Anti-DDoS Advanced

API Documentation

Product Documentation
Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.
Contents

API Documentation
Update History
Overview
API Overview
Calling Method
  Request Structure
    Request Structure Overview
    Common Request Parameters
    API Request Parameters
    Final Request Parameter
  Returned Result
    Successful Response
    Error Response
    Format of Returned Results for Asynchronous Task APIs
Signature Method
Basis Info APIs
  Get Anti-DDoS Advance Instance Info
  Rename Anti-DDoS Advance Instance
  Set CC Protection Threshold
  Set Elastic Protection Limit
  Add Custom CC Policy
  Edit Custom CC Policy
  Get Custom CC Policy
  Get Custom CC Protection Policy List
  Remove Custom CC Protection Policy
  Enable/Disable Custom CC Policy
  Enable CC Protection
  Disable CC Protection
Protection Info APIs
  Get DDoS Attack Count
  Get DDoS Attack Statistics
  Get DDoS Attack Details
  Get CC Attack Count
  Get CC Attack Statistics
  Get CC Attack Details
Get Forwarded Traffic Statistics

Service List APIs
Get Anti-DDoS Advance instance List
Get Anti-DDoS Advance instance Usage Statistics

Forwarding Rule APIs
Add Layer-4 Forwarding Rule
Edit Layer-4 Forwarding Rule
Get Layer-4 Forwarding Rule
Delete Layer-4 Forwarding Rule
Add Layer 7 Forwarding Rule
Edit Layer 7 Forwarding Rule
Get Layer 7 Forwarding Rule
Delete Layer 7 Forwarding Rule

Whitelist APIs
Get URL Whitelist
Add URL Whitelist
Remove URL Whitelist
Get Source IP Whitelist
Add Source IP Whitelist
Remove Source IP Whitelist

Blacklist APIs
Add Source IP Blacklist
Remove Source IP Blacklist

Error Codes
# API Documentation

## Update History


Current Anti-DDoS Advance API version: API 2.0.

<table>
<thead>
<tr>
<th>Release Time</th>
<th>Update Description</th>
<th>Version Description</th>
</tr>
</thead>
</table>
| 2018-12-20   | - Added [API Overview](#)  
               - Added [Getting Started with Tencent Cloud API and Service Limits in Introduction](#) | API 2.0             |
| 2018-03-21   | Released Anti-DDoS Advance API Version 2.0                                      | API 2.0             |
Overview


Anti-DDoS Advanced is a paid protection service to defend user applications outside Tencent Cloud against massive DDoS attacks. It directs attack traffic to anti-DDoS Advanced IP for cleaning, ensuring available and stable operations.

Glossary

To get started with Anti-DDoS Advanced, please see the commonly-used terms below.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service. A DDoS attack is a malicious attempt to make service unavailable by overwhelming the targeted system with a flood of Internet traffic.</td>
</tr>
<tr>
<td>CC</td>
<td>Challenge Collapsar. A type of DDoS attack where attackers use a proxy server to send a large number of deceptive requests to target servers.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall. An application firewall for HTTP applications which applies a set of policies to an HTTP conversation.</td>
</tr>
</tbody>
</table>

**Note**

- For Anti-DDoS Advanced service restrictions, see [here](#).
- Anti-DDoS Advanced instances cannot be purchased via APIs.
- To learn more about restrictions on API-specific parameters, please refer to the relevant API documentation.
# API Overview


## Basis Info APIs

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGPIPGetInfo</td>
<td>Gets details about a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPRename</td>
<td>Renames a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPSetCCThreshold</td>
<td>Sets a CC defense threshold for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPSetElasticProtectionLimit</td>
<td>Sets an elastic defense limit for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>AddCustomCCStrategy</td>
<td>Adds a single CC custom policy</td>
</tr>
<tr>
<td>EditCustomCCStrategy</td>
<td>Edits a single CC custom policy</td>
</tr>
<tr>
<td>GetCustomCCStrategy</td>
<td>Gets a single CC custom policy</td>
</tr>
<tr>
<td>GetCustomCCStrategyList</td>
<td>Gets a CC custom policy list</td>
</tr>
</tbody>
</table>
## API Description

<table>
<thead>
<tr>
<th>API Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RemoveCustomCCStrategy</strong></td>
<td>Removes a single CC custom policy</td>
</tr>
<tr>
<td><strong>SetCustomCCStrategyStatus</strong></td>
<td>Enables or disables a single CC custom policy</td>
</tr>
<tr>
<td><strong>OpenDomainCCProtection</strong></td>
<td>Enables domain rule CC defense</td>
</tr>
<tr>
<td><strong>CloseDomainCCProtection</strong></td>
<td>Disables domain rule CC defense</td>
</tr>
</tbody>
</table>

## Defense Info APIs

<table>
<thead>
<tr>
<th>API Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BGPIPDDoSGetCounter</strong></td>
<td>Gets the number of DDoS attacks suffered by a specific Anti-DDoS Advanced instance, the peak attack size, and the number of elastic defenses enabled for this instance</td>
</tr>
<tr>
<td><strong>BGPIPDDoSGetStatistics</strong></td>
<td>Gets the traffic statistics of DDoS attacks on a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>API Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BGPIPDDoSGetDetails</td>
<td>Gets the details of DDoS attack traffic on a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPCCGetCounter</td>
<td>Gets the number of CC attacks suffered by a specific Anti-DDoS Advanced instance and the peak attack size</td>
</tr>
<tr>
<td>BGPIPCCGetStatistics</td>
<td>Gets the statistic chart of CC attack traffic on a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPCCGetDetails</td>
<td>Gets the details of CC attack traffic on a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPTTransGetStatistics</td>
<td>Gets the statistic chart of the traffic forwarded from an Anti-DDoS Advanced instance to the servers outside Tencent Cloud</td>
</tr>
</tbody>
</table>

**Service List APIs**

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
</table>

©2013-2019 Tencent Cloud. All rights reserved.
<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGPIPGetServicePacks</td>
<td>Gets a list of all the Anti-DDoS Advanced instances under a given user name</td>
</tr>
<tr>
<td>BGPIPGetServiceStatistics</td>
<td>Gets the number of usage days and number of defenses of Anti-DDoS Advanced</td>
</tr>
</tbody>
</table>

**Forwarding Rule APIs**

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGPIPAddTransRules</td>
<td>Adds a Layer-4 forwarding rule for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPEditTransRules</td>
<td>Edits a specific Layer-4 forwarding rule for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPGetTransRules</td>
<td>Gets the Layer-4 forwarding rule list for a specific Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>
### API Description

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGPIPDeleteTransRules</td>
<td>Removes a specific Layer-4 forwarding rule for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPAddWadTransRules</td>
<td>Adds a Layer-7 forwarding rule for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPEditWadTransRules</td>
<td>Edits a specific Layer-7 forwarding rule for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPGetWadTransRules</td>
<td>Gets the Layer-7 forwarding rule list for an Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>BGPIPDeleteWadTransRules</td>
<td>Removes a specific Layer-7 forwarding rule for a specific Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>

### Whitelist APIs

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GetWhiteUrl</td>
<td>Gets the whitelist for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>AddWhiteUrl</td>
<td>Adds the URL whitelist for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>RemoveWhiteUrl</td>
<td>Removes the URL whitelist for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>GetSrcWhiteIP</td>
<td>Gets the source IP whitelist for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>AddSrcWhiteIP</td>
<td>Adds the source IP whitelist for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>RemoveSrcWhiteIP</td>
<td>Removes the source IP whitelist for a specific Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>

**Blacklist APIs**

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AddSrcBlackIP</td>
<td>Adds the source IP blacklist for a specific Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>RemoveSrcBlackIP</td>
<td>Removes an IP from the blacklist of the specified Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>
Calling Method

Request Structure

Request Structure Overview


You can call a Tencent Cloud API by sending a request that include specified request parameters to an API endpoint. A Tencent Cloud API request involves service address, communication protocol, request method, request parameters and character encoding. See below for details.

Endpoint

The endpoint of a Tencent Cloud API depends on the module. For more information, see the description of each API.

Communication Protocol

Most Tencent Cloud APIs can be connected through HTTPS, which provides high-security communication tunnels over the network.

Request Method

Tencent Cloud APIs support both POST and GET requests.

1. POST and GET requests cannot be used together. A GET request arries request parameter appended in Querystring, while a POST request carries request parameter in Request Body and ignores the parameters in Querystring. The request parameters in both types of requests are formatted in the same way. GET requests are more common than POST requests. However, if the request parameters are too long, we recommend POST requests.

2. When you send a GET request, all request parameters need to be URL encoded. This is not required for POST requests.

3. The maximum URL length of GET requests varies by browser and server setting. For example, maximum URL length is 2 KB in traditional IE browsers, while it is 8 KB in Firefox.
browsers. For API requests with long URL and many parameters, we recommend that you use POST method to prevent request failures from exceeding the maximum length.

4. The query parameters of POST requests need to be `x-www-form-urlencoded` because the APIs extract query parameters from `$_POST`.

### Request Parameters

Two types of parameters are required for each Tencent Cloud API request: common request parameters and API request parameters. Common request parameters are required for each API (see Common Request Parameters), while API request parameters are unique to each API (see "Request Parameters" in each API document).

### Character Encoding

All requests sent to Tencent Cloud APIs and their responses are UTF-8 encoded.
Common Request Parameters


A complete Tencent Cloud API request requires two types of request parameters: common request parameters and API request parameters. This document describes 6 common request parameters used in Tencent Cloud API requests. For more information about API request parameters, see API Request Parameters.

Common request parameters are required in every API. When you send requests to Tencent Cloud APIs, please make sure that the requests include both common request parameters and API request parameters. Otherwise, the requests will fail. Also, you need to capitalize the first letter in each common request parameter so that it can be differentiated from a API request parameter.

Common request parameters are shown in the following table:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
<th>Type</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Name of an action-specific API. For example, when a Tencent Cloud CVM user calls the API DescribeInstance, the Action of this request is DescribeInstances.</td>
<td>String</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note:
We take Tencent Cloud CVM-specific API as an example in this document. For other resource-specific APIs, please see relevant documents.
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
<th>Type</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>Name of the region where your desired instance is located. For more information, see Regions and Availability Zones, or use the API DescribeRegions. <strong>Notes:</strong> 1. This parameter is required for the API requests, unless otherwise specified. 2. The product is in closed beta in some of the regions and not available to all users.</td>
<td>String</td>
<td>No</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Current UNIX timestamp, which is the time when the API request was initiated.</td>
<td>UInt</td>
<td>Yes</td>
</tr>
<tr>
<td>Nonce</td>
<td>A random positive integer that is combined with Timestamp to prevent replay attacks.</td>
<td>UInt</td>
<td>Yes</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
<td>Type</td>
<td>Required</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>SecretId</td>
<td>Identity of the Tencent Cloud API access key Applicant Cloud API Key. A SecretId corresponds to one unique SecretKey, which is used to generate a request Signature. For more information, see Signature Method.</td>
<td>String</td>
<td>Yes</td>
</tr>
<tr>
<td>Signature</td>
<td>A signature is used for adding authentication information to the requests so that Tencent Cloud APIs can validate the identity of the request. The creation of signatures is based on input parameters. For more information, see Signature Method.</td>
<td>String</td>
<td>Yes</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
<td>Type</td>
<td>Required</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>SignatureMethod</td>
<td>Types of message authentication methods. HmacSHA256 and HmacSHA1 are supported. If HmacSHA256 is not specified, the default is HmacSHA1. For more information, see Signature Method.</td>
<td>String</td>
<td>No</td>
</tr>
<tr>
<td>Token</td>
<td>No</td>
<td>String</td>
<td>A token must be included in an API call along with temporary credentials. Long-term credentials do not require tokens.</td>
</tr>
</tbody>
</table>

**Use Case**

The following example shows how common request parameters are formatted in an Tencent Cloud API request when you want to query the list of Tencent Cloud CVM instances in the Guangzhou region:

```plaintext
https://cvm.api.qcloud.com/v2/index.php?
Action=DescribeInstances
&SecretId=xxxxxxx
&Region=ap-guangzhou
&Timestamp=1465055529
&Nonce=59485
&Signature=mysignature
&SignatureMethod=HmacSHA256
&
API Request Parameters

Last updated: 2020-01-16 15:46:46

A complete Tencent Cloud API request requires two types of request parameters: common request parameters and API request parameters. This document describes API request parameters that are used to specify which Tencent Cloud API is called. For information about common request parameters, see Common Request Parameters.

API request parameters vary by API. The initial letter of each API request parameter should be in lowercase so that it can be differentiated from a common request parameter.

**Note:**
We take Tencent Cloud CVM-specific API as an example in this document. For other resource-specific APIs, please see relevant documents.

For example, the Tencent Cloud CVM API DescribeInstances has its specific parameters as the following table shown:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
<th>Type</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>instanceIds.n</td>
<td>A array that contains the IDs of CVM instances you want to query with subscripts starting from 0. You can use either instanceId or unInstanceId. The unified resource ID unInstanceId is recommended.</td>
<td>String</td>
<td>No</td>
</tr>
<tr>
<td>lanIps.n</td>
<td>Array of private IPs of the CVMs to be queried.</td>
<td>String</td>
<td>No</td>
</tr>
<tr>
<td>searchWord</td>
<td>CVM alias set by the user.</td>
<td>String</td>
<td>No</td>
</tr>
<tr>
<td>offset</td>
<td>The value of offset. The default is 0.</td>
<td>Int</td>
<td>No</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
<td>Type</td>
<td>Required</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>------</td>
<td>----------</td>
</tr>
<tr>
<td>limit</td>
<td>The maximum number of servers that can be queried at a time. The default is 20. The maximum is 100.</td>
<td>Int</td>
<td>No</td>
</tr>
<tr>
<td>status</td>
<td>Status of the CVM to be queried.</td>
<td>Int</td>
<td>No</td>
</tr>
<tr>
<td>projectId</td>
<td>Project ID. Query CVM instances of all projects if the parameter is null.</td>
<td>String</td>
<td>No</td>
</tr>
<tr>
<td>simplify</td>
<td>Return non-real time data when the input value is 1.</td>
<td>Int</td>
<td>No</td>
</tr>
<tr>
<td>zoneId</td>
<td>Availability zone ID. Query CVM instances in all availability zones if the parameter is null. Call the API DescribeAvailabilityZones to get a list of availability zones.</td>
<td>Int</td>
<td>No</td>
</tr>
</tbody>
</table>

The following describes the elements in a parameter:

**Parameter Name:** The name of the API-supported request parameter. You can use it as an API request parameter when calling the API. “n” at the end of a parameter name represents an array, which means that you need to input multiple parameter values.

**Required:** Whether or not the parameter is required for the requests. "Yes" means you need to specify the parameter value. "No" means the input is optional.

**Type:** Data type of the parameter.

**Description:** A brief description of the parameter.

**Use Case**

The following example shows how common request parameters are formatted in an Tencent Cloud API request when you want to query a list of scaling groups for a Tencent Cloud CVM:
https://cvm.api.qcloud.com/v2/index.php?
&
&instanceIds.0=ins-0hm4gvho
&instanceIds.1=ins-8oby8q00
&offset=0
&limit=20
&status=2
&zoneId=100003
Final Request Parameter


**Concatenation Rule**

The structure of a Tencent Cloud API request URL

```plaintext
https:// + domain name + Request path + ? + lists of request parameters
```

**Description:**

- **Domain name:** The domain name for an API request is subject to product or product module. For example, when you sent an API request to query a list of Tencent Cloud CVM instances (Action: DescribeInstances), the domain name is: `cvm.api.qcloud.com`. For more information about domain names, see relevant API documents.

- **Request path:** The path for an API request is subject to product. Each product has a fixed path. For example, the request path for Tencent Cloud CVM is `/v2/index.php`.

- **Lists of request parameters:** Common request parameters and API request parameters

**Use Case**

This example shows the URL of a Tencent Cloud API request: you sent an API request to query a list of Tencent Cloud CVM instances (Action: DescribeInstances). Domain name is: `cvm.api.qcloud.com`. First 6 parameters are common request parameters, and the last 6 ones are API request parameters.

```plaintext
https://cvm.api.qcloud.com/v2/index.php?
Action=DescribeInstances
&SecretId=xxxxxxx
&Region=gz
&Timestamp=1465055529
&Nonce=59485
&Signature=mysignature //Common request parameters
&instanceIds.0=ins-0hm4gvho
&instanceIds.1=ins-8oby8q00
&offset=0
&limit=20
&status=2
&zoneId=100003 //API request parameters
```
Returned Result
Successful Response


When a API call is successful, 0 "code" (error code), empty "message" (error message) and result data will be turned.

Example:

```json
{
    "code": 0,
    "message": "",
    <Returned result>
}
```
Error Response

Last updated: 2019-11-29 18:05:47

If you fail to call an API, the value of error code returned will not be 0 and a message related to this error will present detailed error information.

Returned error sample:

```json
{
  "code": 5100,
  "message": "(100004)projectId is incorrect"
}
```
Format of Returned Results for Asynchronous Task APIs

Asynchronous task API is not defined in updated API and currently only partial products and services such as CVM are available. For specific usage, see Action documentations.

General Asynchronous Task API Result

Sending one request to general Asynchronous Task API allows you to operate only one type of resource at a time. For example, you can create load balancer or reset server operating system by making a call to the specified general Asynchronous Task API.

**Format**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>code</td>
<td>Int</td>
<td>Error code. 0: Successful; other values: Failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>message</td>
<td>String</td>
<td>Error message</td>
<td>No</td>
</tr>
<tr>
<td>requestId</td>
<td>String</td>
<td>Task ID</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Asynchronous Task-Chain API

Sending one request to Asynchronous Task-Chain API allows you to operate multiple types of resources at a time. For example, you can change passwords and start/shut down servers at the same time by making a call to the specified Asynchronous Task-Chain API.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>code</td>
<td>Int</td>
<td>Error code. 0: Successful; other values: Failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>message</td>
<td>String</td>
<td>Error message</td>
<td>No</td>
</tr>
<tr>
<td>detail</td>
<td>Array</td>
<td>Details of the operation: code, message, and requestId. Key is resource ID</td>
<td>Yes</td>
</tr>
</tbody>
</table>

For example:
```json
{
  "code": 0,
  "message": "success",
  "detail": {
    "qcvm6a456b0d8f01d4b2b1f5073d3fb8ccc0": {
      "code": 0,
      "message": ",
      "requestId": "1231231231231"
    }
  }
}
```

- If you successfully operate all resources, the "code" in the first layer is 0.
- If you fail to operate all resources, the "code" in the first layer is 5100.
- If you fail to operate some resources, the outermost code returns 5400. In this case, you can find the detailed information in "detail" in the result.
Signature Method

Last updated: 2020-01-08 19:36:07

When you send requests to Tencent Cloud API, you need to sign the requests for authentication and security purposes. That is, you include a signature generated by your security credential, which consists of a secret id and a secret key, as a common parameter to the request. Please note that security credentials are required for Tencent Cloud API calls. If you have not had one, feel free to apply on Tencent Cloud official website.

Applying for Security Credentials

Before using Tencent Cloud’s APIs for the first time, you need to apply for security credentials on Tencent Cloud Console -> API Key Management. Security credentials consist of a SecretId and a SecretKey, where:

- **SecretId**: Identifier of the requester.
- **SecretKey**: A key that can be used to encrypt the strings to create a signature so that Tencent Cloud server can validate the identity of the requester.

SecretKeys are very important through which you can access and work with the resources in your Tencent Cloud account via API. For security reasons, please keep your keys safe and rotate them regularly, and make sure you delete the old key when a new one is created.

How to apply for security credentials

1. Log in to the Tencent Cloud Console.
2. Click Products, and select Security Credentials under Monitor & Management to go to the cloud API key management page.
3. On the API Key Management page, click Create Key to create a pair of SecretId/SecretKey.

- A developer account can have two pairs of SecretId/SecretKey at most.
- A developer can add a QQ account as a sub-user and use it to apply for different security credentials in multiple developer consoles.
- A sub-user can only call the specified Tencent Cloud APIs with its security credential.
Generating a Signature

A signature can be created with a set of secret ID and secret key.

Suppose that you have the following SecretId and SecretKey:
SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA
SecretKey: Gu5t9xGARNpq86cd98joQYCN3Cozk1qA

This information is only for demonstration purpose. Make sure you proceed with your actual SecretId, SecretKey and request parameters.

For example, when you call Tencent Cloud CVM's API Viewing Instance List (DescribeInstances), the request parameters are as follows:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Method name</td>
<td>DescribeInstances</td>
</tr>
<tr>
<td>SecretId</td>
<td>Key ID</td>
<td>AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Current timestamp</td>
<td>1465185768</td>
</tr>
<tr>
<td>Nonce</td>
<td>A random positive integer</td>
<td>11886</td>
</tr>
<tr>
<td>Region</td>
<td>The region where the instance resides</td>
<td>ap-guangzhou</td>
</tr>
<tr>
<td>SignatureMethod</td>
<td>Signature method</td>
<td>HmacSHA256</td>
</tr>
<tr>
<td>InstanceIds.0</td>
<td>ID of the instance to be queried</td>
<td>ins-09dx96dg</td>
</tr>
</tbody>
</table>

1. Sort parameters

First, sort all the parameters sent in the HTTP request in ascending lexicographical order by their names. (This is like sorting words in a dictionary in ascending alphabetical order or numerical order. That is, sort the parameters by their first letters, then by their second letters if their first letters are
the same, and so on). You can use sorting functions available in programming languages, such as the ksort function in PHP. For example,

```json
{
  "Action" : "DescribeInstances",
  "InstanceId.0" : "ins-09dx96dg",
  "Nonce" : 11886,
  "Region" : "ap-guangzhou",
  "SecretId" : "AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA",
  "SignatureMethod" : "HmacSHA256",
  "Timestamp" : 1465185768
}
```

You can use any other programming languages to sort parameters as long as you get the same result as the one in the example above.

## 2. Concatenate request elements to form a query string

Assign values to the parameters (see the previous step) by following the logic "parameter name"="parameter value". For example, if the value of "Action" is "DescribeInstances", then `Action=DescribeInstances`.

- "parameter value" is the original value, instead of the URL encoded value.
- Any underscore in the parameter names needs to be replaced with ``, while the one in parameter values is allowed. For example, `Placement.Zone=CN_GUANGZHOU` needs to be converted to `Placement.Zone=CN_GUANGZHOU`.

Then, concatenate the formatted parameters separate them with `&` to generate the query string (ignore the line breaks in the text):

```text
Action=DescribeInstances
&InstanceId.0=ins-09dx96dg
&Nonce=11886
&Region=ap-guangzhou
&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA
&SignatureMethod=HmacSHA256
&Timestamp=1465185768
```

## 3. Create a string to sign

Structure of string to sign:
HTTP Request Method + Server Domain Name + Path + ? + Query String

Components

Description of parameters:

- **HTTP request method**: The POST and GET methods are supported. We use a GET request in this case. Please note that both methods are case-sensitive and should always be mentioned in uppercase.

- **Server domain name**: The domain name varies by the product or product module to which the API belongs. For example, when you send a request to Tencent Cloud CVM’s API to query a list of instances(DescribeInstances), the domain name for this request is: `cvm.api.qcloud.com`. For more information on the domain names for requests in different products, see the description of each API.

- **Request path**: A path that defines how Tencent Cloud product API is exposed to requesters. In general, each product has a fixed and unique request path. For example, the request path for Tencent Cloud CVM is always `/v2/index.php`.

- **Query string**: The string generated in the previous step.

The resulting string to sign (ignore the line breaks in the text):

```
GETcvm.api.qcloud.com/v2/index.php?Action=DescribeInstances
&InstanceIds.0=ins-09dx96dg
&Nonce=11886
&Region=ap-guangzhou
&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA
&SignatureMethod=HmacSHA256
&Timestamp=1465185768
```

4. **Compute a signature**

You can compute a signature using either HmacSHA256 or HmacSHA1 protocols. The HmacSHA1 is preferred unless HmacSHA256 is specified.

** First, create a hash-based message authentication code (HMAC) that uses HmacSHA256 or HmacSHA1 protocols to sign the string from the previous step, then encode the resulting signature to Base64.

In this example, we use PHP language and compute the signature using **HmacSHA256** (Note: you
can use any other programming languages as long as the resulting signature is the same as the one in this example). The sample code is shown as follows:

```php
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3C0zk1qA';
$srcStr = 'GETcvm.api,qcloud.com/v2/index.php?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg &Nonce=11886&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKB2Qpn74WFkmLPx3gnPhESA&SignatureMethod=HmacSHA256&Timestamp=1465185768';
$signStr = base64_encode(hash_hmac('sha256', $srcStr, $secretKey, true));
```

The result is as follows:

```plaintext
0EEm/HtGRr/VJXTAD9tYMth1Bzm3llLHz5RCDv1GdM8s=
```

Similarly, if you use `HmacSHA1`, the code should be organized as follows:

```php
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3C0zk1qA';
$srcStr = 'GETcvm.api,qcloud.com/v2/index.php?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg &Nonce=11886&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKB2Qpn74WFkmLPx3gnPhESA&SignatureMethod=HmacSHA1&Timestamp=1465185768';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
```

The result is as follows:

```plaintext
nPVy6njQmwQ8ciqbP15Qe+0ru4=
```

### Encode the signature

The signature must be URL encoded.

For example, after encoding, the 'raw' signature generated in the previous step

```plaintext
0EEm/HtGRr/VJXTAD9tYMth1Bzm3llLHz5RCDv1GdM8s=
```

is converted to

```plaintext
0EEm%2FHtGRr%2FVJXTAD9tYMth1Bzm3llLHz5RCDv1GdM8s%3D
```

The resulting signature is

```plaintext
0EEm%2FHtGRr%2FVJXTAD9tYMth1Bzm3llLHz5RCDv1GdM8s%3D
```

, which will be used to generate the request URL.

If you are sending a GET request, all parameters in the request need to be URL encoded. Please note that some languages may offer auto-URL encoding, and repeated encoding will cause the failure of signature verification.
## Authentication Failures

The following errors may occur when the authentication fails:

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Type</th>
<th>Error Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100</td>
<td>Authentication failed</td>
<td>Make sure the signature added to your request is calculated correctly (see steps above as reference) and URL encoded.</td>
</tr>
<tr>
<td>4101</td>
<td>No access to this API</td>
<td>The sub-user is not authorized to call the API. Contact the developer for authorization. For more information, see <a href="#">Authorization Policy</a>.</td>
</tr>
<tr>
<td>4102</td>
<td>No access to the API resources</td>
<td>The resources are not accessible. Find the ID of the inaccessible resource in field <strong>Message</strong>. Contact the developer for authorization. For more information, see <a href="#">Authorization Policy</a>.</td>
</tr>
<tr>
<td>4103</td>
<td>Non-developer SecretId cannot be used for this API call</td>
<td>Only the developer can call this API with this SecretId.</td>
</tr>
<tr>
<td>4104</td>
<td>SecretId does not exist</td>
<td>The SecretId does not exist, or the status of SecretKey is incorrect. Make sure the SecretKey is valid to use.</td>
</tr>
<tr>
<td>4110</td>
<td>Authentication failed</td>
<td>Permission verification failed. Make sure you are granted the permission to access to this resource.</td>
</tr>
<tr>
<td>4500</td>
<td>Replay attack error</td>
<td>Invalid nonce- nonce must increase with every request. Invalid timestamp - The difference between Timestamp and Tencent server time should not be greater than 2 hours.</td>
</tr>
</tbody>
</table>
Basis Info APIs
Get Anti-DDoS Advance Instance Info

Last updated : 2019-05-07 10:23:08

API Description

This API (BGPIPGetInfo) is used to obtain details of an Anti-DDoS Advanced instance.
Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPGetInfo

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPGetInfo.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>bgpip-000001</td>
<td>String</td>
<td>ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>lbid</td>
<td>lb-xxxxxxxxxx</td>
<td>String</td>
<td>ID of a load balancer IP. It’s only available when the Anti-DDoS Advanced IP is a Tencent Cloud IP.</td>
</tr>
<tr>
<td>name</td>
<td>dayutest</td>
<td>String</td>
<td>Name of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>name</td>
<td>Service pack 1</td>
<td>String</td>
<td>Name of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>Parameter</td>
<td>Example</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>region</td>
<td>gz</td>
<td>String</td>
<td>Region of the Anti-DDoS Advanced instance. Available Regions: gz: Guangzhou, sh: Shanghai, bj: Beijing</td>
</tr>
<tr>
<td>expire</td>
<td>2016-03-02 01:23:45</td>
<td>Time</td>
<td>Expiration time of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>boundIP</td>
<td>10.2.3.4</td>
<td>String</td>
<td>IP address of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>bandwidth</td>
<td>10000</td>
<td>Integer</td>
<td>Unit: Mbps. Base protection bandwidth of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>ccPeak</td>
<td>10000</td>
<td>Integer</td>
<td>Unit: QPS. Maximum CC protection bandwidth</td>
</tr>
<tr>
<td>ccThreshold</td>
<td>100</td>
<td>Integer</td>
<td>Unit: QPS. Current CC protection threshold</td>
</tr>
<tr>
<td>elasticLimit</td>
<td>10000</td>
<td>Integer</td>
<td>Unit: Mbps. Upper limit of elastic protection bandwidth. The Anti-DDoS Advanced IP will be blocked when this limit is exceeded.</td>
</tr>
<tr>
<td>transTarget</td>
<td>qcloud</td>
<td>String</td>
<td>Forwarding target IP qcloud: Inside Tencent Cloud, nqcloud: Outside Tencent Cloud</td>
</tr>
<tr>
<td>line</td>
<td>1, 2</td>
<td>Integer</td>
<td>Line type 1: BGP, 2: China Mobile/China Union/China Telecom</td>
</tr>
<tr>
<td>vpclId</td>
<td>1234</td>
<td>Integer</td>
<td>VPC-id Available if VPC is used.</td>
</tr>
</tbody>
</table>
Rename Anti-DDoS Advance Instance


API Description

This API (BGPIPRename) is used to rename an Anti-DDoS Advanced instance.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPRename

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPRename.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>name</td>
<td>Yes</td>
<td>String</td>
<td>Name of the Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Set CC Protection Threshold


API Description

This API (BGPIPSetCCThreshold) is used to set the threshold for the CC protection. 0 means disabled CC protection.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: BGPIPSetCCThreshold

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see the Common Request Parameters page. The Action field for this API is BGPIPSetCCThreshold.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>threshold</td>
<td>Yes</td>
<td>String</td>
<td>CC protection threshold. 0 means disabled CC protection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CC protection threshold must be lower than the value of the current CC protection capability. See CC Protection Capabilities.</td>
</tr>
</tbody>
</table>

Description of CC Protection Capabilities

<table>
<thead>
<tr>
<th>DDoS Protection</th>
<th>CC Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 GB</td>
<td>20000 QPS</td>
</tr>
<tr>
<td>20 GB</td>
<td>40000 QPS</td>
</tr>
<tr>
<td>30 GB</td>
<td>70000 QPS</td>
</tr>
<tr>
<td>40 GB</td>
<td>100000 QPS</td>
</tr>
<tr>
<td>50 GB</td>
<td>150000 QPS</td>
</tr>
<tr>
<td>DDoS Protection</td>
<td>CC Protection</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>60 GB</td>
<td>200000 QPS</td>
</tr>
<tr>
<td>80 GB</td>
<td>250000 QPS</td>
</tr>
<tr>
<td>100 GB</td>
<td>300000 QPS</td>
</tr>
<tr>
<td>&gt; 100 GB</td>
<td>300000 QPS</td>
</tr>
</tbody>
</table>

**Response Parameters**

None.
Set Elastic Protection Limit


API Description

This API (BGPIPSetElasticProtectionLimit) is used to configure the elastic protection bandwidth for an Anti-DDoS Advanced instance. 0 means disabled elastic defense.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPSetElasticProtectionLimit

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPSetElasticProtectionLimit.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>limit</td>
<td>Yes</td>
<td>Integer</td>
<td>Elastic protection bandwidth (in MB). 0 means disabled elastic defense.</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Add Custom CC Policy


API Description

This API (AddCustomCCStrategy) is used to add a custom CC protection policy. It's only available when CC protection is enabled, and the policy will not take effect until the threshold of CC protection is triggered.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: AddCustomCCStrategy

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is AddCustomCCStrategy.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>name</td>
<td>Yes</td>
<td>String</td>
<td>Policy name. Must be unique in the instance.</td>
</tr>
<tr>
<td>smode</td>
<td>Yes</td>
<td>String</td>
<td>Policy mode: matching: by matching speedlimit: by limiting the speed)</td>
</tr>
<tr>
<td>exemode</td>
<td>Yes</td>
<td>String</td>
<td>Action mode: alg: verify requests with verification codes drop: block all requests</td>
</tr>
<tr>
<td>exeduration</td>
<td>Yes</td>
<td>Integer</td>
<td>Execution duration. This parameter needs to be reserved and set to 0 as recommended, which means that the policy will be executed until the attacks are defeated.</td>
</tr>
<tr>
<td>frequency</td>
<td>No</td>
<td>Integer</td>
<td>Number of queries per minute. When the policy mode is speedlimit, this parameter is required.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Required</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>rulelist</td>
<td>No</td>
<td>Array</td>
<td>When the <code>smode</code> is matching, this parameter is required.</td>
</tr>
</tbody>
</table>

```json
"rulelist": [
  {
    "key": "host", "operate": "include", "value": "test1"
  },
  {
    "key": "cgi", "operate": "include", "value": "test2"
  }
]
```

Key: host, cgi, ua, referer
Operate: include, not_include, equal
Value: string(no more than 31 characters)

Response Parameters

None.
Edit Custom CC Policy

Last updated : 2019-05-07 10:23:30

API Description

This API (EditCustomCCStrategy) is used to edit a custom CC protection policy. The policy can be edited only when CC protection is enabled for the Anti-DDoS Advanced instance. The old policy can be identified by field `bgpid` and `name`, and overwritten with the new one.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: EditCustomCCStrategy

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see the Common Request Parameters. The Action field for this API is `EditCustomCCStrategy`.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpid</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>name</td>
<td>Yes</td>
<td>String</td>
<td>Policy name. Must be unique in the instance.</td>
</tr>
<tr>
<td>smode</td>
<td>Yes</td>
<td>String</td>
<td>Policy mode: matching: by matching speedlimit: by limiting the speed</td>
</tr>
<tr>
<td>exemode</td>
<td>Yes</td>
<td>String</td>
<td>Execution mode: alg: by verification codes drop: by blocking</td>
</tr>
<tr>
<td>exeduration</td>
<td>Yes</td>
<td>Integer</td>
<td>Execution duration. This parameter needs to be reserved and set to 0 as recommended, which means that the policy will be executed until the attacks are defeated</td>
</tr>
<tr>
<td>frequency</td>
<td>No</td>
<td>Integer</td>
<td>Number of queries per minute. When the policy mode is <code>speedlimit</code>, this parameter is required</td>
</tr>
<tr>
<td>Parameter</td>
<td>Required</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>rulelist</td>
<td>No</td>
<td>Array</td>
<td>When the smode is matching, this parameter is required.</td>
</tr>
</tbody>
</table>

```
"rulelist": [
  {"key": "host", "operate": "include", "value": "test1"},
  {"key": "cgi", "operate": "include", "value": "test2"}
]
```

Key: host, cgi, ua, referer
Operate: include, not_include, equal
value: string (no more than 31 characters)

Response Parameters

None.
Get Custom CC Policy


API Description

This API (GetCustomCCStrategy) is used to obtain the information of a custom CC protection policy.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: GetCustomCCStrategy

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is GetCustomCCStrategy.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>name</td>
<td>Yes</td>
<td>String</td>
<td>Policy name. Must be unique in the instance</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>smode</td>
<td>String</td>
<td>Policy mode: matching: by matching speedlimit: by limiting the speed</td>
</tr>
<tr>
<td>exemode</td>
<td>String</td>
<td>Execution mode: alg: by verification codes drop: by blocking</td>
</tr>
<tr>
<td>status</td>
<td>Integer</td>
<td>Status of CC protection. 1: enabled 0: disabled</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>exeduration</td>
<td>Integer</td>
<td>Execution duration.</td>
</tr>
<tr>
<td>frequency</td>
<td>Integer</td>
<td>Number of queries per minute. When the policy mode is <code>speedlimit</code>, this parameter is returned.</td>
</tr>
<tr>
<td>rulelist</td>
<td>Array</td>
<td>When the <code>smode</code> is <code>matching</code>, this parameter is required.</td>
</tr>
</tbody>
</table>

```json
"rulelist": [  
  {"key":"host","operate":"include","value":"test1"},  
  {"key":"cgi","operate":"include","value":"test2"}  
]
```

**Key:** host, cgi, ua, referer  
**Operate:** include, not_include, equal  
**Value:** string(no more than 31 characters)
Get Custom CC Protection Policy List

API Description

This API (GetCustomCCStrategyList) is used to obtain the list of CC custom policies of an Anti-DDoS Advanced instance.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: GetCustomCCStrategyList

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see the Common Request Parameters. The Action field for this API is GetCustomCCStrategyList.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategy_list</td>
<td>Array</td>
<td>Policy list. For more information, see Example: strategy_list.</td>
</tr>
</tbody>
</table>

Example: strategy_list

```json
"strategy_list": [
{
"createtime": "2017-09-20 18:14:42",
"exemode": "drop",
"name": "testname1",
```
"rulelist": [
{
  "key": "host",
  "operate": "include",
  "value": "1"
},
  "smode": "matching",
  "status": "1"
},
{
  "createtime": "2017-09-25 20:54:16",
  "exemode": "alg",
  "name": "testname2",
  "rulelist": [
  {
    "key": "host",
    "operate": "include",
    "value": "chen"
  }
  ],
  "smode": "matching",
  "status": "1"
}
]
Remove Custom CC Protection Policy


API Description

This API (RemoveCustomCCStrategy) is used to delete a CC custom policy. The policy can be deleted only when CC protection is enabled for the Anti-DDoS Advanced instance. This API identifies the policy by field bgpId and name field and delete it. Please note that the deleted policy cannot be restored.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: RemoveCustomCCStrategy

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see the Common Request Parameters. The Action field for this API is RemoveCustomCCStrategy.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>name</td>
<td>Yes</td>
<td>String</td>
<td>Policy name. Must be unique in the instance.</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Enable/Disable Custom CC Policy


API Description

This API (SetCustomCCStrategyStatus) is used to enable/disable a CC custom policy. The policy can be enabled/disabled only when CC protection is enabled/disabled for the Anti-DDoS Advanced instance. This API identifies the policy by field bgpid and name, and enables/disables the policy.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: SetCustomCCStrategyStatus

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is SetCustomCCStrategyStatus.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpid</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>name</td>
<td>Yes</td>
<td>String</td>
<td>Policy name. Must be unique in the instance.</td>
</tr>
<tr>
<td>status</td>
<td>Yes</td>
<td>Integer</td>
<td>Description of status. 1: Enabled. 0: Disabled.</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Enable CC Protection


API Description

This API (OpenDomainCCProtection) is used to enable the CC protection for a domain name. Layer-7 rule is identified by two fields: bgpId and ruleId.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: OpenDomainCCProtection

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is OpenDomainCCProtection.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>ruleId</td>
<td>Yes</td>
<td>String</td>
<td>Forwarding rule ID</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Disable CC Protection


API Description

This API (CloseDomainCCProtection) is used to disable the CC protection for a domain name. Layer-7 rule is identified by field **bgpId** and **ruleId**.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: CloseDomainCCProtection

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is CloseDomainCCProtection.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>ruleId</td>
<td>Yes</td>
<td>String</td>
<td>Forwarding rule ID</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Protection Info APIs
Get DDoS Attack Count

Last updated: 2019-05-07 10:24:02

API Description

This API (BGPIPDDoSGetCounter) is used to get the detailed information of DDoS attack traffic received by an Anti-DDoS Advanced IP, including total attack count, attack traffic peak, and how many times the elastic protection is enabled.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPDDoSGetCounter

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPDDoSGetCounter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Yes</td>
<td>String</td>
<td>ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>beginDate</td>
<td>Yes</td>
<td>String</td>
<td>Start time of the records. Format: YYYY-MM-DD.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example: 2016-11-10</td>
</tr>
<tr>
<td>endDate</td>
<td>Yes</td>
<td>String</td>
<td>End time of the records. Format: YYYY-MM-DD.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example: 2016-11-11</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attacks</td>
<td>1035</td>
<td>Integer</td>
<td>Number of DDoS attack events</td>
</tr>
<tr>
<td>attackPeak</td>
<td>35000</td>
<td>Integer</td>
<td>Unit: Mbps. DDoS attack peak</td>
</tr>
<tr>
<td>Parameter</td>
<td>Example</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>overload</td>
<td>6</td>
<td>Integer</td>
<td>Number of times that elastic protection is triggered</td>
</tr>
<tr>
<td>bandwidth</td>
<td>80000</td>
<td>Integer</td>
<td>Unit: Mbps. Base protection bandwidth of the Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>
Get DDoS Attack Statistics

Last updated: 2019-05-07 10:24:06

API Description

This API (BGPIPDDoSGetStatistics) is used to obtain the traffic statistics of the DDoS attacks against an Anti-DDoS Advanced IP.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: BGPIPDDoSGetStatistics

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPDDoSGetStatistics.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Yes</td>
<td>String</td>
<td>ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>beginDate</td>
<td>Yes</td>
<td>String</td>
<td>Start time of the records. Format: YYYY-MM-DD. Example: 2016-11-10</td>
</tr>
<tr>
<td>endDate</td>
<td>Yes</td>
<td>String</td>
<td>End time of the records. Format: YYYY-MM-DD. Example: 2016-11-11</td>
</tr>
<tr>
<td>stride</td>
<td>Yes</td>
<td>Integer</td>
<td>Time granularity (in min). If duration=1 day, stride=5; If duration=7 days, stride=60; If duration=30 days, stride=1,440</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>

©2013-2019 Tencent Cloud. All rights reserved.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>before</td>
<td>[1,000 Mbps,...]</td>
<td>Array</td>
<td>Attack traffic peak before protection is enabled, i.e. the maximum traffic in each stride. For example, if duration is 5 minutes, the result is the maximum attack traffic within 5 minutes.</td>
</tr>
<tr>
<td>after</td>
<td>[50 Mbps,...]</td>
<td>Array</td>
<td>Cleaned traffic peak after protection is enabled, i.e. the maximum traffic in each stride. For example, if the duration is 5 minutes, the result is the maximum cleaned traffic within 5 minutes.</td>
</tr>
</tbody>
</table>
Get DDoS Attack Details


API Description

This API (BGPIPDDoSGetDetails) is used to obtain the details of DDoS attack traffic received by an Anti-DDoS Advanced IP.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is NS.BGPIP. Protection.DDoS.GetDetails.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Yes</td>
<td>String</td>
<td>ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>beginDate</td>
<td>Yes</td>
<td>String</td>
<td>Start time of queried period. Format: YYYY-MM-DD. Example: 2016-11-10.</td>
</tr>
<tr>
<td>endDate</td>
<td>Yes</td>
<td>String</td>
<td>End time of queried period. Format: YYYY-MM-DD, such as 2016-11-11.</td>
</tr>
<tr>
<td>filtering.overload</td>
<td>No</td>
<td>String</td>
<td>Valid values: yes/no yes: only list the data of attack traffic exceeding the peak. no: only list the data of traffic not exceeding the peak.</td>
</tr>
<tr>
<td>sorting.field</td>
<td>No</td>
<td>String</td>
<td>Valid value: peak (sort by attack traffic peak).</td>
</tr>
<tr>
<td>sorting.order</td>
<td>No</td>
<td>String</td>
<td>Valid values: asc/desc asc: Sort in ascending order desc: Sort in a descending order</td>
</tr>
</tbody>
</table>
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>paging.index</td>
<td>Yes</td>
<td>Integer</td>
<td>Page index</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0: page 1</td>
</tr>
<tr>
<td>paging.count</td>
<td>Yes</td>
<td>Integer</td>
<td>Number of results returned per page</td>
</tr>
</tbody>
</table>

### Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>123</td>
<td>Integer</td>
<td>Total number of entries</td>
</tr>
<tr>
<td>records</td>
<td>[obj,...]</td>
<td>Array</td>
<td>Details of attacks:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Details of attacks:

```json
{
    "startTime" : "2013-03-01 01:23:45",
    "endTime"   : "2013-03-01 01:23:45",
    "peak"      : 1234,
    "overload"  : "yes/no"
}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startTime</td>
<td>2013-03-01 01:23:45</td>
<td>Time</td>
<td>Start time of the attack</td>
</tr>
<tr>
<td>endTime</td>
<td>2013-03-01 01:23:50</td>
<td>Time</td>
<td>End time of the attack</td>
</tr>
<tr>
<td>peak</td>
<td>80 Gbps</td>
<td>Integer</td>
<td>Attack traffic peak</td>
</tr>
<tr>
<td>overload</td>
<td>yes/no</td>
<td>String</td>
<td>Whether the attack traffic exceeds the protection bandwidth</td>
</tr>
</tbody>
</table>
Get CC Attack Count

API Description

This API (BGPIPCCGetCounter) is used to get the number of CC attacks against an Anti-DDoS Advanced IP and the attack traffic peak.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com
API: BGPIPCCGetCounter

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPCCGetCounter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Yes</td>
<td>String</td>
<td>ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>beginDate</td>
<td>Yes</td>
<td>String</td>
<td>Start time of the records. Format: YYYY-MM-DD. Example: 2016-11-10.</td>
</tr>
<tr>
<td>endDate</td>
<td>Yes</td>
<td>String</td>
<td>End time of the records. Format: YYYY-MM-DD. Example: 2016-11-11.</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Unit</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attacks</td>
<td>1,035</td>
<td>Integer</td>
<td>Number of CC attacks</td>
</tr>
<tr>
<td>attackPeak</td>
<td>35,000 QPS</td>
<td>Integer</td>
<td>CC attack peak</td>
</tr>
</tbody>
</table>
Get CC Attack Statistics


API Description

This API (BGPIPCCGetStatistics) is used to get the statistics of a CC attack targeting an Anti-DDoS Advanced IP.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPCCGetStatistics

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPCCGetStatistics.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Yes</td>
<td>String</td>
<td>ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>beginDate</td>
<td>Yes</td>
<td>String</td>
<td>Start time of the records. Format: YYYY-MM-DD. Example: 2016-11-10</td>
</tr>
<tr>
<td>endDate</td>
<td>Yes</td>
<td>String</td>
<td>End time of the records. Format: YYYY-MM-DD. Example: 2016-11-10</td>
</tr>
<tr>
<td>stride</td>
<td>Yes</td>
<td>Integer</td>
<td>Time granularity (in min). If duration=1 day, then stride=5; If duration=7 days, then stride=60; If duration=30 days, then stride=1,440</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>points</td>
<td>[1000,...]</td>
<td>Array</td>
<td>Number of CC attack events blocked in each stride</td>
</tr>
</tbody>
</table>
Get CC Attack Details


API Description

This API (BGPIPCCGetDetails) is used to obtain the details of a CC attack targeting an Anti-DDoS Advanced IP.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: BGPIPCCGetDetails

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is: BGPIPCCGetDetails.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Yes</td>
<td>String</td>
<td>ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>beginDate</td>
<td>Yes</td>
<td>String</td>
<td>Start time of queried period. Format: YYYY-MM-DD. Example: 2016-11-10</td>
</tr>
<tr>
<td>endDate</td>
<td>Yes</td>
<td>String</td>
<td>End time of queried period. Format: YYYY-MM-DD. Example: 2016-11-11</td>
</tr>
<tr>
<td>sorting.field</td>
<td>No</td>
<td>String</td>
<td>Valid value: <strong>count</strong>, number of CC attack queries</td>
</tr>
<tr>
<td>sorting.order</td>
<td>No</td>
<td>String</td>
<td>Valid values: asc/desc&lt;br&gt;asc: Sort in ascending order&lt;br&gt;desc: Sort in a descending order</td>
</tr>
<tr>
<td>paging.index</td>
<td>Yes</td>
<td>Integer</td>
<td>Page index&lt;br&gt;0: page 1</td>
</tr>
<tr>
<td>paging.count</td>
<td>Yes</td>
<td>Integer</td>
<td>Number of results per page</td>
</tr>
</tbody>
</table>
## Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>123</td>
<td>Integer</td>
<td>Total number of entries</td>
</tr>
<tr>
<td>records</td>
<td>[obj,...]</td>
<td>Array</td>
<td>Details of attacks:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>`{</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;startTime&quot; : &quot;2013-03-01 01:23:45&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;endTime&quot; : &quot;2013-03-01 01:23:45&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;count&quot; : 1234</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>}</td>
</tr>
<tr>
<td>startTime</td>
<td>2013-03-01 01:23:45</td>
<td>Time</td>
<td>Start time of attack</td>
</tr>
<tr>
<td>endTime</td>
<td>2013-03-01 01:23:50</td>
<td>Time</td>
<td>End time of attack</td>
</tr>
<tr>
<td>count</td>
<td>1234</td>
<td>Integer</td>
<td>Attack traffic peak</td>
</tr>
</tbody>
</table>
Get Forwarded Traffic Statistics


API Description

This API (BGPIPTransGetStatistics) is used to obtain the chart describing the statistics of the traffic forwarded from an Anti-DDoS Advanced IP to non-Tencent Cloud servers (valid only for non-Tencent Cloud IPs).

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPTransGetStatistics

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is: BGPIPTransGetStatistics.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Yes</td>
<td>String</td>
<td>ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>beginDate</td>
<td>Yes</td>
<td>String</td>
<td>Start time of queried period. Format: YYYY-MM-DD. Example: 2016-11-10</td>
</tr>
<tr>
<td>endDate</td>
<td>Yes</td>
<td>String</td>
<td>End time of queried period. Format: YYYY-MM-DD. Example: 2016-11-11</td>
</tr>
<tr>
<td>stride</td>
<td>Yes</td>
<td>Integer</td>
<td>Time granularity of the statistics (in min). If duration=1 day, then stride=5; if duration=7 days, then stride=60; If duration=30 days, then stride=1,440</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Example</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>points</td>
<td>[1000 Mbps,...]</td>
<td>Array</td>
<td>Total volume of traffic forwarded to the non-Tencent Cloud servers in each stride</td>
</tr>
</tbody>
</table>
Service List APIs
Get Anti-DDoS Advance instance List

API Description

This API (BGPIPGetServicePacks) is used to get a list of all Anti-DDoS Advanced instances owned by the user.
Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPGetServicePacks

Request Parameters

The following request parameter list only provides the API-specific request parameters. Common request parameters are required when the API is called. For more information, see Common Request Parameters. The Action field of this API is BGPIPGetServicePacks.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filtering.name</td>
<td>No</td>
<td>String</td>
<td>Search by the name of the Anti-DDoS Advanced instance. Fuzzy search is supported.</td>
</tr>
<tr>
<td>filtering.ip</td>
<td>No</td>
<td>String</td>
<td>Search by the IP of the Anti-DDoS Advanced instance. Fuzzy search is supported.</td>
</tr>
<tr>
<td>line</td>
<td>No</td>
<td>Integer</td>
<td>Line type 1: BGP 2: China Mobile/China Union/China Telecom</td>
</tr>
<tr>
<td>sorting.field</td>
<td>No</td>
<td>String</td>
<td>Sort by field: bandwidth: Sort by bandwidth overloadCount: Sort by the number of times the peak value is exceeded</td>
</tr>
<tr>
<td>sorting.order</td>
<td>No</td>
<td>String</td>
<td>Sort in order: asc: Sort in ascending order desc: Sort in descending order</td>
</tr>
</tbody>
</table>
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>paging.index</td>
<td>Yes</td>
<td>Integer</td>
<td>Page index</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0: page 1</td>
</tr>
<tr>
<td>paging.count</td>
<td>Yes</td>
<td>Integer</td>
<td>Number of results per page</td>
</tr>
<tr>
<td>region</td>
<td>Yes</td>
<td>String</td>
<td>Region availability.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>gz: Guangzhou</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sh: Shanghai</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>bj: Beijing</td>
</tr>
</tbody>
</table>

### Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>123</td>
<td>Integer</td>
<td>Number of Anti-DDoS Advanced instances</td>
</tr>
<tr>
<td>records</td>
<td>[obj,...]</td>
<td>Array</td>
<td>Instance details:</td>
</tr>
<tr>
<td>id</td>
<td>bgpip-000001</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>name</td>
<td>Service pack 1</td>
<td>String</td>
<td>Name of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>Parameter</td>
<td>Example</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>region</td>
<td>gz</td>
<td>String</td>
<td>Anti-DDoS Advanced Instance location</td>
</tr>
<tr>
<td></td>
<td>sh</td>
<td></td>
<td>gz: Guangzhou</td>
</tr>
<tr>
<td></td>
<td>bj</td>
<td></td>
<td>sh: Shanghai</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>bj: Beijing</td>
</tr>
<tr>
<td>line</td>
<td>1</td>
<td>Integer</td>
<td>Line type:</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td>1: BGP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2: China Mobile/China Union/China Telecom</td>
</tr>
<tr>
<td>boundIP</td>
<td>10.2.3.4</td>
<td>String</td>
<td>IP address of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>bandwidth</td>
<td>10000</td>
<td>Integer</td>
<td>Unit: Mbps. Base protection bandwidth of the instance</td>
</tr>
<tr>
<td>elasticLimit</td>
<td>10000</td>
<td>Integer</td>
<td>Unit: Mbps. Upper limit of the elastic protection bandwidth. The Anti-DDoS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Advanced IP will be blocked when the limit is exceeded.</td>
</tr>
<tr>
<td>overloadCount</td>
<td>100</td>
<td>Integer</td>
<td>Number of events that the peak attack volume exceeds the maximum protection</td>
</tr>
<tr>
<td>status</td>
<td>idle</td>
<td>String</td>
<td>Status of the Anti-DDoS Advanced IP:</td>
</tr>
<tr>
<td></td>
<td>attacking</td>
<td></td>
<td>idle: no attack</td>
</tr>
<tr>
<td></td>
<td>blocking</td>
<td></td>
<td>attacking: the IP is being attacked</td>
</tr>
<tr>
<td></td>
<td>creating</td>
<td></td>
<td>blocking: the IP is being blocked</td>
</tr>
<tr>
<td></td>
<td>isolating</td>
<td></td>
<td>creating: the IP is being restored</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>isolate: the IP is being isolated</td>
</tr>
<tr>
<td>expire</td>
<td>2016-03-02 01:23:45</td>
<td>Time</td>
<td>Expiration time of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>transTarget</td>
<td>qcloud</td>
<td>String</td>
<td>Forwarding target IP</td>
</tr>
<tr>
<td></td>
<td>nqcloud</td>
<td></td>
<td>qcloud: Inside Tencent Cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>nqcloud: Outside Tencent Cloud</td>
</tr>
<tr>
<td>transRules</td>
<td>12</td>
<td>Integer</td>
<td>Number of forwarding rules configured in the instance</td>
</tr>
</tbody>
</table>
Get Anti-DDoS Advance instance Usage Statistics


API Description

This API (BGPIPGetServiceStatistics) is used to get the number of days an Anti-DDoS Advanced instance used, and the number of DDoS attack events targeted this instance.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPGetServiceStatistics

Request Parameters

None.

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attacks</td>
<td>1035</td>
<td>Integer</td>
<td>Number of DDoS attack events</td>
</tr>
<tr>
<td>days</td>
<td>23</td>
<td>Integer</td>
<td>Number of days the Anti-DDoS Advanced instance has been used</td>
</tr>
</tbody>
</table>
Forwarding Rule APIs

Add Layer-4 Forwarding Rule


API Description

This API (BGPIPAddTransRules) is used to add layer-4 forwarding rules to Anti-DDoS Advanced instances.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: BGPIPAddTransRules

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPAddTransRules.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS instance</td>
</tr>
<tr>
<td>vip</td>
<td>Yes</td>
<td>String</td>
<td>IP of the Anti-DDoS Advance instance</td>
</tr>
<tr>
<td>protocol</td>
<td>Yes</td>
<td>String</td>
<td>Protocol used in forwarding rules. Only TCP is supported</td>
</tr>
<tr>
<td>virtualPort</td>
<td>Yes</td>
<td>Integer</td>
<td>Forwarding port</td>
</tr>
<tr>
<td>sourcePort</td>
<td>Yes</td>
<td>Integer</td>
<td>Real server port</td>
</tr>
<tr>
<td>ipList</td>
<td>Yes</td>
<td>String</td>
<td>IP list of the real server. Up to 20 IPs allowed for each rule</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>

©2013-2019 Tencent Cloud. All rights reserved.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleId</td>
<td>rule-000001</td>
<td>String</td>
<td>ID of the forwarding rule</td>
</tr>
</tbody>
</table>
Edit Layer-4 Forwarding Rule

API Description

This API (BGPIPEditTransRules) is used to modify layer-4 forwarding rules of Anti-DDoS Advanced instances.
Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPEditTransRules

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPEditTransRules.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleId</td>
<td>Yes</td>
<td>String</td>
<td>ID of the forwarding rule</td>
</tr>
<tr>
<td>vip</td>
<td>Yes</td>
<td>String</td>
<td>IP of Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>protocol</td>
<td>Yes</td>
<td>String</td>
<td>IP Protocol of the forwarding rule. Only TCP is supported.</td>
</tr>
<tr>
<td>virtualPort</td>
<td>Yes</td>
<td>Integer</td>
<td>Forwarding port</td>
</tr>
<tr>
<td>sourcePort</td>
<td>Yes</td>
<td>Integer</td>
<td>Real server port</td>
</tr>
<tr>
<td>ipList</td>
<td>Yes</td>
<td>String</td>
<td>a list of real server IPs. Up to 20 IPs allowed for each forwarding rule.</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Get Layer-4 Forwarding Rule


API Description

This API (BGPIPGetTransRules) is used to get the list of layer-4 forwarding rules of an Anti-DDoS Advanced instance.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPGetTransRules

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPGetTransRules.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Yes</td>
<td>String</td>
<td>ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>paging.index</td>
<td>Yes</td>
<td>Integer</td>
<td>Page Index. 0: page 1.</td>
</tr>
<tr>
<td>paging.count</td>
<td>Yes</td>
<td>Integer</td>
<td>Number of results per page</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>123</td>
<td>Integer</td>
<td>Number of forwarding rules that have been configured for the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>Parameter</td>
<td>Example</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>transRules</td>
<td>[obj,...]</td>
<td>Array</td>
<td>Attack details. Elements:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;id&quot;: &quot;rule-00000001&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;protocol&quot;: &quot;TCP&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;virtualPort&quot;: &quot;80&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;sourcePort&quot;: &quot;80&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;ipList&quot;: &quot;10.2.3.4;10.1.1.1&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>}</td>
</tr>
<tr>
<td>id</td>
<td>rule-00000001</td>
<td>String</td>
<td>ID of the forwarding rule</td>
</tr>
<tr>
<td>protocol</td>
<td>TCP</td>
<td>String</td>
<td>IP Protocol of the forwarding rule. Only TCP is supported.</td>
</tr>
<tr>
<td>virtualPort</td>
<td>80</td>
<td>Integer</td>
<td>Forwarding port</td>
</tr>
<tr>
<td>sourcePort</td>
<td>80</td>
<td>Integer</td>
<td>Real server port</td>
</tr>
<tr>
<td>ipList</td>
<td>10.2.3.4 : 10.1.1.1</td>
<td>String</td>
<td>a list of the real server IPs. Up to 20 IPs allowed in each forwarding rule.</td>
</tr>
</tbody>
</table>
Delete Layer-4 Forwarding Rule

Last updated: 2019-05-07 10:25:03

API Description

This API (BGPIPDeleteTransRules) is used to delete layer-4 forwarding rules of an Anti-DDoS Advanced instance.
Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPDeleteTransRules

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPDeleteTransRules.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleId</td>
<td>Yes</td>
<td>String</td>
<td>ID of the forwarding rule</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Add Layer 7 Forwarding Rule

Last updated : 2019-05-07 10:25:07

API Description

This API (BGPIPAddWadTransRules) is used to add layer-7 forwarding rules to an Anti-DDoS Advanced instance.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: BGPIPAddWadTransRules

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPAddWadTransRules.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>vip</td>
<td>Yes</td>
<td>String</td>
<td>IP of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>protocol</td>
<td>Yes</td>
<td>String</td>
<td>IP protocol of forwarding rules. Only TCP is supported</td>
</tr>
<tr>
<td>virtualPort</td>
<td>Yes</td>
<td>Integer</td>
<td>Forwarding port</td>
</tr>
<tr>
<td>sourcePort</td>
<td>Yes</td>
<td>Integer</td>
<td>Real server port</td>
</tr>
<tr>
<td>ipList</td>
<td>Yes</td>
<td>String</td>
<td>a list of IPs or domain names of the real server. A rule can contain a maximum of 20 IPs, which are separated with semicolons</td>
</tr>
<tr>
<td>certType</td>
<td>No</td>
<td>Integer</td>
<td>Certificate type. Always enter 1</td>
</tr>
<tr>
<td>cert</td>
<td>No</td>
<td>String</td>
<td>Certificate content</td>
</tr>
<tr>
<td>privateKey</td>
<td>No</td>
<td>String</td>
<td>Certificate private key</td>
</tr>
</tbody>
</table>
## Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleId</td>
<td>rule-000001</td>
<td>String</td>
<td>ID of the forwarding rule</td>
</tr>
</tbody>
</table>
Edit Layer 7 Forwarding Rule

Last updated: 2019-05-07 10:25:12

API Description

This API (BGPIPEditWadTransRules) is used to modify layer-7 forwarding rules of an Anti-DDoS Advanced instance.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: BGPIPEditWadTransRules

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPEditWadTransRules.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleId</td>
<td>Yes</td>
<td>String</td>
<td>ID of the forwarding rule</td>
</tr>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>domain</td>
<td>Yes</td>
<td>String</td>
<td>Name of the public domain (accessible to the clients)</td>
</tr>
<tr>
<td>protocol</td>
<td>Yes</td>
<td>String</td>
<td>IP protocol of forwarding rules Supported: http, https, http/https. certType, cert and privateKey are required when the protocol type is https or http/https.</td>
</tr>
<tr>
<td>sourceType</td>
<td>Yes</td>
<td>Integer</td>
<td>Types of real servers&lt;br&gt;1: Domain name&lt;br&gt;2: IP</td>
</tr>
<tr>
<td>ipList</td>
<td>Yes</td>
<td>String</td>
<td>a list of IPs or domain names of the real server. A rule can contain a maximum of 20 IPs, which are separated with semicolons</td>
</tr>
<tr>
<td>certType</td>
<td>No</td>
<td>Integer</td>
<td>Certificate type. Always enter 1</td>
</tr>
<tr>
<td>Parameter</td>
<td>Required</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>--------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>cert</td>
<td>No</td>
<td>String</td>
<td>Certificate content</td>
</tr>
<tr>
<td>privateKey</td>
<td>No</td>
<td>String</td>
<td>Certificate private key</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Get Layer 7 Forwarding Rule

Last updated: 2019-05-07 10:25:17

API Description

This API (BGPIPGetWadTransRules) is used to get the list of layer-7 forwarding rules of an Anti-DDoS Advanced instance.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: BGPIPGetWadTransRules

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPGetWadTransRules.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>paging.index</td>
<td>Yes</td>
<td>Integer</td>
<td>Page Index. 0: page 1.</td>
</tr>
<tr>
<td>paging.count</td>
<td>Yes</td>
<td>Integer</td>
<td>Number of results per page</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>123</td>
<td>Integer</td>
<td>Number of forwarding rules that have been configured for the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>Parameter</td>
<td>Example</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>transRules</td>
<td>[obj,...]</td>
<td>Array</td>
<td>Attack details. Elements:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>`{</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;id&quot;: &quot;rule-00000001&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;protocol&quot;: &quot;http&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;domain&quot;: &quot;www.qq.com&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;sourceType&quot;: 1/2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;ipList&quot;: &quot;10.2.3.4;10.1.1.1&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;certType&quot;: 1,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;cert&quot;: &quot;&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;privateKey&quot;: &quot;&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;status&quot;: 1/2/3,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;ssl_id&quot;: &quot;&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>}</td>
</tr>
<tr>
<td>id</td>
<td>rule-00000001</td>
<td>String</td>
<td>ID of the forwarding rule</td>
</tr>
<tr>
<td>protocol</td>
<td>http</td>
<td>String</td>
<td>IP Protocol of the forwarding rule</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The value can be http, https or http/https.</td>
</tr>
<tr>
<td>domain</td>
<td><a href="http://www.qq.com">www.qq.com</a></td>
<td>String</td>
<td>Public domain name (accessible to the clients)</td>
</tr>
<tr>
<td>sourceType</td>
<td>1 2</td>
<td>Integer</td>
<td>Types of real servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1: Domain name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2: IP</td>
</tr>
<tr>
<td>ipList</td>
<td>10.2.3.4 ; 10.1.1.1</td>
<td>String</td>
<td>a list of IPs or domain names of the real server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IPs or domain names are returned according to the value of sourceType.</td>
</tr>
<tr>
<td>certType</td>
<td>1</td>
<td>Integer</td>
<td>Certificate type. Always 1.</td>
</tr>
<tr>
<td>cert</td>
<td></td>
<td>String</td>
<td>Certificate content</td>
</tr>
<tr>
<td>privateKey</td>
<td></td>
<td>String</td>
<td>Certificate private key</td>
</tr>
<tr>
<td>status</td>
<td>0 1 2</td>
<td>Integer</td>
<td>The status of forwarding rule configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0: Configured successfully</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1: Configuring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2: Configuration failed</td>
</tr>
<tr>
<td>ssl_id</td>
<td></td>
<td>String</td>
<td>Optional</td>
</tr>
</tbody>
</table>
Delete Layer 7 Forwarding Rule

Last updated: 2019-05-07 10:25:21

API Description

This API (BGPIPDeleteWadTransRules) is used to delete layer-7 forwarding rules of an Anti-DDoS Advanced instance.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: BGPIPDeleteWadTransRules

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is BGPIPDeleteWadTransRules.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleId</td>
<td>Yes</td>
<td>String</td>
<td>ID of the forwarding rule</td>
</tr>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Whitelist APIs
Get URL Whitelist

Last updated : 2019-05-07 10:26:28

API Description

This API (GetWhiteUrl) is used to obtain the URL whitelist of an Anti-DDoS Advanced instance.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: GetWhiteUrl

Request Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>whitelist</td>
<td>&quot;URL list&quot;,...</td>
<td>Array</td>
<td>Returns configured whitelist:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;whitelist&quot;: [</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;<a href="http://www.website1.com/">http://www.website1.com/</a>&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;<a href="http://www.website2.com/">http://www.website2.com/</a>&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>]</td>
</tr>
</tbody>
</table>
Add URL Whitelist

Last updated: 2019-05-07 10:26:32

API Description

This API (AddWhiteUrl) is used to add the URL whitelist to an Anti-DDoS Advanced instance.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: AddWhiteUrl

Request Parameters

Below is a list of API request parameters. Common request parameters need to be added to your request when calling the API. For more information, see Common Request Parameters. The Action field for this API is AddWhiteUrl.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>
| whitelist | Yes      | Array  | Whitelist:

```
```

Response Parameters

None.
Remove URL Whitelist

Last updated: 2019-05-07 10:26:37

API Description

This API (RemoveWhiteUrl) is used to remove URLs from the whitelist of an Anti-DDoS Advanced instance.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: RemoveWhiteUrl

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is RemoveWhiteUrl.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>whitelist</td>
<td>Yes</td>
<td>Array</td>
<td>Whitelist:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;whitelist&quot;: [</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;<a href="http://www.website1.com/">http://www.website1.com/</a>&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;<a href="http://www.website2.com/">http://www.website2.com/</a>&quot; ]</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Get Source IP Whitelist

Last updated: 2019-05-07 10:26:40

API Description

This API (GetSrcWhiteIP) is used to obtain the source IP whitelist of an Anti-DDoS Advanced instance.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: GetSrcWhiteIP

Request Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>

Response Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>whitelist</td>
<td>[&quot;URL list&quot;,...]</td>
<td>Array</td>
<td>Returns configured whitelist:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;whitelist&quot;: [</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;10.1.1.1&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;10.2.2.2&quot; ]</td>
</tr>
</tbody>
</table>
Add Source IP Whitelist

Last updated : 2019-05-07 10:26:45

API Description

This API (AddSrcWhiteIP) is used to add the source IP whitelist to an Anti-DDoS Advanced instance.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: AddSrcWhiteIP

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is AddSrcWhiteIP.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>
| whitelist  | Yes      | Array | Whitelist: 
"whitelist": [ 
"10.1.1.1",
"10.2.2.2",
"10.3.3.3"
] |

Response Parameters

None.
Remove Source IP Whitelist

Last updated: 2019-05-07 10:26:49

API Description

This API (RemoveSrcWhiteIP) is used to remove an IP from the whitelist of an Anti-DDoS Advanced instance.

Protocol: HTTPS
Domain Name: bgpip.api.qcloud.com
API: RemoveSrcWhiteIP

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is RemoveSrcWhiteIP.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>ID of the Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>
| whitelist  | Yes      | Array  | Whitelist:

| "whitelist": [ "10.1.1.1", "10.2.2.2" ] |

Response Parameters

None.
**Blacklist APIs**

**Add Source IP Blacklist**

Last updated: 2019-05-07 10:26:54

**API Description**

This API (AddSrcBlackIP) is used to add IPs to blacklist of an Anti-DDoS Advanced instance.

**Protocol:** HTTPS

**Domain Name:** bgpip.api.qcloud.com

**API:** AddSrcBlackIP

**Request Parameters**

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is AddSrcBlackIP.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
</tbody>
</table>
| blacklist | Yes      | Array | Blacklist:
                               |
|           |          |       | "blacklist": [                                   |
|           |          |       | "10.1.1.1",                                      |
|           |          |       | "10.2.2.2"                                       |
|           |          |       | "10.3.3.3"                                       |
|           |          |       | ]                                               |

**Response Parameters**

None.
Remove Source IP Blacklist

Last updated: 2019-05-07 10:26:58

API Description

This API (RemoveSrcBlackIP) is used to remove one or more IPs from the blacklist of an Anti-DDoS Advanced instance.

Protocol: HTTPS

Domain Name: bgpip.api.qcloud.com

API: RemoveSrcBlackIP

Request Parameters

Below is a list of API request parameters. You need to add common request parameters to your request when calling this API. For more information, see Common Request Parameters. The Action field for this API is RemoveSrcBlackIP.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpId</td>
<td>Yes</td>
<td>String</td>
<td>Resource ID of the Anti-DDoS Advanced instance</td>
</tr>
<tr>
<td>blacklist</td>
<td>Yes</td>
<td>Array</td>
<td>Blacklist:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;blacklist&quot;: [</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;10.1.1.1&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;10.2.2.2&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>]</td>
</tr>
</tbody>
</table>

Response Parameters

None.
Error Codes
Last updated: 2019-11-29 18:06:27

Feature Description

You will receive a code indicating whether you successfully made a call to the API. 0 indicates that the call is successful and other values indicate that the call is failed. You might identify cause of the error from common error codes and take measures.

An example:

```json
{
  "code": 5100
}
```

### Error Codes

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000</td>
<td>Invalid request parameter.</td>
<td>Required parameter is missing, or parameter value is in an incorrect format. For error message, see the &quot;message&quot; field in error description.</td>
</tr>
<tr>
<td>4100</td>
<td>Authentication failed</td>
<td>The failed authentication is usually caused by signature computing error. See Signature Method section in the document.</td>
</tr>
<tr>
<td>4101</td>
<td>Unauthorized access to the API.</td>
<td>The sub-account is not authorized by the main account to access the API. Contact the main account administrator to grant the permission for the API.</td>
</tr>
<tr>
<td>4102</td>
<td>Unauthorized access to the resource.</td>
<td>The sub-account is not authorized by the main account to access the resource. Contact the main account administrator to grant the permission for the resource.</td>
</tr>
<tr>
<td>4103</td>
<td>Unauthorized access to the resource the current API is working with.</td>
<td>The sub-account is not authorized by the main account to access the resource the current API is working with. Contact the main account administrator to grant the permission for the resource.</td>
</tr>
<tr>
<td>Code</td>
<td>Error Message</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4104</td>
<td>Key does not exist.</td>
<td>The key used for the request does not exist. Verify it and try again.</td>
</tr>
<tr>
<td>4105</td>
<td>Token error.</td>
<td>Token error.</td>
</tr>
<tr>
<td>4106</td>
<td>MFA verification failed.</td>
<td>MFA verification failed.</td>
</tr>
<tr>
<td>4110</td>
<td>Other CAM authentication failed.</td>
<td>Other CAM authentication failed.</td>
</tr>
<tr>
<td>4300</td>
<td>Access denied.</td>
<td>Account is blocked or is not within the user range for the API.</td>
</tr>
<tr>
<td>4400</td>
<td>Quota exceeded.</td>
<td>The number of requests exceeded the quota limit. For more information, see the &quot;Request Quota&quot; section in the document.</td>
</tr>
<tr>
<td>4500</td>
<td>Replay attack</td>
<td>The Nonce and Timestamp parameters can ensure that each request is executed only once on the server. Therefore, the Nonce value cannot be the same as last one, and the difference between Timestamp and Tencent server time cannot be greater than 5 minutes.</td>
</tr>
<tr>
<td>4600</td>
<td>Unsupported protocol.</td>
<td>The protocol is not supported. The current API only supports HTTPS protocol and does not support HTTP protocol.</td>
</tr>
<tr>
<td>5000</td>
<td>Resource does not exist.</td>
<td>The instance corresponding to resource ID does not exist, or the instance has been returned, or another user's resource is accessed.</td>
</tr>
<tr>
<td>5100</td>
<td>Resource operation failed.</td>
<td>The operation performed on the resource failed. For error message, see the &quot;message&quot; field in error description. Try again later or contact customer service.</td>
</tr>
<tr>
<td>5200</td>
<td>Failed to purchase the resource.</td>
<td>The resource purchase failed. This is may be caused by unsupported instance configuration or insufficient resource.</td>
</tr>
<tr>
<td>5300</td>
<td>Insufficient balance.</td>
<td>User account has insufficient balance. Unable to purchase or upgrade the resource.</td>
</tr>
<tr>
<td>5400</td>
<td>The operation was successful on some resources.</td>
<td>The batch operation was successful on some resources. For more information, see the returned value of the method.</td>
</tr>
<tr>
<td>5500</td>
<td>User failed to pass identity</td>
<td>Resource purchase failed because the user failed to pass identity verification.</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td>Message</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>6000</td>
<td>Internal error with the server.</td>
<td>An internal error occurred with the server. Try again later or contact customer service.</td>
</tr>
<tr>
<td>6100</td>
<td>Not supported in the version.</td>
<td>The API is not supported by this version or is under maintenance. Note: When this error occurs, first check whether the domain name of the API is correct. Domain name may vary between different modules.</td>
</tr>
<tr>
<td>6200</td>
<td>API is unavailable.</td>
<td>The API is under maintenance and is unavailable. Please try again later.</td>
</tr>
</tbody>
</table>