c9c3d38e0429.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/ips/protect

{
  "object_id" : "cfebd347-b655-4b84-b938-3c54317599b2",
  "mode" : 1
}
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "id" : "cfebd347-b655-4b84-b938-3c54317599b2"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.0020016",
  "error_msg" : "instance status error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden

Status Code	Description
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.10 Cloud Firewall Information Management

4.10.1 Querying a Firewall Instance

Function

This API is used to query a firewall instance.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/firewall/exist

Table 4-174 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-175 Query Parameters

Parameter	Mandatory	Type	Description
offset	Yes	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	Yes	Integer	Number of records displayed on each page

Parameter	Mandatory	Type	Description
service_type	Yes	Integer	Service type 0. North-south firewall 1. East-west firewall Minimum: **0** Maximum: **1** Enumeration values: • **0** • **1**
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-176 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-177 Response body parameters

Parameter	Type	Description
data	**GetFirewallInstanceData** object	get firewall instance response data

Table 4-178 GetFirewallInstanceData

Parameter	Type	Description
limit	Integer	Number of records displayed on each page
offset	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
total	Integer	total
records	Array of **GetFirewallInstanceResponseRecord** objects	Get firewall instance records

Table 4-179 GetFirewallInstanceResponseRecord

Parameter	Type	Description
fw_instance_id	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.
name	String	Firewall name
ha_type	Integer	Cluster type
charge_mode	Integer	Billing mode. The value can be 0 (yearly/monthly) or 1 (pay-per-use).
service_type	Integer	Service type
engine_type	Integer	Engine type
flavor	**Flavor** object	Firewall specifications
protect_objects	Array of **ProtectObjectVO** objects	Project list
status	Integer	Firewall status list. The options are as follows: -1: waiting for payment; 0: creating; 1: deleting; 2: running; 3: upgrading; 4: deletion completed; 5: freezing; 6: creation failed; 7: deletion failed; 8: freezing failed; 9: storage in progress; 10: storage failed; 11: upgrade failed Enumeration values: • **-1** • **0** • **1** • **2** • **3** • **4** • **5** • **6** • **7** • **8** • **9** • **10** • **11**

Parameter	Type	Description
is_old_firewall_instance	Boolean	Whether the engine is an old engine. The options are true (yes) and false (no). Enumeration values: • **true** • **false**
support_ipv6	Boolean	Whether IPv6 is supported. The options are true (yes) and false (no).
feature_toggle	Map<String,Boolean>	Whether to enable the feature. The options are true (yes) and false (no).
resources	Array of **FirewallInstanceResource** objects	Firewall instance resources
fw_instance_name	String	firewall name
enterprise_project_id	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Table 4-180 Flavor

Parameter	Type	Description
version	Integer	Firewall version. The value can be 0 (standard edition), 1 (professional edition), 2 (platinum edition), or 3 (basic edition). Enumeration values: • **0** • **1** • **2** • **3**
eip_count	Integer	Number of EIPs Minimum: **1**
vpc_count	Integer	Number of VPCs Minimum: **1**
bandwidth	Integer	Bandwidth Minimum: **1**
log_storage	Integer	Log storage

Table 4-181 ProtectObjectVO

Parameter	Type	Description
object_id	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
object_name	String	Protected object name
type	Integer	Project type. The options are as follows: 0: north-south; 1: east-west. Enumeration values: • **0** • **1**

Table 4-182 FirewallInstanceResource

Parameter	Type	Description
resource_id	String	Resource ID
cloud_service_type	String	Service type, which is used by CBC. The value is hws.service.type.cfw.
resource_type	String	Resource type. The options are as follows:1. CFW: hws.resource.type.cfw 2. EIP:hws.resource.type.cfw.exp.eip 3. Bandwidth: hws.resource.type.cfw.exp.bandwidth 4. VPC: hws.resource.type.cfw.exp.vpc 5. Log storage: hws.resource.type.cfw.exp.logaudit
resource_spec_code	String	Inventory unit code
resource_size	Integer	Resource quantity
resource_size_measure_id	Integer	Resource unit name

Example Requests

Query the firewall list of the project whose ID is 9d80d070b6d44942af73c9c3d38e0429.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/firewall/exist?
service_type=0&offset=0&limit=10
```

Example Responses

Status code: 200

Response to the request for obtaining a firewall instance

```
{
  "data" : {
    "limit" : 10,
    "offset" : 0,
    "records" : [ {
      "charge_mode" : 0,
      "engine_type" : 1,
      "feature_toggle" : {
        "long_connect" : true,
        "alarm_config" : true
      },
      "flavor" : {
        "bandwidth" : 60,
        "eip_count" : 52,
        "log_storage" : 0,
        "version" : 1,
        "vpc_count" : 4
      },
      "fw_instance_id" : "2af58b7c-893c-4453-a984-bdd9b1bd6318",
      "fw_instance_name" : "fw_instance_name",
      "enterprise_project_id" : "enterprise_project_id",
      "ha_type" : 1,
      "is_old_firewall_instance" : false,
      "name" : "1663891762130",
      "protect_objects" : [ {
        "object_id" : "cfebd347-b655-4b84-b938-3c54317599b2",
        "object_name" : "1663891762130",
        "type" : 0
      }, {
        "object_id" : "32ecaf73-bbd8-47e5-af51-b9c88affda21",
        "object_name" : "ew-1663892880929",
        "type" : 1
      } ],
      "resources" : [ {
        "cloud_service_type" : "hws.service.type.cfw",
        "resource_id" : "6f8a4871-7258-4560-b396-aba4bb5840a6",
        "resource_size" : 2,
        "resource_size_measure_id" : 14,
        "resource_spec_code" : "cfw.expack.eip.professional",
        "resource_type" : "hws.resource.type.cfw.exp.eip"
      }, {
        "cloud_service_type" : "hws.service.type.cfw",
        "resource_id" : "d7da8a0c-d4f4-43e6-affd-60e20daf4caa",
        "resource_size" : 10,
        "resource_size_measure_id" : 36,
        "resource_spec_code" : "cfw.expack.bandwidth.professional",
        "resource_type" : "hws.resource.type.cfw.exp.bandwidth"
      }, {
        "cloud_service_type" : "hws.service.type.cfw",
        "resource_id" : "550f52af-f6e2-4a9e-bdb3-85bb0b2dd4fa",
        "resource_size" : 2,
        "resource_size_measure_id" : 14,
        "resource_spec_code" : "cfw.expack.vpc.professional",
        "resource_type" : "hws.resource.type.cfw.exp.vpc"
      }, {
        "cloud_service_type" : "hws.service.type.cfw",
        "resource_id" : "53048c0d-45db-4773-b2f3-fca8d43351fe",
        "resource_spec_code" : "cfw.professional",
        "resource_type" : "hws.resource.type.cfw"
      } ],
```



```
    "service_type" : 0,
    "status" : 2,
    "support_ipv6" : true
  } ],
  "total" : 1
 }
}
```

Status Codes

Status Code	Description
200	Response to the request for obtaining a firewall instance
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.11 Service Group Management

4.11.1 Creating a Service Group

Function

This API is used to create a service group.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

POST /v1/{project_id}/service-set

Table 4-183 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-184 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-185 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-186 Request body parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
name	Yes	String	Service group name Minimum: **1** Maximum: **255**
description	No	String	Service group description Minimum: **1** Maximum: **255**

Response Parameters

Status code: 200

Table 4-187 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Data returned when a service group is created

Table 4-188 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-189 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Add a service group whose project ID is 9d80d070b6d44942af73c9c3d38e0429, protected object is cfebd347-b655-4b84-b938-3c54317599b2, and name is ceshi.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/service-set

{
  "object_id" : "cfebd347-b655-4b84-b938-3c54317599b2",
  "name" : "ceshi",
  "description" : ""
}
```

Example Responses

Status code: 200

Return value of creating a service group

```
{
  "data" : {
    "id" : "221cfdca-3abf-4c30-ab0d-516a03c70866"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200024",
  "error_msg" : "Exceeded maximum quantity limit"
}
```

Status Codes

Status Code	Description
200	Return value of creating a service group
400	Bad Request
401	Unauthorized

Status Code	Description
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.11.2 Querying Service Group Details

Function

This API is used to query the details about a service group.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/service-sets/{set_id}

Table 4-190 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
set_id	Yes	String	Service group ID

Table 4-191 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-192 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-193 Response body parameters

Parameter	Type	Description
data	**ServiceSetDetailResponseDto** object	service set detail response

Table 4-194 ServiceSetDetailResponseDto

Parameter	Type	Description
id	String	Service group ID
name	String	Service group name Minimum: **1** Maximum: **255**
description	String	Service group description Minimum: **1** Maximum: **255**

Status code: 400

Table 4-195 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query details about the service group whose project ID is 9d80d070b6d44942af73c9c3d38e0429 and service group ID is 221cfdca-3abf-4c30-ab0d-516a03c70866.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/service-sets/221cfdca-3abf-4c30-ab0d-516a03c70866
```

Example Responses

Status code: 200

Response to the request for querying details about a service group member

```
{
  "data" : {
    "description" : "Description",
    "id" : "221cfdca-3abf-4c30-ab0d-516a03c70866",
    "name" : "ceshi2"
```

```
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	Response to the request for querying details about a service group member
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.11.3 Modifying a Service Group

Function

This API is used to update a service group.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

PUT /v1/{project_id}/service-sets/{set_id}

Table 4-196 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Parameter	Mandatory	Type	Description
set_id	Yes	String	Service group ID

Table 4-197 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-198 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-199 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Service group name Minimum: **1** Maximum: **255**
description	No	String	Service group description Minimum: **1** Maximum: **255**

Response Parameters

Status code: 200

Table 4-200 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Data returned when a service group is updated

Table 4-201 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-202 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Change the name and description of service group 221cfdca-3abf-4c30-ab0d-516a03c70866 of project 9d80d070b6d44942af73c9c3d38e0429 to ceshi2.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/service-sets/221cfdca-3abf-4c30-ab0d-516a03c70866

{
  "name" : "ceshi2",
  "description" : "Description"
}
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "id" : "221cfdca-3abf-4c30-ab0d-516a03c70866"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.11.4 Deleting a Service Group

Function

This API is used to delete a service group.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

DELETE /v1/{project_id}/service-sets/{set_id}

Table 4-203 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
set_id	Yes	String	Indicates the service set ID.

Table 4-204 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-205 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-206 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Data returned after a service group is deleted

Table 4-207 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-208 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Delete the service group whose project ID is 9d80d070b6d44942af73c9c3d38e0429 and service group ID is 221cfdca-3abf-4c30-ab0d-516a03c70866.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/service-sets/221cfdca-3abf-4c30-ab0d-516a03c70866
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "id" : "221cfdca-3abf-4c30-ab0d-516a03c70866"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200004",
  "error_msg" : "can not delete for used"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.11.5 Obtaining the Service Group List

Function

This API is used to obtain the service group list.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/service-sets

Table 4-209 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-210 Query Parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
key_word	No	String	Keyword
limit	Yes	Integer	Number of queries on each page Minimum: **1** Maximum: **1024**
offset	Yes	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**. Minimum: **0**
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-211 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-212 Response body parameters

Parameter	Type	Description
data	**ServiceSetRecords** object	QueryServiceSetResponse

Table 4-213 ServiceSetRecords

Parameter	Type	Description
offset	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	Integer	Number of records displayed on each page
total	Integer	Total number of records queried
records	Array of **ServiceSet** objects	Service group list

Table 4-214 ServiceSet

Parameter	Type	Description
set_id	String	Service group ID
name	String	Name
description	String	Description
ref_count	Integer	Reference count
status	String	Status

Status code: 400

Table 4-215 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query the service group list on the first page of protected object a37bb4eb-c49e-4e88-bf77-944a75b0ce8a in project 2349ba469daf4b7daf268bb0261d18b0.

```
https://{Endpoint}/v1/2349ba469daf4b7daf268bb0261d18b0/service-sets?object_id=a37bb4eb-c49e-4e88-bf77-944a75b0ce8a&limit=10&offset=0
```

Example Responses

Status code: 200

Response to the request for querying service group information

```
{
  "data" : {
    "limit" : 10,
    "offset" : 0,
    "records" : [ {
      "description" : "ceshi",
      "name" : "ceshi",
      "ref_count" : 0,
      "set_id" : "ca66078c-da47-4b8d-b366-ded16afb034d"
    } ],
    "total" : 1
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.0020016",
  "error_msg" : "instance status error"
}
```

Status Codes

Status Code	Description
200	Response to the request for querying service group information
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.12 Service Group Member Management

4.12.1 Querying the Service Group Member List

Function

This API is used to query service group members.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/service-items

Table 4-216 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-217 Query Parameters

Parameter	Mandatory	Type	Description
set_id	Yes	String	Service group ID
key_word	No	String	Query field
limit	Yes	Integer	Number of records displayed on each page
offset	Yes	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-218 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-219 Response body parameters

Parameter	Type	Description
data	**data** object	Service group member list

Table 4-220 data

Parameter	Type	Description
offset	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	Integer	Number of records displayed on each page
total	Integer	Total number of records
set_id	String	service set id
records	Array of **records** objects	Record

Table 4-221 records

Parameter	Type	Description
item_id	String	Service member ID
protocol	Integer	Protocol type. The value 6 indicates TCP, 17 indicates UDP, 1 indicates ICMP, 58 indicates ICMPv6, and -1 indicates any protocol. Regarding the addition type, a null value indicates it is automatically added.
source_port	String	Source port
dest_port	String	Destination port
name	String	Service member name
description	String	Service member description

Status code: 400

Table 4-222 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query the member list of the service group whose project ID is 9d80d070b6d44942af73c9c3d38e0429 and service group ID is 7cdebed3-af07-494e-a3c2-b88bb8d58b57.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/service-items?set_id=7cdebed3-af07-494e-a3c2-b88bb8d58b57&limit=10&offset=0
```

Example Responses

Status code: 200

Return value of the service group member list

```
{
  "data" : {
    "limit" : 10,
    "offset" : 0,
    "records" : [ {
      "dest_port" : "0",
      "item_id" : "805b711d-c558-41e3-aab1-a4b8c3f1f90b",
      "name" : "icmp",
      "protocol" : 1,
      "source_port" : "0"
    } ],
    "set_id" : "7cdebed3-af07-494e-a3c2-b88bb8d58b57",
    "total" : 1
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	Return value of the service group member list
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.12.2 Creating a Service Member

Function

This API is used to add group members in batches.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

POST /v1/{project_id}/service-items

Table 4-223 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-224 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-225 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-226 Request body parameters

Parameter	Mandatory	Type	Description
set_id	Yes	String	Service group ID
service_items	Yes	Array of **service_items** objects	Add a member to a service group.

Table 4-227 service_items

Parameter	Mandatory	Type	Description
item_id	No	String	Service member ID
protocol	Yes	Integer	Protocol type. The value 6 indicates TCP, 17 indicates UDP, 1 indicates ICMP, 58 indicates ICMPv6, and -1 indicates any protocol. Regarding the addition type, a null value indicates it is automatically added.
source_port	Yes	String	Source port
dest_port	Yes	String	Destination port
name	No	String	Service member name
description	No	String	Service member description

Response Parameters

Status code: 200

Table 4-228 Response body parameters

Parameter	Type	Description
data	**ServiceItemIds** object	Data returned when a service group member is created

Table 4-229 ServiceItemIds

Parameter	Type	Description
items	Array of **IdObject** objects	Service group member ID list

Table 4-230 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-231 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Add a service group member named ceshi to the project whose ID is 9d80d070b6d44942af73c9c3d38e0429.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/service-items

{
  "set_id" : "7cdebed3-af07-494e-a3c2-b88bb8d58b57",
  "service_items" : [ {
    "description" : "Add a member to a service group",
    "name" : "ceshi",
    "dest_port" : "1",
    "source_port" : "1",
    "protocol" : 6
  } ]
}
```

Example Responses

Status code: 200

Return value for adding a service group member

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200001",
  "error_msg" : "empty param"
}
```

Status Codes

Status Code	Description
200	Return value for adding a service group member

Status Code	Description
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.12.3 Deleting a Service Member

Function

This API is used to delete a member from a service group.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

DELETE /v1/{project_id}/service-items/{item_id}

Table 4-232 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
item_id	Yes	String	ID of a service group member

Table 4-233 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-234 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-235 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Delete service group member data.

Table 4-236 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-237 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

This API is used to Delete the service group member whose project ID is 9d80d070b6d44942af73c9c3d38e0429 and service group member ID is 6b37ed55-1e21-46a5-a7dc-a59ef418d359.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/service-items/6b37ed55-1e21-46a5-a7dc-a59ef418d359
```

Example Responses

Status code: 200

Response to the request for deleting a service group member.

```
{
  "data" : {
    "id" : "26f562c4-fe11-43d0-9654-f54298d5b12e"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.0020016",
  "error_msg" : "instance status error"
}
```

Status Codes

Status Code	Description
200	Response to the request for deleting a service group member.
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.13 EIP Management

4.13.1 Querying the Number of EIPs

Function

This API is used to query the number of EIPs.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/eip-count/{object_id}

Table 4-238 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID Minimum: **32** Maximum: **32**

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ. Minimum: **36** Maximum: **36**

Table 4-239 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-240 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-241 Response body parameters

Parameter	Type	Description
data	**EipCountRespData** object	eip count response data

Table 4-242 EipCountRespData

Parameter	Type	Description
object_id	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ. Minimum: **36** Maximum: **36**
eip_total	Integer	Total EIPs Minimum: **0** Default: **0**
eip_protected	Integer	Number of protected EIPs Minimum: **0** Default: **0**

Status code: 400

Table 4-243 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query the number of EIPs whose project ID is 9d80d070b6d44942af73c9c3d38e0429 and protected object ID is cfebd347-b655-4b84-b938-3c54317599b2.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/eip-count/cfebd347-b655-4b84-b938-3c54317599b2
```


Example Responses

Status code: 200

OK

```
{
  "data" : {
    "eip_protected" : 1,
    "eip_total" : 5,
    "object_id" : "6d3db4fd-fd58-4d8e-914b-ef91aa268f62"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.13.2 Enabling or Disabling an EIP

Function

This API is used to enable or disable EIP.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

POST /v1/{project_id}/eip/protect

Table 4-244 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID Minimum: **32** Maximum: **32**

Table 4-245 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-246 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-247 Request body parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ. Minimum: **36** Maximum: **36**
status	Yes	Integer	EIP Status,0:protected,1:unprotected Minimum: **0** Maximum: **1**
ip_infos	Yes	Array of **ip_infos** objects	EIP information list

Table 4-248 ip_infos

Parameter	Mandatory	Type	Description
id	No	String	EIP data ID Minimum: **36** Maximum: **36**
public_ip	No	String	EIP Minimum: **0** Maximum: **255**
public_ipv6	No	String	EIP IPv6

Response Parameters

Status code: 200

Table 4-249 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Data returned after enabling or disabling the EIP

Table 4-250 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-251 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

- Enable EIP (100.85.121.62) traffic protection.

```
https://{Endpoint}/v1/857ddec2-55f2-4503-a93a-fe70021b743c/eip/protect

{
  "object_id" : "6d3db4fd-fd58-4d8e-914b-ef91aa268f62",
  "status" : 0,
  "ip_infos" : [ {
    "id" : "4a589be0-b40a-4694-94ff-c0710af9a0a2",
    "public_ip" : "100.85.121.62"
  } ]
}
```

- Disable EIP (100.85.121.62) traffic protection.

```
/v1/857ddec2-55f2-4503-a93a-fe70021b743c/eip/protect

{
  "object_id" : "6d3db4fd-fd58-4d8e-914b-ef91aa268f62",
  "status" : 1,
  "ip_infos" : [ {
    "id" : "4a589be0-b40a-4694-94ff-c0710af9a0a2",
    "public_ip" : "100.85.121.62"
  } ]
}
```

Example Responses

Status code: 200

Return value for enabling or disabling EIP protection

```
{
  "data" : {
    "id" : "449d165f-f1bc-4964-8cf4-e5420a4af529"
  }
}
```

Status Codes

Status Code	Description
200	Return value for enabling or disabling EIP protection
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.13.3 Querying the EIP List

Function

This API is used to query the EIP list.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/eips/protect

Table 4-252 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID Minimum: **32** Maximum: **32**

Table 4-253 Query Parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ. Minimum: **36** Maximum: **36**
key_word	No	String	Public network ID or EIP Minimum: **0** Maximum: **255**

Parameter	Mandatory	Type	Description
status	No	String	Specifies the protection status. The value can be null, 0 (enabled), or 1 (disabled). Enumeration values: • **null** • **0** • **1**
sync	No	Integer	Specifies whether to synchronize tenant EIP data. The options are as follows: 0: no; 1: yes Enumeration values: • **0** • **1**
limit	Yes	Integer	Number of records displayed on each page Minimum: **0**
offset	Yes	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**. Minimum: **0**
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
device_key	No	String	Device key
address_type	No	Integer	Specifies the address type. The value can be 0 (IPv4) or 1 (IPv6).

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.
fw_key_word	No	String	The bound firewall name
eps_id	No	String	The enterprise project id of the eip

Request Parameters

Table 4-254 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-255 Response body parameters

Parameter	Type	Description
data	**EipResponseData** object	eip query response

Table 4-256 EipResponseData

Parameter	Type	Description
limit	Integer	Number of records displayed on each page
offset	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
total	Integer	total
records	Array of **EipResource** objects	eip records

Table 4-257 EipResource

Parameter	Type	Description
id	String	EIP ID
public_ip	String	EIP
status	Integer	EIP protection status,0:protected,1:unprotected Enumeration values: • **0** • **1**
public_ipv6	String	EIP IPv6
enterprise_project_id	String	Enterprise project ID
device_id	String	Device ID
device_name	String	Device name
device_owner	String	Device owner
associate_instance_type	String	Type of the associated instance
fw_instance_name	String	firewall name

Parameter	Type	Description
fw_instance_id	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.
fw_enterprise_project_id	String	Firewall enterprise project id bound to Eip

Status code: 400

Table 4-258 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query the data on the non-synchronized first page whose project ID is 9d80d070b6d44942af73c9c3d38e0429 and protected object ID is cfebd347-b655-4b84-b938-3c54317599b2.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/eips/protect?object_id=cfebd347-b655-4b84-b938-3c54317599b2&limit=10&offset=0&sync=0
```

Example Responses

Status code: 200

Return value of EIP data query

```
{
  "data" : {
    "limit" : 10,
    "offset" : 0,
    "records" : [ {
      "id" : "03e11b49-cddc-4d21-9971-969744a56c1c",
      "public_ip" : "100.95.150.41",
      "status" : 0
    }, {
      "id" : "088c3aa1-82ba-40b0-98b6-476c8a7f1e22",
      "public_ip" : "100.95.145.155",
      "status" : 1
    }, {
      "id" : "199473ce-a09a-496d-902b-c3aba58990ac",
```



```
    "public_ip" : "100.85.122.202",
    "status" : 1
   }, {
    "id" : "2d0f799c-0285-49cd-a25a-065f3ae1ab52",
    "public_ip" : "100.85.118.98",
    "status" : 1
   }, {
    "id" : "2d934ad5-ee5b-4d4e-9f62-9a59051cb138",
    "public_ip" : "100.85.123.11",
    "status" : 1
   }, {
    "id" : "3603a902-e731-4ce1-9241-369510509655",
    "public_ip" : "100.85.113.240",
    "status" : 1
   }, {
    "id" : "406641fd-f712-478c-86ee-86de75434408",
    "public_ip" : "100.85.118.102",
    "status" : 1
   }, {
    "id" : "4d218dd9-235f-44f9-b763-7b2a8174751c",
    "public_ip" : "100.85.120.114",
    "status" : 1
   }, {
    "id" : "4d560006-bd48-4be7-9389-1ebe5bb3f73b",
    "public_ip" : "100.85.114.20",
    "status" : 1
   }, {
    "id" : "6afcaf2b-f52c-401c-b709-10156bfde36a",
    "public_ip" : "100.85.122.86",
    "status" : 1
   } ],
   "total" : 25
  }
}
```


Status code: 400

Bad Request


```
{
  "error_code" : "CFW.00109004",
  "error_msg" : "http to external service error"
}
```


Status Codes

Status Code	Description
200	Return value of EIP data query
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.14 Address Group Member Management

4.14.1 Deleting an Address Group Member

Function

This API is used to delete a member from an address group.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

DELETE /v1/{project_id}/address-items/{item_id}

Table 4-259 Path Parameters

Parameter	Mandatory	Type	Description
item_id	Yes	String	ID of an address group member
project_id	Yes	String	Project ID

Table 4-260 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-261 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-262 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Delete address group member data.

Table 4-263 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-264 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Delete the address group member whose ID is 65cb47fc-e666-4af4-8c2c-1fbd2f4b1eae from the project whose ID is 9d80d070b6d44942af73c9c3d38e0429.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/address-items/65cb47fc-e666-4af4-8c2c-1fbd2f4b1eae
```

Example Responses

Status code: 200

Return value for deleting an address group member

```
{
  "data" : {
    "id" : "65cb47fc-e666-4af4-8c2c-1fbd2f4b1eae"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.0020016",
  "error_msg" : "Incorrect instance status."
}
```

Status Codes

Status Code	Description
200	Return value for deleting an address group member
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.14.2 Querying Address Group Members

Function

This API is used to query address group members.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/address-items

Table 4-265 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-266 Query Parameters

Parameter	Mandatory	Type	Description
set_id	Yes	String	ID of the IP address group
key_word	No	String	Keyword

Parameter	Mandatory	Type	Description
limit	Yes	Integer	Number of records displayed on each page
offset	Yes	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
address	No	String	IP address
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-267 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-268 Response body parameters

Parameter	Type	Description
data	**data** object	Response for address group member query

Table 4-269 data

Parameter	Type	Description
offset	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	Integer	Number of records displayed on each page
total	Integer	Total
set_id	String	ID of the IP address group
records	Array of **records** objects	Member information

Table 4-270 records

Parameter	Type	Description
item_id	String	ID of an address group member
name	String	Name of an address group member
description	String	Description

Parameter	Type	Description
address_type	Integer	Address group type. The value can be 0 (IPv4) or 1 (IPv6).
address	String	Address group

Status code: 400

Table 4-271 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query members in address group 8773c082-2a6c-4529-939a-edc28ef1a67c of project 9d80d070b6d44942af73c9c3d38e0429.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/address-items?
set_id=8773c082-2a6c-4529-939a-edc28ef1a67c&limit=10&offset=0
```

Example Responses

Status code: 200

Return value for querying address group members

```
{
  "data" : {
    "limit" : 10,
    "offset" : 0,
    "records" : [ {
      "address" : "1.1.1.1",
      "address_type" : 0,
      "description" : "",
      "item_id" : "294fab71-34bf-4858-a380-8f7530e1c816",
      "name" : "ceshi"
    } ],
    "set_id" : "8773c082-2a6c-4529-939a-edc28ef1a67c",
    "total" : 1
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	Return value for querying address group members
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.14.3 Adding an Address Group Member

Function

This API is used to add an address group member.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

POST /v1/{project_id}/address-items

Table 4-272 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-273 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-274 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-275 Request body parameters

Parameter	Mandatory	Type	Description
set_id	No	String	ID of the IP address group

Parameter	Mandatory	Type	Description
address_items	No	Array of address_items objects	Address group member information

Table 4-276 address_items

Parameter	Mandatory	Type	Description
name	Yes	String	Address name
address_type	No	Integer	Address type. The value can be 0 (IPv4) or 1 (IPv6).
address	No	String	IP address information of the address group
description	No	String	Address group member description

Response Parameters

Status code: 200

Table 4-277 Response body parameters

Parameter	Type	Description
data	AddressItems object	Data returned after an address group member is added

Table 4-278 AddressItems

Parameter	Type	Description
items	Array of IdObject objects	List of address group member IDs

Table 4-279 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-280 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Add an address group member whose IP address is 2.2.2.2 and name is ceshi to the group whose set_id is 8773c082-2a6c-4529-939a-edc28ef1a67c in project 9d80d070b6d44942af73c9c3d38e0429.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/address-items

{
  "set_id" : "8773c082-2a6c-4529-939a-edc28ef1a67c",
  "address_items" : [ {
    "description" : "",
    "name" : "ceshi",
    "address" : "2.2.2.2"
  } ]
}
```

Example Responses

Status code: 200

Return value for adding an address group member

```
{
  "data" : {
    "items" : [ {
      "id" : "65cb47fc-e666-4af4-8c2c-1fbd2f4b1eae"
    } ]
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200001",
  "error_msg" : "empty param"
}
```

Status Codes

Status Code	Description
200	Return value for adding an address group member
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.15 Address Group Management

4.15.1 Adding an Address Group

Function

This API is used to add an address group.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

POST /v1/{project_id}/address-set

Table 4-281 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-282 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-283 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-284 Request body parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
name	Yes	String	IP address group name
description	No	String	Address group description
address_type	No	Integer	Address type. The value can be 0 (IPv4) or 1 (IPv6). Enumeration values: • **0** • **1**

Response Parameters

Status code: 200

Table 4-285 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Data returned after an address group is added

Table 4-286 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-287 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Add an IPv4 address group whose project ID is 14181c1245cf4fd786824efe1e2b9388, protected object ID is 1530de8a-522d-4771-9067-9fa4e2f53b48, and name is ceshi.

```
https://{Endpoint}/v1/14181c1245cf4fd786824efe1e2b9388/address-set

{
  "object_id" : "1530de8a-522d-4771-9067-9fa4e2f53b48",
  "name" : "ceshi",
  "description" : "",
  "address_type" : 0
}
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "id" : "9dffcd62-23bf-4456-83fa-80fa0fee47db"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00900020",
  "error_msg" : "Address groups exceed the maximum limit"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request

Status Code	Description
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.15.2 Querying IP Address Groups

Function

Querying IP Address Groups

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/address-sets

Table 4-288 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-289 Query Parameters

Parameter	Mandatory	Type	Description
object_id	Yes	String	Protected object ID, which is used to distinguish Internet border protection from VPC border protection after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. Note that the value 0 indicates the ID of a protected object on the Internet border, and the value 1 indicates the ID of a protected object on the VPC border. For details, see the API Explorer and Help Center FAQ.
key_word	No	String	Keyword
limit	Yes	Integer	Number of records displayed on each page
offset	Yes	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
address	No	String	IP address
address_type	No	Integer	Specifies the address type. The value can be 0 (IPv4) or 1 (IPv6). Enumeration values: • **0** • **1**
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-290 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-291 Response body parameters

Parameter	Type	Description
data	**data** object	Data returned for the address group list query

Table 4-292 data

Parameter	Type	Description
offset	Integer	Offset, which specifies the start position of the record to be returned. The value must be a number no less than 0. The default value is **0**.
limit	Integer	Number of records displayed on each page
total	Integer	Total
records	Array of **records** objects	IP address group list

Table 4-293 records

Parameter	Type	Description
set_id	String	ID of the IP address group
ref_count	Integer	Reference count
description	String	Description
name	String	IP address group name
address_type	Integer	Address type. The value can be 0 (IPv4) or 1 (IPv6).

Status code: 400

Table 4-294 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

This API is used to query the IP address group information on the first page of project 8a41d6a5-f215-428a-a76c-dc923b5d599a. The protected object ID is 5c69cf330cda42369cbd726ee1bc5e76.

```
https://{Endpoint}/v1/5c69cf330cda42369cbd726ee1bc5e76/address-sets?object_id=8a41d6a5-f215-428a-a76c-dc923b5d599a&limit=10&offset=0
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "limit" : 10,
    "offset" : 0,
    "records" : [ {
      "address_type" : 0,
      "description" : "",
      "name" : "ceshi",
      "ref_count" : 0,
      "set_id" : "50da1eff-e58d-4380-b899-a78f94137d3b"
    } ],
    "total" : 1
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.0020016",
  "error_msg" : "instance status error"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.15.3 Querying Address Group Details

Function

This API is used to query details about an address group.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

GET /v1/{project_id}/address-sets/{set_id}

Table 4-295 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
set_id	Yes	String	ID of the IP address group

Table 4-296 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-297 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-298 Response body parameters

Parameter	Type	Description
data	**data** object	Query address group details.

Table 4-299 data

Parameter	Type	Description
id	String	ID of the IP address group
name	String	IP address group name
description	String	Address group description
address_type	Integer	Specifies the address type. The value can be 0 (IPv4) or 1 (IPv6). Enumeration values: • **0** • **1**

Status code: 400

Table 4-300 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**

Parameter	Type	Description
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Query details about address group cf18f0b1-0ce7-4eb8-83b6-4b33c8448e16 in project 9d80d070b6d44942af73c9c3d38e0429.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/address-sets/
cf18f0b1-0ce7-4eb8-83b6-4b33c8448e16
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "address_type" : 0,
    "description" : "",
    "id" : "cf18f0b1-0ce7-4eb8-83b6-4b33c8448e16",
    "name" : "ABC"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.15.4 Updating Address Group Information

Function

This API is used to update address group information.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

PUT /v1/{project_id}/address-sets/{set_id}

Table 4-301 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
set_id	Yes	String	ID of the IP address group

Table 4-302 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-303 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Table 4-304 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	IP address group name
description	No	String	Address group description

Parameter	Mandatory	Type	Description
address_type	No	Integer	Address type. The value can be 0 (IPv4), 1 (IPv6), or 2 (domain). Enumeration values: • **0** • **1** • **2**

Response Parameters

Status code: 200

Table 4-305 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Data returned after an address group is updated

Table 4-306 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-307 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

In the project cf18f0b1-0ce7-4eb8-83b6-4b33c8448e16, change the name of the address group whose ID is cf18f0b1-0ce7-4eb8-83b6-4b33c8448e16 to ABCD. Change its address group type to ipV4

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/address-sets/
cf18f0b1-0ce7-4eb8-83b6-4b33c8448e16

{
  "name" : "ABCD",
  "description" : "",
  "address_type" : 0
}
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "id" : "cf18f0b1-0ce7-4eb8-83b6-4b33c8448e16"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200005",
  "error_msg" : "operation content does not exist"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

Error Codes

See **Error Codes**.

4.15.5 Deleting an Address Group

Function

This API is used to delete an address group.

Debugging

You can debug this API through automatic authentication in or use the SDK sample code generated by API Explorer.

URI

DELETE /v1/{project_id}/address-sets/{set_id}

Table 4-308 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
set_id	Yes	String	ID of the IP address group

Table 4-309 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project id, the id generated by the enterprise project after the user supports the enterprise project.

Parameter	Mandatory	Type	Description
fw_instance_id	No	String	Firewall instance ID, which is automatically generated after a CFW instance is created. You can obtain the ID by calling the API used for querying a firewall instance. For details, see the API Explorer and Help Center FAQ.By default, if fw_instance_Id is not specified, information about the first firewall under the account is returned. If fw_instance_Id is specified, information about the firewall with this fw_instance_Id is returned.If object_Id is specified, information about the firewall with this object_Id is returned by default. If both fw_instance_Id and object_Id are specified, the specified object_Id must belong to the specified firewall.

Request Parameters

Table 4-310 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is a token.

Response Parameters

Status code: 200

Table 4-311 Response body parameters

Parameter	Type	Description
data	**IdObject** object	Data returned after an address group is deleted

Table 4-312 IdObject

Parameter	Type	Description
id	String	ID

Status code: 400

Table 4-313 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: **8** Maximum: **36**
error_msg	String	Description Minimum: **2** Maximum: **512**

Example Requests

Delete address group cf18f0b1-0ce7-4eb8-83b6-4b33c8448e16 from project 9d80d070b6d44942af73c9c3d38e0429.

```
https://{Endpoint}/v1/9d80d070b6d44942af73c9c3d38e0429/address-sets/
cf18f0b1-0ce7-4eb8-83b6-4b33c8448e16
```

Example Responses

Status code: 200

OK

```
{
  "data" : {
    "id" : "cf18f0b1-0ce7-4eb8-83b6-4b33c8448e16"
  }
}
```

Status code: 400

Bad Request

```
{
  "error_code" : "CFW.00200004",
  "error_msg" : "can not delete for used"
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
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

Status Code	Error Codes	Error Message	Description	Solution
400	CFW.00109004	http to external service error.	http to external service error.	Try again later or contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
400	CFW.00200001	empty param	empty param.	contact technical support.
400	can not delete for used.	can not delete for used.	can not delete for used.	contact technical support.
400	CFW.00200005	operation content does not exist.	operation content does not exist.	contact technical support.
400	CFW.00200007	name conflict.	name conflict.	please rename the name.
400	CFW.00200009	A request with the same param already exists.	A request with the same param already exists.	contact technical support.
400	CFW.00200010	Config type error.	Config type error.	contact technical support.
400	CFW.00200011	Not support batch operation.	Not support batch operation.	contact technical support.
400	CFW.00200013	url syntax error.	url syntax error.	contact technical support.
400	CFW.00200020	added acl rules can't exceed 20.	added acl rules can't exceed 20.	Please reduce the number of added acl rules.
400	CFW.00200022	all IP address segments is not allowed in black and white list.	all IP address segments is not allowed in black and white list.	Please specify the black and white list ip address segment.
400	CFW.00200023	PARAM_UPGRADING_TASK_OUT_OF_RANGE	PARAM_UPGRADING_TASK_OUT_OF_RANGE.	contact technical support.
400	CFW.00200024	Exceeded maximum quantity limit.	Exceeded maximum quantity limit.	contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
400	CFW.00200025	long connection acl rules time out of range.	long connection acl rules time out of range.	Please make sure the long connection rule duration is from one second to a thousand days.
400	CFW.00200026	Long connection acl rules reach limit.	Long connection acl rules reach limit.	Please delete some long connection rules.
400	CFW.00200027	acl address is error.	acl address is error.	Please make sure that the acl rule address conforms to the specification.
400	CFW.00200028	inconsistent address types.	inconsistent address types.	Please make sure the address type is the same.
400	CFW.00200030	address type is error.	address type is error.	contact technical support.
400	CFW.00200032	The engine does not support IPv6.	The engine does not support IPv6.	contact technical support.
400	CFW.00200036	The network segment cannot be changed to a private network segment.	The network segment cannot be changed to a private network segment.	contact technical support.
400	CFW.00200041	address is null.	address is null.	Please add address type parameter.
400	CFW.00200016	instance status error.	instance status error.	contact technical support.
400	CFW.0020001110	Can't operate basic defense	Can't operate basic defense	contact technical support.
400	CFW.00300001	Parse command error.	Parse command error.	contact technical support.
400	CFW.00400002	not need to operate.	not need to operate.	contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
400	CFW.00400004	item already exist.	item already exist.	Please delete some service items.
400	CFW.00400006	clear rule hit count param error.	clear rule hit count param error.	Please check and confirm whether the parameter value is legal.
400	CFW.00400007	ACL_RULE_TYPE_INCONSISTENT.	ACL_RULE_TYPE_INCONSISTENT.	Make sure to add the same rule type.
400	CFW.00400008	protect object doesn't exist.	protect object doesn't exist.	contact technical support.
400	CFW.00400009	The number of wildcard domain name protection rules exceeds the upper limit	The number of wildcard domain name protection rules exceeds the upper limit	Please delete some generic domain name protection rules.
400	CFW.00400010	not supported protocol for long connection.	not supported protocol for long connection.	Please make sure that the rule protocol belongs to TCP, UDP.
400	CFW.00400011	BLACK_WHITE_LIST_REPEAT.	BLACK_WHITE_LIST_REPEAT.	Make sure to add a different black and white list.
400	CFW.00400012	East west protection not existed,private Ip blackWhite list cannot be submitted.	East west protection not existed,private Ip blackWhite list cannot be submitted.	Please add east-west protection.
400	CFW.00400013	The number of blocklists or trustlists exceeds the maximum 2000.	The number of blocklists or trustlists exceeds the maximum 2000.	Please delete some black and white lists.
400	CFW.00500002	time range error.	time range error.	contact technical support.
400	CFW.00500004	time range error.	time range error.	contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
400	CFW.00600003	HTTP response status code does not match.	HTTP response status code does not match.	contact technical support.
400	CFW.00700001	er not exist error.	er not exist error.	Please check if er exists.
400	CFW.00700002	vpc not exist error.	vpc not exist error.	Please check if vpc exists.
400	CFW.00700003	associated subnet conflict.	associated subnet conflict.	Please make sure that the created subnet does not overlap with the subnet segment under the existing vpc.
400	CFW.00700004	create subnet error.	create subnet error.	contact technical support.
400	CFW.00700007	er attach vpc error.	er attach vpc error.	contact technical support.
400	CFW.00700012	change route error.	change route error.	contact technical support.
400	CFW.00700015	Get VPC quotas error.	Get VPC quotas error.	contact technical support.
400	CFW.00700016	Vpc contain route table quota not enough.	Vpc contain route table quota not enough.	Please delete the existing routing table under vpc.
400	CFW.00800001	An error occurred when querying from etcd.	An error occurred when querying from etcd.	contact technical support.
400	CFW.00800002	An error occurred when deleting from etcd.	An error occurred when deleting from etcd.	contact technical support.
400	CFW.00800003	An error occurred when save to etcd.	An error occurred when save to etcd.	contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
400	CFW.00900016	The import task is in progress. Please operate after the task is completed.	The import task is in progress. Please operate after the task is completed.	Please wait some time until the import task finishes.
400	CFW.00900020	Address groups exceed the maximum limit	Address groups exceed the maximum limit	Please delete some address groups.
400	CFW.00900030	Global services reach limit.	Global services reach limit.	Please delete some service items.
400	CFW.01100008	Configurations cannot be delivered during cluster capacity expansion.	Configurations cannot be delivered during cluster capacity expansion.	contact technical support.

B Change History

Release Date	Description
2023-07-30	This issue is the first official release.

