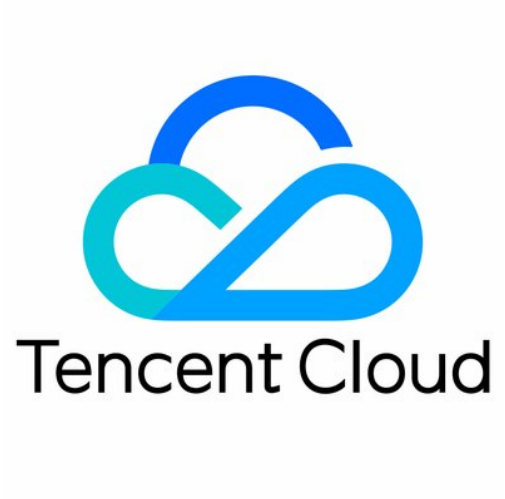
Anti-DDoS Advanced

API Documentation

Product Documentation



Contents

API Documentation
Update History

Last updated : 2019-05-07 10:22:13

Current Anti-DDoS Advance API version: API 2.0.

Release Time	Update Description	Version Description
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

Last updated : 2019-05-07 10:22:19

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.

Term	Description
DDoS	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.
CC	Challenge Collapsar. A type of DDoS attack where attackers use a proxy server to send a large number of deceptive requests to target servers.

Term	Description
WAF	Web Application Firewall. An application firewall for HTTP applications which applies a set of policies to an HTTP conversation.

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

Last updated : 2019-05-07 10:22:24

Basis Info APIs

API	Description
BGPIPGetInfo	Gets details about a specific Anti-DDoS Advanced instance
BGPIPRename	Renames a specific Anti-DDoS Advanced instance
BGPIPSetCCThreshold	Sets a CC defense threshold for a specific Anti-DDoS Advanced instance
BGPIPSetElasticProtectionLimit	Sets an elastic defense limit for a specific Anti-DDoS Advanced instance
AddCustomCCStrategy	Adds a single CC custom policy
EditCustomCCStrategy	Edits a single CC custom policy
GetCustomCCStrategy	Gets a single CC custom policy
GetCustomCCStrategyList	Gets a CC custom policy list

API	Description
RemoveCustomCCStrategy	Removes a single CC custom policy
SetCustomCCStrategyStatus	Enables or disables a single CC custom policy
OpenDomainCCProtection	Enables domain rule CC defense
CloseDomainCCProtection	Disables domain rule CC defense

Defense Info APIs

API Name	Description
BGPIPDDoSGetCounter	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
BGPIPDDoSGetStatistics	Gets the traffic statistics of DDoS attacks on a specific Anti-DDoS Advanced instance

API Name	Description
BGPIPDDoSGetDetails	Gets the details of DDoS attack traffic on a specific Anti-DDoS Advanced instance
BGPIPCCGetCounter	Gets the number of CC attacks suffered by a specific Anti-DDoS Advanced instance and the peak attack size
BGPIPCCGetStatistics	Gets the statistic chart of CC attack traffic on a specific Anti-DDoS Advanced instance
BGPIPCCGetDetails	Gets the details of CC attack traffic on a specific Anti-DDoS Advanced instance
BGPIPTransGetStatistics	Gets the statistic chart of the traffic forwarded from an Anti-DDoS Advanced instance to the servers outside Tencent Cloud

Service List APIs

API	Description

API	Description
BGPIPGetServicePacks	Gets a list of all the Anti-DDoS Advanced instances under a given user name
BGPIPGetServiceStatistics	Gets the number of usage days and number of defenses of Anti-DDoS Advanced

Forwarding Rule APIs

API	Description
BGPIPAddTransRules	Adds a Layer-4 forwarding rule for a specific Anti-DDoS Advanced instance
BGPIPEditTransRules	Edits a specific Layer-4 forwarding rule for a specific Anti-DDoS Advanced instance
BGPIPGetTransRules	Gets the Layer-4 forwarding rule list for a specific Anti-DDoS Advanced instance

API	Description
BGPIPDeleteTransRules	Removes a specific Layer-4 forwarding rule for a specific Anti-DDoS Advanced instance
BGPIPAddWadTransRules	Adds a Layer-7 forwarding rule for a specific Anti-DDoS Advanced instance
BGPIPEditWadTransRules	Edits a specific Layer-7 forwarding rule for a specific Anti-DDoS Advanced instance
BGPIPGetWadTransRules	Gets the Layer-7 forwarding rule list for an Anti-DDoS Advanced instance
BGPIPDeleteWadTransRules	Removes a specific Layer-7 forwarding rule for a specific Anti-DDoS Advanced instance

Whitelist APIs

API	Description

API	Description
GetWhiteUrl	Gets the whitelist for a specific Anti-DDoS Advanced instance
AddWhiteUrl	Adds the URL whitelist for a specific Anti-DDoS Advanced instance
RemoveWhiteUrl	Removes the URL whitelist for a specific Anti-DDoS Advanced instance
GetSrcWhiteIP	Gets the source IP whitelist for a specific Anti-DDoS Advanced instance
AddSrcWhiteIP	Adds the source IP whitelist for a specific Anti-DDoS Advanced instance
RemoveSrcWhiteIP	Removes the source IP whitelist for a specific Anti-DDoS Advanced instance

Blacklist APIs

API	Description

API	Description
AddSrcBlackIP	Adds the source IP blacklist for a specific Anti-DDoS Advanced instance
RemoveSrcBlackIP	Removes an IP from the blacklist of the specified Anti-DDoS Advanced instance

Calling Method
Request Structure
Request Structure Overview

Last updated : 2019-05-07 10:22:31

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

Last updated : 2019-05-07 10:22:35

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:

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

Parameter Name	Description	Type	Required
Action	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.	String	Yes

Parameter Name	Description	Type	Required
Region	Name of the region where your desired instance is located. For more information, see Regions and Availability Zones, or use the API DescribeRegions. **Notes:** 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.	String	No
Timestamp	Current UNIX timestamp, which is the time when the API request was initiated.	UInt	Yes
Nonce	A random positive integer that is combined with Timestamp to prevent replay attacks.	UInt	Yes

Parameter Name	Description	Type	Required
SecretId	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.	String	Yes
Signature	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.	String	Yes

Parameter Name	Description	Type	Required
SignatureMethod	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.	String	No
Token	No	A token must be included in an API call along with temporary credentials. Long-term credentials do not require tokens.	String

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:

```
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:

Parameter Name	Description	Type	Required
instanceIds.n	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.	String	No
lanIps.n	Array of private IPs of the CVMs to be queried.	String	No
searchWord	CVM alias set by the user.	String	No
offset	The value of offset. The default is 0.	Int	No

Parameter Name	Description	Type	Required
limit	The maximum number of servers that can be queried at a time. The defaul is 20. The maximum is 100.	Int	No
status	Status of the CVM to be queried.	Int	No
projectId	Project ID. Query CVM instances of all projects if the parameter is null.	String	No
simplify	Return non-real time data when the input value is 1.	Int	No
zoneId	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.	Int	No

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

Last updated : 2019-05-07 10:22:44

Concatenation Rule

The structure of an Tencent Cloud API request URL

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.

```
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

Last updated : 2019-05-07 10:22:49

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

```
{
”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:

```
{
"code": 5100,
"message": "(100004)projectId is incorrect"
}
```

Format of Returned Results for Asynchronous Task APIs

Last updated : 2019-05-07 10:22:58

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

Name	Type	Description	Required
code	Int	Error code. 0: Successful; other values: Failed.	Yes
message	String	Error message	No
requestId	String	Task ID	Yes

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/shutt down servers at the same time by making a call to the specified Asynchronous Task-Chain API.

Name	Type	Description	Required
code	Int	Error code. 0: Successful; other values: Failed.	Yes
message	String	Error message	No
detail	Array	Details of the operation: code, message, and requestId. Key is resource ID	Yes

For example:

```
{
"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** : Identify 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:

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

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,

```
{
"Action" : "DescribeInstances",
"InstanceIds.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 seperate them with `"&"` to generate the query string (ignore the line breaks in the text):

```
Action=DescribeInstances
&InstanceIds.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:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3Cozk1qA';
$srcStr = 'GETcvm.api.qcloud.com/v2/index.php?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Nonce=11886&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA&SignatureMethod=HmacSHA256&Timestamp=1465185768';
$signStr = base64_encode(hash_hmac('sha256', $srcStr, $secretKey, true));
echo $signStr;
```

The result is as follows:

```
0EEm/HtGRr/VJXTAD9tYMth1Bzm3lLHz5RCDv1GdM8s=
```

Similarly, if you use**HmacSHA1** , the code should be orgainzed as follows:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3Cozk1qA';
$srcStr = 'GETcvm.api.qcloud.com/v2/index.php?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Nonce=11886&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA&SignatureMethod=HmacSHA1&Timestamp=1465185768';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

The result is as follows:

```
nPVnY6njQmwQ8ciqbPl5Qe+Oru4=
```

Encode the signature

The signature must be URL encoded.

For example, after encoding, the 'raw' signature generated in the previous step `0EEm/HtGRr/VJXTAD9tYMth1Bzm3lLHz5RCDv1GdM8s=` is converted to `0EEm%2FHtGRr%2FVJXTAD9tYMth1Bzm3lLHz5RCDv1GdM8s%3D` . The resulting signature is `0EEm%2FHtGRr%2FVJXTAD9tYMth1Bzm3lLHz5RCDv1GdM8s%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:

Error Code	Error Type	Error Description
4100	Authentication failed	Make sure the signature added to your request is calculated correctly (see steps above as reference) and URL encoded.
4101	No access to this API	The sub-user is not authorized to call the API. Contact the developer for authorization. For more information, see Authorization Policy.
4102	No access to the API resources	The resources are not accessible. Find the ID of the inaccessible resource in field **Message** Contact the developer for authorization. For more information, see Authorization Policy.
4103	Non-developer SecretId cannot be used for this API call	Only the developer can call this API with this SecretId.
4104	SecretId does not exist	The SecretId does not exist, or the status of SecretKey is incorrect. Make sure the SecretKey is valid to use.
4110	Authentication failed	Permission verification failed. Make sure you are granted the permission to access to this resource.
4500	Replay attack error	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.

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance

Response Parameters

Parameter	Example	Type	Description
id	bgpip-000001	String	ID of the Anti-DDoS Advanced instance
lbid	lb-xxxxxxxx	String	ID of a load balancer IP. It’s only available when the Anti-DDoS Advanced IP is a Tencent Cloud IP.
name	dayutest	String	Name of the Anti-DDoS Advanced instance
name	Service pack 1	String	Name of the Anti-DDoS Advanced instance

Parameter	Example	Type	Description
region	gz sh bj	String	Region of the Anti-DDoS Advanced instance. Available Regions: gz: Guangzhou sh: Shanghai bj: Beijing
status	idle attacking blocking creating isolate	String	Status of the Anti-DDoS Advanced instance: idle: no attacks attacking: being attacked blocking: the IP is blocked creating: creating an Anti-DDoS Advanced instance isolate: Anti-DDoS Advanced instance is expired and isolated
expire	2016-03-02 01:23:45	Time	Expiration time of the Anti-DDoS Advanced instance
boundIP	10.2.3.4	String	IP address of the Anti-DDoS Advanced instance
bandwidth	10000	Integer	Unit: Mbps. Base protection bandwidth of the Anti-DDoS Advanced instance
ccPeak	10000	Integer	Unit: QPS. Maximum CC protection bandwidth
ccThreshold	100	Integer	Unit: QPS. Current CC protection threshold
elasticLimit	10000	Integer	Unit: Mbps. Upper limit of elastic protection bandwidth. The Anti-DDoS Advanced IP will be blocked when this limit is exceeded.
transTarget	qcloud nqcloud	String	Forwarding target IP qcloud: Inside Tencent Cloud nqcloud: Outside Tencent Cloud
line	1 2	Integer	Line type 1: BGP 2: China Mobile/China Union/China Telecom
vpcId	1234	Integer	VPC-id Available if VPC is used.

Rename Anti-DDoS Advance Instance

Last updated : 2019-05-07 10:23:13

API Description

This API (BGPIPRename) is used to remane 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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
name	Yes	String	Name of the Anti-DDoS Advanced instance

Response Parameters

None.

Set CC Protection Threshold

Last updated : 2019-05-07 10:23:17

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
threshold	Yes	String	CC protection threshold. 0 means disabled CC protection. CC protection threshold must be lower than the value of the current CC protection capability. See **CC Protection Capabilities**.

Description of CC Protection Capabilities

DDoS Protection	CC Protection
10 GB	20000 QPS
20 GB	40000 QPS
30 GB	70000 QPS
40 GB	100000 QPS
50 GB	150000 QPS

DDoS Protection	CC Protection
60 GB	200000 QPS
80 GB	250000 QPS
100 GB	300000 QPS
> 100 GB	300000 QPS

Response Parameters

None.

Set Elastic Protection Limit

Last updated : 2019-05-07 10:23:21

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
limit	Yes	Integer	Elastic protection bandwidth (in MB). 0 means disabled elastic defense.

Response Parameters

None.

Add Custom CC Policy

Last updated : 2019-05-07 10:23:26

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
name	Yes	String	Policy name. Must be unique in the instance.
smode	Yes	String	Policy mode: matching: by matching speedlimit: by limiting the speed)
exemode	Yes	String	Action mode: alg: verify requests with verification codes drop: block all requests
exeduration	Yes	Integer	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.
frequency	No	Integer	Number of queries per minute. When the policy mode is `speedlimit` , this parameter is required.

Parameter	Required	Type	Description
rulelist	No	Array	When the `smode` is `matching`, this parameter is required. `"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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
name	Yes	String	Policy name. Must be unique in the instance.
smode	Yes	String	Policy mode: matching: by matching speedlimit: by limiting the speed
exemode	Yes	String	Execution mode: alg: by verification codes drop: by blocking
exeduration	Yes	Integer	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
frequency	No	Integer	Number of queries per minute. When the policy mode is `speedlimit` , this parameter is required

Parameter	Required	Type	Description
rulelist	No	Array	When the smode is matching, this parameter is required. `"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

Last updated : 2019-05-07 10:23:35

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
name	Yes	String	Policy name. Must be unique in the instance

Response Parameters

Parameter	Type	Description
smode	String	Policy mode: matching: by matching speedlimit: by limiting the speed
exemode	String	Execution mode: alg: by verification codes drop: by blocking
status	Integer	Status of CC protection. 1: enabled 0: disabled

Parameter	Type	Description
exeduration	Integer	Execution duration.
frequency	Integer	Number of queries per minute. When the policy mode is `speedlimit`, this parameter is returned.
rulelist	Array	When the `smode` is `matching`, this parameter is required. `"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

Last updated : 2019-05-07 10:23:40

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance

Response Parameters

Parameter	Type	Description
strategy_list	Array	Policy list. For more information, see **Example: strategy_list**.

Example: strategy_list

```
"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

Last updated : 2019-05-07 10:23:44

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
name	Yes	String	Policy name. Must be unique in the instance.

Response Parameters

None.

Enable/Disable Custom CC Policy

Last updated : 2019-05-07 10:23:48

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
name	Yes	String	Policy name. Must be unique in the instance.
status	Yes	Integer	Description of status. 1: Enabled. 0: Disabled.

Response Parameters

None.

Enable CC Protection

Last updated : 2019-05-07 10:23:52

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	ID of the Anti-DDoS Advanced instance
ruleId	Yes	String	Forwarding rule ID

Response Parameters

None.

Disable CC Protection

Last updated : 2019-05-07 10:23:56

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
ruleId	Yes	String	Forwarding rule ID

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 informtion 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` .

Parameter	Required	Type	Description
id	Yes	String	ID of the Anti-DDoS Advanced instance
beginDate	Yes	String	Start time of the records. Format: YYYY-MM-DD. Example: 2016-11-10
endDate	Yes	String	End time of the records. Format: YYYY-MM-DD. Example: 2016-11-11

Response Parameters

Parameter	Example	Type	Description
attacks	1035	Integer	Number of DDoS attack events
attackPeak	35000	Integer	Unit: Mbps. DDoS attack peak

Parameter	Example	Type	Description
overload	6	Integer	Number of times that elastic protection is triggered
bandwidth	80000	Integer	Unit: Mbps. Base protection bandwidth of the Anti-DDoS Advanced instance

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` .

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

Response Parameters

Parameter	Example	Type	Description

Parameter	Example	Type	Description
before	[1,000 Mbps,...]	Array	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.
after	[50 Mbps,...]	Array	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.

Get DDoS Attack Details

Last updated : 2019-05-07 10:24:11

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`
`BGPIPDDoSGetDetails`

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` .

Parameter	Required	Type	Description
id	Yes	String	ID of the Anti-DDoS Advanced instance
beginDate	Yes	String	Start time of queried period. Format: YYYY-MM-DD. Example: 2016-11-10.
endDate	Yes	String	End time of queried period. Format: YYYY-MM-DD, such as 2016-11-11.
filtering.overload	No	String	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.
sorting.field	No	String	Valid value: peak (sort by attack traffic peak).
sorting.order	No	String	Valid values: asc/desc asc: Sort in ascending order desc: Sort in a descending order

Parameter	Required	Type	Description
paging.index	Yes	Integer	Page index 0: page 1
paging.count	Yes	Integer	Number of results returned per page

Response Parameters

Parameter	Example	Type	Description
total	123	Integer	Total number of entries

records	[obj,...]	Array	Details of attacks:
			{
			”startTime” : ”2013-03-01 01:23:45”,
			”endTime” : ”2013-03-01 01:23:45”,
			”peak” : 1234
			”overload” : ”yes/no”
			}

startTime	2013-03-01 01:23:45	Time	Start time of the attack
endTime	2013-03-01 01:23:50	Time	End time of the attack
peak	80 Gbps	Integer	Attack traffic peak
overload	yes/no	String	Whether the attack traffic exceeds the protection bandwidth

Get CC Attack Count

Last updated : 2019-05-07 10:24:14

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` .

Parameter	Required	Type	Description
id	Yes	String	ID of the Anti-DDoS Advanced instance
beginDate	Yes	String	Start time of the records. Format: YYYY-MM-DD. Example: 2016-11-10.
endDate	Yes	String	End time of the records. Format: YYYY-MM-DD. Example: 2016-11-11.

Response Parameters

Parameter	Unit	Type	Description
attacks	1,035	Integer	Number of CC attacks
attackPeak	35,000 QPS	Integer	CC attack peak

Get CC Attack Statistics

Last updated : 2019-05-07 10:24:20

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` .

Parameter	Required	Type	Description
id	Yes	String	ID of the Anti-DDoS Advanced instance
beginDate	Yes	String	Start time of the records. Format: YYYY-MM-DD. Example: 2016-11-10
endDate	Yes	String	End time of the records. Format: YYYY-MM-DD. Example: 2016-11-10
stride	Yes	Integer	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

Response Parameters

Parameter	Example	Type	Description
points	[1000,...]	Array	Number of CC attack events blocked in each stride

Get CC Attack Details

Last updated : 2019-05-07 10:24:25

API Description

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

Parameter	Required	Type	Description
id	Yes	String	ID of the Anti-DDoS Advanced instance
beginDate	Yes	String	Start time of queried period. Format: YYYY-MM-DD. Example: 2016-11-10
endDate	Yes	String	End time of queried period. Format: YYYY-MM-DD. Example: 2016-11-11
sorting.field	No	String	Valid value: `count` , number of CC attack queries
sorting.order	No	String	Valid values: asc/desc asc: Sort in ascending order desc: Sort in a descending order
paging.index	Yes	Integer	Page index 0: page 1
paging.count	Yes	Integer	Number of results per page

Response Parameters

Parameter	Example	Type	Description
total	123	Integer	Total number of entries

records	[obj,...]	Array	Details of attacks:
			{
			”startTime” : ”2013-03-01 01:23:45”,
			”endTime” : ”2013-03-01 01:23:45”,
			”count” : 1234
			}

startTime	2013-03-01 01:23:45	Time	Start time of attack
endTime	2013-03-01 01:23:50	Time	End time of attack
count	1234	Integer	Attack traffic peak

Get Forwarded Traffic Statistics

Last updated : 2019-05-07 10:24:29

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` .

Parameter	Required	Type	Description
id	Yes	String	ID of the Anti-DDoS Advanced instance
beginDate	Yes	String	Start time of queried period. Format: YYYY-MM-DD. Example: 2016-11-10
endDate	Yes	String	End time of queried period. Format: YYYY-MM-DD. Example: 2016-11-11
stride	Yes	Integer	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

Response Parameters

Parameter	Example	Type	Description

Parameter	Example	Type	Description
points	[1000 Mbps,...]	Array	Total volume of traffic forwarded to the non-Tencent Cloud servers in each stride

Service List APIs
Get Anti-DDoS Advance instance List

Last updated : 2019-05-07 10:24:37

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` .

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

Parameter	Required	Type	Description
paging.index	Yes	Integer	Page index 0: page 1
paging.count	Yes	Integer	Number of results per page
region	Yes	String	Region availability. gz: Guangzhou sh: Shanghai bj: Beijing

Response Parameters

Parameter	Example	Type	Description
total	123	Integer	Number of Anti-DDoS Advanced instances

records	[obj,...]	Array	Instance details:
			{
			”id”: ”bgpip-00000001”,
			”name”: ”Service pack 1”,
			”region”: ”gz/sh/bj”,
			”line”: ”1/2”,
			”boundIP”:
			”10.2.3.4”,
			”bandwidth”: 10000,
			”elasticLimit” : 100000,
			”overloadCount” : 100,
			”status”:”idle/attacking/blocking/creating”,
			”expire”: ”2016-03-02 01:23:45”,
			”locked”: ”yes/no”
			”transTarget”:”qcloud/nqcloud/blackstone/finance”,
			”transRules”: ”12”
			}

id	bgpip-000001	String	Resource ID of the Anti-DDoS Advanced instance
name	Service pack 1	String	Name of the Anti-DDoS Advanced instance

Parameter	Example	Type	Description
region	gz sh bj	String	Anti-DDoS Advanced Instance location gz: Guangzhou sh: Shanghai bj: Beijing
line	1 2	Integer	Line type: 1: BGP 2: China Mobile/China Union/China Telecom
boundIP	10.2.3.4	String	IP address of the Anti-DDoS Advanced instance
bandwidth	10000	Integer	Unit: Mbps. Base protection bandwidth of the instance
elasticLimit	10000	Integer	Unit: Mbps. Upper limit of the elastic protection bandwidth. The Anti-DDoS Advanced IP will be blocked when the limit is exceeded.
overloadCount	100	Integer	Number of events that the peak attack volume exceeds the maximum protection bandwidth
status	idle attacking blocking creating isolate	String	Status of the Anti-DDoS Advanced IP: idle: no attack attacking: the IP is being attacked blocking: the IP is being blocked creating: the IP is being restored isolate: the IP is being isolated
expire	2016-03-02 01:23:45	Time	Expiration time of the Anti-DDoS Advanced instance
transTarget	qcloud nqcloud	String	Forwarding target IP qcloud: Inside Tencent Cloud nqcloud: Outside Tencent Cloud
transRules	12	Integer	Number of forwarding rules configured in the instance

Get Anti-DDoS Advance instance Usage Statistics

Last updated : 2019-05-07 10:24:41

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

Parameter	Example	Type	Description
attacks	1035	Integer	Number of DDoS attack events
days	23	Integer	Number of days the Anti-DDoS Advanced instance has been used

Forwarding Rule APIs
Add Layer-4 Forwarding Rule

Last updated : 2019-05-07 10:24:48

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` .

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

Response Parameters

Parameter	Example	Type	Description

Parameter	Example	Type	Description
ruleId	rule-000001	String	ID of the forwarding rule

Edit Layer-4 Forwarding Rule

Last updated : 2019-05-07 10:24:54

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` .

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

Response Parameters

None.

Get Layer-4 Forwarding Rule

Last updated : 2019-05-07 10:24:59

API Description

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

Parameter	Required	Type	Description
id	Yes	String	ID of the Anti-DDoS Advanced instance
paging.index	Yes	Integer	Page Index. 0: page 1.
paging.count	Yes	Integer	Number of results per page

Response Parameters

Parameter	Example	Type	Description
total	123	Integer	Number of forwarding rules that have been configured for the Anti-DDoS Andvanced instance

Parameter	Example	Type	Description

transRules	[obj,...]	Array	Attack details. Elements:
			`{`
			`"id": "rule-00000001",`
			`"protocol": "TCP"`
			`"virtualPort": "80",`
			`"sourcePort": "80",`
			`"ipList": "10.2.3.4;10.1.1.1"`
			`}`
			.

id	rule-00000001	String	ID of the forwarding rule
protocol	TCP	String	IP Protocol of the forwarding rule. Only TCP is supported.
virtualPort	80	Integer	Forwarding port
sourcePort	80	Integer	Real server port
ipList	10.2.3.4 ; 10.1.1.1	String	a list of the real server IPs. Up to 20 IPs allowed in each forwarding rule.

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` .

Parameter	Required	Type	Description
ruleId	Yes	String	ID of the forwarding rule

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
vip	Yes	String	IP of the Anti-DDoS Advanced instance
protocol	Yes	String	IP protocol of forwarding rules. Only TCP is supported
virtualPort	Yes	Integer	Forwarding port
sourcePort	Yes	Integer	Real server port
ipList	Yes	String	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
certType	No	Integer	Certificate type. Always enter 1
cert	No	String	Certificate content
privateKey	No	String	Certificate private key

Response Parameters

Parameter	Example	Type	Description
ruleId	rule-000001	String	ID of the forwarding rule

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` .

Parameter	Required	Type	Description
ruleId	Yes	String	ID of the forwarding rule
bgpId	Yes	String	Resource ID of Anti-DDoS Advanced instance
domain	Yes	String	Name of the pulic domain (accessible to the clients)
protocol	Yes	String	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` .
sourceType	Yes	Integer	Types of real servers 1: Domain name 2: IP
ipList	Yes	String	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
certType	No	Integer	Certificate type. Always enter 1

Parameter	Required	Type	Description
cert	No	String	Certificate content
privateKey	No	String	Certificate private key

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
paging.index	Yes	Integer	Page Index. 0: page 1.
paging.count	Yes	Integer	Number of results per page

Response Parameters

Parameter	Example	Type	Description
total	123	Integer	Number of forwarding rules that have been configured for the Anti-DDoS Advanced instance

Parameter	Example	Type	Description
transRules	[obj,...]	Array	Attack details. Elements: `{ ”id”: ”rule-00000001”, ”protocol”: ”http” ”domain”: ”www.qq.com”, ”sourceType”: 1/2, ”ipList”: ”10.2.3.4；10.1.1.1”, ”certType”: 1, ”cert”: ””, ”privateKey”: ””, ”status”: 1/2/3, ”ssl_id”: ”” }` .
id	rule-00000001	String	ID of the forwarding rule
protocol	http	String	IP Protocol of the forwarding rule The value can be `http`, `https` or `http/https`.
domain	www.qq.com	String	Public domain name (accessible to the clients)
sourceType	1 2	Integer	Types of real servers 1: Domain name 2: IP
ipList	10.2.3.4 ; 10.1.1.1	String	a list of IPs or domain names of the real server. IPs or domain names are returned according to the value of `sourceType`.
certType	1	Integer	Certificate type. Always 1.
cert		String	Certificate content
privateKey		String	Certificate private key
status	0 1 2	Integer	The status of forwarding rule configuration 0: Configured successfully 1: Configuring 2: Configuration failed
ssl_id		String	Optional

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` .

Parameter	Required	Type	Description
ruleId	Yes	String	ID of the forwarding rule
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance

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

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance

Response Parameters

Parameter	Example	Type	Description
whitelist	["URL list",...]	Array	Returns configured whitelist: `”whitelist”: [ ”http://www.website1.com/”, ”http://www.website2.com/” ]`

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
whitelist	Yes	Array	Whitelist: `”whitelist”: [ ”http://www.website1.com/”, ”http://www.website2.com/” ]`

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance
whitelist	Yes	Array	Whitelist: `"whitelist": [ "http://www.website1.com/", "http://www.website2.com/" ]`

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

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance

Response Parameters

Parameter	Example	Type	Description
whitelist	["URL list",...]	Array	Returns configured whitelist: `"whitelist": [ "10.1.1.1", "10.2.2.2" ]`

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	ID of the Anti-DDoS Advanced instance

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance

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` .

Parameter	Required	Type	Description
bgpId	Yes	String	Resource ID of the Anti-DDoS Advanced instance

blacklist	Yes	Array	Blacklist:
			`"blacklist": [`
			`"10.1.1.1",`
			`"10.2.2.2"`
			`]`

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:

```
{
”code”: 5100
}
```

Error Codes

Error Code	Description	Reason
4000	Invalid request parameter.	Required parameter is missing, or parameter value is in an incorrect format. For error message, see the "message" field in error description.
4100	Authentication failed	The failed authentication is usually caused by signature computing error. See Signature Method section in the document.
4101	Unauthorized access to the API.	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.
4102	Unauthorized access to the resource.	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.
4103	Unauthorized access to the resource the current API is working with.	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.

4104	Key does not exist.	The key used for the request does not exist. Verify it and try again.
4105	Token error.	Token error.
4106	MFA verification failed.	MFA verification failed.
4110	Other CAM authentication failed.	Other CAM authentication failed.
4300	Access denied.	Account is blocked or is not within the user range for the API.
4400	Quota exceeded.	The number of requests exceeded the quota limit. For more information, see the "Request Quota" section in the document.
4500	Replay attack	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.
4600	Unsupported protocol.	The protocol is not supported. The current API only supports HTTPS protocol and does not support HTTP protocol.
5000	Resource does not exist.	The instance corresponding to resource ID does not exist, or the instance has been returned, or another user's resource is accessed.
5100	Resource operation failed.	The operation performed on the resource failed. For error message, see the "message" field in error description. Try again later or contact customer service.
5200	Failed to purchase the resource.	The resource purchase failed. This is may be caused by unsupported instance configuration or insufficient resource.
5300	Insufficient balance.	User account has insufficient balance. Unable to purchase or upgrade the resource.
5400	The operation was successful on some resources.	The batch operation was successful on some resources. For more information, see the returned value of the method.
5500	User failed to pass identity	Resource purchase failed because the user failed to pass identity verification.

	verification.	
6000	Internal error with the server.	An internal error occurred with the server. Try again later or contact customer service.
6100	Not supported in the version.	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.
6200	API is unavailable.	The API is under maintenance and is unavailable. Please try again later.