Alibaba Cloud
Anti-DDoS Pro

New Anti-DDoS Pro Service

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility
of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to
works, products, images, archives, information, materials, website architecture,
website graphic layout, and webpage design, are intellectual property of Alibaba
Cloud and/or its affiliates. This intellectual property includes, but is not limited
to, trademark rights, patent rights, copyrights, and trade secrets. No part of the
Alibaba Cloud website, product programs, or content shall be used, modified
, reproduced, publicly transmitted, changed, disseminated, distributed, or
published without the prior written consent of Alibaba Cloud and/or its affiliates
. The names owned by Alibaba Cloud shall not be used, published, or reproduced
for marketing, advertising, promotion, or other purposes without the prior written
consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are
not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba
Cloud and/or its affiliates, which appear separately or in combination, as well as
the auxiliary signs and patterns of the preceding brands, or anything similar to
the company names, trade names, trademarks, product or service names, domain
names, patterns, logos, marks, signs, or special descriptions that third parties
identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⛔　Danger: Resetting will result in the loss of user configuration data.
⚠️	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	⚠️　Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
📋	This indicates warning information, supplementary instructions, and other content that the user must understand.	ⓘ　Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋　Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd / d  C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae  log  list  -- instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 Product Introduction

1.1 What is Anti-DDoS Pro

Anti-DDoS Pro provides BGP bandwidth resources to help you mitigate massive DDoS attacks peaking at 1 Tbit/s. Compared with older versions, Anti-DDoS Pro currently supports more reliable networks with less latency, enabling quicker disaster recovery.

Anti-DDoS Pro provides the following benefits:

· Maximum BGP bandwidth resources in mainland China. Supports mitigating 1.5 Tbit/s DDoS attacks.
· Top-quality bandwidth resources covering eight major ISP networks in mainland China, including China Telecom, China Unicom, China Mobile, and CERNET.

Only one IP address is needed to quickly access different ISP networks in mainland China.

Differences between older and current versions of Anti-DDoS Pro

	Older version (China Telecom, China Unicom, and China Mobile networks)	Older version (BGP-line)	Current version
ISP networks	Only supports China Telecom, China Unicom, and China Mobile networks.	Supports multiple small and medium-sized ISPs' networks in addition to China Telecom, China Unicom, and China Mobile networks.	Supports multiple small and medium-sized ISPs' networks in addition to China Telecom, China Unicom, and China Mobile networks.

	Older version (China Telecom , China Unicom, and China Mobile networks)	Older version (BGP-line)	Current version
Network latency	Average latency of 30 ms in mainland Chinese regions . Cross-network access may occur when using networks provided by small-sized ISPs.	Average latency of 20 ms in mainland Chinese regions. No cross-network access is needed.	Average latency of 20 ms in mainland Chinese regions. No cross-network access is needed.
Dedicated line	Not supported. Traffic is forwarded back to the origin server through public networks with latency.	If the origin server is deployed on Alibaba Cloud services, traffic is forwarded back to the origin server through dedicated lines with negligible latency. Otherwise, traffic is forwarded back to the origin server through public networks.	If the origin server is deployed on Alibaba Cloud services, traffic is forwarded back to the origin server through dedicated lines with negligible latency. Otherwise, traffic is forwarded back to the origin server through public networks.
Disaster recovery	When a server fault occurs, automatic scheduling of layer 4 traffic is not supported. Due to DNS resolution limits, automatic scheduling of layer 7 traffic cannot take effect immediately.	Supports automatic scheduling of all traffic based on BGP routing. The switchover time can be within several seconds.	Supports automatic scheduling of all traffic based on BGP routing. The switchover time can be within several seconds.

	Older version (China Telecom, China Unicom, and China Mobile networks)	Older version (BGP-line)	Current version
IP addresses	Needs more than two IP addresses, which require more configuration workload.	Needs only one IP address.	Needs only one IP address.
Maximum protection capability	Supports mitigating up to 1 Tbit/s DDoS attack based on China Telecom or China Unicom networks.	Supports mitigating up to 100 Gbit/s DDoS attacks.	Supports mitigating up to 1.5 Tbit/s DDoS attacks.
Layer 4 protection capability	Supports mitigating flood attacks such as SYN floods, ACK floods, and ICMP floods. Filters out abnormal requests, empty requests, and requests from zombies.	The same.	The same.
Layer 7 protection capability	Supports mitigating HTTP flood attacks.	Supports mitigating HTTP flood attacks.	Supports mitigating HTTP flood attacks.

Scenarios

We recommend that you use Anti-DDoS Pro if you have the following needs:

· Reliable networking that supports minimal latency, quick disaster recovery, and multiple ISP networks.

· Basic protection that offers 20 Gbit/s or more BGP bandwidth.

· Capability to mitigate DDoS attacks peaking at more than 300 Gbit/s.

2 Pricing

2.1 Billing methods

Anti-DDoS provides BGP bandwidth to help you mitigate 300+ Gbit/s DDoS attacks.

We recommend that you use Anti-DDoS Pro to minimize latency and safeguard the security of your business.

For more information about Anti-DDoS Pro, see *What is Anti-DDoS Pro*.

Basic protection (monthly subscription)

Protection capability (peak attack bandwidth)	Network	Price
30 Gbit/s	Eight BGP-line	USD 3,220 per month
60 Gbit/s	Eight BGP-line	USD 7,250 per month
100 Gbit/s	Eight BGP-line	Special offer: USD 50,880 per year
300 Gbit/s	Eight BGP-line	Special offer: USD 81,840 per year
400 Gbit/s	Eight BGP-line	Special offer: USD 149,880 per year
500 Gbit/s	Eight BGP-line	Special offer: USD 581,040 per year
600 Gbit/s	Eight BGP-line	Special offer: USD 691,560 per year
700 Gbit/s	Eight BGP-line	Special offer: USD 789,360 per year
800 Gbit/s	Eight BGP-line	Special offer: USD 884,160 per year
900 Gbit/s	Eight BGP-line	Special offer: USD 978,840 per year
1 Tbit/s	Eight BGP-line	Special offer: USD 1,073,640 per year

Flexible protection (Pay-As-You-Go daily plan)

Anti-DDoS Pro charges additional fees for flexible protection on a daily basis. The fee is determined by the difference between the peak attack bandwidth and the basic bandwidth.

> 📋 Note:
>
> If you set the burstable bandwidth and basic bandwidth to the same value, no additional fees will be charged and your Anti-DDoS Pro instance provides no flexible protection.

Assume that you have an Anti-DDoS Pro instance whose basic bandwidth is 30 Gbit/s and burstable bandwidth is 100 Gbit/s. On the same day, the instance experienced two DDoS attacks, whose maximum bandwidth reached 80 Gbit/s and 40 Gbit/s respectively. In above example, the peak attack bandwidth is 80 Gbit/s. The difference between the peak attack bandwidth and the basic bandwidth is 50 Gbit/s. According to the billing table below, Anti-DDoS Pro charges RMB 6,400 for flexible protection. The fee will be automatically generated in the morning of the following day.

Notes:

· No additional fee is charged if the peak attack bandwidth does not exceed the basic bandwidth.

· No additional fee is charged if the peak attack bandwidth exceeds the burstable bandwidth. This means if the Anti-DDoS Pro instance enters the black hole status, no additional fee is charged.

· The additional fee for the current day is usually generated between 8 am to 9 am the next day.

Bandwidth difference	Fees
0 Gbit/s < Bandwidth difference ⩽ 5 Gbit/s	USD 125 per day
5 Gbit/s < Bandwidth difference ⩽ 10 Gbit/s	USD 186 per day
10 Gbit/s < Bandwidth difference ⩽ 20 Gbit/s	USD 340 per day
20 Gbit/s < Bandwidth difference ⩽ 30 Gbit/s	USD 588 per day

Bandwidth difference	Fees
30 Gbit/s < Bandwidth difference ⩽ 40 Gbit/s	USD 756 per day
40 Gbit/s < Bandwidth difference ⩽ 50 Gbit/s	USD 1,000 per day
50 Gbit/s < Bandwidth difference ⩽ 60 Gbit/s	USD 1,210 per day
60 Gbit/s < Bandwidth difference ⩽ 70 Gbit/s	USD 1,430 per day
70 Gbit/s < Bandwidth difference ⩽ 80 Gbit/s	USD 1,650 per day
80 Gbit/s < Bandwidth difference ⩽ 100 Gbit/s	USD 1,830 per day
100 Gbit/s < Bandwidth difference ⩽ 150 Gbit/s	USD 2,260 per day
150 Gbit/s < Bandwidth difference ⩽ 200 Gbit/s	USD 3,350 per day
200 Gbit/s < Bandwidth difference ⩽ 300 Gbit/s	USD 4,340 per day
300 Gbit/s < Bandwidth difference ⩽ 400 Gbit/s	USD 6,200 per day
400 Gbit/s < Bandwidth difference ⩽ 500 Gbit/s	USD 7,740 per day
500 Gbit/s < Bandwidth difference ⩽ 600 Gbit/s	USD 9,290 per day
600 Gbit/s < Bandwidth difference ⩽ 700 Gbit/s	USD 10,840 per day
700 Gbit/s < Bandwidth difference ⩽ 800 Gbit/s	USD 12,390 per day
800 Gbit/s < Bandwidth difference ⩽ 900 Gbit/s	USD 13,930 per day
900 Gbit/s < Bandwidth difference ⩽ 1, 000 Gbit/s	USD 15,480 per day
1,000 Gbit/s < Bandwidth difference ⩽ 1, 100 Gbit/s	USD 17,030 per day

Bandwidth difference	Fees
1,100 Gbit/s < Bandwidth difference ⩽ 1, 200 Gbit/s	USD 18,580 per day
1,200 Gbit/s < Bandwidth difference ⩽ 1, 300 Gbit/s	USD 20,130 per day
1,300 Gbit/s < Bandwidth difference ⩽ 1, 400 Gbit/s	USD 21,670 per day
1,400 Gbit/s < Bandwidth difference ⩽ 1, 500 Gbit/s	USD 23,220 per day

2.2 Buy Anti-DDoS Pro instances

To buy an Anti-DDoS Pro instance, perform the following steps:

Procedure

1. Open the *Anti-DDoS Pro buy page*.

2. Select the Basic Bandwidth, Burstable Bandwidth, Ports, and Service Bandwidth based on your needs.

   · Basic Bandwidth: The minimum bandwidth provided by the Anti-DDoS Pro instance during protection. Your subscription fee is calculated based on the basic bandwidth and subscription duration.

   · Burstable Bandwidth: The maximum bandwidth provided by the Anti-DDoS Pro instance during protection. When the attack bandwidth exceeds the basic bandwidth, the burstable bandwidth is consumed to defend against the attack. Additional fees will be charged based on the difference between the peak attack bandwidth and basic bandwidth.

     Note:
     If you do not want to consume the burstable bandwidth, you can set the burstable bandwidth and basic bandwidth to the same value. No additional fees will be charged and the maximum bandwidth provided by the Anti-DDoS Pro instance equals the basic bandwidth.

   · Ports: The maximum number of forwarding ports the Anti-DDoS Pro instance can use during port forwarding.

   · Service Bandwidth: The maximum bandwidth provided by the Anti-DDoS Pro instance for normal requests when no attack is in progress.

3. Select the Duration and Quantity, and click Buy Now to make your payment.

Result

For more information about the billing methods, see *Billing methods*.

2.3 Upgrade Anti-DDoS Pro instance configurations

If your current Anti-DDoS Pro instance cannot meet your needs, you can always upgrade its configurations to increase the basic bandwidth, domains, ports, or service bandwidth in the Anti-DDoS Pro console.

Context

Currently, Anti-DDoS Pro allows you to increase the basic bandwidth, domains, ports , and service bandwidth during the upgrade. You need to pay additional fees for the increased capabilities. The new configurations immediately take effect after you make the payment.

> 📋 **Note:**
> You cannot decrease the basic bandwidth, domains, ports, or service bandwidth after the upgrade.

The price for the upgrades is calculated as follows:

· Domains: For each new domain, Anti-DDoS Pro charges USD 46.88 per month. This fee is calculated based on your remaining subscription time.

> 📋 **Note:**
> If your Anti-DDoS Pro instance is associated with 100 domains, Anti-DDoS Pro charges USD 35.16 per month for each domain over the 100 threshold.

· Ports: For each new port, Anti-DDoS Pro charges USD 7.81 per month. This fee is calculated based on your remaining subscription time.

· Service Bandwidth: For each Mbit/s of bandwidth, Anti-DDoS Pro charges additional USD 15.63 per month. This fee is calculated based on your remaining subscription time.

> 📋 **Note:**
> Anti-DDoS Pro offers different prices for different bandwidth usage. If your service bandwidth ranges from 100 Mbit/s to 600 Mbit/s, Anti-DDoS Pro charges USD 15.63 per month for each Mbit/s of bandwidth. If your service bandwidth is greater than 600 Mbit/s, Anti-DDoS Pro charges USD 11.72 per month for each Mbit/s of bandwidth over the 600 threshold.

Procedure

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Management > Instances, select an Anti-DDoS Pro instance, and click Upgrade.

3. On the Configuration Upgrade page, specify the basic bandwidth, domains, ports, and service bandwidth.

4. **Make your payment and the new configurations take effect immediately.**

3 Quick Start

3.1 Set up Anti-DDoS Pro to protect your business

After you purchase Anti-DDoS Pro instances, you need to set up your instances to protect your business.

You can set up Anti-DDoS Pro instances by using one of the following methods:

- *Set up Anti-DDoS Pro instances using domains*
- *Set up Anti-DDoS Pro instances using IPs and ports*

Set up Anti-DDoS Pro instances using domains

1. Log on to the *Anti-DDoS Pro console*.

   In the left-side navigation pane, choose Management > Instances to view your Anti-DDoS Pro instances.

Instance	Line	IP Address	Date	Protection ⓘ	Actions
ID: ddoscoo-cn-78v12b12e003 Name: -- ☑ Plan: Insurance Plan Normal Bandwidth : 100M	Eight-line BGP ⓘ	203 ▦▦ ▦	Purchase Date:2019-3-29 Expiration Date:2019-4-30	Status : ● Normal Protected Ports: 0 (Maximum: 5) ☑ Protected Domains: 0 (Maximum: 10) ☑ Available Advanced Mitigations in this Month:2 📑	Renew Upgrade View Reports

2. Choose Management > Websites and click Add Domain.

   > 📋 **Note:**
   >
   > To set up Anti-DDoS Pro instances to protect your business, you only need to configure your domain in the Anti-DDoS Pro console.

3. You need to configure the following parameters:

Parameter	Description
Domain	Enter the domain name of your website.
Protocol	Select the protocols supported by your website. By default, `HTTP` and `HTTPS` are selected. 📋 Note: If your website supports HTTPS encrypted connections, you must select `HTTPS`. Select other protocols if applicable.
Server Address	Select the address type of the origin server and specify the address. · If `Origin Server IP` is selected, you can enter up to 20 IP addresses. When multiple origin server IPs are specified, Anti-DDoS Pro uses IP hash load balancing to forward traffic back to the origin server. · If you want to use Anti-DDoS Pro and WAF together for enhanced protection, you can select `Origin Server Domain` and enter the CNAME provided by your WAF instance.

Parameter	Description
Server Port/ Forwarding Port	The system automatically sets the ports based on the protocols you have selected. You cannot modify these parameters. · When `HTTP` or `Websocket` is selected, the port of the origin server is 80 by default. · When `HTTPS` or `Websockets` is selected, the port of the origin server is 443 by default. The forwarding port is the same as the port of the origin server.
Select Anti-DDoS Pro Instance	Select Anti-DDoS Pro instances based on your needs. Note: For each domain, you can select up to eight Anti-DDoS Pro instances.

4. Click Add to go to the Modify DNS Records page. Change the DNS records of your domain to forward incoming traffic to the IP addresses of selected Anti-DDoS Pro instances.

Note:
Anti-DDoS Pro currently does not generate CNAME records. After you verify that Anti-DDoS Pro instances can forward traffic to the origin server, you need to change A record values to the IP addresses of these Anti-DDoS instances through your DNS provider. This forwards incoming traffic to these Anti-DDoS Pro instances.

Before you modify DNS records to forward incoming traffic to Anti-DDoS Pro, we recommend that you verify that Anti-DDoS Pro instances can forward traffic back to your origin server. For more information about testing domain configurations, see *Test domain configurations*.

5. Click Next to view the back-to-origin IP addresses that Anti-DDoS Pro instances use to forward traffic back to the origin server.

If you are using additional firewalls to protect the origin server, disable the firewalls or add the back-to-origin IP addresses used by Anti-DDoS Pro instances to the whitelist. After you forward incoming traffic to Anti-DDoS Pro, Anti-DDoS Pro instances filter your traffic and use these back-to-origin IP addresses to forward

traffic back to the origin server. If you do not add these back-to-origin IP addresses to the whitelists of your firewalls, your traffic may be mistakenly blocked, causing service interruptions.

After you add a domain to Anti-DDoS Pro, the system automatically generates forwarding rules for the Anti-DDoS Pro instances you have selected. Your traffic is forwarded based on these rules.

· If the forwarding port is 80, the system automatically generates a rule that forwards traffic on TCP port 80 to the origin server. The rule is not generated if the same rule already exists.

· If the forwarding port is 443, the system automatically generates a rule that forwards traffic on TCP port 443 to the origin server. The rule is not generated if the same rule already exists.

You cannot edit or delete rules that are automatically generated by the system. These rules are automatically deleted when the domains to which these rules apply are no longer associated with the Anti-DDoS Pro instances.

You can create rules to forward traffic on TCP port 80 or 443 only when these rules are automatically deleted from the Anti-DDoS Pro instances.

Set up Anti-DDoS Pro instances using IPs and ports

1. Log on to the *Anti-DDoS Pro console*.

   In the left-side navigation pane, choose Management > Instances to view your Anti-DDoS Pro instances.

2. Choose Management > Port Settings, select an Anti-DDoS Pro instance, and click Create Rule.

   Note:

   To set up Anti-DDoS Pro instances to protect your business, you only need to configure forwarding rules in the Anti-DDoS Pro console.

3. You need to configure the following parameters:

Parameter	Description
Forwarding Protocol	Specify the forwarding protocol used by the origin server. Valid values: `TCP` and `UDP` .
Forwarding Port	Specify the port that the Anti-DDoS Pro instance uses to forward traffic. 📋 **Note:** We recommend that you keep the forwarding port the same as the port of the origin server.
Origin Server Port	Specify the port of the origin server.
Origin Server IP	Specify the IP address of the origin server. 📋 **Note:** You can enter up to 20 IP addresses for load balancing.

4. Click Complete.

After a forwarding rule is generated, you can configure session persistence, health check, and Anti-DDoS protection policies based on your needs. For more information, see documents on *session persistence*, *health check*, and *Anti-DDoS protection policies*.

5. Change the service IP to the IP address of the Anti-DDoS Pro instance. This forwards incoming traffic to Anti-DDoS Pro.

   Before you forward incoming traffic to Anti-DDoS Pro, we recommend that you verify that the Anti-DDoS Pro instance can forward traffic back to your origin server. For more information about testing port forwarding, see *Test forwarding rules*.

4 User Guide

4.1 Use NS records to set up Anti-DDoS Pro

To set up Anti-DDoS Pro to protect your business, you must modify the DNS records of your domain to forward incoming traffic to your Anti-DDoS Pro instances. If your domain is managed by Alibaba Cloud DNS, you can enable NS Mode Access to automatically modify DNS records. Otherwise, you can only manually modify DNS records through your DNS provider. This topic describes how to enable NS Mode Access in the Anti-DDoS Pro console.

Prerequisites

Your domain is managed under a paid version of Alibaba Cloud DNS. Otherwise, you cannot enable NS Mode Access. We recommend that you *activate a paid version of Alibaba Cloud DNS*.

Context

NS Records are nameserver records. You can use NS records to specify which DNS server is used to resolve your domain name.

Anti-DDoS Pro supports two modes when you enable NS Mode Access: Anti-DDoS Pro and Back-to-Origin.

· The Anti-DDoS Pro mode automatically modifies DNS records to forward incoming traffic to your Anti-DDoS Pro instances.
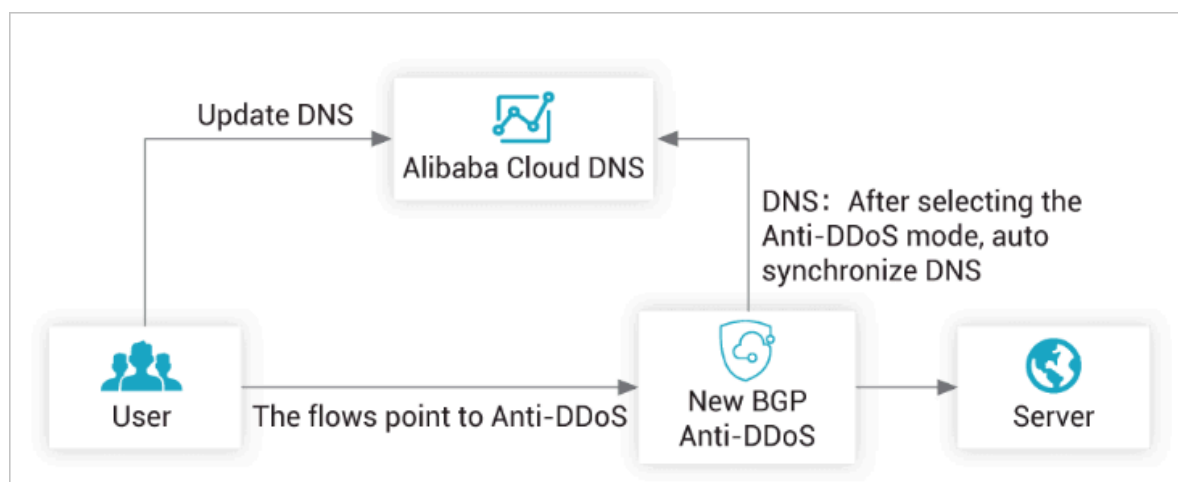
· The Back-to-Origin mode automatically synchronizes DNS records between Anti-DDoS Pro instances and Alibaba Cloud DNS. Incoming traffic is still directed to your origin server.
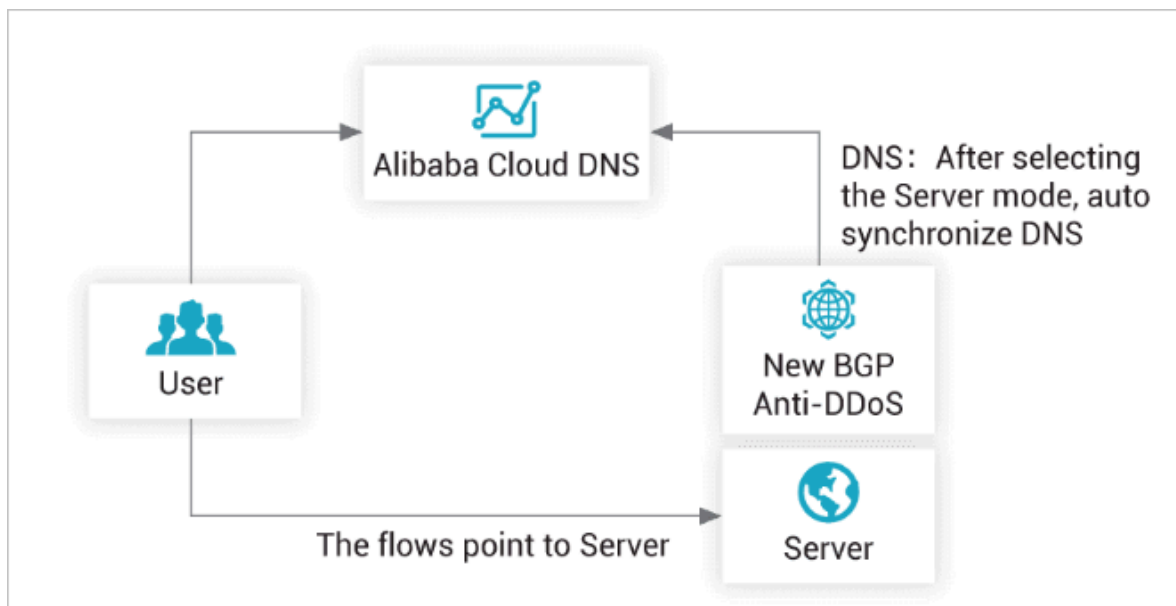
We recommend that you use the following steps to enable NS Mode Access. If you cannot enable NS Mode Access, you must manually change the DNS records of your domain through your DNS provider.

To forward incoming traffic to Anti-DDoS Pro, you need to change A record values to the IP addresses of your Anti-DDoS Pro instances.

Procedure

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Management > Websites.

3. Select your domain and click Configure DNS Settings.

4. Enable NS Mode Access.

   Note:

> **If you are not using a paid version of Alibaba Cloud DNS, an error message appears when you enable NS Mode Access.**

5. Select the `Anti - DDoS  Pro` or `Back - to - Origin` mode based on your needs.

   · When the `Anti - DDoS  Pro` mode is selected, Anti-DDoS Pro automatically modifies the DNS records at Alibaba Cloud DNS so that incoming traffic is directed to your Anti-DDoS Pro instances.

   · When the `Back - to - Origin` mode is selected, DNS records are automatically synchronized between Anti-DDoS Pro and Alibaba Cloud DNS. Incoming traffic is still directed to your origin server.

6. After the configuration is complete, you can use DNS testing tools to verify whether the configuration works as expected.

4.2 Configure layer 4 protection

4.2.1 Configure layer 4 anti-DDoS protection settings

Anti-DDoS Pro supports protection against layer 4 DDoS attacks and provides multiple protection settings to safeguard the security of your business.

Context

Anti-DDoS Pro provides protection against DDoS attacks based on `IPs` and `ports` when no domain names are provided. You can set limits on parameters such as the request rate, and packet length to mitigate DDoS attacks.

Anti-DDoS Pro supports the following anti-DDoS protection settings for you to choose from:

📋 Note:

The New Connection Speed Limits for Source IP setting supports the automatic protection mode. If the automatic protection mode is selected, Anti-DDoS Pro dynamically calculates the limit on the number of new connections per second from a single source IP. If the manual mode is selected, you need to manually specify the limit on the new connection rate.

Settings	Description
False Sources	Detects and blocks false source IPs. This setting is only applicable to TCP rules.
Null Session Connections	Detects and blocks null session connections. This setting is only applicable to TCP rules.
New Connection Speed Limits for Source IP	The maximum number of new connections per second from a single source IP. All new connections exceeding the limit are discarded. The actual limit on the new connection rate may be slightly different because the protection servers are deployed in clusters.
Concurrent Connection Speed Limits for Source IP	The maximum number of concurrent connections from a single source IP. All connections exceeding the limit are discarded.
New Connection Speed Limits for Destination IP	The maximum number of new connections per second to a single destination IP and port. All new connections exceeding the limit are discarded. The actual limit on the new connection rate may be slightly different because the protection servers are deployed in clusters.
Concurrent Connection Speed Limits for Destination IP	The maximum number of concurrent connections to a single destination IP and port. All connections exceeding the limit are discarded.
Packet Length Filtering	The limit on the payload size of a packet. Unit: byte. All packets exceeding the size limit are discarded.

You can configure anti-DDoS protection settings for specific ports on specific IP addresses.

📋 Note:

Anti-DDoS protection settings take effect for single ports.

Procedure

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Management > Port Settings, select an Anti-DDoS Pro instance and forwarding rule, and click Configure under the Anti-DDoS Protection Policy column.
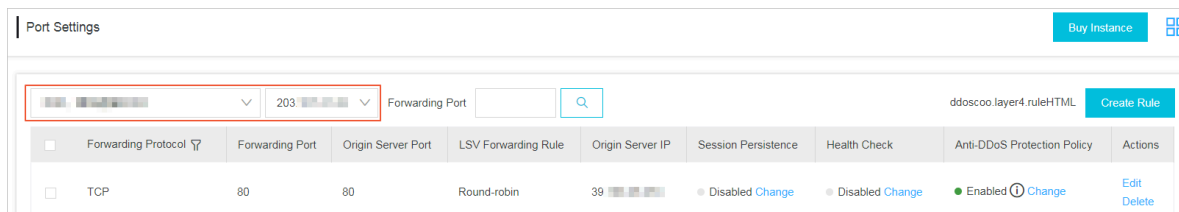
3. In the Anti-DDoS Protection Policy dialog box, configure Anti-DDoS protection settings for the selected IP and port.
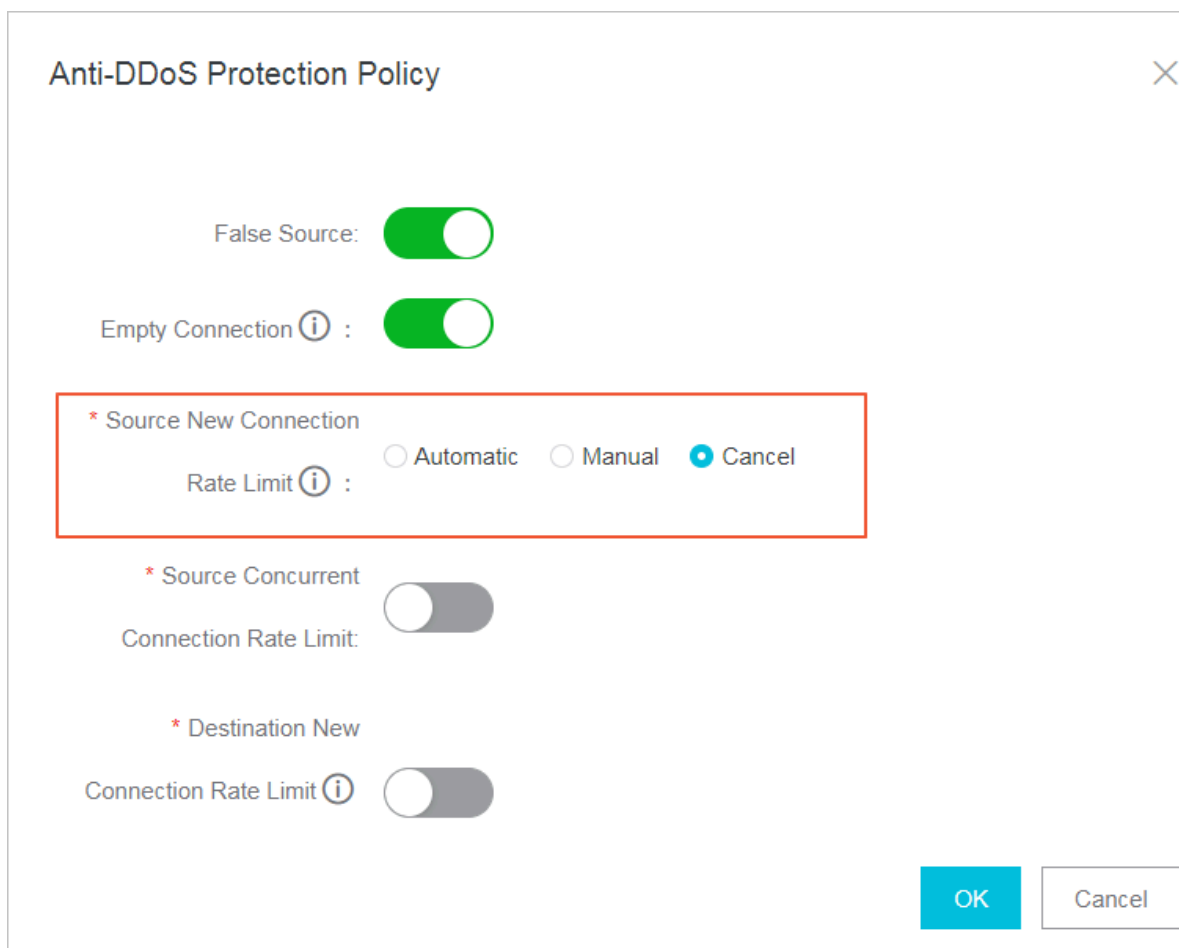
4.2.2 Configure layer 4 smart defense settings

Anti-DDoS Pro provides the smart defense feature to help you defend against layer 4 DDoS attacks. This feature supports three modes for you to choose from. You can

change the smart defense mode based on your needs. Once changed, the selected mode takes effect within a few minutes.

The smart defense feature supports the following modes:

· Low: This mode automatically identifies and scrubs traffic that displays common attack patterns based on historical traffic patterns and years of experience defending against Web attacks. The mode is based on an algorithm that automatically identifies malicious IP addresses and adds them to the blacklist. This mode may not be able to block all layer 4 floods but has a low false positive rate.

· Normal: This mode automatically identifies and scrubs traffic that displays common and likely attack patterns based on historical traffic patterns and years of experience defending against Web attacks. We recommend that you use this mode in most situations as it maintains an optimal balance between protection and false positives.

· Strict: This mode provides the most rigorous protection against ongoing attacks based on historical traffic patterns and years of experience defending against Web attacks. The mode may cause false positives.

The normal mode is enabled by default. Smart defense bases its decisions on historical traffic pattern data. If this is the first time that you have set up Anti-DDoS Pro to protect your business, it takes Anti-DDoS Pro about three days to learn your traffic pattern in order to provide the best protection.

You can view or delete the IP addresses that are automatically added to the blacklist by smart defense. You can also manually add other malicious IP addresses to the blacklist. Meanwhile, you can add specific IP addresses to the whitelist so that Anti-DDoS Pro allows access to these IP addresses without further inspection.
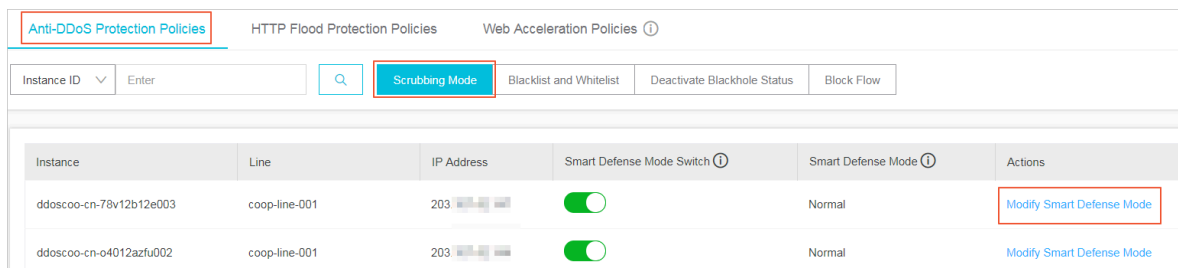
Change smart defense modes

After you buy an Anti-DDoS Pro instance, the smart defense feature is enabled and the normal mode is used by default. You can change smart defense modes based on your needs.

1. Log on to the *Anti-DDoS Pro console*.

2. Choose Protection > Protection Settings > Anti-DDoS Protection Policies > Scrubbing Mode, select an Anti-DDoS Pro instance, and click Modify Smart Defense Mode.

> **Note:**
>
> The smart defense feature is enabled by default. You can click the switch to disable smart defense.

3. Change the smart defense mode based on your needs and click OK.

> **Note:**
>
> The selected mode takes effect within a few minutes.

Manage the blacklist and whitelist

You can view and manage the IP addresses that are added to the blacklist by smart defense. You can also add specific IP addresses to the whitelist so that Anti-DDoS Pro allows access to these IP addresses without further inspection.

· **The blacklist**

Choose Protection > Protection Settings > Anti-DDoS Protection Policies > Blacklist and Whitelist, click Blacklist, and select Anti-DDoS Pro to view and manage all IP addresses in the whitelist under the instance.

 Note:

Each IP address in the blacklist has an expiration time. An IP address is automatically removed from the blacklist when its expiration time is reached. Smart defense automatically specifies an expiration time when it adds an IP address to the blacklist. The expiration time ranges from 5 minutes to 1 hour. If a blacklisted IP address continuously sends malicious requests before the expiration time is reached, Anti-DDoS Pro automatically extends the expiration

time. You also need to specify an expiration time when you manually add an IP address to the blacklist.

You can perform the following operations on the blacklist:

- Search by keyword: Enter a keyword in the search box and click the search icon to search for specific IP addresses in the blacklist.

- Download: Click Download to download all blacklisted IP addresses to your local computer.

- Clear Blacklist: Click Clear Blacklist to remove all blacklisted IP addresses.

- Manually Add: Click Manually Add to manually add IP addresses to the blacklist. You need to specify an expiration time for each IP address.

Note:

You can manually add up to 2,000 IP addresses to the blacklist.

· The whitelist

Choose Protection > Protection Settings > Anti-DDoS Protection Policies > Blacklist and Whitelist, click Whitelist, and select an Anti-DDoS Pro instance to manage the whitelist under the instance.

> **Note:**
>
> The IP addresses in the whitelist can only be removed manually. The whitelist has a higher priority over the blacklist. If an IP address is already listed in the whitelist, this IP address cannot be added to the blacklist.

You can perform the following operations on the whitelist:

- Search by keyword: Enter a keyword in the search box and click the search icon to search for specific IP addresses in the whitelist.
- Download: Click Download to download all whitelisted IP addresses to your local computer.
- Clear Whitelist: Click Clear Whitelist to remove all whitelisted IP addresses.
- Manually Add: Click Manually Add to manually add IP addresses to the whitelist.

> **Note:**
>
> You can add up to 500 IP addresses to the whitelist.

4.3 Configure layer 7 protection

4.3.1 Configure HTTP flood protection

Anti-DDoS Pro provides four protection modes to help you defend against HTTP flood attacks.

· Normal: The default HTTP flood protection mode. We recommend that you use this mode when the traffic pattern on your website is normal.

This mode defends against typical HTTP flood attacks and does not block normal requests.

· Emergency: You can enable this mode when you notice HTTP response errors, traffic anomalies, or CPU and memory usage spikes.

The emergency mode provides relatively rigorous protection. This mode can defend against more complicated flood attacks, but may mistakenly block a small number of normal requests.

· Strict: This mode provides rigorous protection against HTTP flood attacks. The mode uses captcha verification to verify the identity of all visitors. Only verified visitors are allowed to access the site.

> **Note:**
> The strict mode is built on a verification mechanism that verifies whether the request is sent from a browser by a real user. If this mode is enabled for API services and native applications, false positives may occur, disrupting the availability of your service.

· Super Strict: This mode provides the most rigorous protection against HTTP flood attacks. The mode uses captcha verification to verify the identity of all visitors. Only verified visitors are allowed to access the site.

Compared with the strict mode, this mode combines captcha verification with anti-debugging techniques to enhance the protection of your site.

> **Note:**
> The super strict mode is built on a verification mechanism that verifies whether the request is sent from a browser by a real user. In very rare situations, a browser error may occur and cause service interruptions. Users only need to restart the browser to resolve this issue. However, if this mode is enabled for API services and native applications, false positives may occur, disrupting the availability of your service.

Procedure

By default, normal HTTP flood protection is used. You can change protection modes based on your needs.

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Management > Websites, select a domain, and click Protection Settings.

3. In the HTTP Flood Protection area, select a protection mode.

> 📋 **Note:**
>
> You can click Status to disable HTTP flood protection.

Custom rules

The HTTP flood protection feature also allows you to create custom rules to defend against HTTP flood attacks. You can add custom rules to protect specific URLs.

On the Protection Settings page, find the HTTP Flood Protection area and enable custom rules. You can then click Change Settings to create custom rules.

Best practices for HTTP flood protection

The protection effects provided by different protection modes are as follows: Super Strict > Strict > Emergency > Normal. The chances of false positives when using these protection modes are as follows: Super Strict > Strict > Emergency > Normal.

In normal situations, we recommend that you use the normal HTTP flood protection mode to protect your site. This mode only blocks IP addresses that frequently send requests to your website. We recommend that you enable the emergency or strict mode when your website is overwhelmed by flood attacks and the normal protection mode fails to protect your site.

> **Note:**
>
> For API services and native applications, you cannot use the strict or super strict mode because false positives are likely to occur. You can instead create custom rules to protect specific URLs from flood attacks.

4.3.2 Configure the blacklist and whitelist

Anti-DDoS Pro allows you to configure a blacklist and whitelist to control access to your domain.

- You can use the whitelist to allow access to a list of IPs and CIDR blocks without further inspection.
- You can use the blacklist to deny access to a list of IPs and CIDR blocks.

> **Note:**
>
> The configurations of the blacklist and whitelist are effective for single domains, not Anti-DDoS Pro instances. For each domain, you can add up to 200 entries in the blacklist and whitelist respectively. You can enter either IP addresses or CIDR blocks in the blacklist and whitelist.

To block IPs that send a large number of malicious requests to your server, you can add them to the blacklist. Meanwhile, you can add internal CIDR blocks, service interface IPs, and verified IPs to the whitelist so that requests from these IPs are not blocked.

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Management > Websites, select a domain, and click Protection Settings.

3. In the Blacklist and Whitelist area, click Change Settings.

> **Note:**
> To configure the blacklist or whitelist, you must enable HTTP flood protection.

- · Click the Blacklist tab, enter the IP addresses or CIDR blocks that you want to block, and click OK.
- · Click the Whitelist tab, enter the IP addresses or CIDR blocks that you want to allow access to, and click OK.

> **Note:**
> You can enter up to 200 entries in the blacklist and whitelist respectively. Each entry can be an IP address or CIDR block. Separate multiple entries with commas (,).

> **Note:**
> - · The blacklist and whitelist feature is only available in domain configurations.

- The configurations of the blacklist and whitelist take effect immediately after creation.

  (!) Notice:

  In some situations, it may take a few minutes for the configurations to take effect. If the configurations of the blacklist and whitelist do not take effect immediately, wait a few minutes.

- You can add 0.0.0.0/0 to the blacklist, which blocks requests from all IP addresses except the ones listed in the whitelist.

- Once created, the configurations of the blacklist and whitelist are effective for all Anti-DDoS Pro instances that are associated with the specified domain.

4.3.3 Deactivate the black hole status

After your website is configured in Anti-DDoS Pro, incoming traffic to your site is forwarded to a black hole when the attack bandwidth exceeds your basic or burstable bandwidth. To restore your service, you can deactivate the black hole status in the Anti-DDoS Pro console. Each user can deactivate the black hole status up to five times every day.

Context

To avoid activating a black hole multiple times, we recommend that you increase your basic or burstable bandwidth before you deactivate the black hole status.

Procedure

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Protection > Protection Settings.

3. Click Anti-DDoS Protection Policies and select Deactivate Black Hole.

   📋 Note:

   - Each user can deactivate the black hole status up to five times every day. This quota is reduced by one each time the black hole status is successfully lifted.

   - When you deactivate the black hole status for the first time that day, the black hole status is immediately lifted. When you deactivate the black hole status

consecutively, the time interval between each operation must be no less than 10
minutes.

Anti-DDoS Protection Policies	HTTP Flood Protection Policies	Web Acceleration Policies ⓘ				
Instance ID ∨ ddoscoo-cn-78v12b12e003 Q	Scrubbing Mode	Blacklist and Whitelist	Deactivate Blackhole Status	Block Flow		
					You have 5 time(s) remaining to deactivate the blackhole state (5 time(s) in total)	
Instance Info	ISP Line	Service Address	Status	Automatic Deactivated Time		Action
ddoscoo-cn-78v12b12e003	coop-line-001	203▮▮▮▮	Normal	--		

4. Select the Anti-DDoS Pro instance that is in black hole status. Check the time
   before the black hole status is automatically lifted. You can also click Deactivate
   under the Actions column to manually deactivate the block hole status.

   · The black hole status is a risk management strategy used by the backend
     services of Alibaba Cloud. Attempts to deactivate the black hole status may fail
     , which does not reduce your quota for manually deactivating the block hole
     status. If an attempt to deactivate the black hole status fails, an error message
     appears. You can try to deactivate the black hole status later.

   · If the message "Cannot deactivate the black hole status due to risk management.
     Wait 10 minutes and try again." appears, please wait and try again later.

   · If no error message appears, the black hole status is lifted. You can refresh the
     page to check if network access is restored.

4.3.4 Block traffic flow

Anti-DDoS Pro allows you to block overseas traffic transmitted through China
Telecom and China Unicom networks. Overseas traffic is any traffic originating from
countries and regions outside mainland China. Each user can block overseas traffic
up to 10 times and unblock traffic at any time.

Context

We recommend that you block overseas traffic when your service is suffering DDoS
attacks and the attack bandwidth is likely to exceed your burstable bandwidth. If
overseas traffic accounts for 30% of the attack bandwidth, you can block overseas
traffic to quickly bring the attacks under control.

Once blocked, overseas traffic is discarded at the Anti-DDoS scrubbing center. This
lowers the chance of triggering a black hole when the Anti-DDoS Pro instance is
overwhelmed by attack traffic. Anti-DDoS Pro takes multiple factors into account
when it comes to activating a black hole, such as the attack bandwidth and the source

of the attack traffic. Blocking overseas traffic can to some degree reduce the chance of triggering a black hole.

Procedure

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Protection > Protection Settings.

3. On the Anti-DDoS Protection Policies page, click Block Flow.
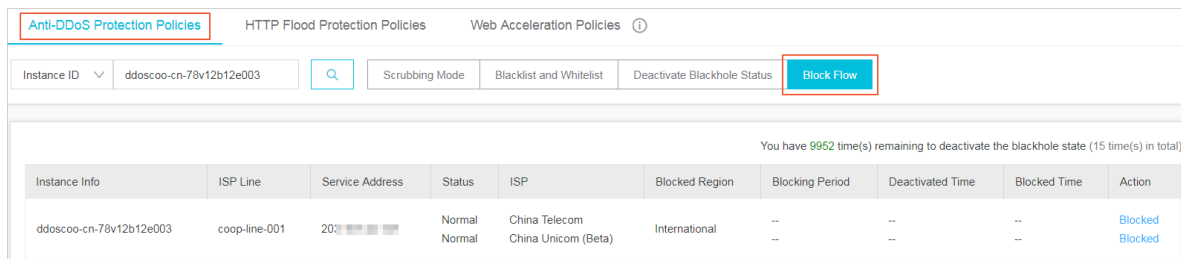
4. Select the Anti-DDoS Pro instance and network type, and click Block.
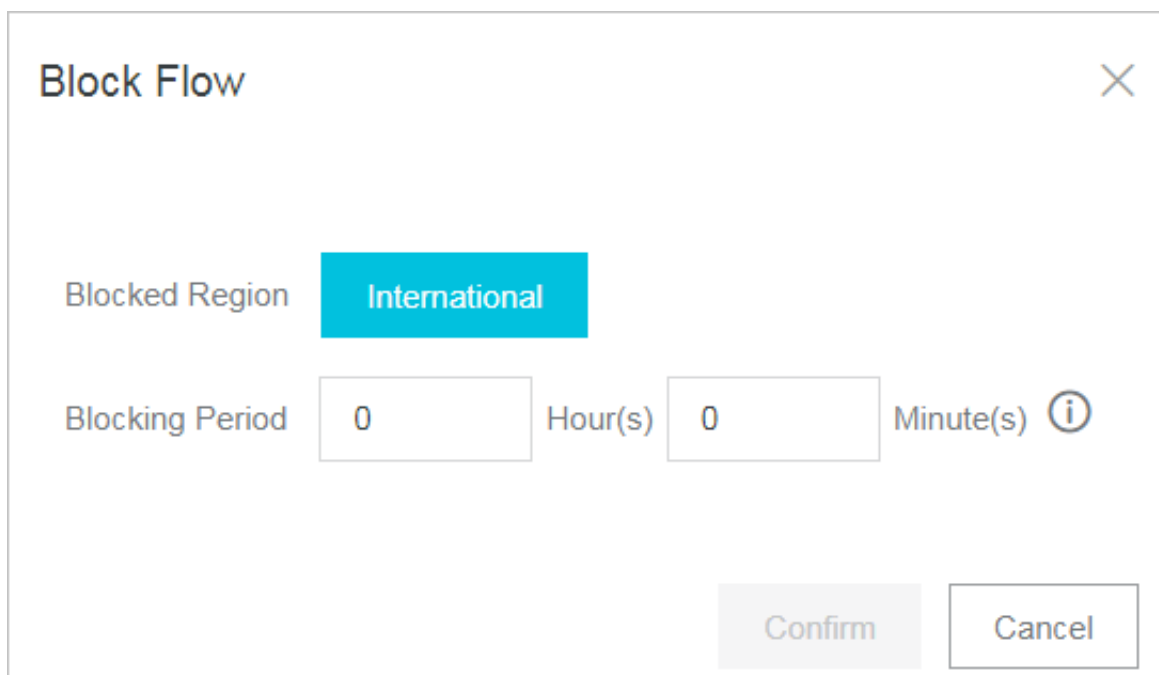
> 📋 **Note:**
>
> · You can block overseas traffic transmitted through China Telecom and China Unicom networks. We recommend that you block traffic transmitted through China Telecom networks first and observe the trend of attacks. If the attack bandwidth is still increasing, you can then block traffic transmitted through China Unicom networks.
>
> · Each user can block overseas traffic up to 10 times. This quota is reduced by one each time you block traffic transmitted through China Telecom or China Unicom networks.

5. In the Block Traffic Flow dialog box, select the blocked region and the blocking duration, and click Confirm. Currently, you can only select the international region.

> 📋 **Note:**

The blocking duration can range from 15 minutes to 23 hours and 59 minutes.

Block Flow   ✕

Blocked Region   [International]

Blocking Period   [0] Hour(s)   [0] Minute(s) ⓘ

[Confirm]   [Cancel]

6. Click Confirm.

   · If an error occurs when blocking overseas traffic, an error message appears. Resolve the issue and try again later.

   · If no error message appears, overseas traffic is blocked. Refresh the page and you can find the blocked region and blocking duration. The block button is replaced by Unblock. To immediately unblock traffic, click Unblock under the Actions column.

4.3.5 Change the IP of an ECS instance

If your origin server IP is exposed, we recommend that you deploy your service on an ECS instance to prevent attackers from bypassing Anti-DDoS Pro and hacking into your server. You can change IPs of ECS instances up to 10 times in the Anti-DDoS Pro console.

Context

📋 Note:
You can only change public IPs of ECS instances that are connected to classic networks.

Procedure

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Management > Websites.

3. Click Change ECS IP.

> ⓘ **Notice:**
>
> When you change the IP of an ECS instance, your service deployed on the instance is interrupted for a few minutes. We recommend that you back up your data in advance.

4. You must stop an ECS instance if you want to change its IP address. If the target ECS instance is stopped, go to step 6. In the Change ECS IP dialog box, click Go to ECS to stop the target ECS instance in the ECS console.

   a) In the instances list, select the target ECS instance and click its instance ID.

   b) On the instance details page, click Stop in the upper-right corner.

   c) Select a stop method and click OK.

   > ⓘ **Notice:**
   >
   > To stop the instance, you must pass SMS verification.

   d) Wait until the target ECS instance is Stopped.

5. Return to the Change ECS IP dialog box, enter the ID of the target ECS instance, and click Next.

6. Make sure you have selected the right ECS instance and click Release IP.

7. After the original IP address is released, click Next and the system assigns a new IP address to the instance.

8. Click OK.

> 📋 **Note:**
>
> After you change the IP of an ECS instance, configure Anti-DDoS Pro to protect the instance and make sure the new IP address is not exposed to the public.

4.4 New protection policies

4.4.1 New protection policies

Anti-DDoS Pro provides the following new features to help you defend against HTTP flood attacks: Geo-blocking, Accurate Access Control, and Intelligent Protection. Meanwhile, Web Acceleration is now available to speed up your website.

> **Note:**
>
> Currently, new protection policies are in beta testing until May 31, 2019.

Enable new protection policies

During the beta testing period, HTTP flood protection policies only include two features by default: Blacklist and Whitelist, and HTTP Flood Protection.

To start using new protection policies, perform the following steps:

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Protection > Protection Settings, select your domain, and click Try out New Protection Policies.

3. In the dialog box that appears, read the note and click OK.

> **Note:**
>
> · After you start using the new protection policies, your Anti-DDoS Pro instance uses a new CIDR block to forward traffic back to your origin server. If you have configured access control policies on your origin server, make sure to add the new CIDR block to the whitelist.
>
> · To switch back to the old protection policies, click Old Version on the Protection Settings page.
>
> · The new protection policies only support strong cipher suites. Before you switch to the new protection policies, make sure your cipher suite is supported. For more information, see *Cipher suites supported by the new protection policies*.

Introduce new protection policies

After you switch to new protection policies, refresh the Protection Settings page and you will see the following new features: Geo-blocking, Accurate Access Control, Intelligent Protection, and Web Acceleration Policies.

- Geo-blocking: This feature enables you to block traffic based on geographical location. Chinese regions are divided into 34 provincial regions and international regions are divided into 7 continents. The Anti-DDoS scrubbing center directly discards traffic originating from blocked regions.

- Accurate Access Control: This feature allows you to customize access control rules to filter requests based on the client IP, request URL, and common HTTP header fields, such as the referer, user-agent, and parameter. You can handle matching requests with different actions, such as clear, block, and challenge.

- Intelligent Protection: Based on a big data analysis engine, this feature can analyze your traffic patterns to preemptively detect and block DDoS attacks.

- Web Acceleration Policies: Integrated with Web caching techniques, this feature uses the scrubbing center to speed up your site and protect it from DDoS attacks You can add custom rules to cache specific URLs. Meanwhile, you can select from two cache modes:

  - Standard: Only caches static files on the page, such as .css, .js, and .txt files.

  - Enhanced: Caches all contents on the page.

> **Note:**
>
> When the beta testing period ends, the configurations of the new protection policies remain effective. You can only enable or disable new features but not change the configurations. To change configurations, you need to buy the new features.

Cipher suites supported by the new protection policies

New protection policies support the following cipher suites:

- "ECDHE-ECDSA-AES256-GCM-SHA384"
- "ECDHE-RSA-AES256-GCM-SHA384"
- "ECDHE-ECDSA-AES128-GCM-SHA256"
- "ECDHE-RSA-AES128-GCM-SHA256"
- "ECDHE-ECDSA-WITH-CHACHA20-POLY1305"
- "ECDHE-RSA-WITH-CHACHA20-POLY1305"
- "ECDHE-RSA-AES256-CBC-SHA"
- "ECDHE-RSA-AES128-CBC-SHA"
- "ECDHE-ECDSA-AES256-CBC-SHA"
- "ECDHE-ECDSA-AES128-CBC-SHA"

4.5 View security reports

After you set up Anti-DDoS Pro to protect your business, you can find statistics about your traffic and protection status in the Anti-DDoS Pro console.

Procedure

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Security Reports.

   · On the Service page, select an Anti-DDoS Pro instance and port, and specify a time range to view the inbound and outbound bandwidth, trends, and connections to your service.

   > **Note:**
   > You can query traffic and connection data for up to 30 days.
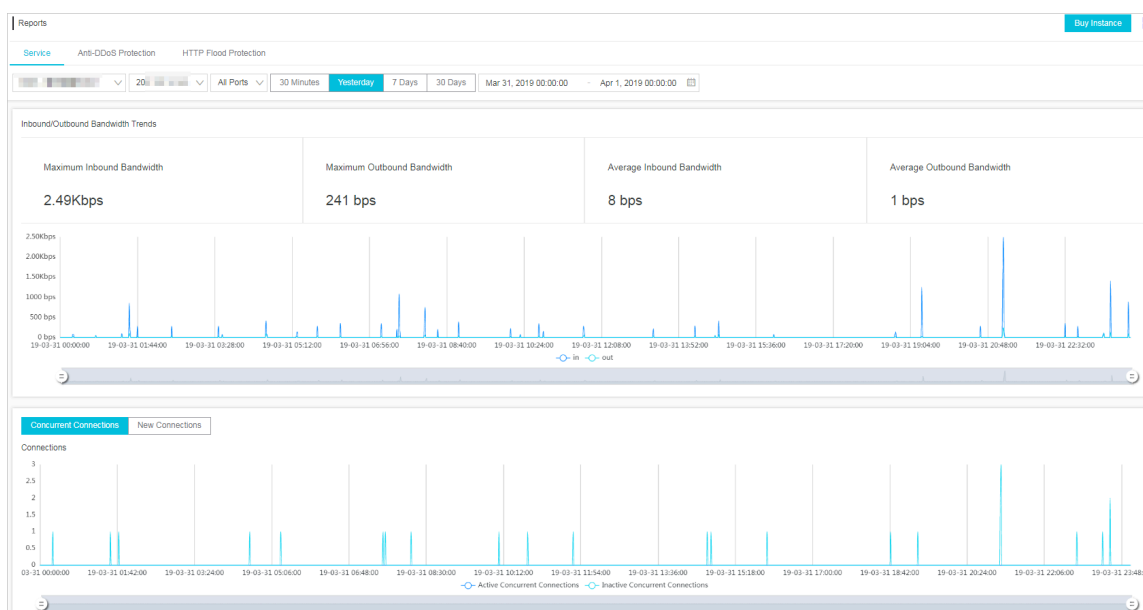
   You can drag the slider to quickly change time ranges.

   · On the Anti-DDoS Protection page, select an Anti-DDoS Pro instance and specify a time range to view the traffic trends to your site and information about DDoS attacks.

   > **Note:**

You can query traffic data and DDoS attacks for up to 30 days.
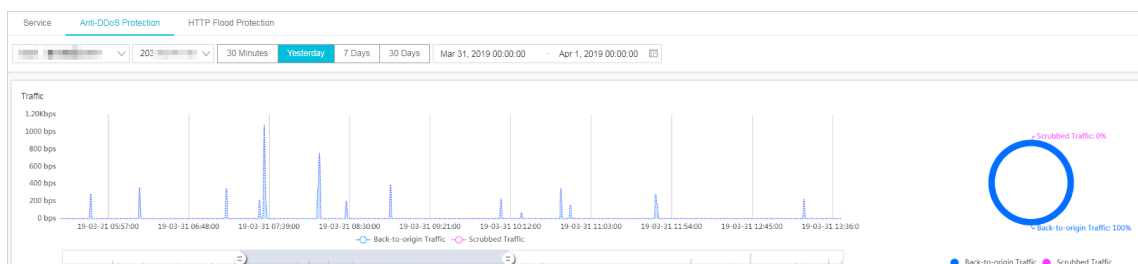
Note:

Anti-DDoS Pro automatically filters out abnormal packets, for example, SYN packets, packets with invalid flags, and invalid TCP packets. This helps save server resources. Incoming traffic is scrubbed when abnormal packets are detected. This is why scrubbed traffic appears in the traffic chart when the traffic bandwidth to your server does not reach the scrubbing threshold.

· On the HTTP Flood Protection page, select a domain and specify a time range to view the trend of requests and information about HTTP flood attacks.

Note:

You can query request data and HTTP flood attacks for up to 30 days.

4.6 Log queries

4.6.1 Full log

Alibaba Cloud Anti-DDoS Pro is now integrated with Log Service to provide real-time analysis and reports of access and attack logs.

The *APNIC DDoS threat landscape in 2017* states that more than 80% of DDoS attacks are combined with HTTP flood attacks, which can be difficult to detect. Hence, it is important to analyze access logs in real time to identify attack behaviors and apply a suitable protection policy in a timely manner.

After you set up Anti-DDoS Pro for your website, Log Service starts to collect access logs and attack logs in real time. You can query and analyze log data collected by Anti-DDoS Pro, and the results are displayed as easy-to-read dashboards.

Activate the full log service

Perform the following steps to activate the Anti-DDoS Pro full log service:

> 📋 **Note:**
>
> The Anti-DDoS Pro full log service is in the open beta phase. The open beta will end on April 30, 2019. During the open beta phase, full log retains log data of up to 3 TB for 30 days for free. If you want to continue using the full log service after the open beta, you will be billed based on storage specifications.

1. Log on to the *Anti-DDoS Pro console*. In the left-side navigation pane, choose System > Full Log. Click Enable Now to go to the *full log service purchase page*.

2. Select a storage capacity and a service duration based on your business needs.

   · Log Storage: the log storage capacity. Unit: TB.

     When the log storage capacity you purchase is full, new logs cannot be stored. We recommend that you monitor the remaining log storage space and expand the storage space preemptively.

   · Duration: the validity period of the full log service.

     After the full log service expires, new logs cannot be stored. If you do not renew the full log service within seven days after it expires, all log data will be automatically deleted.

   > 📋 **Note:**
   >
   > If the full log service has sufficient storage capacity while it is valid, it will store the logs of 180 consecutive days starting from the day the full log service is enabled. Logs from day 181 will overwrite the logs from day 1. Logs from subsequent days will overwrite logs from the next earliest dates. Therefore, with sufficient storage capacity, only full logs of the last 180 days are stored.

   Example of how to select a log storage capacity

   Typically, each request log occupies about 2 KB of storage space. If the average request volume of your business is 500 queries per second (QPS), the storage space required for one day is: 500 x 60 x 60 x 24 x 2 = 86,400,000 KB (82 GB). The default storage period is 180 days. To store logs of the last 180 days, you need to select a log storage capacity of 14,832 GB (14.5 TB).

3. Click Buy Now and complete the payment.

After the full log service is activated, you can go to the Log Service page and click Details to view the service specifications.

> 📋 **Note:**
>
> We recommend that you monitor the remaining log storage space and validity period during use. When the utilization of the log storage capacity reaches 70%, expand the log storage capacity to make sure that new logs can be stored.

Enable the full log service

To enable the full log service for your protected website domain in Anti-DDoS Pro, perform the following steps:

1. Log on to the *Anti-DDoS Pro console*. In the left-side navigation pane, choose System > Full Log.

2. Click Enable Now. Follow the on-screen prompts to authorize Anti-DDoS Pro to store logs in your dedicated logstore.

3. On the Full Log page, select the target domain and turn on Status to enable full log for the selected domain.

After you enable full log, you can query and analyze the collected logs in real time, view and edit dashboards, and set monitoring alerts on the Full Log page.

Scenarios

Anti-DDoS Pro full log is applicable to the following scenarios:

· Troubleshoot website access problems

After Anti-DDoS Pro full log is enabled for your website, you can query and analyze the logs collected from your website in real time. You can use SQL statements to analyze the access logs on your website. This allows you to quickly troubleshoot and analyze access problems, and view information about read/write latency and the distribution of ISPs.

For example, the following statement can be used to view access logs on your website:

```
__topic__ :  DDoS_acces  s_log
```

· Track HTTP flood attack sources

Access logs record information about the sources and distribution of HTTP flood attacks. You can query and analyze access logs in real time to identify the origins of attacks, and use this information to select the most effective protection strategy.

- For example, the following statement can be used to analyze the geographical distribution of HTTP flood attacks:

```
__topic__ : DDoS_acces  s_log   and   cc_blocks  >  0 |  SELECT
   ip_to_coun  try ( if ( real_clien  t_ip ='-',  remote_add  r ,
real_clien  t_ip ))  as   country ,  count ( 1 )  as  " number   of
   attacks "  group   by   country
```

- For example, the following statement can be used to view PVs:

```
__topic__ : DDoS_acces  s_log  |  select   count ( 1 )  as   PV
```

· Analyze website operations

Access logs record information about website traffic in real time. You can use SQL queries to analyze log data and better understand your users. For example, you can identify the most visited web pages, the source IP addresses of the clients, the browsers that initiated the requests, and the distribution of client devices, which can help you analyze website operations.

For example, the following statement can be used to view the distribution of traffic by ISP:

```
__topic__ : DDoS_acces  s_log  |  select   ip_to_prov  ider ( if (
real_clien  t_ip ='-',  remote_add  r ,  real_clien  t_ip ))  as
provider ,  round ( sum ( request_le  ngth )/ 1024 . 0 / 1024 . 0 ,
3 )  as   mb_in   group   by   provider   having   ip_to_prov  ider (
if ( real_clien  t_ip ='-',  remote_add  r ,  real_clien  t_ip )) <>
''  order   by   mb_in   desc   limit   10
```

4.6.2 Fields

In Anti-DDoS Pro, each log entry consists of a wide variety of fields.

You can query and analyze log data on the Full Log page. Field details are as follows:

Field	Description	Example
__topic__	The topic of the log entry. Default value: ddos_acces s_log. You cannot change this value.	-
body_bytes_sent	The size of the request body. Unit: byte.	2
content_type	The content type of the body of the request.	application/x-www-form-urlencoded
host	The domain of the origin server.	api.abc.com
http_cookie	The request cookie.	k1=v1;k2=v2
http_referer	The referer of the request. If this field is empty, - is displayed.	http://xyz.com
http_user_agent	The user agent of the request.	Dalvik/2.1.0 (Linux; U; Android 7.0; EDI-AL10 Build/HUAWEIEDISON-AL10)
http_x_forwarded_for	The originating IP addresses, including the IP addresses of the client and proxy servers.	-
https	Whether the request is an HTTPS request. · true: The request is an HTTPS request. · false: The request is an HTTP request.	true
matched_host	The domain or wildcard subdomain in the request that matches the domain of the origin server. If no match is found, - is displayed.	*.zhihu.com

Field	Description	Example
real_client_ip	The actual IP address of the client. If the actual IP address is unavailable, `-` is displayed.	1.2.3.4
isp_line	The network informatio n, such as BGP, China Telecom, and China Unicom.	China Telecom
remote_addr	The client IP address.	1.2.3.4
remote_port	The client port number.	23713
request_length	The length of the request. Unit: byte.	123
request_method	The HTTP request method.	GET
request_time_msec	The time of the request. Unit: milliseconds.	44
request_uri	The request path.	/answers/377971214/ banner
server_name	The domain name in the request. If this field is empty, `default` is displayed.	api.abc.com
status	The HTTP status code.	200
time	The time when the log entry is written.	2018-05-02T16:03:59+08:00
cc_action	The action that is used to handle the request, such as none, challenge, pass, close, captcha, wait, login, and n.	close

Field	Description	Example
cc_blocks	Whether the request is blocked by HTTP flood protection. · `1` : The request is blocked. · Otherwise, the request is accepted. 📋 Note: In some situations, this field may not exist. The `last_resul t` field indicates whether the request is blocked by HTTP flood protection.	1
last_result	Whether the request is blocked by HTTP flood protection. · ok: The request is accepted. · failed: The request fails verification or is blocked. 📋 Note: In some situations, this field may not exist. The `cc_blocks` field indicates whether the request is blocked by HTTP flood protection.	failed
cc_phase	The HTTP flood protection policy that is used, such as seccookie, server_ip_ blacklist, static_whitelist , server_header_blacklist , server_cookie_blacklist, server_args_blacklist, and qps_overmax.	server_ip_blacklist

Field	Description	Example
ua_browser	The browser that initiated the request. 📋 **Note:** In some situations, this field may not exist.	ie9
ua_browser_family	The browser type. 📋 **Note:** In some situations, this field may not exist.	internet explorer
ua_browser_type	Whether the browser is a Web browser, mobile browser, or other. 📋 **Note:** In some situations, this field may not exist.	web_browser
ua_browser_version	The browser version. 📋 **Note:** In some situations, this field may not exist.	9.0
ua_device_type	The type of the client device. 📋 **Note:** In some situations, this field may not exist.	computer
ua_os	The operating system of the client device. 📋 **Note:** In some situations, this field may not exist.	windows_7

Field	Description	Example
ua_os_family	The family of the operating system. 📋 Note: In some situations, this field may not exist.	windows
upstream_addr	The list of back-to-origin addresses. The format is `IP : Port`. Multiple addresses are separated by commas (,).	1.2.3.4:443
upstream_ip	The actual back-to-origin IP address.	1.2.3.4
upstream_response_time	The response time when the request is forwarded back to the origin server. Unit: seconds.	0.044
upstream_status	The HTTP status when the request is forwarded back to the origin server.	200
user_id	The Alibaba Cloud account ID.	12345678
querystring	The request string.	token=bbcd&abc=123

4.7 Anti-DDoS packages

Anti-DDoS Pro provides anti-DDoS packages as a value-added service to help you reduce the cost of defending against DDoS attacks.

What is an anti-DDoS package

In most scenarios, when the bandwidth during a DDoS attack exceeds the basic bandwidth provided by your Anti-DDoS Pro instance, the burstable bandwidth is consumed or the black hole is triggered if you set the burstable bandwidth and basic bandwidth to the same value.

· If your service survived the attack after the burstable bandwidth is consumed, additional fees will be charged based on the difference between the peak attack

> bandwidth and basic bandwidth. Click here to view *billing methods*. This method involves increased cost to maintain the security of your service.
>
> · If you set the burstable bandwidth and basic bandwidth to the same value, when the attack bandwidth exceeds the basic bandwidth, the black hole is triggered and your service is interrupted till the black hole status is lifted. This method may affect the performance of your service but does not incur additional fees.

Anti-DDoS packages can help you defend against DDoS attacks when the attack bandwidth exceeds the basic bandwidth without incurring any additional cost. Each anti-DDoS package has two parameters: bandwidth and available protections. For example, if an anti-DDoS package has 300 Gbit/s bandwidth and 3 available protections,

- · you can use this anti-DDoS package to offset the fees incurred from defending against attacks whose maximum bandwidth reaches the sum of 300 Gbit/s and your basic bandwidth. If the attack bandwidth is greater than the sum of 300 Gbit/s and your basic bandwidth, you cannot use this anti-DDoS package to offset additional fees. Based on the *billing methods*, additional fees may be charged to your account.

- · you can use this anti-DDoS package to offset additional fees up to three times. Each time you use an anti-DDoS package, it is valid for the entire day.

Notes

Note the following details when you use anti-DDoS packages:

- · Anti-DDoS packages do not improve the protection capability of Anti-DDoS Pro. You can only use anti-DDoS packages to offset the fees incurred by consuming burstable bandwidth. The protection capability of Anti-DDoS Pro is dependent on the basic and burstable bandwidth settings.

  We recommend that users who have anti-DDoS packages increase the burstable bandwidth so that you can actually take advantage of anti-DDoS packages. You

can set the burstable bandwidth to the sum of the basic bandwidth and anti-DDoS package bandwidth.

For example, if your basic bandwidth is 30 Gbit/s and you have an anti-DDoS package with 300 Gbit/s bandwidth, we recommend that you set the burstable bandwidth to 330 Gbit/s.
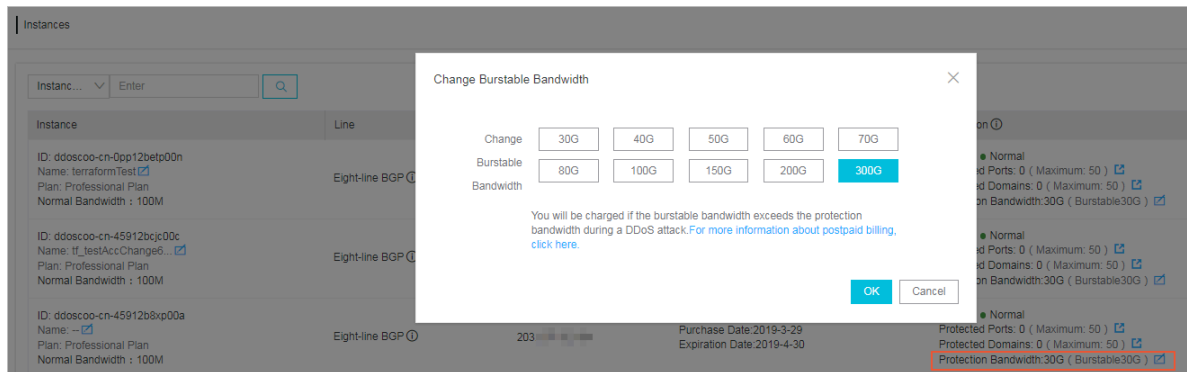
· You can only use anti-DDoS packages to offset additional fees when the peak attack bandwidth is no greater than the sum of the basic bandwidth and anti-DDoS package bandwidth.

· When the number of available protections of your anti-DDoS package is reduced to zero, we recommend that you set the burstable bandwidth to the same as the basic bandwidth to avoid additional fees.

· You can only use anti-DDoS packages to offset additional fees that are billed no earlier than the day you obtained the anti-DDoS packages.

Table 4-1: Differences between current and older versions of anti-DDoS packages

Item	Older version	Current version
Conditions of use	Must be associated with Anti-DDoS Pro instances.	No need to be associated with Anti-DDoS Pro instances. The anti-DDoS package that has the shortest expiration time is automatically used.
Intended use	Offset additional fees that are incurred from defending against attacks whose maximum bandwidth is no greater than the anti-DDoS package bandwidth.	Offset additional fees that are incurred from defending against attacks whose maximum bandwidth is no greater than the sum of the anti-DDoS package bandwidth and your basic bandwidth.

How to obtain anti-DDoS packages

Currently, anti-DDoS packages are provided to qualified users as a value-added service. If you meet one of the following conditions, you can contact customer service to obtain anti-DDoS packages for free:
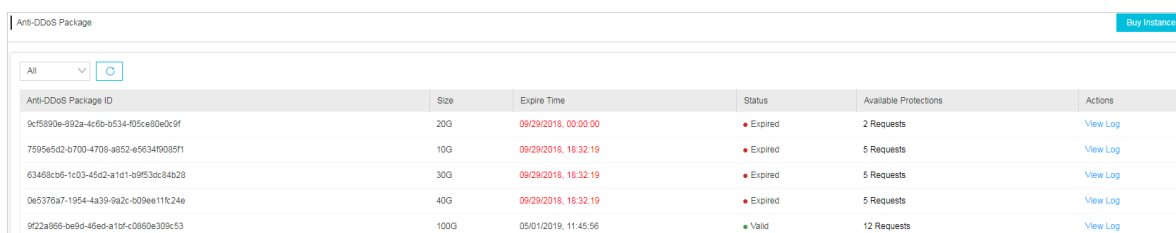
· It is the first time that you activated Anti-DDoS Pro.

· You have been continuously using Anti-DDoS Pro for three months or more.

· You have purchased a yearly subscription.

How to use anti-DDoS packages

Anti-DDoS packages are automatically applied when DDoS attacks trigger protection policies. You can view records of your anti-DDoS packages in the Anti-DDoS Pro console. Anti-DDoS packages are only valid when they are not expired, and the number of available protections is larger than zero.

You can view the records of your anti-DDoS packages using the following steps:

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Management > Anti-DDoS Package to view all anti-DDoS packages.

   · Anti-DDoS Package ID: The unique identifier of the anti-DDoS package.

   · Size: The bandwidth of the anti-DDoS package.

   · Expire Time: The expiration time of the anti-DDoS package.

   · Status: The anti-DDoS package status, including valid, exhausted, and expired.

   · Available Protections: The number of times you can use the anti-DDoS package.

Anti-DDoS Package ID	Size	Expire Time	Status	Available Protections	Actions
9cf5890e-892a-4c6b-b534-f05ce80e0c9f	20G	09/29/2018, 00:00:00	● Expired	2 Requests	View Log
7595e5d2-b700-4708-a852-e5634f9085f1	10G	09/29/2018, 18:32:19	● Expired	5 Requests	View Log
63468cb6-1c03-45d2-a1d1-b9f53dc84b28	30G	09/29/2018, 18:32:19	● Expired	5 Requests	View Log
0e5376a7-1954-4a39-9a2c-b09ee11fc24e	40G	09/29/2018, 18:32:19	● Expired	5 Requests	View Log
9f22a866-be9d-46ed-a1bf-c0860e309c53	100G	05/01/2019, 11:45:56	● Valid	12 Requests	View Log

3. Select an anti-DDoS package and click View Log under the Actions column to view logs about the anti-DDoS package.

4.8 Import and export configurations

Anti-DDoS Pro provides batch import and export features to help you quickly download or migrate domain configurations and forwarding rules.

· You can import and export layer 4 forwarding rules in TXT files.

· You can import and export domain configurations in XML files, which offer better compatibility. The XML format also provides better readability and extensibility than the TXT format. Meanwhile, you can import and export the configurations of websites that only have their origin server domain names specified.

Batch import domain configurations

1. Log on to the *Anti-DDoS Pro console*.

2. In the left-side navigation pane, choose Management > Websites and click Batch Domains Import at the end of the website list to add multiple domain configurations.

3. In the Add Multiple Rules dialog box that appears, enter the configuration parameters in XML format.

Note:

You can copy and paste the contents of the text box.

XML format

Each XML file must start with `< DomainList >` and end with `</ DomainList >`. You must enter all domain configurations between these tags. Each domain configuration must start with `< DomainConf  ig >` and end with `</ DomainConf  ig >`. You must enter all parameters of a domain between these tags. For more information about these parameters, see the following table.

> 📋 **Note:**
>
> Each domain configuration corresponds to a `< DomainConf  ig >`…… `</ DomainConf  ig >` tag pair.

XML parameter	Description
`< Domain > a . com </ Domain >`	The domain to be configured. You can only enter one domain.
`< ProtocolCo  nfig >< ProtocolLi st > http , https </ ProtocolLi st ></ ProtocolCo  nfig >`	The Web protocols used by the domain . Separate multiple protocols with commas (,). In this example, the protocols used by the domain are HTTP and HTTPS.

`< InstanceCo  nfig >< InstanceLi  st > ddoscoo - cn - 4590lwcny0  01 </ InstanceLi  st ></ InstanceCo  nfig >`	The Anti-DDoS Pro instance that is configured for the domain. 📋 **Note:** **Each Anti-DDoS Pro instance has only one IP address. You can just enter the instance ID. Separate multiple instance IDs with commas (,).**
`< RealServer  Config >< ServerType > 0 </ ServerType >< ServerList > 1 . 2 . 3 . 4 </ ServerList ></ RealServer  Config >`	Information about the origin server . · `< ServerType > 0 </ ServerType  >` indicates that the IP address of the origin server is specified. · `< ServerType > 1 </ ServerType  >` indicates that the domain of the origin server is specified. `< ServerList > 1 . 2 . 3 . 4 </  ServerList >` indicates the address of the origin server. Separate multiple addresses with commas (,). 📋 **Note:** **For each domain, you can only specify either the IP address or the domain of the origin server as the address of the origin server.**

Sample

```
< DomainList >
 < DomainConf  ig >
 < Domain > a . com </ Domain >
 < ProtocolCo  nfig >
 < ProtocolLi  st > http , https </ ProtocolLi  st >
 </ ProtocolCo  nfig >
 < InstanceCo  nfig >
 < InstanceLi  st > ddoscoo - cn - 4590lwcny0  01 </ InstanceLi  st
 >
 </ InstanceCo  nfig >
 < RealServer  Config >
 < ServerType > 0 </ ServerType >
 < ServerList > 1 . 2 . 3 . 4 </ ServerList >
 </ RealServer  Config >
 </ DomainConf  ig >
 < DomainConf  ig >
 < Domain > b . com </ Domain >
 < ProtocolCo  nfig >
 < ProtocolLi  st > http , websocket , websockets </ ProtocolLi  st
 >
```

```
</ ProtocolCo  nfig >
< InstanceCo  nfig >
< InstanceLi  st > ddoscoo - cn - mp90oeort0  02 , ddoscoo - cn -
0pp0o5vz50  0d </ InstanceLi  st >
</ InstanceCo  nfig >
< RealServer  Config >
< ServerType > 1 </ ServerType >
< ServerList > q840a82zf2  j23afs . gfvip05al . com </ ServerList >
</ RealServer  Config >
</ DomainConf  ig >
</ DomainList >
```

4. Click Next. If the XML file is correctly formatted, the domain configurations you have entered are displayed.

5. Select the domain configurations you want to import and click OK to import these domain configurations.

Batch export domain configurations

1. In the left-side navigation pane, choose Management > Websites and click Batch Domains Export at the end of the website list. In the dialog box that appears, click OK to export domain configurations.

2. On the Websites page, click the button in the upper-right corner to view the progress of the export task.
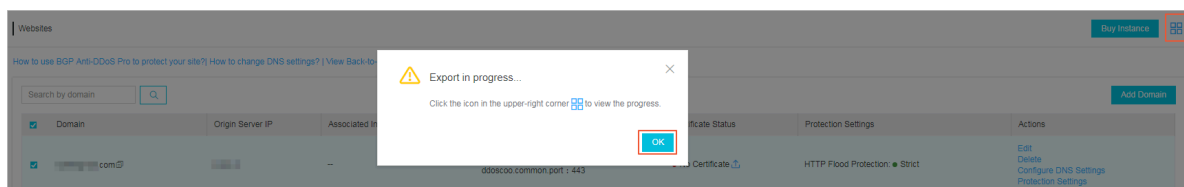
3. After the task is complete, click Download in the Tasks dialog box to download domain configurations to your local computer.

📋 **Note:**

If the task status is Pending Export, wait for the task to complete.

Batch import forwarding rules

1. In the left-side navigation pane, choose Management > Port Settings and click
   Batch Operations at the end of the rules list. Choose Create Rule to configure
   multiple forwarding rules.

   Note:

You can also choose Session Persistence/Health Check or DDoS Protection Policy Settings to add corresponding settings.

2. **Follow the given examples to enter rules.**

   · **Create forwarding rules**

   · **Create session persistence/health check settings**

   · **Create anti-DDoS protection policies**

3. **Click OK to add settings.**

Batch export forwarding rules

1. In the left-side navigation pane, choose Management > Port Settings and click
   Batch Export at the end of the rules list. Choose Export Rule and click OK to export
   forwarding rules.

   > **Note:**
   >
   > You can also choose Export Session/Health Settings or Export Anti-DDoS
   > Protection Policy to export corresponding settings.
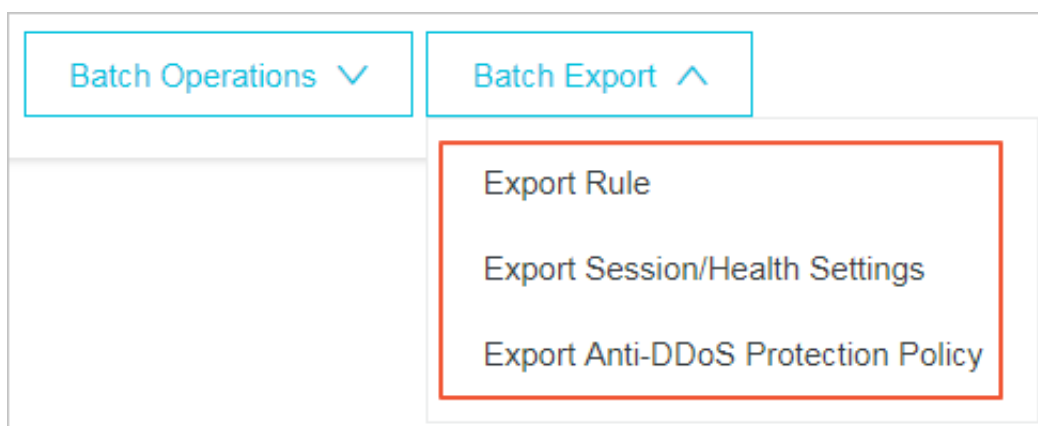
2. On the Port Settings page, click the button in the upper-right corner to view the
   progress of the export task.

3. After the task is complete, click Download in the Tasks dialog box to download
   forwarding rules to your local computer.

   > **Note:**
   >
   > If the task status is Pending Export, wait for the task to complete.

5 Managed Security Service

Anti-DDoS Pro provides free one-on-one consulting services to help you make full use of the features and benefits offered by Anti-DDoS Pro.

Context

If you have any issues using Anti-DDoS Pro, join the Anti-DDoS Pro consulting group in DingTalk through the Anti-DDoS Pro console.

Our experienced security professionals will aid you in resolving your issues in a timely manner.

Procedure

1. Log on to the *Anti-DDoS Pro console*.

2. Click the Technical Support icon, open the DingTalk app on your phone, and scan the QR code to join the Anti-DDoS Pro consulting group.

> **Note:**
> You can find the Technical Support icon in the lower left-side navigation pane.
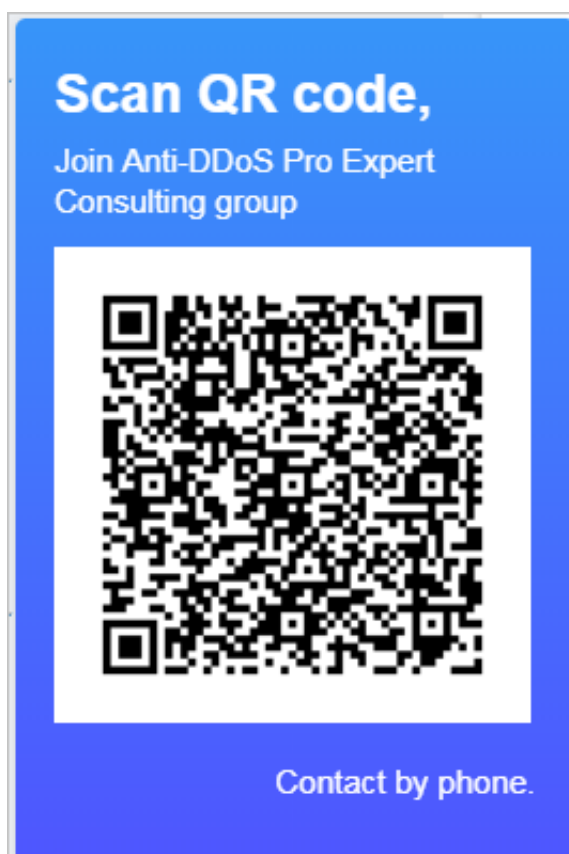
3. After you join the DingTalk group, our security professionals will provide you with one-on-one assistance to help you resolve any issues regarding Anti-DDoS Pro.

> **Note:**
>
> You can also click Contact by phone and leave your contact number. Security professionals will contact you as soon as possible.

6 API Reference

6.1 API overview

This topic summarizes all callable Anti-DDoS Pro APIs. For more information about each API, see the corresponding topics.

For more information about API resources, visit *API Explorer*.

Instances

API	Description
DescribeInstances	Query all instances.
ReleaseInstance	Release instances.
DescribeInstanceDetails	Query instance details.
DescribeInstanceSpecs	Query instance configurations.
DescribeInstanceStatistics	Query rules configured on instances.
DescribeElasticBandwidthSpec	Query the burstable bandwidth of instances.
ModifyElasticBandWidth	Modify the burstable bandwidth of instances.
ModifyInstanceRemark	Modify the remarks on instances.

Layer 4 rules

API	Description
CreateLayer4Rule	Create layer 4 forwarding rules.
ConfigLayer4Rule	Edit layer 4 forwarding rules.
DeleteLayer4Rule	Delete layer 4 forwarding rules.
ConfigLayer4RuleAttribute	Configure the attributes of layer 4 forwarding rules, including session persistence and anti-DDoS protection policies.
ConfigHealthCheck	Configure layer 4 or layer 7 health check.
DescribeLayer4Rules	Query layer 4 forwarding rules.

DescribeLayer4RuleAttributes	Query the attributes of layer 4 forwarding rules, including session persistence and anti-DDoS protection policies.
DescribeHealthCheckList	Query layer 4 or layer 7 health check settings.
DescribeHealthCheckStatusList	Query health check status.

Layer 7 rules

API	Description
DescribeDomains	Query layer 7 forwarding rules.
CreateLayer7Rule	Create layer 7 forwarding rules.
ConfigLayer7Rule	Edit layer 7 forwarding rules.
DeleteLayer7Rule	Delete layer 7 forwarding rules.
ConfigLayer7Cert	Configure certificates.
ConfigLayer7BlackWhiteList	Configure the blacklist and whitelist.
DescribleLayer7InstanceRelations	Query instances by domain.
DescribleCertList	Query certificates.
EnableLayer7CC	Enable layer 7 HTTP flood protection.
DisableLayer7CC	Disable layer 7 HTTP flood protection.
EnableLayer7CCRule	Enable layer 7 HTTP flood protection rules.
DisableLayer7CCRule	Disable layer 7 HTTP flood protection rules.
AddLayer7CCRule	Add layer 7 HTTP flood protection rules.
ConfigLayer7CCRule	Edit layer 7 HTTP flood protection rules.
DescribeLayer7CCRules	Query layer 7 HTTP flood protection rules.
DeleteLayer7CCRule	Delete layer 7 HTTP flood protection rules.
ConfigLayer7CCTemplate	Set the mode of layer 7 HTTP flood protection.
DescribeDomainAccessMode	Query the modes that are used to set up instances.

ConfigDomainAccessMode	Configure the modes that are used to set up instances.
DescribeBackSourceCidr	Query back-to-origin CIDR blocks.

Tasks

API	Description
ListAsyncTask	Query asynchronous tasks.
CreateAsyncTask	Create asynchronous tasks.
DeleteAsyncTask	Delete asynchronous tasks.

Logs

API	Description
DescribeOpEntities	Query operation logs.

6.2 Use the API

When an API call is made, an HTTP GET request is sent to the endpoint of the API. You need to specify request parameters in the request. A response is then returned in reply to the request. The request and response are encoded using the UTF-8 character set.

Request structure

Anti-DDoS Pro APIs support RPC-type Web services. You can send HTTP GET requests to make API calls.

The request structure is as follows:

```
https :// Endpoint /? Action = xx & Parameters
```

In the example:

- `Endpoint` indicates the endpoint of Anti-DDoS Pro APIs. The current endpoint is `ddoscoo . cn - hangzhou . aliyuncs . com .`
- `Action` indicates the action that you want to perform. For example, you can call `DescribeIn  stances` to perform queries on all Anti-DDoS Pro instances.
- `Version` indicates the version of the API. The current version of Anti-DDoS Pro APIs is `2017 - 12 - 28 .`

- `Parameters` indicates the request parameters. Separate multiple parameters with ampersands (&).
- Request parameters consist of common parameters and API specific parameters. Common parameters include variables such as the API version and credentials. For more information, see *Common parameters*.

The following example calls the DescribeInstances operation to perform queries on Anti-DDoS Pro instances:

> **Note:**
> The sample code has been formatted to make it more readable.

```
 https :// ddoscoo . cn - hangzhou . aliyuncs . com /? Action =
 DescribeIn   stances
& Region = cn
& InstanceId = ddoscoo - cn - XXXX1
& Format = xml
& Version = 2017 - 12 - 28
& Signature = xxxx % xxxx % 3D
& SignatureM  ethod = HMAC - SHA1
& SignatureN  once = 1521552885  2396
& SignatureV  ersion = 1 . 0
& AccessKeyI  d = key - test
& TimeStamp = 2012 - 06 - 01T12 : 00 : 00Z
…
```

Authorization

To ensure the security of your Alibaba Cloud account, we recommend that you call the APIs as a RAM user. Before you can use a RAM user to call the APIs, you must create a RAM user account and grant corresponding permissions to this account.

Signature

Anti-DDoS Pro requires identity authentication for each API request. You must include signature information in either HTTP or HTTPS requests. For more information about the signature calculation process, see *RPC API signatures*.

Anti-DDoS Pro implements symmetric encryption through AccessKey ID and AccessKey Secret to authenticate the requester. AccessKey is an identity credential issued to Alibaba Cloud accounts and RAM users (similar to the login password). The AccessKey ID is used to identify the user. The AccessKey Secret is used to encrypt the signature string on the client side and to verify the signature string on the server side . The AccessKey Secret must be kept strictly confidential.

When you call an RPC API, you need to add the signature to your request using the following format:

```
https :// endpoint /? SignatureV  ersion = 1 . 0 & SignatureM  ethod
= HMAC – SHA1 & Signature = CT9X0VtwR8  6fNWSnsc6v  8YGOjuE % 3D &
SignatureN  once = 3ee8c1b8 – 83d3 – 44af – a94f – 4e0ad82fd6  cf
```

Take DescribeInstances as an example. Assume that the AccessKey ID is testid and the AccessKey Secret is testsecret. The original request URL is as follows:

```
https :// ddoscoo . cn – hangzhou . aliyuncs . com /? Action =
 DescribeIn  stances
& Region = cn
& InstanceId = ddoscoo – cn – XXXX1
& TimeStamp = 2016 – 02 – 23T12 : 46 : 24Z
& Format = XML
& AccessKeyI  d = testid
& SignatureM  ethod = HMAC – SHA1
& SignatureN  once = 3ee8c1b8 – 83d3 – 44af – a94f – 4e0ad82fd6  cf
& Version = 2017 – 12 – 28
& SignatureV  ersion = 1 . 0
```

Perform the following steps to calculate the signature:

1. Use the request parameters to create the string to be signed.

```
GET &% 2F & AccessKeyI  d % 3Dtestid & Action % 3DDescribe
DomainName  s & Region % 3Dcn & InstanceId % 3Dwaf_elas  ticity –
cn – 0xldbqtm00  5 & Format % 3XML & SignatureM  ethod % 3DHMAC
– SHA1 & SignatureN  once % 3D3ee8c1b8 – 83d3 – 44af – a94f –
4e0ad82fd6  cf & SignatureV  ersion % 3D1 . 0 & TimeStamp % 3D2016
– 02 – 23T12 % 253A46 % 253A24Z & Version % 3D2018 – 01 – 17
```

2. Calculate the HMAC value of the string.

Append an ampersand (&) to the AccessKey Secret and use this string as the key to calculate the HMAC value. In this example, the key is `testsecret &`.

```
CT9X0VtwR8  6fNWSnsc6v  8YGOjuE =
```

3. Add the signature to the request URL:

```
https :// ddoscoo . cn – hangzhou . aliyuncs . com /? Action =
 DescribeIn  stances
& Region = cn
& InstanceId = ddoscoo – cn – XXXX1
& TimeStamp = 2016 – 02 – 23T12 : 46 : 24Z
& Format = XML
& AccessKeyI  d = testid
& SignatureM  ethod = HMAC – SHA1
& SignatureN  once = 3ee8c1b8 – 83d3 – 44af – a94f – 4e0ad82fd6  cf

& Version = 2017 – 12 – 28
& SignatureV  ersion = 1 . 0
```

```
& Signature = CT9X0VtwR8  6fNWSnsc6v  8YGOjuE % 3D
```

6.3 Common parameters

This topic describes the common parameters required by Anti-DDoS Pro APIs.

Common request parameters

Common request parameters refer to the request parameters that all APIs require.

Name	Type	Required	Description
Region	String	Yes	The region where the Anti-DDoS Pro instance is located. Valid value: `cn - hangzhou` .
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance.
Format	String	No	The format of the response. Valid value (default): · `JSON` · `XML`
Version	String	Yes	The version of the API in the format of YYYY-MM-DD. Valid value: `2017 - 12 - 28` .
AccessKeyId	String	Yes	The AccessKey ID of the API caller.
Signature	String	Yes	The signature of the request.
SignatureMethod	String	Yes	The algorithm that is used to calculate the signature. Valid value: `HMAC - SHA1` .
Timestamp	String	Yes	The timestamp when the request is signed. The UTC time in ISO-8601 format: `YYYY - MM - DDThh : mm : ssZ` . For example, `2013 - 01 - 10T12 : 00 : 00Z` indicates 20:00:00, January 10, 2013 Beijing time.
SignatureVersion	String	Yes	The version of the signature algorithm. Valid value: `1` .
SignatureNonce	String	Yes	The unique random number that is used to prevent replay attacks. You must use different random numbers for different requests.
ResourceOwnerAccount	String	No	The account owner of the requested resources. Set the value to the logon username.

Examples

```
https :// ddoscoo . cn - hangzhou . aliyuncs . com /? Action =
 DescribeIn   stances
& Region = cn
& InstanceId = ddoscoo - cn - XXXX1
& Timestamp = 2014 - 05 - 19T10 % 3A33 % 3A56Z
& Format = xml
& AccessKeyI  d = testid
& SignatureM  ethod = Hmac - SHA1
& SignatureN  once = NwDAxvLU6t  FE0DVb
& Version = 2017 - 12 - 28
& SignatureV  ersion = 1 . 0
& Signature = Signature
```

Common response parameters

The API response uses a unified format. A 2XX HTTP status code is returned if the call is successful. A 4xx or 5xx HTTP status code is returned if the call has failed. The responses can be returned in JSON or XML format. The XML format is used by default . You can specify the format when calling an API.

Each time you send an API call, the system returns a unique identifier RequestId, no matter whether the invocation is successful or not.

- XML format

```
<?  xml   version =" 1 . 0 "  encoding =" utf - 8 "? >
    <!- The   root   node   of   the   response -->
    < API   name + Response >
       <!- The   request   tag   returned -->
       < RequestId > 4C467B38 - 3910 - 447D - 87BC - AC049166F2  16
 </ RequestId >
       <!- The   response   data -->
    </ API   name + Response >
```

- JSON format

```
{
    " RequestId ":" 4C467B38 - 3910 - 447D - 87BC - AC049166F2  16
 ",
    /* The   response   data */
```

```
    }
```

6.4 Instances

6.4.1 DescribeInstances

You can call this operation to perform queries on Anti-DDoS Pro instances.

Request parameters

Name	Type	Required	Description
InstanceId s	String	No	The array of IDs of Anti-DDoS Pro instances represented as a JSON string. Exact match is supported. For example, [" ddoscoo - cn - XXXX1 ", " ddoscoo - cn - XXXX2 "]. Note: If this parameter is specified, `Ip` or `Remark` is not needed.
Ip	String	No	The IP addresses of Anti-DDoS Pro instances. Exact match is supported. Note: If this parameter is specified, `InstanceId s` or `Remark` is not needed.
Remark	String	No	The remarks on the Anti-DDoS Pro instances. Fuzzy match is supported. Note: If this parameter is specified, `InstanceId s` or `Ip` is not needed.
PageNo	Integer	Yes	The number of the starting page returned in the query result. Minimum value: `1` .
PageSize	Integer	Yes	The number of result records per page. Maximum value: `50` .

Response parameters

Name	Type	Description
Total	Integer	The total number of Anti-DDoS Pro instances.

Name	Type	Description
Instances	Instance	The list of Anti-DDoS Pro instances. For more information, see *instance*.
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Table 6-1: instance

Name	Type	Description
InstanceId	String	The ID of the Anti-DDoS Pro instance.
Remark	String	The remark on the Anti-DDoS Pro instance. Maximum length: 500 bytes.
Status	Integer	The subscription status of the Anti-DDoS Pro instance. · `1` : Indicates that the subscription of the instance is valid. · `2` : Indicates that the subscription of the instance has expired. · `3` : Indicates that the instance has been released.
ExpireTime	Long	The timestamp when the subscription of the instance expires. Unit: milliseconds.
GmtCreate	Long	The timestamp when the instance was created. Unit: milliseconds.

Examples

Sample requests

```
{
  " InstanceId  s ": "[\" 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx
 bc \",\" 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc \"]",
  " PageNo ":  1 ,
  " PageSize ":  1
}
```

Sample responses

```
{
  " Total ":  1 ,
  " Instances ": [
    {
      " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc
 ",
      " Remark ": " xxx ",
      " Status ":  1 ,
      " ExpireTime ":  20384032 ,
      " GmtCreate ":  2308402384
```

```
    }
  ],
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.4.2 ReleaseInstance

You can call this operation to release Anti-DDoS Pro instances.

Request parameters

Name	Type	Required	Description
InstanceId	String	No	The ID of the Anti-DDoS Pro instance that you want to release.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.4.3 DescribeInstanceDetails

You can call this operation to perform queries on instance details.

Request parameters

Name	Type	Required	Description
InstanceId s	String	Yes	The array of IDs of Anti-DDoS Pro instances represented as a JSON string.

Response parameters

Name	Type	Description
InstanceDe tails	InstanceDe tail	The list of instance details. For more information, see *InstanceDetail*.
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Table 6-2: InstanceDetail

Name	Type	Description
InstanceId	String	The ID of the Anti-DDoS Pro instance.
Line	String	The network lines used by the instance. For example, `coop - line - 001` .
[] EipInfoLis t	EipInfo	The list of EIPs that are associated with the instance. For more information, see *EipInfo*.

Table 6-3: EipInfo

Name	Type	Description
Eip	String	The elastic IP address.
Status	String	The status of the EIP. Valid values: · `normal` : Indicates that the instance is running correctly. · `cleaning` : Indicates that the instance is scrubbing traffic. · `blackhole` : Indicates that the instance is routing traffic to a black hole.

Examples

Sample requests

```
{
  " InstanceId  s ": "[\" 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx
 bc \",\" 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc \"]"
}
```

Sample responses

```
{
  " InstanceDe  tails ": [
    {
```

```
      " InstanceId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx   bc
 ",
      " Line ": " coop - line - 001 ",
      " EipInfoLis  t ": [
        {
          " Eip ": " 1 . 1 . 1 . 1 ",
          " Status ": " normal "
        }
      ]
    }
  ],
  " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx   bc "
}
```

6.4.4 DescribeInstanceSpecs

You can call this operation to perform queries on the configurations of Anti-DDoS Pro instances.

Request parameters

Name	Type	Required	Description
InstanceId s	String	Yes	The array of IDs of Anti-DDoS Pro instances represented as a JSON string.

Response parameters

Name	Type	Description
InstanceSp ecs	Instance Spec	The configurations of the instances. For more information, see *InstanceSpec*.
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Table 6-4: InstanceSpec

Name	Type	Description
InstanceId	String	The ID of the Anti-DDoS Pro instance.
BaseBandwi dth	Integer	The basic bandwidth of the instance.
ElasticBan dwidth	Integer	The burstable bandwidth of the instance.
PortLimit	Integer	The limit on the number of layer 4 forwarding rules on the instance.
DomainLimi t	Integer	The limit on the number of layer 7 forwarding rules on the instance.

Name	Type	Description
BandwidthM bps	Integer	The service bandwidth of the instance.

Examples

Sample requests

```
{
  " InstanceId  s ": "[\" 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx
 bc \",\" 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc \"]"
}
```

Sample responses

```
{
  " InstanceSp  ecs ": [
    {
      " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc
 ",
      " BaseBandwi  dth ":  20 ,
      " ElasticBan  dwidth ":  10 ,
      " PortLimit ": 10 ,
      " DomainLimi  t ":  20 ,
      " BandwidthM  bps ":  100
    }
  ],
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.4.5 DescribeInstanceStatistics

You can call this operation to perform queries on the rules configured on instances.

Request parameters

Name	Type	Required	Description
InstanceId s	String	Yes	The array of IDs of Anti-DDoS Pro instances represented as a JSON string.

Response parameters

Name	Type	Description
InstanceSt atistics	Instance atistic	The details of the rules on Anti-DDoS Pro instances. For more information, see *InstanceStatistic*.
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Table 6-5: InstanceStatistic

Name	Type	Description
InstanceId	String	The ID of the Anti-DDoS Pro instance.
PortUsage	Integer	The number of layer 4 forwarding rules configured on the instance.
DomainUsage	Integer	The number of layer 7 forwarding rules configured on the instance.

Examples

Sample requests

```
{
  " InstanceId  s ": "[\" 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx
 bc \",\" 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc \"]"
}
```

Sample responses

```
{
  " InstanceSt  atistics ": [
    {
      " InstanceId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc
  ",
      " PortUsage ":  20 ,
      " DomainUsag  e ":  10
    }
  ],
  " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
}
```

6.4.6 DescribeElasticBandwidthSpec

You can call this operation to perform queries on the burstable bandwidth of Anti-DDoS Pro instances.

Request parameters

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance. You can only query the burstable bandwidth of one instance at a time.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
ElasticBan dwidthSpec	Integer array	The burstable bandwidth of the instance.

Examples

Sample requests

```
{
  " InstanceId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
}
```

Sample responses

```
{
  " ElasticBan  dwidthSpec ": [ 5 , 10 , 20 , 30 ],
  " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
}
```

6.4.7 ModifyElasticBandWidth

You can call this operation to modify the burstable bandwidth of Anti-DDoS Pro instances.

Request parameters

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance. You can only modify the burstable bandwidth of one instance at a time and the instance must be in normal status.
ElasticBan dwidth	Integer	Yes	The new burstable bandwidth.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc ",
  " ElasticBan  dwidth ":  50
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.4.8 ModifyInstanceRemark

You can call this operation to modify the remarks on instances.

Request parameters

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance. You can only modify the remark on one instance at a time.
Remark	String	Yes	The new remark.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc ",
  " Remark ": " huadong2 "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
```

```
}
```

6.5 Layer 4 rules

6.5.1 CreateLayer4Rule

You can call this operation to create layer 4 forwarding rules.

Request parameters

Name	Type	Required	Description
Listeners	String	Yes	The array of listeners that you want to create represented as a JSON string. For more information, see *Listener*.

Table 6-6: Listener

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance that you want to change settings for.
Protocol	String	Yes	The listener protocol.
FrontendPo rt	Integer	Yes	The port for front-end (client to Anti-DDoS Pro) connections. Valid values: 0-65535.
BackendPor t	Integer	Yes	The port for back-end (Anti-DDoS Pro to origin server) connections. Valid values: 0-65535.
RealServer s	JSON array	Yes	The IP addresses of the origin servers.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Listeners ": "[{\" InstanceId \":\" 0bcf28g5 – d57c – 11e7 – 9bs0
 – d89d6717dx  bc \",\" Protocol \":\" tcp \",\" FrontendPo  rt \": 80
 ,\" BackendPor  t \": 5 ,\" RealServer  s \":[\" 1 . 1 . 1 . 1 \",\"
 2 . 2 . 2 . 2 \"]}]"
```

```
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.5.2 ConfigLayer4Rule

You can call this operation to edit layer 4 forwarding rules.

Request parameters

Name	Type	Required	Description
Listeners	String	Yes	The array of listeners that you want to edit represented as a JSON string. For more information, see *Listener*.

Table 6-7: Listener

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance that you want to change settings for.
Protocol	String	Yes	The listener protocol.
FrontendPort	Integer	Yes	The port for front-end (client to Anti-DDoS Pro) connections. Valid values: 0-65535.
BackendPort	Integer	Yes	The port for back-end (Anti-DDoS Pro to origin server) connections. Valid values: 0-65535.
RealServers	JSON array	Yes	The IP addresses of the origin servers.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
```

```
  " Listeners ": "[{\" InstanceId \":\" 0bcf28g5 – d57c – 11e7 – 9bs0
 – d89d6717dx  bc \",\" Protocol \":\" tcp \",\" FrontendPo  rt \": 80
 ,\" BackendPor  t \": 5 ,\" RealServer  s \":[\" 1 . 1 . 1 . 1 \",\"
 2 . 2 . 2 . 2 \"]}]"
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.5.3 DeleteLayer4Rule

You can call this operation to delete layer 4 forwarding rules.

Request parameters

Name	Type	Required	Description
Listeners	String	Yes	The listener that you want to delete represented as a JSON string. For more information, see *Listener*. Note: Currently, you can only delete one listener at a time.

Table 6-8: Listener

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance that you want to change settings for.
Protocol	String	Required	The listener protocol.
FrontendPo rt	Integer	Yes	The port for front-end (client to Anti-DDoS Pro) connections. Valid values: 0-65535.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
```

```
  " Listeners ": "[{\" InstanceId \":\" 0bcf28g5 - d57c - 11e7 - 9bs0
 - d89d6717dx  bc \",\" Protocol \":\" tcp \",\" FrontendPo  rt \": 80
 }]"
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
}
```

6.5.4 ConfigLayer4RuleAttribute

You can call this operation to set the attributes of layer 4 forwarding rules, including session persistence and anti-DDoS protection policies.

Request parameters

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance that you want to change settings for.
ForwardProtocol	String	Yes	The forwarding protocol. Valid values: `TCP` and `UDP`.
FrontendPort	Integer	Yes	The port for front-end connections.
Config	String	Yes	The configuration information. You may specify a TcpConfig or UdpConfig object represented as a JSON string. For more information, see *TcpConfig* and *UdpConfig*.

Table 6-9: TcpConfig

Name	Type	Required	Description
PersistenceTimeout	Integer	Yes	The session timeout. Unit: seconds. Default value: `0`. A value of 0 indicates that session persistence is disabled.
Synproxy	String	Yes	The false sources feature of anti-DDoS protection. Valid values: `off` and `on`.
NodataConn	String	Yes	The null session connections feature of anti-DDoS protection. Valid values: `off` and `on`.
Sla	Sla	Yes	The connection limit on destination IPs. For more information, see *Sla*.

Name	Type	Required	Description
Slimit	Slimit	Yes	The connection limit on source IPs. For more information, see *Slimit*.
PayloadLen	PayloadLen	Yes	The limit on the payload size of each packet. For more information, see *PayloadLen*.

Table 6-10: UdpConfig

Name	Type	Required	Description
Persistenc eTimeout	Integer	Yes	The session timeout. Unit: seconds. Default value: `0` . A value of 0 indicates that session persistence is disabled.
Synproxy	String	Yes	The false sources feature of anti-DDoS protection. Valid values: `off` and `on` .
NodataConn	String	Yes	The null session connections feature of anti-DDoS protection. Valid values: `off` and `on` .
Sla	Sla	Yes	The connection limit on destination IPs. For more information, see *Sla*.
Slimit	Slimit	Yes	The connection limit on source IPs. For more information, see *Slimit*.
PayloadLen	PayloadLen	Yes	The limit on the payload size of each packet. For more information, see *PayloadLen*.

Table 6-11: Sla

Name	Type	Required	Description
Cps	Integer	Yes	The maximum number of new connections per second to a single destination IP and port . Valid values: 100-100,000.
Maxconn	Integer	Yes	The maximum number of concurrent connections to a single destination IP and port. Valid values: 1,000-1,000,000.
CpsEnable	Integer	No	Indicates whether Cps is enabled. Valid values: · `0` : Disabled · `1` (Default): Enabled

Name	Type	Required	Description
MaxconnEnable	Integer	No	Indicates whether Maxconnection is enabled. Valid values: · `0` : Disabled · `1` (Default): Enabled

Table 6-12: Slimit

Name	Type	Required	Description
Cps	Integer	Yes	The maximum number of new connections per second from a single source IP. Valid values: 100-100,000.
Maxconn	Integer	Yes	The maximum number of concurrent connections from a single source IP. Valid values: 1,000-1,000,000.
CpsEnable	Integer	No	Indicates whether Cps is enabled. Valid values: · `0` : Disabled · `1` (Default): Enabled
MaxconnEnable	Integer	No	Indicates whether Maxconnection is enabled. Valid values: · `0` : Disabled · `1` (Default): Enabled

Table 6-13: PayloadLen

Name	Type	Required	Description
Min	Integer	Yes	The minimum payload size of a packet.
Max	Integer	Yes	The maximum payload size of a packet.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc ",
  " ForwardPro  tocol ": " tcp ",
  " FrontendPo  rt ":  80 ,
  " Config ": "{\" Persistenc  eTimeout \": 80 ,\" Synproxy \":\"
 off \",\" NodataConn \":\" off \",\" Sla \":{\" Cps \": 10 ,\"
 Maxconn \": 10 },\" Slimit \":{\" Cps \": 10 ,\" Maxconn \": 30 },\"
 PayloadLen \":{\" Min \": 1 ,\" Max \": 2 }}"
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.5.5 ConfigHealthCheck

You can call this operation to configure layer 4 or layer 7 health check settings.

Request parameters

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance that you want to change settings for.
ForwardPro tocol	String	Yes	The forwarding protocol. Valid values: · TCP (Layer 4) · UDP (Layer 4) · HTTP (Layer 7)
FrontendPo rt	Integer	Yes	The port for front-end connections.
HealthChec k	String	Yes	The HealthCheck objects represented as a JSON string. For more information, see *HealthCheck*.

Table 6-14: HealthCheck

Name	Type	Required	Description
Type	String	Yes	The listener protocol. Valid values: · TCP : Layer 4 · HTTP : Layer 7

Name	Type	Required	Description
Domain	String	No	In layer 7 health check, the domain name.
Uri	String	No	In layer 7 health check, the URI path.
Timeout	Integer	No	In layer 4 health check, the response timeout.
Port	Integer	No	In layer 4 health check, the port that is used to connect with the origin server.
Interval	Integer	No	In layer 4 health check, the time interval between health checks.
Up	Integer	No	In layer 4 health check, the healthy threshold.
Down	Integer	No	In layer 4 health check, the unhealthy threshold.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc ",
  " ForwardPro  tocol ": " tcp ",
  " FrontendPo  rt ":  80 ,
  " HealthChec  k ": "{\" Type \":\" tcp \",\" Timeout \": 10 ,\" Port
 \": 80 ,\" Interval \": 10 ,\" Up \": 10 ,\" Down \": 40 }"
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.5.6 DescribeLayer4Rules

You can call this operation to perform queries on layer 4 forwarding rules of Anti-DDoS Pro instances.

Request parameters

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance that you want to query.
ForwardProtocol	String	No	The forwarding protocol. Valid value: `TCP` .
FrontendPort	Integer	No	The port for front-end connections.
Offset	Integer	Yes	The number of records to skip when returning the result records. Note: If not specified, all result records are returned.
PageSize	Integer	Yes	The number of result records per page. Maximum value: `50` .

Response parameters

Name	Type	Description
Total	Integer	The total number of result records.
Listeners	Listener[]	The array of listeners. For more information, see *Listener*.
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Table 6-15: Listener

Name	Type	Description
InstanceId	String	The ID of the Anti-DDoS Pro instance.
Protocol	String	The listener protocol.

Name	Type	Description
FrontendPo rt	Integer	The port for front-end (client to Anti-DDoS Pro) connections. Valid values: 0-65535.
BackendPor t	Integer	The port for back-end (Anti-DDoS Pro to origin server) connections. Valid values: 0-65535.
RealServer s	JSON array	The IP addresses of the origin servers.
IsAutoCrea te	Boolean	Indicates whether the listener is automatically created. If true, the listener cannot be deleted or modified.

Examples

Sample requests

```
{
  " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc ",
  " ForwardPro  tocol ": " tcp ",
  " FrontendPo  rt ":  80 ,
  " Offset ":  1 ,
  " PageSize ":  10
}
```

Sample responses

```
{
  " Total ":  1 ,
  " Listeners ": [
    {
      " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc
 ",
      " Protocol ": " tcp ",
      " FrontendPo  rt ":  80 ,
   " BackendPor  t ": 80 ,
      " RealServer  s ": [
        " 1 . 1 . 1 . 1 ",
        " 2 . 2 . 2 . 2 "
      ],
      " IsAutoCrea  te ":  true
    }
  ],
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
```

```
}
```

6.5.7 DescribeLayer4RuleAttributes

You can call this operation to perform queries on the attributes of layer 4 forwarding rules, including session persistence and anti-DDoS protection settings.

Request parameters

Name	Type	Required	Description
Listeners	String	Yes	The array of listeners that you want to query represented as a JSON string. For more information, see *Listener*.

Table 6-16: Listener

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance.
Protocol	String	Yes	The listener protocol.
FrontendPort	Integer	Yes	The port for front-end (client to Anti-DDoS Pro) connections. Valid values: 0-65535.
BackendPort	Integer	No	The port for back-end (Anti-DDoS Pro to origin server) connections. Valid values: 0-65535.
RealServers	JSON array	No	The IP addresses of the origin servers.
IsAutoCreate	Boolean	No	Indicates whether the listener is automatically created. If true, the listener cannot be deleted or modified.

Response parameters

Name	Type	Description
Total	Integer	The total number of result records.
Listeners	String	The array of listeners represented as a JSON string. For more information, see *Listener*.
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Table 6-17: Listener

Name	Type	Description
InstanceId	String	The ID of the Anti-DDoS Pro instance.
Protocol	String	The listener protocol.
FrontendPort	Integer	The port for front-end (client to Anti-DDoS Pro) connections. Valid values: 0-65535.
Config	TcpConfig	The TCP configuration. For more information, see *TcpConfig*.

Table 6-18: TcpConfig

Name	Type	Description
PersistenceTimeout	Integer	The session timeout. Unit: seconds. Default value: `0`. A value of 0 indicates that session persistence is disabled.
Synproxy	String	The false sources feature of anti-DDoS protection. Valid values: `off` and `on`.
NodataConn	String	The null session connections feature of anti-DDoS protection. Valid values: `off` and `on`.
Sla	Sla	The connection limit on destination IPs. For more information, see *Sla*.
Slimit	Slimit	The connection limit on source IPs. For more information, see *Slimit*.
PayloadLen	PayloadLen	The limit on the payload size of each packet. For more information, see *PayloadLen*.

Table 6-19: Sla

Name	Type	Description
Cps	Integer	The maximum number of new connections per second to a single destination IP and port. Valid values: 100-100,000.
Maxconn	Integer	The maximum number of concurrent connections to a single destination IP and port. Valid values: 1,000-1,000,000.

Name	Type	Description
CpsEnable	Integer	Indicates whether Cps is enabled. Valid values: ・ `0` : Disabled ・ `1` (Default): Enabled
MaxconnEna ble	Integer	Indicates whether Maxconnection is enabled. Valid values: ・ `0` : Disabled ・ `1` (Default): Enabled

Table 6-20: Slimit

Name	Type	Description
Cps	Integer	The maximum number of new connections per second from a single source IP. Valid values: 100-100,000.
Maxconn	Integer	The maximum number of concurrent connections from a single source IP. Valid values: 1,000-1,000,000.
CpsEnable	Integer	Indicates whether Cps is enabled. Valid values: ・ `0` : Disabled ・ `1` (Default): Enabled
MaxconnEna ble	Integer	Indicates whether Maxconnection is enabled. Valid values: ・ `0` : Disabled ・ `1` (Default): Enabled

Table 6-21: PayloadLen

Name	Type	Description
Min	Integer	The minimum payload size of a packet.
Max	Integer	The maximum payload size of a packet.

Examples

Sample requests

```
{
  " Listeners ": "[{\" InstanceId \":\" 0bcf28g5 - d57c - 11e7 - 9bs0
  - d89d6717dx  bc \",\" Protocol \":\" tcp \",\" FrontendPo  rt \": 80
  }]"
```

```
    }
```

Sample responses

```
{
   " Total ":  1 ,
   " Listeners ": [
      {
         " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc
 ",
         " Protocol ": " tcp ",
         " FrontendPo  rt ":  80 ,
         " Config ": {
            " Persistenc  eTimeout ":  80 ,
            " Synproxy ": " off ",
   " NodataConn ": " on ",
         " Sla ": {
            " Cps ":  10 ,
            " Maxconn ":  10 ,
      " CpsEnable ":  1 ,
      " MaxconnEna  ble ":  1
         },
         " Slimit ": {
            " Cps ":  10 ,
            " Maxconn ":  10 ,
      " CpsEnable ":  1 ,
      " MaxconnEna  ble ":  1
         },
         " PayloadLen ": {
            " Min ":  1 ,
            " Max ":  2
         }
      }
   }
   ],
   " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.5.8 DescribeHealthCheckList

You can call this operation to perform queries on layer 4 or layer 7 health check
settings.

Request parameters

Name	Type	Required	Description
Listeners	String	Yes	The array of listeners that you want to query represented as a JSON string. For more information, see *Listener*.

Table 6-22: Listener

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance.

Name	Type	Required	Description
Protocol	String	Yes	The listener protocol.
FrontendPort	Integer	Yes	The port for front-end (client to Anti-DDoS Pro) connections. Valid values: 0-65535.
BackendPort	Integer	No	The port for back-end (Anti-DDoS Pro to origin server) connections. Valid values: 0-65535.
RealServers	JSON array	No	The IP addresses of the origin servers.
IsAutoCreate	Boolean	No	Indicates whether the listener is automatically created. If true, the listener cannot be deleted or modified.

Response parameters

Name	Type	Description
Total	Integer	The total number of result records.
HealthCheck	HealthCheck	The health check information. For more information, see *HealthCheck*.
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Table 6-23: HealthCheck

Name	Type	Description
Type	String	The protocol type. Valid values: · `TCP` : Layer 4 · `HTTP` : Layer 7
Domain	String	In layer 7 health check, the domain name.
Uri	String	In layer 7 health check, the URI path.
Timeout	Integer	In layer 4 health check, the response timeout.
Port	Integer	In layer 4 health check, the port that is used to connect with the origin server.
Interval	Integer	In layer 4 health check, the time interval between health checks.
Up	Integer	In layer 4 health check, the healthy threshold.

Name	Type	Description
Down	Integer	In layer 4 health check, the unhealthy threshold.

Examples

Sample requests

```
{
  " Listeners ": "[{\" InstanceId \":\" 0bcf28g5 – d57c – 11e7 – 9bs0
 – d89d6717dx  bc \",\" Protocol \":\" tcp \",\" FrontendPo  rt \": 80
 }]"
}
```

Sample responses

```
{
  " Total ":  1 ,
  " HealthChec  k ": [
    {
      " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc
 ",
      " Protocol ": " tcp ",
      " FrontendPo  rt ":  80 ,
      " HealthChec  k ": {
        " Type ": " tcp ",
        " Timeout ":  10 ,
        " Port ":  80 ,
        " Interval ":  10 ,
        " Up ":  10 ,
        " Down ":  20
      }
    }
  ],
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.5.9 DescribeHealthCheckStatusList

You can call this operation to perform queries on health check statuses.

Request parameters

Name	Type	Required	Description
Listeners	String	Yes	The array of listeners that you want to query represented as a JSON string. For more information, see *Listener*.

Table 6-24: Listener

Name	Type	Required	Description
InstanceId	String	Yes	The ID of the Anti-DDoS Pro instance.

Name	Type	Required	Description
Protocol	String	Yes	The listener protocol.
FrontendPort	Integer	Yes	The port for front-end (client to Anti-DDoS Pro) connections. Valid values: 0-65535.
BackendPort	Integer	No	The port for back-end (Anti-DDoS Pro to origin server) connections. Valid values: 0-65535.
RealServers	JSON array	No	The IP addresses of the origin servers.
IsAutoCreate	Boolean	No	Indicates whether the listener is automatically created. If true, the listener cannot be deleted or modified.

Response parameters

Name	Type	Description
HealthCheckStatusList	HealthCheckStatus	The array of health check statuses. For more information, see *HealthCheckStatus*.
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Table 6-25: HealthCheckStatus

Name	Type	Description
InstanceId	String	The ID of the Anti-DDoS Pro instance.
Protocol	String	The listener protocol.
FrontendPort	Integer	The port for front-end connections.
RealServerStatusList	RealServerStatus	The statuses of origin servers represented as a JSON array. For more information, see *RealServerStatus*.
Status	String	The health check status. Valid values: `normal` and `abnormal` .

Table 6-26: RealServerStatus

Name	Type	Description
Address	String	The IP address of the origin server.
Status	String	The status of the origin server. Valid values: `normal` and `abnormal`.

Examples

Sample requests

```
{
  " Listeners ": "[{\" InstanceId \":\" 0bcf28g5 – d57c – 11e7 – 9bs0
 – d89d6717dx  bc \",\" Protocol \":\" tcp \",\" FrontendPo  rt \": 80
 }]"
}
```

Sample responses

```
{
  " HealthChec  kStatusLis  t ": [
    {
      " InstanceId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc
 ",
      " Protocol ": " tcp ",
      " FrontendPo  rt ":  80 ,
    " Status ": " normal ",
    " RealServer  StatusList ": [
        " Status ": " normal ",
        " Address ": " 1 . 1 . 1 . 1 "
      ]
    }
  ],
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.6 Layer 7 rules

6.6.1 DescribeDomains

You can call this operation to perform queries on layer 7 forwarding rules.

Request parameters

Name	Type	Required	Description
Domain	String	No	The domain name that you want to query.

Name	Type	Required	Description
QueryDomainPattern	String	No	The query mode. Valid values: • `fuzzy` (Default): Fuzzy query. • `exact` : Exact query.
Offset	Integer	Yes	The number of records to skip when returning the result records. Default value: `0`.
PageSize	Integer	Yes	The number of result records per page. Maximum value: `10` .

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Total	Integer	The total number of domain names.
Domains	[] Domain	The array of domain names and associated forwarding rules. For more information, see *Domain*.

Table 6-27: Domain

Name	Type	Description
Domain	String	The domain name.
ProxyTypes	[] String	The array of forwarding protocols. Valid values: • `http` • `https` • `websocket` • `websockets`
RealServers	[] String	The array of origin servers.
CcEnabled	Boolean	Indicates whether HTTP flood protection is enabled.
CcRuleEnabled	Boolean	Indicates whether HTTP flood protection rules are enabled.
CcTemplate	String	The template of HTTP flood protection.
WhiteList	[] String	The array of IP addresses in the whitelist.

Name	Type	Description
BlackList	[] String	The array of IP addresses in the blacklist.
CertName	String	The name of the certificate.
RealSevers	[] Layer7Real Server	The array of origin servers. For more information, see *Layer7RealServer*.

Table 6-28: Layer7RealServer

Name	Type	Description
RealServer	String	The address of the origin server.
RsType	Integer	The address type. Valid values: · `0` : IP address. · `1` : Domain name.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com ",
  " QueryDomai  nPattern ": " fuzzy ",
  " Offset ": 0 ,
  " PageSize ": 10
}
```

Sample responses

```
{
  " Total ":  2 ,
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc ",
  " Domains ": [
   {
  " Domain ": " www . alibaba . com ",
  " ProxyTypes ": [" https "," http "],
  " RealServer   s ": [{
   " RealServer ": " 1 . 1 . 1 . 1 ",
   " RsType ": 0
  },{
   " RealServer ":" 1 . 1 . 1 . 1 ",
   " RsType ": 1
  }
 ],
  " CcEnabled " :  false ,
  " CcRuleEnab  led " :  true ,
  " CcTemplate " : " default ",
  " BlackList " : [" 1 . 1 . 1 . 1 / 1 "," 1 . 1 . 1 . 2 / 2 "],
  " WhiteList " : [" 1 . 1 . 1 . 1 / 1 "," 1 . 1 . 1 . 2 / 2 "],
```

```
   " CertName " : " www_alibab  a_com . pem "
 },{
  " Domain ": " www . alibaba . com ",
  " ProxyTypes ": [" https "," http "],
  " RealServer   s ": [{
   " RealServer ": " 1 . 1 . 1 . 1 ",
   " RsType ": 0
  },{
   " RealServer ": " 1 . 1 . 1 . 2 ",
   " RsType ": 1
   }
  ],
  " CcEnabled " :  false ,
  " CcRuleEnab  led " :  true ,
  " CcTemplate " : " default ",
  " BlackList " : [" 1 . 1 . 1 . 1 / 1 "," 1 . 1 . 1 . 2 / 2 "],
  " WhiteList " : [" 1 . 1 . 1 . 1 / 1 "," 1 . 1 . 1 . 2 / 2 "],
  " CertName " : " www_alibab  a_com . pem "
 }
 ]
}
```

6.6.2 CreateLayer7Rule

You can call this operation to create layer 7 forwarding rules.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to add.
RsType	Integer	Yes	The type of the origin server's address. Valid values: · `0` : IP address. · `1` : Domain name.
InstanceId s . N	String	No	The ID of the Anti-DDoS Pro instance that you want to set up for the domain. If you want to set up multiple Anti-DDoS Pro instances, specify multiple parameters as follows: InstanceIds. 1, InstanceIds. 2, InstanceIds. 3, .. 📋 Note: If this parameter is not specified, the domain name is not associated with any Anti-DDoS Pro instance.
Rules	String	Yes	The array of layer 7 rules represented as a JSON string. For more information, see *Layer7Rule*.

Table 6-29: Layer7Rule

Name	Type	Description
ProxyRules	[] ProxyRule	The array of rule objects. For more information, see *ProxyRule*.
ProxyType	String	The forwarding protocol. Valid values: · http · https · websocket · websockets

Table 6-30: ProxyRule

Name	Type	Description
ProxyPort	Integer	The forwarding port. Valid values: `80` and `443`.
RealServers	[] String	The IP address and port of the origin server. For example, `1.1.1.1:443`.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com ",
  " RsType ":  1 ,
  " InstanceId  s .  1 ": " xxxx ",
  " Rules ": "[{\" ProxyRules \":[{\" ProxyPort \": 443 ,\"
 RealServer  s \":[\" 1 . 1 . 1 . 1 : 443 \"]}],\" ProxyType \":\"
 https \"},{\" ProxyRules \":[{\" ProxyPort \": 80 ,\" RealServer  s
 \":[\" 1 . 1 . 1 . 1 : 80 \"]}],\" ProxyType \":\" http \"}]"
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
```

```
}
```

6.6.3 ConfigLayer7Rule

You can call this operation to edit layer 7 forwarding rules.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to change settings for.
RsType	Integer	Yes	The type of the origin server's address. Valid values: · `0` : IP address. · `1` : Domain name.
InstanceIds . N	String	No	The ID of the Anti-DDoS Pro instance that you want to set up for the domain. If you want to set up multiple Anti-DDoS Pro instances, specify multiple parameters as follows: InstanceIds. 1, InstanceIds. 2, InstanceIds. 3, … Note: If this parameter is not specified, the domain name is not associated with any Anti-DDoS Pro instance.
RealServer s . N	String	Yes	The IP address of the origin server. If you have multiple IP addresses, specify multiple parameters as follows: RealServers. 1, RealServers. 2, RealServers. 3, …
ProxyTypes . N	String	Yes	The protocol supported by the origin server . To add multiple protocols, specify multiple parameters as follows: ProxyTypes. 1, ProxyTypes. 2, ProxyTypes. 3, …

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com ",
  " RsType " :  0 ,
  " RealServer  s .  1 ": " 1 . 1 . 1 . 1 ",
  " InstanceId  s .  1 ": " xxxx ",
  " ProxyTypes .  1 " : " http "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.6.4 DeleteLayer7Rule

You can call this operation to delete layer 7 forwarding rules.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	**The domain name that you want to change settings for.**

Response parameters

Name	Type	Description
RequestId	String	**The GUID generated by Alibaba Cloud for the request.**

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
```

```
}
```

6.6.5 ConfigLayer7Cert

You can call this operation to configure digital certificates for domains.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to change settings for.
CertId	Integer	No	The ID of the certificate. **Note:** If this parameter is specified, `CertName`, `Cert`, or `Key` is not needed.
CertName	String	No	The name of the certificate. **Note:** If this parameter is specified, you must also specify `Cert` and `Key`. If `CertName`, `Cert`, and `Key` are specified, `CertId` is not needed.
Cert	String	No	The public key of the certificate. **Note:** If this parameter is specified, you must also specify `CertName` and `Key`. If `CertName`, `Cert`, and `Key` are specified, `CertId` is not needed.
Key	String	No	The private key of the certificate. **Note:** If this parameter is specified, you must also specify `CertName` and `Cert`. If `CertName`, `Cert`, and `Key` are specified, `CertId` is not needed.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain " : " www . alibaba . com ",
  " CertId " :   1 ,
  " CertName " : " xxxx ",
  " Cert " : " abc ",
  " Key " : " bcd "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.6.6 ConfigLayer7BlackWhiteList

You can call this operation to add IP addresses to the blacklist or whitelist of domains.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to change settings for.
BlackList . N	String	No	The IP addresses that you want to add to the blacklist. If you want to blacklist multiple IP addresses, specify multiple parameters as follows: BlackList. 1, BlackList. 2, BlackList. 3 , ...
WhiteList . N	String	No	The IP addresses that you want to add to the whitelist. If you want to whitelist multiple IP addresses, specify multiple parameters as follows: WhiteList. 1, WhiteList. 2, WhiteList. 3, ...

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com ",
  " BlackList .  1 " : " 1 . 1 . 1 . 1 ",
  " BlackList .  2 " : " 2 . 2 . 2 . 2 / 24 ",
  " WhiteList .  1 " : " 3 . 3 . 3 . 3 ",
  " WhiteList .  2 " : " 4 . 4 . 4 . 4 / 24 "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.6.7 DescribleLayer7InstanceRelations

You can call this operation to perform queries on Anti-DDoS Pro instances by domain.

Request parameters

Name	Type	Required	Description
DomainList	[] String	Yes	The array of domain names that you want to query.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Layer7Inst anceRelati on	[] Layer7Inst anceRelati on	The array of domain names and associated Anti-DDoS Pro instances. For more information, see *Layer7InstanceRelation*.

Table 6-31: Layer7InstanceRelation

Name	Type	Description
Domain	String	The domain name that you have specified.
InstanceDe tails	[] Instance Detail	The list of Anti-DDoS Pro instances that are associated with the domain name. For more information, see *InstanceDetail*.

Table 6-32: InstanceDetail

Name	Type	Description
InstanceId	String	The ID of the Anti-DDoS Pro instance.
Line	String	The network line of the Anti-DDoS Pro instance. For example, `coop - line - 001` .
EipList	[] String	The array of EIPs of the Anti-DDoS Pro instance. For example, [" 1 . 1 . 1 . 1 "].

Examples

Sample requests

```
{
  " DomainList ": [" 1 . aliyun . com "," 2 . aliyun . com "]
}
```

Sample responses

```
{
    " Layer7Inst   anceRelati   ons ":[
        {
            " Domain ":" 1 . aliyun . com ",
            " InstanceDe   tails ":[
                {
                    " EipList ":[
                        " 203 . x . x . 0 ",
                        " 203 . x . x . 1 "
                    ],
                    " InstanceId ":" xxxxxx "
                },
                {
                    " EipList ":[
                        " 203 . x . x . 0 ",
                        " 203 . x . x . 1 "
                    ],
                    " InstanceId ":" xxxxxx "
                }
            ]
        }
    ]
}
```

6.6.8 DescribleCertList

You can call this operation to perform queries on certificates.

Request parameters

None.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CertList	[] CertItem	The array of certificates. For more information, see CertItem*CertItem*.

Table 6-33: CertItem

Name	Type	Description
Id	Integer	The ID of the certificate.
Name	String	The name of the certificate.

Examples

Sample requests

None.

Sample responses

```
{
    " CertList ": [
        {
            " Id ":  80 ,
    " Name " : " name1 "
        },
    {
            " Id ":  81 ,
    " Name " : " name2 "
        }
    ]
}
```

6.6.9 EnableLayer7CC

You can call this operation to enable layer 7 HTTP flood protection for domains.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to change settings for.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
}
```

6.6.10 DisableLayer7CC

You can call this operation to disable layer 7 HTTP flood protection for domains.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to change settings for.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc "
```

```
}
```

6.6.11 EnableLayer7CCRule

You can call this operation to enable layer 7 HTTP flood protection rules for domains.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to change settings for.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
}
```

6.6.12 DisableLayer7CCRule

You can call this operation to disable layer 7 HTTP flood protection rules for domains.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to change settings for.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
}
```

6.6.13 AddLayer7CCRule

You can call this operation to add layer 7 HTTP flood protection rules for domains.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to change settings for.
Name	String	Yes	The name of the HTTP flood protection rule.
Act	String	Yes	The action to perform when the rule is triggered. · `close` : Block the request. · `captcha` : Enable captcha verification.
Count	Integer	Yes	The number of requests. This parameter is used together with the `Interval` parameter. The rule is triggered when the number of requests sent by an IP address reaches the `Count` limit during the `Interval` period.
Interval	Integer	Yes	The time interval. This parameter is used together with the `Count` parameter. The rule is triggered when the number of requests sent by an IP address reaches the `Count` limit during the `Interval` period.

Name	Type	Required	Description
Mode	String	Yes	The URI matching algorithm. · `match` : Exact match. Requests are counted only when the request URI exactly matches the URI that is protected under the rule. · `prefix` : Prefix match. Requests are counted when the request URI contains the URI that is protected under the rule.
Ttl	Integer	Yes	The blocking duration when the rule is triggered.
Uri	String	Yes	The URI that is protected under the rule.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com ",
  " Name ":" XXXX ",
  " Act ":" close ",
  " Count ": 11 ,
  " Interval ": 5 ,
  " Mode ":" match ",
  " Ttl ": 1 ,
  " Uri ":"/ a / b / c . htm "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
```

```
}
```

6.6.14 ConfigLayer7CCRule

You can call this operation to edit layer 7 HTTP flood protection rules.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to change settings for.
Name	String	Yes	The name of the HTTP flood protection rule.
Act	String	Yes	The action to perform when the rule is triggered. · `close` : Block the request. · `captcha` : Enable captcha verification.
Count	Integer	Yes	The number of requests. This parameter is used together with the `Interval` parameter. The rule is triggered when the number of requests sent by an IP address reaches the `Count` limit during the `Interval` period.
Interval	Integer	Yes	The time interval. This parameter is used together with the `Count` parameter. The rule is triggered when the number of requests sent by an IP address reaches the `Count` limit during the `Interval` period.
Mode	String	Yes	The URI matching algorithm. · `match` : Exact match. Requests are counted only when the request URI exactly matches the URI that is protected under the rule. · `prefix` : Prefix match. Requests are counted when the request URI contains the URI that is protected under the rule.
Ttl	Integer	Yes	The blocking duration when the rule is triggered.
Uri	String	Yes	The URI that is protected under the rule.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com ",
  " Name ":" XXXX ",
  " Act ":" close ",
  " Count ": 11 ,
  " Interval ": 5 ,
  " Mode ":" match ",
  " Ttl ": 1 ,
  " Uri ":"/ a / b / c . htm "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
}
```

6.6.15 DescribeLayer7CCRules

You can call this operation to perform queries on layer 7 HTTP flood protection rules.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to query.
Offset	Integer	Yes	The number of records to skip when returning the result records. 📋 **Note:** If not specified, all result records are returned.
PageSize	Integer	Yes	The number of result records per page. Maximum value: `10` .

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Name	Type	Description
Layer7CCRules	[] Layer7CCRule	The array of HTTP flood protection rules. For more information, see *Layer7CCRule*.
Total	Integer	The total number of rules.

Table 6-34: Layer7CCRule

Name	Type	Description
Name	String	The name of the HTTP flood protection rule.
Act	String	The action to perform when the rule is triggered. · `close` : Block the request. · `captcha` : Enable captcha verification.
Count	Integer	The number of requests. This parameter is used together with the `Interval` parameter. The rule is triggered when the number of requests sent by an IP address reaches the `Count` limit during the `Interval` period.
Interval	Integer	The time interval. This parameter is used together with the `Count` parameter. The rule is triggered when the number of requests sent by an IP address reaches the `Count` limit during the `Interval` period.
Mode	String	The URI matching algorithm. · `match` : Exact match. Requests are counted only when the request URI exactly matches the URI that is protected under the rule. · `prefix` : Prefix match. Requests are counted when the request URI contains the URI that is protected under the rule.
Ttl	Integer	The blocking duration when the rule is triggered.
Uri	String	The URI that is protected under the rule.

Examples

Sample requests

```
{
 " Domain ": " www . alibaba . com ",
 " Offset ":  0 ,
 " PageSize ":  10
```

```
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc ",
  " Total ":  10 ,
  " Layer7CCRu  les " :[
   {
  " Name ":" XXXX ",
  " Act ":" close ",
  " Count ": 11 ,
  " Interval ": 5 ,
  " Mode ":" match ",
  " Ttl ": 1 ,
  " Uri ":"/ a / b / c . htm "
 },{
  " Name ":" XXXX ",
  " Act ":" close ",
  " Count ": 11 ,
  " Interval ": 5 ,
  " Mode ":" match ",
  " Ttl ": 1 ,
  " Uri ":"/ a / b / c . htm "
  }
  ]
}
```

6.6.16 DeleteLayer7CCRule

You can call this operation to delete layer 7 HTTP flood protection rules.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to change settings for.
Name	String	Yes	The name of the HTTP flood protection rule that you want to delete.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com ",
  " Name ":" XXXX "
```

```
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
}
```

6.6.17 ConfigLayer7CCTemplate

You can call this operation to set the mode of layer 7 HTTP flood protection for domains.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to change settings for.
Template	String	Yes	The mode of HTTP flood protection that you want to use. Valid values: · `default` : **Normal** · `gf_under_a  ttack` : **Emergency** · `gf_sos_ver  ify` : **Strict** · `gf_sos_enh  ance` : **Super Strict**

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com ",
  " Template ":" XXXX "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
```

```
}
```

6.6.18 DescribeDomainAccessMode

You can call this operation to perform queries on modes that are used to set up Anti-DDoS Pro for different domain names.

Request parameters

Name	Type	Required	Description
DomainList	[] String	Yes	The list of domain names that you want to query.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
DomainMode List	[] Object	The list of modes that are used to set up Anti-DDoS Pro. For more information, see *DomainModeList*.

Table 6-35: DomainModeList

Name	Type	Description
Domain	String	The domain name.
AccessMode	Integer	The mode that is used to set up Anti-DDoS Pro for the domain. Valid values: · 0 : A value of 0 indicates that A records are used. · 1 : A value of 1 indicates that the Anti-DDoS Pro mode is used. · 2 : A value of 2 indicates that the back-to-origin mode is used.

Examples

Sample requests

```
{
  " DomainList ": [" www . alibaba . com "," www . aliyun . com "]
}
```

Sample responses

```
{
    " RequestId ":" 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc ",
```

```
    " DomainMode  List ":[
        {
            " Domain ":" www . alibaba . com ",
            " AccessMode ": 1
        },
        {
            " Domain ":" www . aliyun . com ",
            " AccessMode ": 2
        }
    ]
}
```

6.6.19 ConfigDomainAccessMode

You can call this operation to specify the mode that is used to set up Anti-DDoS Pro for a domain name.

Request parameters

Name	Type	Required	Description
Domain	String	Yes	The domain name that you want to set up Anti-DDoS Pro for.
AccessMode	Integer	Yes	The mode that is used to set up Anti-DDoS Pro. Valid values: · `0` : A value of 0 indicates that A records are used. · `1` : A value of 1 indicates that the Anti-DDoS Pro mode is used. · `2` : A value of 2 indicates that the back-to-origin mode is used.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " Domain ": " www . alibaba . com ",
  " AccessMode ":  1
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc ",
```

```
}
```

6.6.20 DescribeBackSourceCidr

You can call this operation to perform queries on back-to-origin CIDR blocks.

Request parameters

Name	Type	Required	Description
Line	String	Yes	The network line that you want to query.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CidrList	[] String	The list of back-to-origin CIDR blocks.

Examples

Sample requests

```
{
  " Line ":" coop – line – 001 "
}
```

Sample responses

```
{
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc ",
  " CidrList " : [" 47 . 97 . 128 . 0 / 25 "," 47 . 97 . 128 . 128 /
 25 "]
```

```
}
```

6.7 Tasks

6.7.1 ListAsyncTask

You can call this operation to perform queries on asynchronous tasks.

Request parameters

Name	Type	Required	Description
TaskType	Integer	No	The type of the task that you want to query. Valid values: · `1` : A value of 1 indicates that the task is to export multiple layer 4 forwarding rules. · `2` : A value of 2 indicates that the task is to export multiple layer 7 forwarding rules. · `3` : A value of 3 indicates that the task is to export session and health check settings. · `4` : A value of 4 indicates that the task is to export anti-DDoS protection policies. 📋 Note: If this parameter is not specified, all types of tasks are returned.

Name	Type	Required	Description
TaskStatus	Integer	No	The status of the task that you want to query. Valid values: · `0` : A value of 0 indicates that the task is initializing. · `1` : A value of 1 indicates that the task is in progress. · `2` : A value of 2 indicates that the task is successful. · `3` : A value of 3 indicates that the task has failed. 📋 Note: If this parameter is not specified, tasks of all statuses are returned.
PageNo	Integer	Yes	The number of the starting page that is displayed. Must be an integer no less than `1` .
PageSize	Integer	Yes	The number of records per page. Maximum value: `20` .

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Total	Integer	The total number of domain names.
AsyncTasks	[] AsyncTask	The list of tasks. For more information, see *AsyncTask*.

Table 6-36: AsyncTask

Name	Type	Description
TaskId	Long	The ID of the task. You can delete tasks by ID.

Name	Type	Description
TaskType	Integer	The type of the task. Valid values: · `1` : A value of 1 indicates that the task is to export multiple layer 4 forwarding rules. · `2` : A value of 2 indicates that the task is to export multiple layer 7 forwarding rules. · `3` : A value of 3 indicates that the task is to export session and health check settings. · `4` : A value of 4 indicates that the task is to export anti-DDoS protection policies.
TaskStatus	Integer	The status of the task. Valid values: · `0` : A value of 0 indicates that the task is initializing. · `1` : A value of 1 indicates that the task is in progress. · `2` : A value of 2 indicates that the task is successful. · `3` : A value of 3 indicates that the task has failed.
StartTime	Long	The start timestamp of the task. Unit: milliseconds.
EndTime	Long	The end timestamp of the task. Unit: milliseconds.
TaskParams	TaskParam	The task parameter represented as a JSONObject string. For more information, see *TaskParam*.
TaskResult	TaskResult	The task execution result represented as a JSONObject string. For more information, see *TaskResult*.

Table 6-37: TaskParam

Name	Type	Description
instanceId	String	The ID of the Anti-DDoS Pro instance.
domain	String	The domain name.

Table 6-38: TaskResult

Name	Type	Description
instanceId	String	The ID of the Anti-DDoS Pro instance.
url	String	The OSS URL where the files were downloaded.

Examples

Sample requests

```
{
  " TaskType ":  1 ,
  " TaskStatus ":  0 ,
  " PageNo ": 1 ,
  " PageSize ": 10
}
```

Sample responses

```
{
  " Total ":  2 ,
  " RequestId ": " 0bcf28g5 – d57c – 11e7 – 9bs0 – d89d6717dx  bc ",
  " AsyncTasks ": [
   {
  " TaskId ":  1 ,
    " TaskType ":  1 ,
    " TaskStatus ":  2 ,
    " StartTime ":  156927362 ,
   " EndTime ":  156927362
    " TaskParams ": "{}", //  Layer   4   task : {" instanceId ": "
ddoscoo – 1234 – qrq2134 "},  Layer   7   task : {" domain ": " www .
aliyun . com "}
      " TaskResult ": "{}" //  Layer   4   task : {" instanceId ": "
ddoscoo – 1234 – qrq2134 ", " url ": " https :// oss . xxx . xxx "},
Layer   7   task : {" domain ": " www . aliyun . com ", " url ": "
https :// oss . xxx . xxx "},  Session   and   health   check   task
: {" instanceId ": " ddoscoo – 1234 – qrq2134 ", " url ": " https ://
oss . xxx . xxx "},  Anti – DDoS   protection   policy   task : {"
instanceId ": " ddoscoo – 1234 – qrq2134 ", " url ": " https :// oss
. xxx . xxx "}
  }
   ]
```

```
    }
```

6.7.2 CreateAsyncTask

You can call this operation to create asynchronous tasks.

Request parameters

Name	Type	Required	Description
TaskType	Integer	Yes	The type of the task. Valid values: · `1` : A value of 1 indicates that the task is to export multiple layer 4 forwarding rules. · `2` : A value of 2 indicates that the task is to export multiple layer 7 forwarding rules. · `3` : A value of 3 indicates that the task is to export session and health check settings. · `4` : A value of 4 indicates that the task is to export anti-DDoS protection policies.
TaskParams	String	Yes	The task parameter represented as a JSON string. The parameters vary depending on the task type. · When `TaskType` is set to `1` , specify the ID of the Anti-DDoS Pro instance where the rules to be exported come from. For example, {" instanceId ": " ddoscoo - cn - XXXXX "}. · When `TaskType` is set to `2` , specify an empty string. For example, {}. · When `TaskType` is set to `3` , specify the ID of the Anti-DDoS Pro instance where the rules to be exported come from. For example, {" instanceId ": " ddoscoo - cn - XXXXX "}. · When `TaskType` is set to `4` , specify the ID of the Anti-DDoS Pro instance where the rules to be exported come from. For example, {" instanceId ": " ddoscoo - cn - XXXXX "}.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " TaskType ":  1 ,
  " TaskParams ": "{}" //  Layer   4   task : {" instanceId ": "
 ddoscoo - woieuroi23  4 "},  Layer   7   task : {},  Session   and
   health   check   task : {" instanceId ": " xxxxxxxxxx "},  Anti -
 DDoS   protection   policy   task : {" instanceId ": " xxxxxxxxxx "}
}
```

Sample responses

```
{
   " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
}
```

6.7.3 DeleteAsyncTask

You can call this operation to delete asynchronous tasks.

Request parameters

Name	Type	Required	Description
TaskId	Long	Yes	The ID of the task that you want to delete.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Examples

Sample requests

```
{
  " TaskId ":  1
}
```

Sample responses

```
{
   " RequestId ": " 0bcf28g5 - d57c - 11e7 - 9bs0 - d89d6717dx  bc "
```

```
}
```

6.8 Logs

6.8.1 DescribeOpEntities

You can call this operation to perform queries on operation logs.

Request parameters

Name	Type	Required	Description
StartTime	Long	Yes	The start timestamp of the query. Unit: milliseconds.
EndTime	Long	Yes	The end timestamp of the query. Unit: milliseconds.
PageNo	Integer	Yes	The number of the starting page returned in the query result.
PageSize	Integer	Yes	The number of log records on each page. Maximum value: `50` .

Response parameters

Name	Type	Description
Total	Integer	The total number of log records.
OpEntities	OpEntity	The operation log records. For more information, see *OpEntity*.

Table 6-39: OpEntity

Name	Type	Description
GmtCreate	Long	The time when the log record was generated. Unit: milliseconds.
EntityType	Integer	The type of the operation object. Valid value: `1` . A value of 1 indicates that the operation object is an IP address.
EntityObject	String	The value of the operation object.
OpAction	Integer	The operation type. Valid value: `1` . A value of 1 indicates that the operation is to change the burstable bandwidth.
OpAccount	String	The user who performed the operation.

Name	Type	Description
OpDesc	String	The details of the operation. For more information, see *OpDesc*.

Table 6-40: OpDesc

Parameter	Type	Description
oldValue	EntityValue	The old value. For more information, see *EntityValue*.
newValue	EntityValue	The new value. For more information, see *EntityValue*.

Table 6-41: EntityValue

Name	Type	Description
elasticBandwidth	Integer	The value of the burstable bandwidth.

Examples

Sample requests

```
{
  " StartTime ":  123 ,
  " EndTime ":  456 ,
  " PageNo ":  1 ,
  " PageSize ":  10
}
```

Sample responses

```
{
  " Total ":  10 ,
  " OpEntities ": [
    {
      " gmtCreate ":  1120384 ,
      " entityObje  ct ": " 1 . 1 . 1 . 1 ",
      " opAction ":  2 ,
      " opDesc ": {
     " oldValue ": {
    " elasticBan  dwidth ":  10
 },
 " newValue ": {
    " elasticBan  dwidth ":  30
 }
  },
      " opResult ":  1
    }
  ]
```

```
    }
```

6.9 Error codes

Error code	Error message	Description
InvalidOrderType	Invalid Order Type.	The error message returned when the order type is invalid.
InvalidBaseBandwidth	Invalid Base Bandwidth.	The error message returned when the basic bandwidth is invalid.
InvalidElasticBandwidth	Invalid Elastic Bandwidth.	The error message returned when the burstable bandwidth is invalid.
InvalidPortLimit	Invalid Port Limit.	The error message returned when the number of ports is invalid.
InvalidDomainLimit	Invalid Domain Limit.	The error message returned when the number of domains is invalid.
InvalidNormalBandwidth	Invalid Normal Bandwidth.	The error message returned when the service bandwidth is invalid.
InvalidInstanceId	Invalid Instance Id.	The error message returned when the specified instance ID is invalid.
InvalidAliUid	Invalid Ali Uid.	The error message returned when the specified aliUid is invalid.
InstanceIdFormatError	Instance Id format error.	The error message returned when the format of the instance ID is invalid.
InvalidPageNo	Invalid Page No.	The error message returned when the page number is invalid.

Error code	Error message	Description
InvalidPageSize	Invalid Page Size.	The error message returned when the page size is invalid.
InvalidLine	Invalid Line.	The error message returned when the network line is invalid.
InvalidStatus	Invalid Status.	The error message returned when the status is invalid.
InvalidExpireTime	Invalid Expire Time.	The error message returned when the expiration time is invalid.
InvalidProductType	Invalid Product Type.	The error message returned when the product type is invalid.
InvalidStartTime	Invalid Start Time.	The error message returned when the start time is invalid.
InvalidEndTime	Invalid End Time.	The error message returned when the end time is invalid.
InvalidInstanceIdsSize	Invalid instanceIds size.	The error message returned when the number of instance IDs exceeds the limit.
InvalidInstanceRemark	Invalid instance remark.	The error message returned when the remark about the instance is invalid.
InternalError	Internal Error!	The error message returned when an internal error occurs.
ddos_coop3000	unknown error	The error message returned when an unknown error occurs.
ddos_coop3001	error request method	The error message returned when the request method is invalid.

Error code	Error message	Description
ddos_coop3002	http call failed	The error message returned when an error occurs while calling HTTP requests.
ddos_coop3003	no authority to do request	The error message returned when you are not authorized to perform the operation.
ddos_coop3004	receive unknown action	The error message returned when the specified request is invalid.
ddos_coop3005	auth failed	The error message returned when authentication fails.
ddos_coop3006	query db failed	The error message returned when an error occurs while querying the database.
ddos_coop3007	remote call selb central failed	The error message returned when an error occurs while calling the central controller.
ddos_coop3008	remote call ddos web failed	The error message returned when an error occurs while calling the specified service.
ddos_coop3101	encoding json failed	The error message returned when an error occurs while encoding JSON data.
ddos_coop3102	decoding json failed	The error message returned when an error occurs while decoding JSON data.
ddos_coop3103	failed parse string to int	The error message returned when an error occurs while parsing String to Int.

Error code	Error message	Description
ddos_coop3201	no enough params in request	The error message returned when one or more parameters are missing.
ddos_coop3202	params out of range	The error message returned when the parameter value exceeds the limit.
ddos_coop3203	start time must be earlier than end time	The error message returned when the start time is no earlier than the end time.
ddos_coop3301	no instance for process in db	The error message returned when the specified instance is not found in the database.
ddos_coop3302	reache port limit in spec	The error message returned when the number of ports exceeds the limit.
ddos_coop3303	l4 rule port is exist	The error message returned when the forwarding rule already exists.
ddos_coop3304	invalid rs ip address	The error message returned when the IP address is invalid.
ddos_coop12001	backend service exception	The error message returned when a service exception occurs.
ddos_coop12003	system exception	The error message returned when a system exception occurs.
ddos_coop12010	illegal sign	The error message returned when the signature is invalid.
ddos_coop12020	illegal timestamp	The error message returned when the timestamp is invalid.

Error code	Error message	Description
ddos_coop12030	illegal format	The error message returned when the data format is invalid.
ddos_coop12040	illegal service	The error message returned when the specified service does not exist.
ddos_coop12052	illegal aliyun idkp	The error message returned when the aliUid parameter is missing or the value is empty.
ddos_coop12302	listener not exists	The error message returned when the specified listener does not exist.
ddos_coop12610	lb or vs not exist	The error message returned when the specified load balancer or listener does not exist.
ddos_coop13000	db failed	The error message returned when a database connection error occurs.
ddos_coop13001	failed	The error message returned when the specified parameter is incorrect.
ddos_coop13010	json err	The error message returned when the JSON format is incorrect.
ddos_coop13020	param not enough	The error message returned when one or more parameters are missing.
ddos_coop13104	eip is released	The error message returned when the specified IP address is released.

Error code	Error message	Description
ddos_coop13105	eip not exist	The error message returned when the specified IP address does not exist.
ddos_coop15001	action not exist	The error message returned when the specified operation does not exist.
ddos_coop16020	auth fail	The error message returned when verification fails.
ddos_coop20403	auth failed	The error message returned when authentication fails.
ddos_coop20404	not found	The error message returned when the specified service is not found.
ddos_coop21001	invalid parameter	The error message returned when the specified parameter is invalid.
ddos_coop21002	invalid method	The error message returned when the specified method is invalid.
ddos_coop21003	invalid product	The error message returned when the specified product is invalid.
ddos_coop21004	invalid region	The error message returned when the specified region is invalid.
ddos_coop21005	no action found	The error message returned when the specified operation does not exist.

Error code	Error message	Description
ddos_coop21006	invalid action	The error message returned when the specified operation is invalid.
ddos_coop221007	action disabled	The error message returned when the specified API is disabled.
ddos_coop29999	system error	The error message returned when a system error occurs.