

Alibaba Cloud Anti-DDoS Pro

New Anti-DDoS Pro Service

Issue: 20200102

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, consequent

ial, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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

.

Document conventions

Style	Description	Example
	A danger notice 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.
	A warning notice 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 restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	Courier font is used for commands.	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Contents

Legal disclaimer.....	I
Document conventions.....	I
1 Product Introduction.....	1
1.1 What is Anti-DDoS Pro.....	1
2 Pricing.....	4
2.1 Billing and metering.....	4
2.2 Protection packages.....	10
2.3 Buy Anti-DDoS Pro instances.....	14
2.4 Upgrade Anti-DDoS Pro instance configurations.....	16
3 Quick Start.....	18
3.1 Set up Anti-DDoS Pro using domains.....	18
3.1.1 Overview.....	18
3.1.2 Step 1: Add a website.....	19
3.1.3 Step 2: Change DNS records.....	24
3.1.4 Step 3: Configure DDoS protection policies.....	27
3.1.5 Step 4: Configure HTTP flood protection policies.....	31
3.1.6 Step 5: View security reports and log data.....	36
3.2 Set up Anti-DDoS Pro using IPs and ports.....	39
3.2.1 Overview.....	39
3.2.2 Step 1: Create a port forwarding rule.....	40
3.2.3 Step 2: Configure protection policies.....	43
3.2.4 Step 3: View traffic statistics.....	49
4 Deploy Anti-DDoS Pro.....	52
4.1 Websites.....	52
4.1.1 Custom non-standard ports.....	52
4.1.2 Upload SSL certificates.....	53
4.1.3 Custom TLS security settings.....	56
4.1.4 Import and export configurations.....	58
4.2 Provisioning settings.....	65
4.2.1 Use NS records to set up Anti-DDoS Pro.....	65
4.3 Security traffic manager.....	68
4.4 Add Anti-DDoS Pro back-to-origin CIDR blocks to the whitelist.....	78
4.5 Change the IP of an ECS instance.....	80
5 Security overview.....	82
6 View security reports.....	88
7 Configure protection policies.....	90
7.1 Protection for Infrastructure.....	90
7.1.1 Block traffic flow.....	90

7.1.2 Deactivate the black hole status.....	92
7.2 Configure layer 7 protection.....	93
7.2.1 Configure the blacklist and whitelist.....	93
7.2.2 Block requests from specific regions.....	95
7.2.3 Configure fine-grained access control rules.....	97
7.2.4 Configure HTTP flood protection.....	104
7.2.5 Enable intelligent protection.....	107
7.3 Configure layer 4 protection.....	108
7.3.1 Configure layer 4 anti-DDoS protection settings.....	108
7.3.2 Configure layer 4 smart defense settings.....	110
7.4 Configure static page caching rules.....	114
8 Security statistics.....	117
8.1 Full log.....	117
8.2 Fields.....	120
8.3 Operation logs.....	125
9 Resource management.....	126
10 API Reference.....	127
10.1 API overview.....	127
10.2 Use the API.....	129
10.3 Common parameters.....	132
10.4 Instances.....	134
10.4.1 DescribeInstances.....	134
10.4.2 DescribeInstanceDetails.....	136
10.4.3 DescribeInstanceSpecs.....	137
10.4.4 DescribeInstanceStatistics.....	138
10.4.5 DescribeElasticBandwidthSpec.....	140
10.4.6 ModifyElasticBandWidth.....	141
10.4.7 ModifyInstanceRemark.....	141
10.5 Layer 4 rules.....	142
10.5.1 CreateLayer4Rule.....	142
10.5.2 ConfigLayer4Rule.....	143
10.5.3 DeleteLayer4Rule.....	144
10.5.4 ConfigLayer4RuleAttribute.....	145
10.5.5 ConfigHealthCheck.....	148
10.5.6 DescribeLayer4Rules.....	150
10.5.7 DescribeLayer4RuleAttributes.....	152
10.5.8 DescribeHealthCheckList.....	155
10.5.9 DescribeHealthCheckStatusList.....	157
10.6 Layer 7 rules.....	159
10.6.1 DescribeDomains.....	159
10.6.2 CreateLayer7Rule.....	162
10.6.3 ConfigLayer7Rule.....	163
10.6.4 DeleteLayer7Rule.....	165
10.6.5 ConfigLayer7Cert.....	165

10.6.6 ConfigLayer7BlackWhiteList.....	167
10.6.7 DescribeLayer7InstanceRelations.....	168
10.6.8 DescribeCertList.....	169
10.6.9 EnableLayer7CC.....	170
10.6.10 DisableLayer7CC.....	171
10.6.11 EnableLayer7CCRule.....	171
10.6.12 DisableLayer7CCRule.....	172
10.6.13 AddLayer7CCRule.....	173
10.6.14 ConfigLayer7CCRule.....	174
10.6.15 DescribeLayer7CCRules.....	176
10.6.16 DeleteLayer7CCRule.....	178
10.6.17 ConfigLayer7CCTemplate.....	178
10.6.18 DescribeDomainAccessMode.....	179
10.6.19 ConfigDomainAccessMode.....	181
10.6.20 DescribeBackSourceCidr.....	182
10.7 Logs.....	182
10.7.1 DescribeOpEntities.....	182
10.8 Tasks.....	185
10.8.1 ListAsyncTask.....	185
10.8.2 CreateAsyncTask.....	188
10.8.3 DeleteAsyncTask.....	189
10.9 Error codes.....	190
11 Best Practices.....	197
11.1 Managed Security Service.....	197
11.2 Create an Anti-DDoS Pro alert rule.....	198
11.3 Monitor black hole events and traffic scrubbing events on Anti-DDoS Pro.....	207
11.4 Create an Anti-DDoS Pro dashboard.....	214
11.5 Migrate to the latest Anti-DDoS Pro.....	221

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 and metering

Anti-DDoS Pro uses high-bandwidth BGP lines to protect your workloads against volumetric DDoS attacks (over 300 Gbit/s). We recommend that you use Anti-DDoS Pro to safeguard your workloads if they are sensitive to the response latency. This topic describes billing and metering about Anti-DDoS Pro.

Basic protection (subscription)

Basic mitigation capacity	Network	Price (standard function)	Price (enhanced function)
30 Gbit/s	Eight BGP-line	USD 3,120/month	USD 4,320/month
60 Gbit/s	Eight BGP-line	USD 7,020/month	USD 8,220/month
100 Gbit/s	Eight BGP-line	USD 49,230/year (discount price for annual subscription)	USD 63,630/year (discount price for annual subscription)
300 Gbit/s	Eight BGP-line	USD 79,260/year (discount price for annual subscription)	USD 93,660/year (discount price for annual subscription)
400 Gbit/s	Eight BGP-line	USD 145,300/year (discount price for annual subscription)	USD 159,700/year (discount price for annual subscription)
500 Gbit/s	Eight BGP-line	USD 563,430/year (discount price for annual subscription)	USD 577,830/year (discount price for annual subscription)
600 Gbit/s	Eight BGP-line	USD 670,610/year (discount price for annual subscription)	USD 685,010/year (discount price for annual subscription)



Note:

- For more information about the differences between the standard and enhanced function plans, see [Protection packages](#).
- If you need a higher bandwidth to safeguard your workloads, submit a ticket.

The following table shows the specification of an Anti-DDoS Pro instance.



Note:

You can expand the capacity of an Anti-DDoS Pro instance when you purchase the instance, or upgrade the instance after you purchase it.

Specification	Description	Default	Unit price for capacity expansion
Number of protected ports	The number of TCP and UDP ports that can be protected by the instance.	50 ports	Every 5 additional ports: USD 7.5/month
Number of protected domain names	The number of HTTP and HTTPS domain names that can be protected by the instance.	50 domain names <div> Note: A maximum of 5 top-level domains are supported. The subdomains that you add to the instance can belong to no more than 5 top-level domains. </div>	<ul style="list-style-type: none"> • Every 10 additional domain names (standard function): USD 4.5/month • Every 10 additional domain names (enhanced function): USD 7.5/month <div> Note: Every 10 additional protected domain names contain one top-level domain. </div>

Specification	Description	Default	Unit price for capacity expansion
Clean bandwidth	The maximum bandwidth for your workloads when no attack is launched to the instance.	100 Mbit/s	<ul style="list-style-type: none"> 100 Mbit/s < Bandwidth ≤ 600 Mbit/s (tier 1): You are charged at a price of USD 15/month for every Mbit/s that exceeds the default bandwidth. 600 Mbit/s < Bandwidth ≤ 5000 Mbit/s (tier 2): You are charged at a price of USD 11/month for every Mbit/s that exceeds tier 1.
Clean QPS	The maximum number of HTTP and HTTPS requests that can be concurrently processed per second when no attack is launched to the instance.	3,000 QPS	Every 100 additional QPS: USD 1.5/month

Burstable protection (Pay-As-You-Go)

Burstable protection is used as an addition to protect your workloads when the peak of DDoS attacks exceeds the bandwidth limit of basic protection. Burstable protection is charged based on the difference between the highest peak of DDoS attacks of a day and the bandwidth limit of basic protection.



Note:

If you set the basic bandwidth and burstable bandwidth to the same value, no fee is charged. This means that your Anti-DDoS Pro instance does not provide burstable protection.

Assume that you have an Anti-DDoS Pro instance whose basic bandwidth is 30 Gbit/s and burstable bandwidth is 100 Gbit/s. Two DDoS attacks are launched to the instance on the same day. The peaks of the two DDoS attacks are 80 Gbit/s and 40 Gbit/s. Consequently, burstable protection is charged based on the higher peak 80 Gbit/s. The difference between the peak and basic bandwidth is 50 Gbit/s. According to the following pricing tier table, Anti-DDoS Pro charges USD 960 for burstable protection.

**Note:**

- No fee is charged for burstable protection if the highest peak of DDoS attacks on the current day is lower than the basic bandwidth.
- No fee is charged for burstable protection if the highest peak of DDoS attacks on the current day is higher than the burstable bandwidth. This means that the instance is not able to mitigate all the DDoS attacks. To protect your workloads, all the network traffic destined for the instance is routed to the black hole.
- Bill statements for burstable protection on the current day are generated between 8:00 to 9:00 the next day.

Pricing tier	Price
0 Gbit/s < Bandwidth difference \leq 5 Gbit/s	USD 120/day
5 Gbit/s < Bandwidth difference \leq 10 Gbit/s	USD 180/day
10 Gbit/s < Bandwidth difference \leq 20 Gbit/s	USD 330/day
20 Gbit/s < Bandwidth difference \leq 30 Gbit/s	USD 540/day
30 Gbit/s < Bandwidth difference \leq 40 Gbit/s	USD 730/day
40 Gbit/s < Bandwidth difference \leq 50 Gbit/s	USD 960/day

Pricing tier	Price
50 Gbit/s < Bandwidth difference ≤ 60 Gbit/s	USD 1,170/day
60 Gbit/s < Bandwidth difference ≤ 70 Gbit/s	USD 1,380/day
70 Gbit/s < Bandwidth difference ≤ 80 Gbit/s	USD 1,590/day
80 Gbit/s < Bandwidth difference ≤ 100 Gbit/s	USD 1,770/day
100 Gbit/s < Bandwidth difference ≤ 150 Gbit/s	USD 2,190/day
150 Gbit/s < Bandwidth difference ≤ 200 Gbit/s	USD 3,240/day
200 Gbit/s < Bandwidth difference ≤ 300 Gbit/s	USD 4,200/day
300 Gbit/s < Bandwidth difference ≤ 400 Gbit/s	USD 6,000/day
400 Gbit/s < Bandwidth difference ≤ 500 Gbit/s	USD 7,510/day
500 Gbit/s < Bandwidth difference ≤ 600 Gbit/s	USD 9,010/day
600 Gbit/s < Bandwidth difference ≤ 700 Gbit/s	USD 10,510/day
700 Gbit/s < Bandwidth difference ≤ 800 Gbit/s	USD 12,010/day
800 Gbit/s < Bandwidth difference ≤ 900 Gbit/s	USD 13,510/day
900 Gbit/s < Bandwidth difference ≤ 1,000 Gbit/s	USD 15,010/day
1,000 Gbit/s < Bandwidth difference ≤ 1,100 Gbit/s	USD 16,510/day
1,100 Gbit/s < Bandwidth difference ≤ 1,200 Gbit/s	USD 18,010/day
1,200 Gbit/s < Bandwidth difference ≤ 1,300 Gbit/s	USD 19,510/day

Pricing tier	Price
1,300 Gbit/s < Bandwidth difference ≤ 1,400 Gbit/s	USD 21,010/day
1,400 Gbit/s < Bandwidth difference ≤ 1,500 Gbit/s	USD 22,520/day

Refunding

You cannot refund subscription or Pay-As-You-Go Anti-DDoS Pro instances. After you purchase a subscription Anti-DDoS Pro instance, you cannot cancel the subscription.

Bandwidth sizing

You can select an appropriate bandwidth specification based on the daily inbound and outbound traffic peaks of all workloads that have or will be connected to your Anti-DDoS Pro instance. Make sure that the clean bandwidth of the instance is higher than the larger of the inbound and outbound traffic peaks.

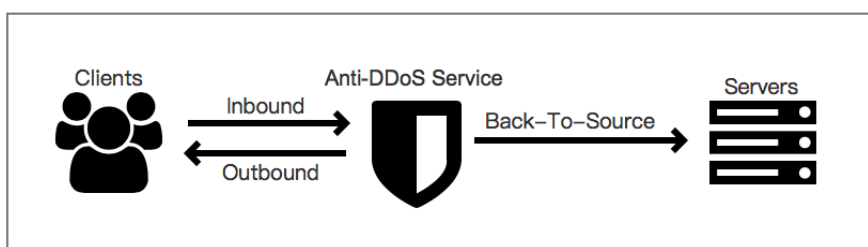


Note:

In most cases, the peak of the outbound traffic is higher than that of the inbound traffic.

You can estimate the actual bandwidth according to the traffic statistics collected by the ECS console or other monitoring tools on your origin server. The traffic described here refers to the user traffic that traverses through your services.

For example, you have connected a website to an Anti-DDoS Pro instance for protection. When no attack is launched to your website, Anti-DDoS Pro only needs to reroute user traffic to the origin server. When your website is under attack, Anti-DDoS Pro blocks malicious traffic, and reroutes only user traffic to the origin server. Therefore, the ECS console only collects statistics about inbound and outbound user traffic from the origin server. If your workloads are deployed on multiple origin servers, you must sum up the traffic volumes on all origin servers.



For example, you want to connect three websites to an Anti-DDoS Pro instance. The peak of the outbound user traffic on each website is 50 Mbit/s or lower. The total bandwidth required by the three websites is 150 Mbit/s or lower. In this case, you only need to make sure that the clean bandwidth of the purchased instance is higher than 150 Mbit/s.

Domain name sizing

The number of top-level domains supported by an Anti-DDoS instance depends on the number of domain names supported by the instance. Every 10 domain names contain one top-level domain. By default, an Anti-DDoS Pro instance supports a maximum of 50 domain names, including subdomains, wildcard domains, and up to 5 top-level domains.

For example, you add the top-level domain `abc.com` to the instance, and then add subdomains and wildcard domains, including `www.abc.com`, `*.abc.com`, `mail.abc.com`, `user.pay.abc.com`, and `x.y.z.abc.com`.



Note:

All the domain names, including the top-level domain `abc.com`, are taken into account by the quota limit of the instance.

If you want to add more top-level domains or subdomains, you must increase the maximum number of protected domain names by upgrading the instance. If you add a top-level domain or subdomain before you upgrade the instance, you receive the following notification:

The quota of top-level domains has been exceeded. Upgrade the instance to expand the quota for protected domain names.

In this case, you must upgrade the instance for 10 additional protected domain names.

2.2 Protection packages

The new Anti-DDoS Pro provides two protection packages: standard and enhanced. The enhanced package includes all features of the standard package and provides the following exclusive features: static page caching, non-standard ports support,

and geo-blocking. You can select the protection package based on your business needs.

When you purchase Anti-DDoS Pro instances, the standard package is selected by default. You can choose the enhanced package for advanced DDoS protection capabilities. For each instance, Anti-DDoS Pro charges additional RMB 8,000 per month for the enhanced package.

If you have already purchased Anti-DDoS Pro instances of the standard package, you can [Upgrade Anti-DDoS Pro instance configurations](#).

**Note:**


After you purchased the enhanced package or upgraded your instance, you need to modify domain configurations to enable the enhanced capabilities.


Comparison of the standard and enhanced package

The enhanced package offers advanced protection capabilities and supports non-standard ports.

Category	Feature	Description	Standard package	Enhanced package
Protection algorithm	Protection against DDoS attacks	Supports protection against common DDoS attacks such as malformed packet attacks and flood attacks.	✓	✓
	Protection against resource exhaustion attacks	Supports protection against common HTTP flood attacks, such as HTTP GET floods and HTTP POST floods. For more information, see Configure HTTP flood protection .	✓	✓

Category	Feature	Description	Standard package	Enhanced package
	Intelligent protection	<ul style="list-style-type: none"> • Supports intelligent protection against application layer floods and effectively mitigates HTTP flood attacks. • Supports intelligent protection against transport layer floods and effectively mitigates TCP flood attacks. <p>For more information, see Enable intelligent protection.</p>	✓	✓
Protection rule	Blacklist and whitelist	<p>For each protected domain, the blacklist and whitelist can each contain a maximum of 200 IP addresses or CIDR blocks.</p> <p>For more information, see Configure the blacklist and whitelist.</p>	✓	✓

Category	Feature	Description	Standard package	Enhanced package
	Accurate access control	<p>Supports fine-grained access control based on HTTP fields.</p> <p>For more information, see Configure fine-grained access control rules.</p>	For each protected domain, a maximum of five rules can be configured based on the following fields: IP, URL, Referer, and User-Agent.	For each protected domain, a maximum of 10 rules can be configured.
	Geo-blocking	<p>Supports blocking traffic based on geographical locations.</p> <p>For more information, see Block requests from specific regions.</p>	✗	✓
Connection method	Standard HTTP ports (80, 8080) and HTTPS ports (443, 8443).	Supports DDoS protection based on standard HTTP ports (80, 8080) and HTTPS ports (443, 8443).	✓	✓
	Non-standard HTTP and HTTPS ports.	<p>Supports DDoS protection based on non-standard HTTP and HTTPS ports.</p> <div>  <p>Note: For each instance, the associated domains can use a maximum of 10 ports.</p> </div>	✗	✓

Category	Feature	Description	Standard package	Enhanced package
Other	Static page caching	<p>Supports static page caching to reduce page loading time.</p> <div>  Note: Currently, static page caching is in preview stage. For each protected domain, a maximum of three rules can be configured. </div> <p>For more information, see Configure static page caching rules.</p>	✗	✓

2.3 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](#).

Edition

Profession

Line Resource

Eight Line BGP

Basic Bandwidth

30Gb	60Gb	100Gb	300Gb	400Gb	500Gb
600Gb					

This part is base bandwidth.Prepayment.

Burstable Bandwidth

30Gb	40Gb	50Gb	60Gb	70Gb	80Gb
100Gb	150Gb	200Gb	300Gb		

The burstable bandwidth is the maximum bandwidth provided by the instance during protection. If you set the burstable bandwidth and basic bandwidth to the same value, no additional fees will be incurred and the maximum bandwidth provided by the instance equals the basic bandwidth. If you set the burstable bandwidth to a value greater than the basic bandwidth, the instance can provide protection against attacks with bandwidth greater than the basic bandwidth but no greater than the burstable bandwidth. Additional fees will be incurred based on the peak attack bandwidth.

Clean Bandwidth

11

1250M

2500M

5000M

100

M

When the traffic on your website exceeds the service bandwidth, packet loss may occur or the server performance may degrade. We recommend that you increase your service bandwidth to resolve these issues.

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](#).

2.4 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.

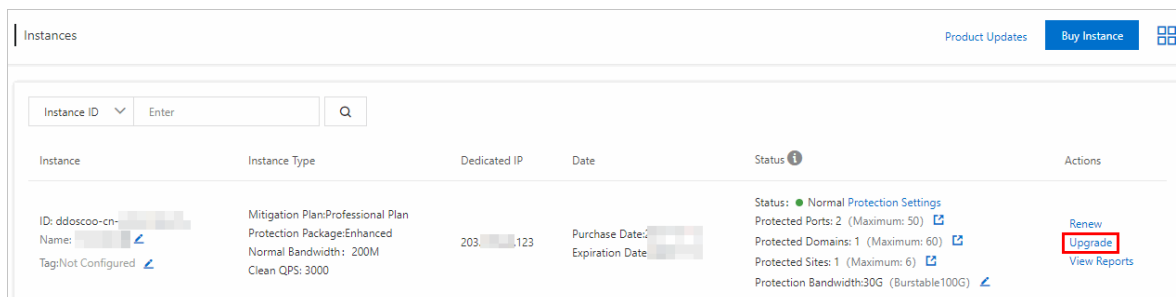
- **Service Bandwidth:** For each Mbit/s of bandwidth, Anti-DDoS Pro charges additional USD 15.63 per month. This fee is calculated based on your remaining subscription time.

**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 using domains

3.1.1 Overview

This topic describes how to set up Anti-DDoS Pro by using domains to enable DDoS protection and HTTP flood protection for your website.

To set up Anti-DDoS Pro using domains, use the following steps:

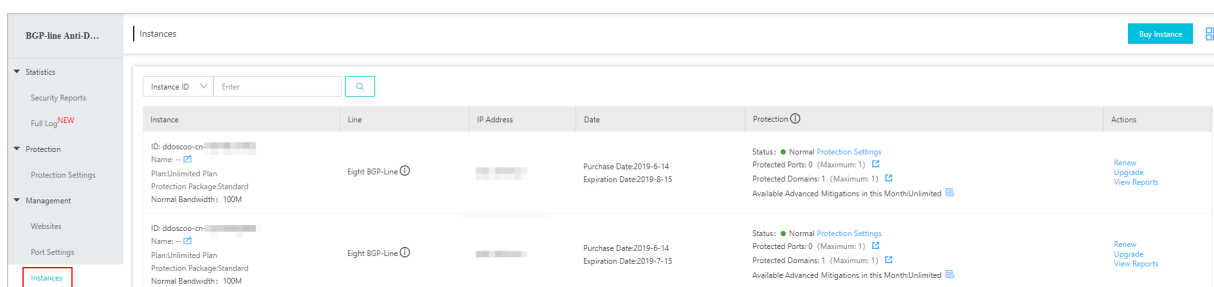
Task	Description
<i>Step 1: Add a website</i>	In the Anti-DDoS Pro console, add your website to associate its domain with an Anti-DDoS Pro instance, and configure traffic forwarding.
<i>Step 2: Change DNS records</i>	<p>Modify the DNS records of your domain to forward incoming traffic to your site to the Anti-DDoS Pro instance that is associated with your domain.</p> <p>After DNS records are modified, all traffic to your protected domain is forwarded to Anti-DDoS Pro first. Anti-DDoS Pro filters out malicious traffic and forwards traffic back to the origin server.</p>
<i>Step 3: Configure DDoS protection policies</i>	<p>After you set up an Anti-DDoS Pro instance to protect your service, Anti-DDoS Smart Defense is enabled by default. You can modify the following DDoS protection policies to meet your changing needs:</p> <p>scrubbing mode, blacklist and whitelist, black hole, and traffic blocking.</p>
<i>Step 4: Configure HTTP flood protection policies</i>	<p>After you set up an Anti-DDoS Pro instance to protect your service, you can configure the following HTTP flood protection policies to protect your site against HTTP flood attacks:</p> <p>blacklist and whitelist, HTTP flood protection.</p>
<i>Step 5: View security reports and log data</i>	After you set up an Anti-DDoS Pro instance to protect your service, you can view security reports and log data in the Anti-DDoS Pro console.

3.1.2 Step 1: Add a website

After you buy an Anti-DDoS Pro instance, you must add your website in the Anti-DDoS Pro console. To set up an Anti-DDoS Pro instance to protect your service, you need to enter your domain information in the Anti-DDoS Pro console.

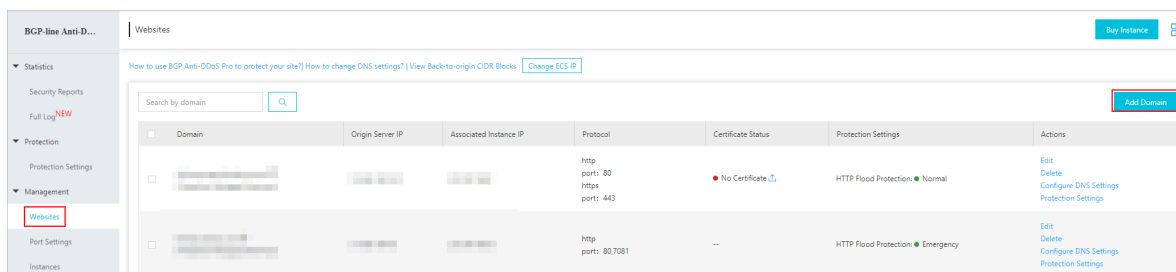
Prerequisites

You have purchased an Anti-DDoS Pro instance. To view your instance, go to the **Management > Instances** page. For more information about purchasing Anti-DDoS Pro instances, see [Buy Anti-DDoS Pro instances](#).







Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, select **Management > Websites**.
3. On the **Websites** page, click **Add Domain**.




4. On the **Add Domain** page, complete the configuration under the **Enter Site Information** tab. The configuration details are as follows:

Item	Description
Protection Package	<p>The type of Anti-DDoS Pro instance that you want to associate with the domain. Valid values:</p> <ul style="list-style-type: none"> • Standard • Enhanced

Item	Description
Instance	<p>Available instances are listed based on the specified Protection Package.</p> <div>  Note: If no instance is displayed, it means you have no instance under the specified Protection Package. We recommend that you buy an Enhanced instance or upgrade the existing Standard instance to the Enhanced type. </div> <p>Select one or more instances to associate with the domain.</p> <div>  Note: You can associate a domain with a maximum of eight Anti-DDoS Pro instances. Besides, these instances must under the same Protection Package. </div>
Domain	<p>The domain of the website that you want to protect.</p> <div>  Note: <ul style="list-style-type: none"> • Supports wildcard domains, such as *.aliyun.com. Anti-DDoS Pro automatically matches all subdomains for the wildcard domain. • If you enter a wildcard domain and a specific domain name, such as *.aliyun.com and www.aliyun.com, Anti-DDoS Pro will use the redirection rules and protections policies of the specific domain name. </div>
Protocol	<p>The protocols supported by your website. Valid values:</p> <ul style="list-style-type: none"> • HTTP (Selected by default) • HTTPS (Selected by default) • WebSocket • Websockets <div>  Note: If your website supports HTTPS encrypted connections, you must select HTTPS. Select other protocols if applicable. </div>

Item	Description
Server Address	<p>Select the address type of the origin server and specify the address. Supported address types are as follows:</p> <ul style="list-style-type: none">• Origin Server IP: You can enter up to 20 IP addresses of the origin server. When multiple origin server IPs are specified, Anti-DDoS Pro uses IP hash load balancing to forward traffic back to the origin server.• Origin Server Domain: 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.

Item	Description
Origin server ports	<p>The server ports are automatically assigned based on the protocols you have selected.</p> <div>  Note: The forwarding port is the same as the port of the origin server. </div> <ul style="list-style-type: none"> When HTTP or Websocket is selected, the port is set to 80 by default. When HTTPS or Websockets is selected, the port is set to 443 by default. <p>Anti-DDoS Pro allows you to specify custom ports. You can click Custom to select ports other than the default ones.</p> <div> <p>Server Port: HTTP 80 HTTPS 443 Custom</p> <p>Server Port: HTTP HTTPS Save Cancel</p> <p>80,8080</p> <p>If there are other ports, please add them and separate them by " View optional range</p> </div> <ul style="list-style-type: none"> Standard instance: The optional HTTP/Websocket ports are 80 and 8080. The optional HTTPS/Websockets ports are 443 and 8443. Enhanced instance: The optional HTTP/Websocket and HTTPS/Websockets ports are described in the following figures. <div> <p>Optional port range</p> <p>http/websocket https/websockets Q</p> <p>80, 83, 84, 88, 89, 800, 808, 1000, 1090, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7060, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8106, 8181, 8334, 8336, 8800, 8686, 8787, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9999, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702</p> </div> <div> <p>Optional port range</p> <p>http/websocket https/websockets Q</p> <p>443, 4443, 5443, 6443, 7443, 8443, 9443, 8553, 8663, 9553, 9663, 18980</p> </div>

* Protection Package ⓘ Standard Enhanced

* Instance ☐ ddoscoo-cn-
☐ ddoscoo-cn-
(You can associate a domain with a maximum of eight Anti-DDoS Pro instances. You have selected 0 instances.)

* Domain:
Supports top-level domains, such as test.com, and secondary level domains, such as www.test.com.

* Protocol: ☒ HTTP ☒ HTTPS ☐ Websocket ☐ Websockets

* Server IP: ☒ Origin Server IP ☐ Origin Server Domain

Separate multiple IP addresses with commas (.). You can add a maximum of 20 IP addresses. Do not repeat.

✔ If the IP addresses of your origin server have been exposed, [click here](#) to learn how to fix the issue.

Server Port: HTTP 80 HTTPS 443 Custom

Add

5. Click Add.

Result

After a domain is added, you are automatically directed to the **Modify DNS Records** page. You can click **Back** to go to the **Websites** page and view the newly added domain information.

Enter Site Information Modify DNS Records Complete

Change the DNS settings by following these steps:

Change the DNS settings by following these steps:


- ☐ Copy the IP address of the Anti-DDoS Pro instance.
- ☒ Modify DNS settings at your DNS provider.

BGP-line Anti-DDoS Pro starts to protect your site after the modifications are completed.

Why should I modify the DNS settings? ▼

Common DNS Providers ▼

Scan QR code,
Join Anti-DDoS Pro Expert Consulting group



Contact by phone.

Technical Support

Return to Sites Next

Anti-DDoS Pro automatically associates each domain with an Anti-DDoS Pro instance IP address. You need to change the A record value of your domain to the Anti-DDoS Pro instance IP address. The incoming traffic to your site is then forwarded to your Anti-DDoS Pro Instance.

Domain	Origin Server IP	Associated Instance IP	Protocol	Certificate Status	Protection Settings	Actions
a-doctest.aliyun.com Protection Package: Standard			http port: 80 https port: 443	No Certificate	HTTP Flood Protection: Normal	Edit Delete Configure DNS Settings Protection Settings
			https port: 443 http port: 80	No Certificate	HTTP Flood Protection: Normal	Edit Delete Configure DNS Settings Protection Settings

What's next

- [Step 2: Change DNS records](#)
- [Upload SSL certificates](#): If your website supports the HTTPS protocol, you must upload your SSL certificate to enable Anti-DDoS Pro to filter HTTPS requests.

3.1.3 Step 2: Change DNS records

This topic describes how to change A records in the Alibaba Cloud DNS console to forward incoming traffic to your site to your Anti-DDoS Pro instance.

Prerequisites

Make sure to complete the following tasks before you change DNS records.

- You have added your website in the Anti-DDoS Pro console. For more information, see [Step 1: Add a website](#).
- If you are using additional firewalls to protect your origin server, disable the firewalls or add the back-to-origin IP addresses used by your Anti-DDoS Pro instance to the whitelist. For more information, see [Add Anti-DDoS Pro back-to-origin CIDR blocks to the whitelist](#).

After the incoming traffic to your site is forwarded to the IP address of your Anti-DDoS Pro instance, the instance scrubs your traffic and uses the back-to-origin IP addresses to forward normal traffic back to your origin server. Therefore, if the back-to-origin IP addresses used by your Anti-DDoS Pro instance are not added to the whitelist of your firewall, normal traffic to your site may be blocked by mistake, making your website inaccessible.

- Verify that your forwarding configuration works as expected. Before you change DNS records to forward incoming traffic to Anti-DDoS Pro, we recommend that you verify that your Anti-DDoS Pro instance can forward traffic back to the origin server. For more information, see [Verify forwarding configurations](#).

Context

The following example assumes that your domain is managed by [Alibaba Cloud DNS](#). If you are using other domain name resolution services, log on to the DNS server and change the A record value of your domain to the IP addresses of your Anti-DDoS Pro instance.



Note:

Alibaba Cloud provides free and paid versions of Alibaba Cloud DNS. If your domain is managed under a paid version of Alibaba Cloud DNS, we recommend that you use NS records to set up your Anti-DDoS Pro instance. For more information, see [Use NS records to set up Anti-DDoS Pro](#).

Assume that you added the following domain in step 1: `bgp.ddostest.com`. The following example describes how to change or add A records in the Alibaba Cloud DNS console.

Procedure

1. Log on to the [Alibaba Cloud DNS console](#).
2. On the Manage DNS page, select domain `doctest.com`, and click **Configure** in the Actions column.

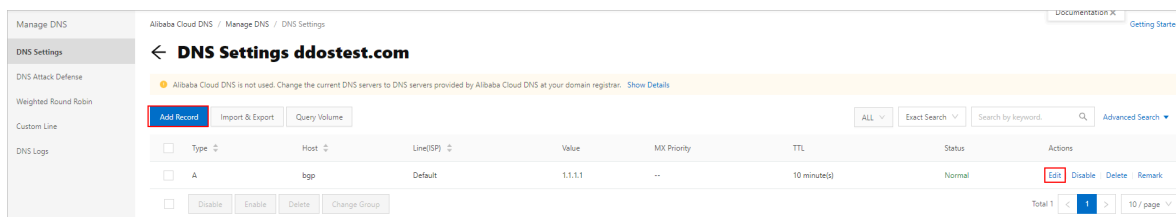


3. On the DNS Settings page, select the A record whose host is `bgp`, and click **Edit** in the Actions column.



Note:

If you cannot find the A record in the list, you can click **Add Record**.



4. On the Edit Record or Add Record dialog box, change the Value to the IP address of your Anti-DDoS Pro instance.

**Note:**

After you add a domain in the Anti-DDoS Pro console, the domain is automatically associated with an Anti-DDoS Pro instance. To view the IP address of the Anti-DDoS Pro instance associated with your domain, go to the [Anti-DDoS Pro console](#) and select Management > Websites. For more information, see [Step 1: Add a website](#).

Domain	Origin Server IP	Associated Instance IP	Protocol	Certificate Status	Protection Settings	Actions
[Redacted]	[Redacted]	[Redacted]	http port: 80 https port: 443	No Certificate	HTTP Flood Protection: Emergency	Edit Delete Configure DNS Settings Protection Settings
bgp.ddostest.com Protection Package: Standard	[Redacted]	[Redacted]	https port: 443 http port: 80	No Certificate	HTTP Flood Protection: Normal	Edit Delete Configure DNS Settings Protection Settings

Edit Record

Type: A- IPv4 address

Host: bgp .ddostest.com

ISP Line: Default - Return to the default value when the query is not ...

* Value: [Redacted]

* TTL: 10 minute(s)

Cancel OK

5. Click OK and wait for the configuration to take effect.

What's next

[Step 3: Configure DDoS protection policies](#)

3.1.4 Step 3: Configure DDoS protection policies

After you set up an Anti-DDoS Pro instance to protect your service, Anti-DDoS Smart Defense is enabled by default. You can modify DDoS protection policies based on your needs.

Prerequisites

You have added your website in the Anti-DDoS Pro console. For more information, see [Step 1: Add a website](#).

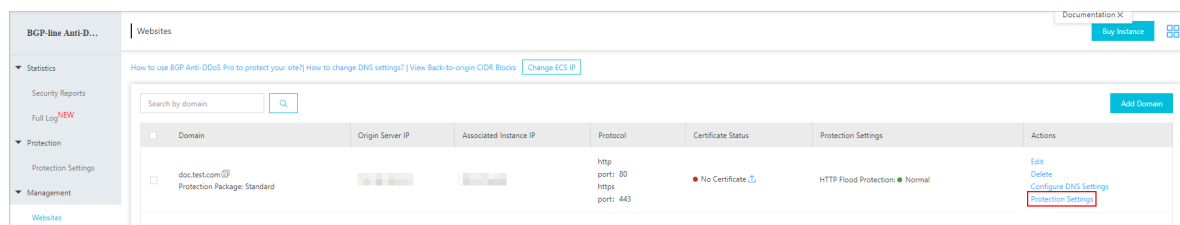
Context

You can modify the following DDoS protection policies:

DDoS protection policy	Description
Scrubbing mode	Smart Defense bases its decisions on historical traffic data. If this is the first time that you set up an Anti-DDoS Pro instance to protect your service, note that it takes Smart Defense about three days to learn your traffic pattern to provide the best protection. If attacks are launched against your service within these three days, you can mitigate attacks by limiting the number of new connections from specific IP addresses. If Smart Defense fails to meet your needs under the normal mode, you can set the mode to strict to enable the most rigorous protection.
Blacklist and whitelist	For IP addresses that send a large number of malicious requests to your server, you can add them to the blacklist to block their requests. You can add the following IP addresses to the whitelist to allow their requests without further inspection: internal CIDR blocks, service interface IP addresses, and verified IP addresses.
Deactivate black holes	After you set up an Anti-DDoS Pro instance to protect your site, incoming traffic to your site is forwarded to a black hole when the peak attack bandwidth exceeds your basic or burstable bandwidth. To restore your service, you can deactivate the black hole in the Anti-DDoS Pro console.
Block traffic	We recommend that you block traffic when your service is experiencing DDoS attacks and the peak attack bandwidth is likely to exceed your burstable bandwidth. You can block overseas traffic transmitted through China Telecom and China Unicom networks to mitigate attacks.

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose Management > Websites.
3. In the websites list, select a domain and click Protection Settings.



4. On the Protection Settings page, click Anti-DDoS Protection Policies and perform the following steps based on your needs:

- **Scrubbing Mode**

Select an Anti-DDoS Pro instance and click **Modify Smart Defense Mode** in the Actions column. In the **Modify Smart Defense Mode** dialog box, select a scrubbing mode. Anti-DDoS Pro supports the following scrubbing modes:

- **Low:** This mode scrubs traffic that displays common attack patterns. The mode provides moderate protection capabilities and has a low false positive rate.
- **Normal:** This mode scrubs traffic that displays common and likely attack patterns. The mode maintains an optimal balance between protection and false positives.
- **Strict:** This mode provides the most rigorous protection against malicious traffic and may cause a certain number of false positives.

The screenshot shows the 'Protection Settings' page with the 'Anti-DDoS Protection Policies' tab selected. A table lists four instances, each with a 'Smart Defense Mode Switch' (turned on) and a 'Smart Defense Mode' (Strict, Normal, Normal, Normal). The 'Modify Smart Defense Mode' link in the 'Actions' column for the second instance is highlighted with a red box. Below the table, the 'Modify Smart Defense Mode' dialog box is open, showing 'Scrubbing Mode' with three buttons: 'Low', 'Normal' (selected), and 'Strict'. A description states: 'Based on historical service logs and expert experience algorithm, this mode defends against suspicious IP with obvious attack behaviors. It has a good balance between protection effect and false interruption.' The 'OK' button is highlighted in blue.

Instance	Line	IP Address	Smart Defense Mode Switch	Smart Defense Mode	Actions
ddoscoo-cn-...	coop-line-shenzhen-CT	...	On	Strict	Modify Smart Defense Mode
ddoscoo-cn-...	coop-line-shenzhen-CT	...	On	Normal	Modify Smart Defense Mode
ddoscoo-cn-...	coop-line-001	...	On	Normal	Modify Smart Defense Mode
ddoscoo-cn-...	coop-line-001	...	On	Normal	Modify Smart Defense Mode

Modify Smart Defense Mode

Scrubbing Mode:

Based on historical service logs and expert experience algorithm, this mode defends against suspicious IP with obvious attack behaviors. It has a good balance between protection effect and false interruption.

- **Blacklist and Whitelist**

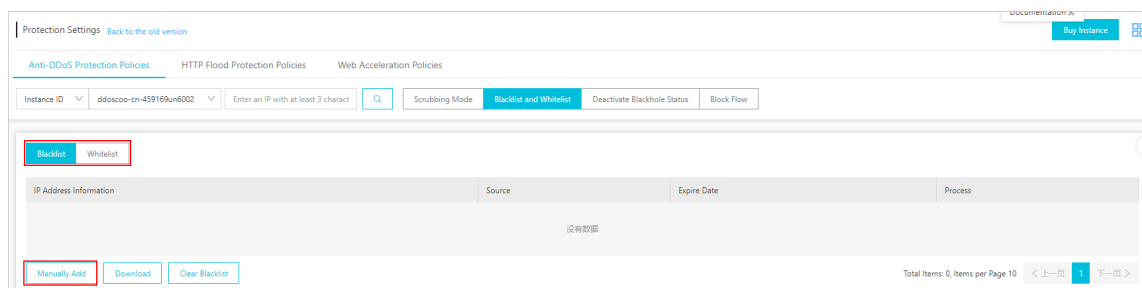


Note:

The configurations of the blacklist and whitelist are effective for individual domains, not Anti-DDoS Pro instances.

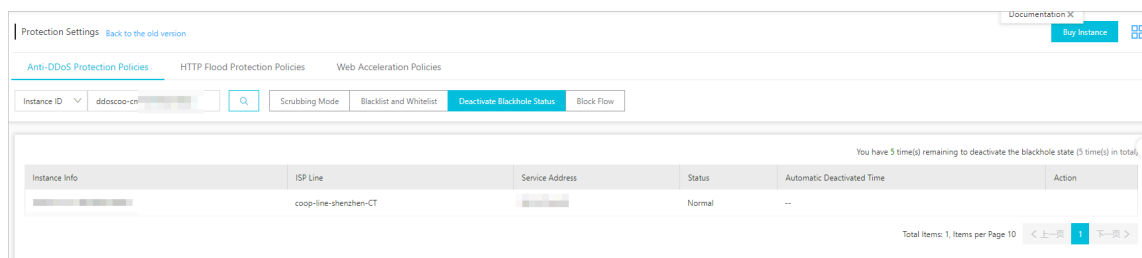
You can click Manually Add to add IP addresses to the blacklist or whitelist.

For more information, see [Configure the blacklist and whitelist](#).



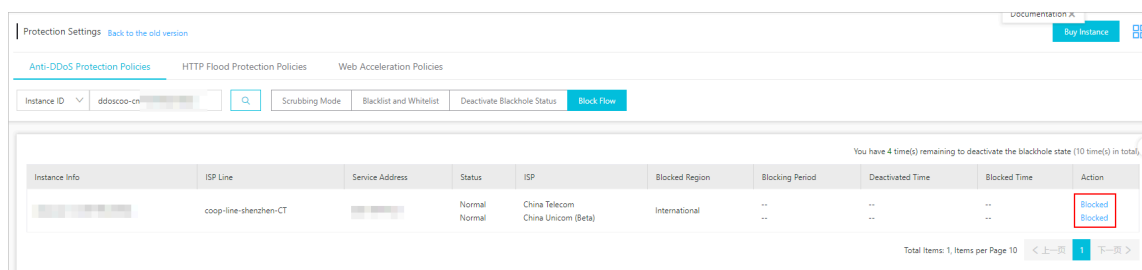
• Deactivate Blackhole Status

You can click Deactivate in the Actions column to deactivate the black hole when your Anti-DDoS Pro instance is in the Black Hole status. For more information, see [Deactivate the black hole status](#).



• Block Flow

Select an Anti-DDoS Pro instance, and click Blocked in the Actions column to block overseas traffic transmitted through China Telecom and China Unicom networks. For more information, see [Block traffic flow](#).



3.1.5 Step 4: Configure HTTP flood protection policies

After you set up an Anti-DDoS Pro instance to protect your service, you can configure HTTP flood protection policies to protect your site against HTTP flood attacks.

Prerequisites

You have added your website in the Anti-DDoS Pro console. For more information, see [Step 1: Add a website](#).

Context

Anti-DDoS Pro provides the following HTTP flood protection policies:

- **Blacklist and Whitelist:** You can use the blacklist to block requests from specific IP addresses, or use the whitelist to allow specific IP addresses to access your site without further inspection.
- **HTTP Flood Protection:** You can enable HTTP Flood Protection to automatically detect and block flood requests. You can select default protection settings or create custom protection rules based on your needs.
 - **Default protection settings:** You can select from four modes that have different protection capabilities to meet your business needs.
 - **Custom protection rules:** You can create custom rules to limit the requests to specific directories on your site.



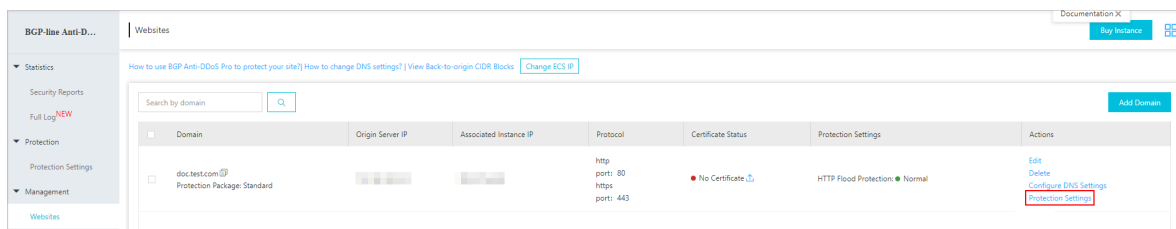
Note:

Currently, a series of new protection policies are in preview testing. By default, Anti-DDoS Pro only provides the following features for mitigating flood attacks: Blacklist, Whitelist, and HTTP Flood Protection. If you want to use the following new features: Geo-blocking, Accurate Access Control, Intelligent Protection, and Web Acceleration, we recommend that you switch to new protection policies. For more information, see [#unique_30](#).

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose Management > Websites.

3. In the website list, select a domain and click Protection Settings.

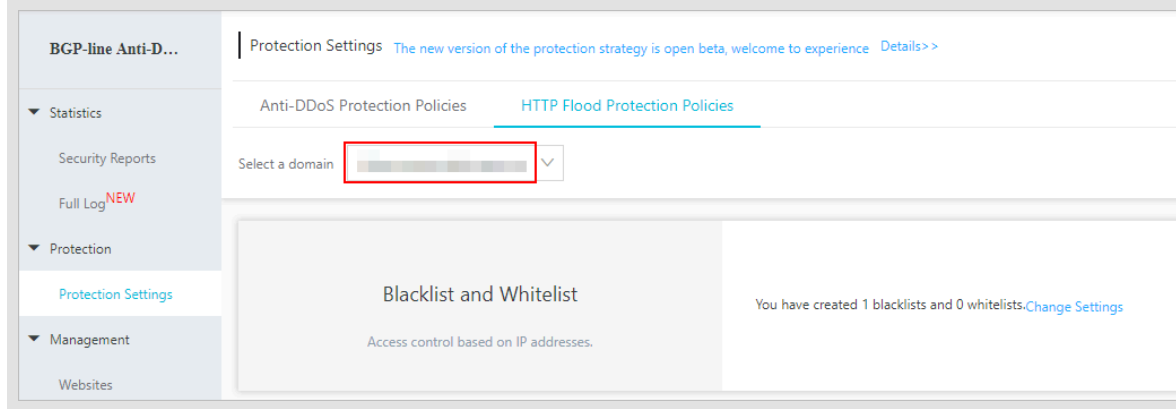


4. On the Protection Settings page, click HTTP Flood Protection Policies and perform the following steps based on your needs:



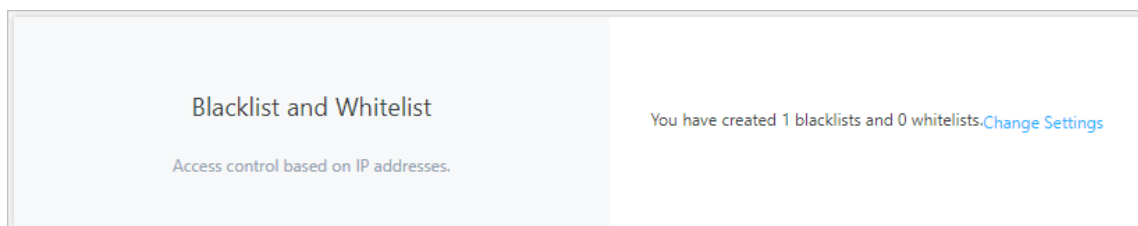
Note:

HTTP flood protection policies take effect for domains. Make sure to specify the correct domain before you configure HTTP flood protection policies.



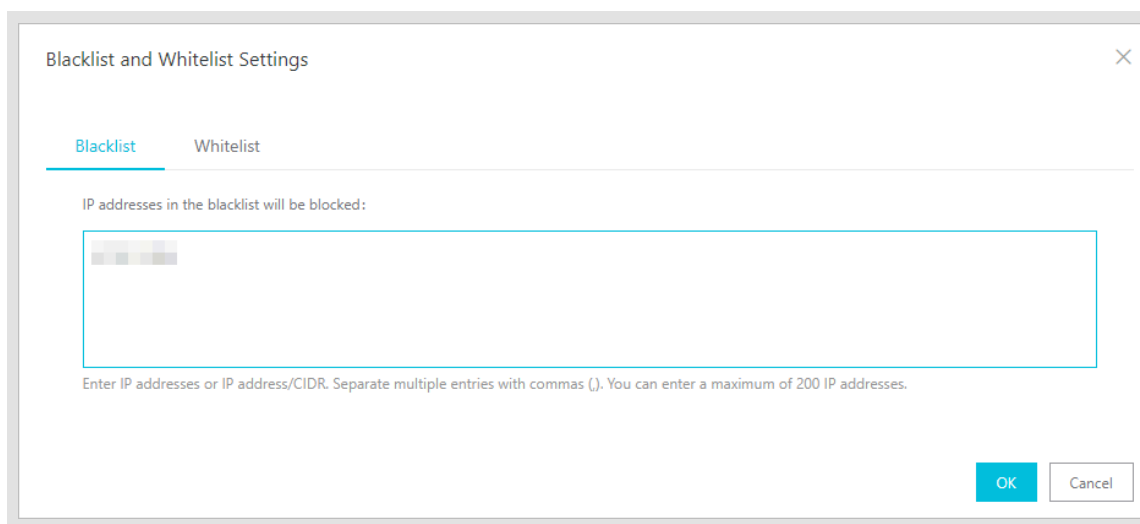
- **Blacklist and Whitelist**

Select Blacklist and Whitelist, and click Change Settings. In the Blacklist and Whitelist Settings dialog box, add IP addresses or CIDR blocks to the blacklist and whitelist respectively.



Note:

You can enter up to 200 IP addresses or CIDR blocks in the blacklist and whitelist respectively. Separate multiple IP addresses or CIDR blocks with commas (,).



Blacklist and Whitelist Settings

Blacklist Whitelist

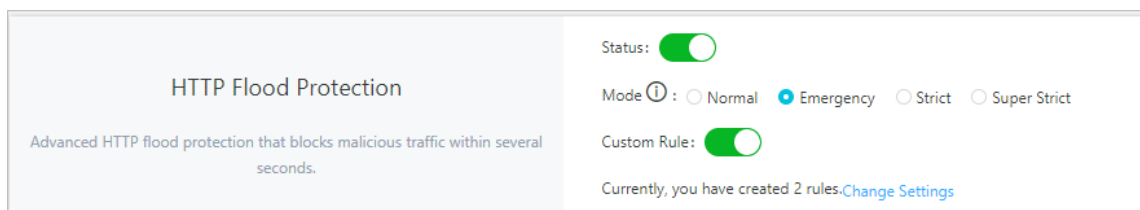
IP addresses in the blacklist will be blocked:

Enter IP addresses or IP address/CIDR. Separate multiple entries with commas (.). You can enter a maximum of 200 IP addresses.

OK Cancel

- **HTTP Flood Protection**

Select HTTP Flood Protection, and click the Switch icon next to Status to enable HTTP Flood Protection. You can then select default protection settings or create custom rules based on your business needs.



HTTP Flood Protection

Advanced HTTP flood protection that blocks malicious traffic within several seconds.

Status: ☒

Mode ⓘ : ☐ Normal ☒ Emergency ☐ Strict ☐ Super Strict

Custom Rule: ☒

Currently, you have created 2 rules. [Change Settings](#)

- **Default protection settings**

You can select one of the following modes to protect your service: Normal, Emergency, Strict, and Super Strict.



Note:

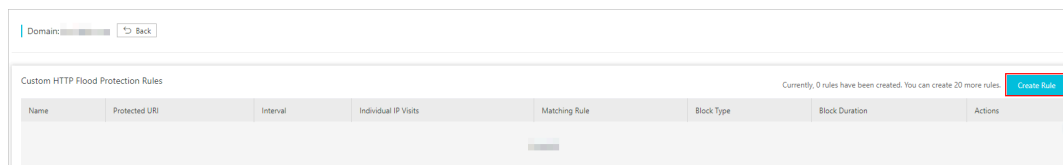
Different modes provide different protection capabilities. Modes that offer higher protection capabilities usually have higher false positive rates. We recommend that you enable modes with higher capabilities only when the

other modes fail to mitigate attacks effectively. For more information, see [Configure HTTP flood protection](#).

- Custom rules

a. Click the Switch icon next to Custom Rule, and click Change Settings.

b. On the Custom HTTP Flood Protection Rules page, click Create Rule.



c. In the Create Rule dialog box, specify the following parameters.

Parameter	Description
Name	The name of the rule.
URI	The address of the page that you want to protect.
Matching Rule	<p>The rule that determines whether a request is counted. Valid values:</p> <ul style="list-style-type: none"> ■ Exact Match: A request is counted when the requested URI is the same as the protected URI. ■ Prefix Match: A request is counted when the prefix of the requested URI is the same as the protected URI.
Interval	The rule that determines whether a source IP address triggers the custom rule. When the number of counted requests from an IP address exceeds the Individual IP Visits limit during the Interval, the custom rule is triggered.
Individual IP Visits	

Parameter	Description
Block Type	<p>The action to be performed when the custom rule is triggered.</p> <ul style="list-style-type: none">■ Block: Blocks requests from the source IP address for a specific time period.■ Captcha Verification: Redirects the request to a captcha verification page. To access your site, the user must pass the captcha verification.

Create Rule

* Name:

login_5s_20_block5

* URI:

/login

* Matching Rule

☒ Exact Match ☐ Prefix Match

* Interval:

5

Seconds

Enter an integer from 5 to 10800.

* Individual IP Visits:

20

Requests

Enter an integer from 2 to 2000.

* Block Type:

☒ Block ☐ Captcha Verification

5

Minutes

Enter an integer from 1 to 1440.

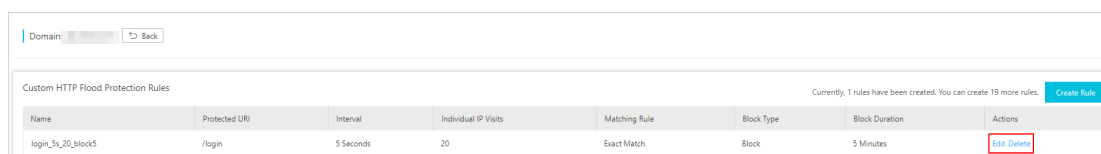
OK

Cancel

In the previous example, when the number of requests to the `/login` page from an IP address exceeds 20 within 5 seconds, the IP address is blocked for 5 minutes.

d. Click OK.

After a rule is created, it is displayed in the rule list. You can Edit or Delete rules based on your needs.



3.1.6 Step 5: View security reports and log data

After you set up an Anti-DDoS Pro instance to protect your service, you can view security reports and log data in the Anti-DDoS Pro console.

Prerequisites

- You have added your website in the Anti-DDoS Pro console. For more information, see [Step 1: Add a website](#).
- You have changed DNS records to forward traffic to Anti-DDoS Pro. For more information, see [Step 2: Change DNS records](#).

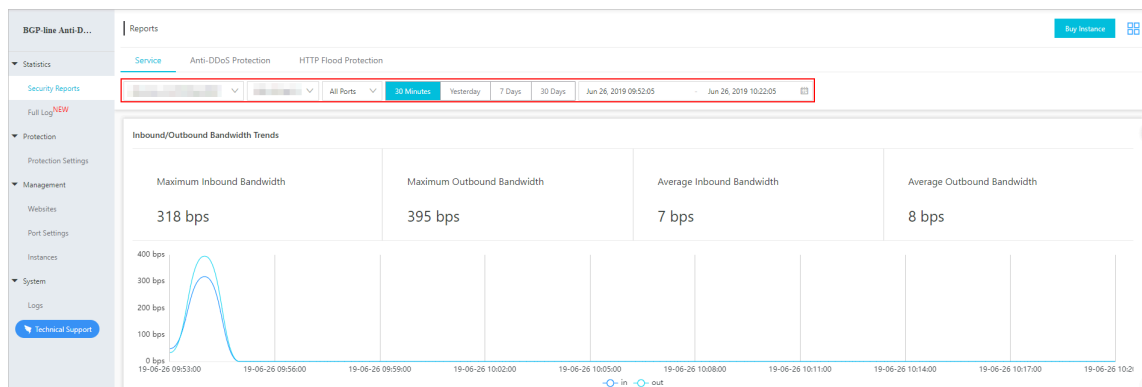
Procedure

1. Log on to the [Anti-DDoS Pro console](#).

2. Perform the following steps based on your needs:

- **View security reports**

In the left-side navigation pane, choose **Statistics > Security Reports**. On the **Reports** page, select one of the following to view the corresponding reports: **Service**, **Anti-DDoS Protection**, and **HTTP Flood Protection**.



You can add multiple filter conditions to customize the reports. For example, time range, Anti-DDoS Pro instance, instance IP, and port number. The differences between these reports are as follows:

Report	Content	Filter condition
Service	<ul style="list-style-type: none"> - Changes of inbound and outbound bandwidth - Changes of concurrent connections and new connections 	<ul style="list-style-type: none"> - Time range - Anti-DDoS Pro instance - Anti-DDoS Pro instance IP - Forwarding port
Anti-DDoS Protection	<ul style="list-style-type: none"> - Changes of back-to-origin traffic and scrubbed traffic - Records of DDoS attacks 	<ul style="list-style-type: none"> - Time range - Anti-DDoS Pro instance - Anti-DDoS Pro instance IP

Report	Content	Filter condition
HTTP Flood Protection	<ul style="list-style-type: none"> - Changes of malicious requests and total requests - Records of HTTP flood attacks 	<ul style="list-style-type: none"> - Time range - Protected domain

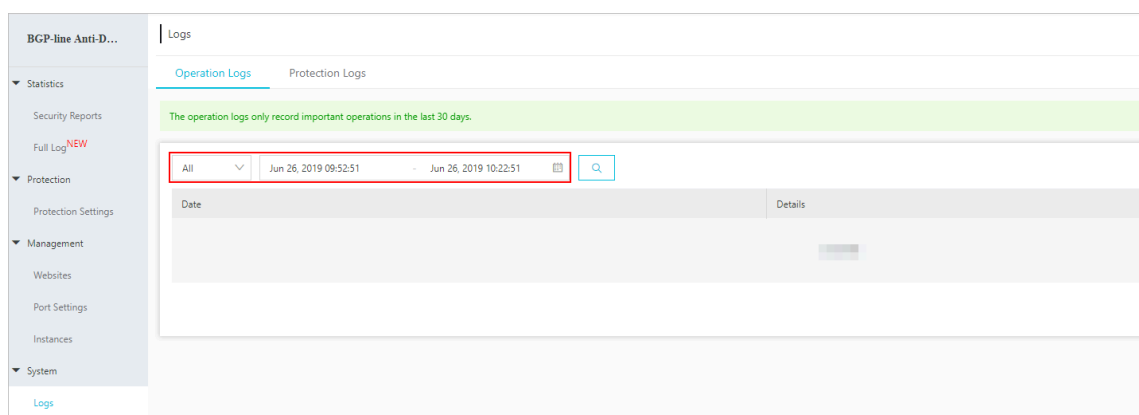
For more information, see [View security reports](#).

- Query and analyze log data

In the left-side navigation pane, choose **System > Logs**. On the Logs page, select the type of log data that you want to query: **Operation Logs**, **Protection Logs**.

The differences between these types of log data are as follows:

- Operation logs record important operations of the last 30 days. For example , operations performed on IP addresses of protected assets, Anti-DDoS packages, and ECS instances. You can filter log records by time.
- Protection logs record the attacks that are experienced by Anti-DDoS Pro instances. You can filter log records by time.



If you need to analyze log data in real time and display results with graphs, we recommend that you activate Anti-DDoS Pro Full Log Service. After Anti-DDoS Pro Full Log Service is activated, access logs on your site are collected

and maintained by [Alibaba Cloud Log Service](#). You can search and analyze log data in real time, and view search results through dashboards.

Anti-DDoS Pro Full Log Service is a value-added service. To use the service, you must activate and enable it. To use Anti-DDoS Pro Full Log Service, perform the following steps:

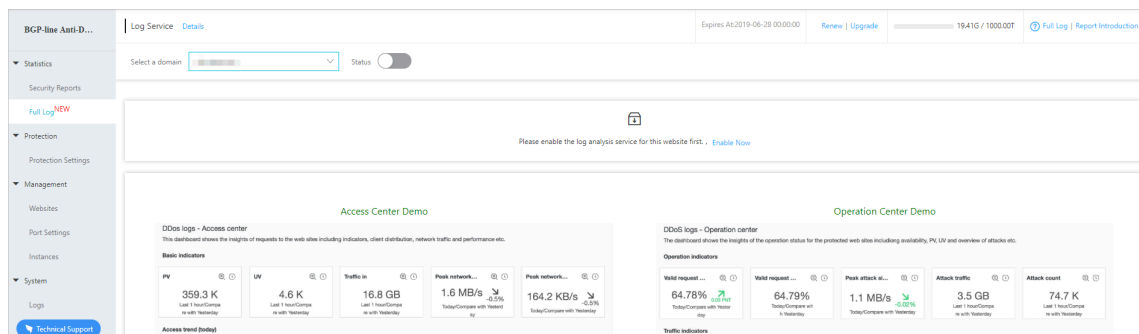
- a. Activate Anti-DDoS Pro Full Log Service. For more information, see [Activate the full log service](#).
- b. Enable Anti-DDoS Pro Full Log Service. For more information, see [Enable the full log service](#).

After Anti-DDoS Pro Full Log Service is enabled, you can choose **Statistics > Full Log** to search and analyze log data in real time. You can also view and edit dashboards, and set monitoring alerts on this page.



Note:

For more information about the fields that are displayed in a log record, see [Fields](#).



3.2 Set up Anti-DDoS Pro using IPs and ports

3.2.1 Overview

This topic describes how to set up Anti-DDoS Pro by using IPs and ports to protect services such as client-based games, mobile games and native apps.

To set up Anti-DDoS Pro using IPs and ports, use the following steps:

Task	Description
Step 1: Create a port forwarding rule	Create port forwarding rules in the Anti-DDoS Pro console. Change the service IP to the IP address of your Anti-DDoS Pro instance.

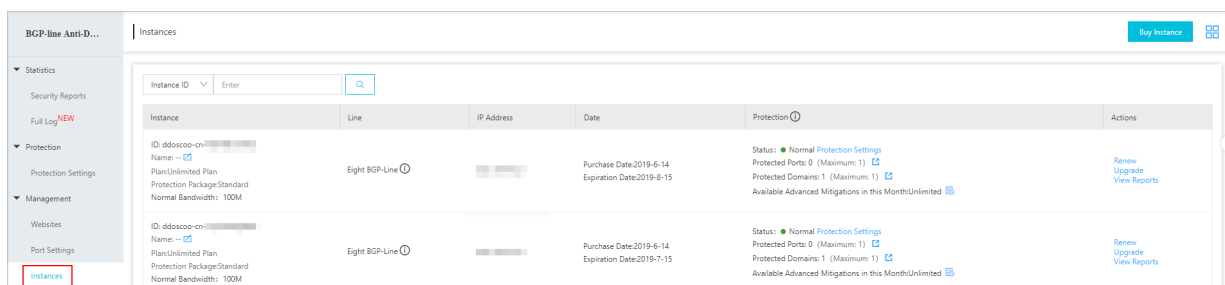
Task	Description
Step 2: Configure protection policies	After creating a port forwarding rule, you can edit custom settings, such as session persistence, health check, and DDoS protection policies.
Step 3: View traffic statistics	After you set up an Anti-DDoS Pro instance to protect your service, you can view the traffic that goes through your service in the Anti-DDoS Pro console.

3.2.2 Step 1: Create a port forwarding rule

To use Anti-DDoS Pro to protect services, such as client-based games, mobile games, and native apps, you must create port forwarding rules and change the service IP to the IP address of your Anti-DDoS Pro instance. This topic describes how to create port forwarding rules in the Anti-DDoS Pro console.

Prerequisites

You have purchased an Anti-DDoS Pro instance. To view your instance, choose **Management > Instances**. For more information about purchasing Anti-DDoS Pro instances, see [Buy Anti-DDoS Pro instances](#).



Context

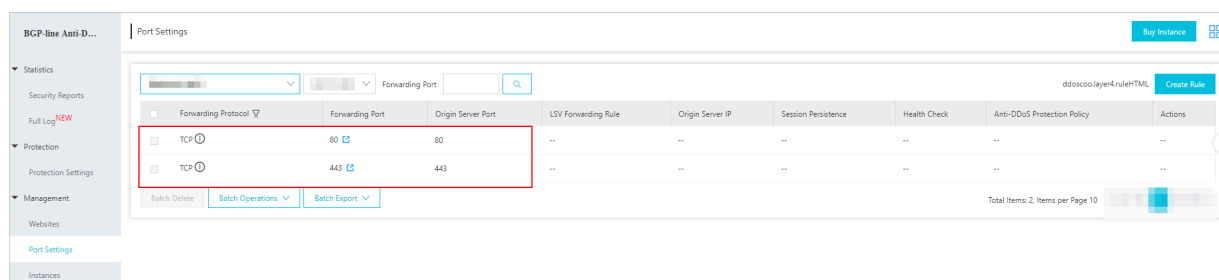
If you set up Anti-DDoS Pro instances using IPs and ports, these instances only support layer 4 forwarding. Anti-DDoS Pro only provides defense against layer 4 attacks, such as SYN flood attacks and UDP flood attacks. The service does not parse layer 7 packets or mitigate layer 7 attacks, such as HTTP flood attacks and Web attacks. To set up Anti-DDoS Pro instances using IPs and ports, you only need to create port forwarding rules in the Anti-DDoS Pro console.

Manage forwarding rule conflicts

If you have added your website in the Anti-DDoS Pro console and set up an Anti-DDoS Pro instance using the website domain, the system automatically generates a forwarding rule for the domain. Incoming traffic to the website is forwarded

according to this forwarding rule. For more information about adding a website in the Anti-DDoS Pro console, see [Step 1: Add a website](#).

- If the forwarding port is set to 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 set to 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. The rule is automatically deleted when the domain to which the rule applies is no longer associated with the Anti-DDoS Pro instance.

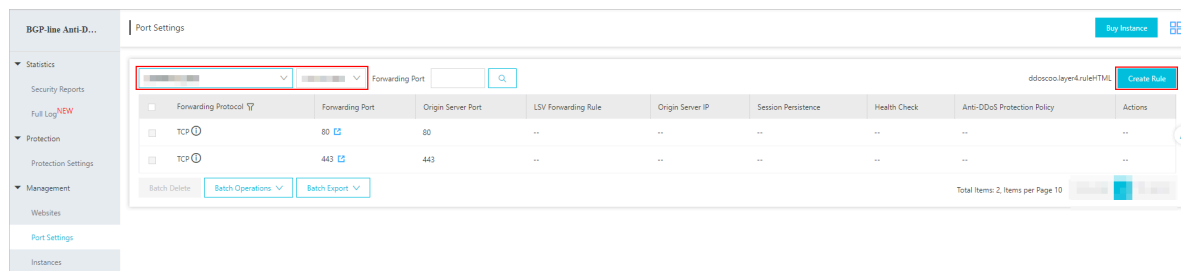


Notice:



For each Anti-DDoS Pro instance, the forwarding rules must use unique ports under the same protocol. If an Anti-DDoS Pro instance already has a forwarding rule that uses TCP port 80 or 443, a conflict error occurs when you try to add a rule that uses the same port and protocol.

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose Management > Port Settings.
3. On the Port Settings page, select an Anti-DDoS Pro instance and click Create Rule.



4. In the Create Rule dialog box, complete the configuration. The configuration details are as follows:

Item	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. <div>  Note: We recommend that you keep the forwarding port the same as the port of the origin server. </div>
Origin Server Port	Specify the port of the origin server.
Origin Server IP	Specify the IP address of the origin server. <div>  Note: You can enter up to 20 IP addresses for load balancing. </div>

Create Rule

×

* Forwarding ☒ TCP ☐ UDP

Protocol:

* Forwarding Port:

* Origin Server Port:

LSV Forwarding Round-robin

Rule:

* Origin Server IP:

Separate multiple IP addresses with commas (.). You can add a maximum of 20 IP addresses.

Complete

Cancel

5. Click Complete.

After a forwarding rule is created, you can configure session persistence, health check, and anti-DDoS protection policies based on your needs. For more information, see [Step 2: Configure protection policies](#).

You can also edit or delete the rule based on your needs.

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

Before you forward incoming traffic to your Anti-DDoS Pro instance, we recommend that you verify that the forwarding rules are in effect. For more information about testing port forwarding, see [Test forwarding rules](#).



Notice:

If the forwarding rules are not in effect, your service may become unavailable to your users after you change the service IP address.

3.2.3 Step 2: Configure protection policies

After a port forwarding rule is added, you can configure the following protection policies based on your needs: session persistence, health check, and anti-DDoS protection.

Prerequisites

You have added port forwarding rules. For more information, see [Step 1: Create a port forwarding rule](#).

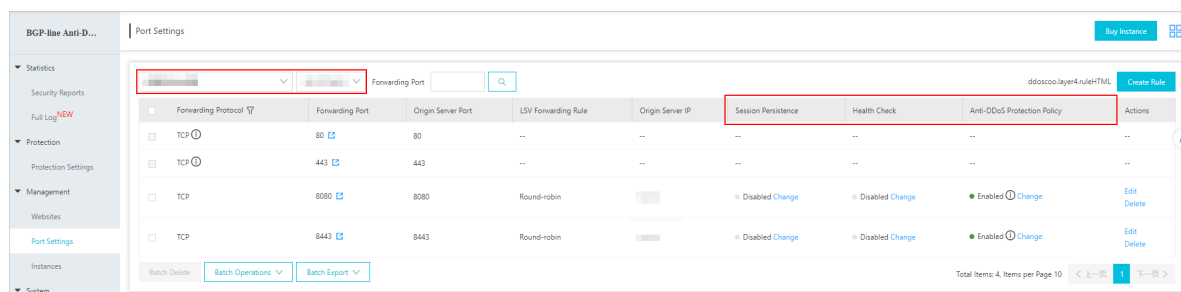
Context

You can configure protection policies based on different business scenarios. For example,

- you can configure a session persistence policy based on IP address to forward requests from the same IP address to the same origin server.
- You can configure a health check policy to check the availability of the origin server. The purpose of a health check is to ensure that requests from the client are not forwarded to servers where exceptions have occurred.
- Anti-DDoS protection policies are based on IPs and ports. To mitigate DDoS attacks, you can configure policies to set limits on parameters, such as the request rate or packet length.

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose Management > Port Settings.
3. On the Port Settings page, select an Anti-DDoS Pro instance.



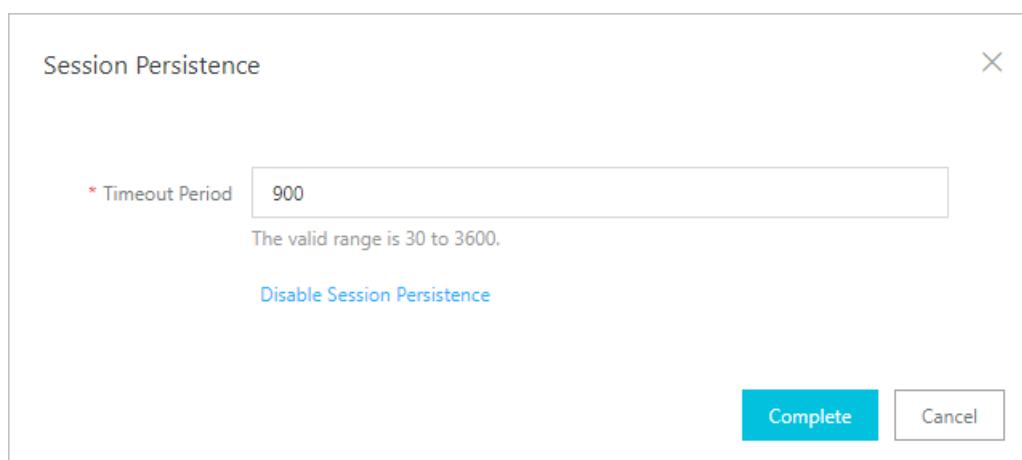
4. Select a port forwarding rule and configure the session persistence, health check, and anti-DDoS protection policies based on your needs.

- Session persistence

a. Click Change in the Session Persistence column.

b. In the Session Persistence dialog box, enable or disable session persistence based on your needs.

- To enable session persistence, specify the Timeout Period and click Complete.
- To disable session persistence, click Disable Session Persistence.

The image shows a 'Session Persistence' dialog box. It has a title bar with the text 'Session Persistence' and a close button (X). Inside the dialog, there is a label '* Timeout Period' followed by a text input field containing the value '900'. Below the input field, a message states 'The valid range is 30 to 3600.' Below this message is a blue link labeled 'Disable Session Persistence'. At the bottom right of the dialog, there are two buttons: 'Complete' (in a blue box) and 'Cancel' (in a white box with a grey border).

- Health check

a. Click Change in the Health Check column.

b. In the Health Check dialog box, complete the configuration. The configuration details are as follows. You can click Advanced Settings to show or hide advanced settings.

Type	Item	Description
Layer 4 and layer 7	Port	The port that the health check service uses to communicate with the origin server. Default is the port of the origin server. Valid values: 1 to 65535.

Type	Item	Description
Layer 7	Domain, Path	<p>This setting is only applicable to TCP rules. During a layer 7 health check, the Anti-DDoS Pro forwarding system sends an HTTP header request to the default homepage on the origin server.</p> <ul style="list-style-type: none"> - If you do not want to use the default homepage for health checks, you must enter a domain and path of another page. - If you have limited the host header field to specific values, you only need to specify the URI for health checks. The domain parameter is optional and set to the IP address of the origin server by default.
Advanced setting	Response Timeout Period	The timeout period during a health check. Valid values: 1 to 30 seconds . If the origin server does not respond within the timeout period , it indicates that the health check failed.
Advanced setting	Check Interval	The time interval between two health checks. Valid values: 1 to 30 seconds. All scrubbing nodes in the Anti-DDoS Pro cluster perform health checks on origin servers at the specified interval independently and concurrently. Scrubbing nodes may perform health checks on the same origin server at different times . This is the reason that the health check records on the origin server do not indicate a check interval.
Advanced setting	Unhealthy Threshold	The number of consecutive failed health checks performed by the same scrubbing node that must occur before declaring an origin server unhealthy. Valid values: 1 to 10.

Type	Item	Description
Advanced setting	Healthy Threshold	The number of consecutive successful health checks performed by the same scrubbing node that must occur before declaring an origin server healthy. Valid values: 1 to 10.

Health Check ×

Layer 4 Health Check Layer 7 Health Check

* Port

8080

The origin port is used by default. The valid range is 1 to 65535.

Advanced Settings

* Response Timeout

5

Period The amount of time during which no response means a failed health check. The valid range is 1 to 30 seconds.

* Check Interval

15

The amount of time between health checks. The valid range is 1 to 30 seconds.

* Unhealthy

3

Threshold The consecutive times of failed health checks after which the server is considered down. The valid range is 1 to 10.

* Healthy Threshold

3

The consecutive times of successful health checks after which the server is considered running. The valid range is 1 to 10.

Complete Cancel

Health Check ×

Layer 4 Health Check Layer 7 Health Check

Domain

Enter a domain. For example: www.aliyun.com

* Path

Enter a path. For example: /abc/a.php

* Port

8080

The origin port is used by default. The valid range is 1 to 65535.


Advanced Settings

Complete Cancel

- c. Click **Complete** to enable health check policies. To disable health check policies, click **Change** in the Health Check column. In the Health Check dialog box that appears, click **Disable Health Check**.
- Anti-DDoS protection policies
 - a. Click **Change** in the Anti-DDoS Protection Policy column.

b. In the Anti-DDoS Protection Policy dialog box, complete the configuration.

The configuration details are as follows:

Item	Description
False Source	Detects and blocks false source IPs. This setting is only applicable to TCP rules.
Empty Connection	<p>Detects and blocks null session connections. This setting is only applicable to TCP rules.</p> <div>  Note: To enable Empty Connections, you must enable False Source first. </div>
Source New Connection Rate Limit	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 scrubbing nodes are deployed in clusters. The rate limit can be set to Automatic or Manual. Valid values: 1 to 50,000.
Source Concurrent Connection Rate Limit	The maximum number of concurrent connections from a single source IP. All connections exceeding the limit are discarded. When enabled, you must specify a rate limit. Valid values: 1 to 50,000.
Destination New Connection Rate Limit	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 scrubbing nodes are deployed in clusters. When enabled, you must specify a rate limit. Valid values: 100 to 100,000.
Destination Concurrent Connection Rate Limit	The maximum number of concurrent connections to a single destination IP and port. All connections exceeding the limit are discarded. When enabled, you must specify a rate limit. Valid values: 1,000 to 1,000,000.

Item	Description
Packet Length Limit	The limit on packet payload length. Unit: byte. All packets exceeding the limit are discarded. Valid values: 0 to 6,000.

Anti-DDoS Protection Policy

False Source:

☒

Empty Connection ⓘ :

☒

* Source New Connection

Rate Limit ⓘ :

☐ Automatic

☐ Manual

☒ Cancel

* Source Concurrent

Connection Rate Limit:

☐

* Destination New

Connection Rate Limit ⓘ :

☐

* Destination Concurrent

Connection Rate Limit:

☐

* Packet Length Limit ⓘ :

- Byte

Range 0 - 6000

OK

Cancel

c. Click OK.

3.2.4 Step 3: View traffic statistics

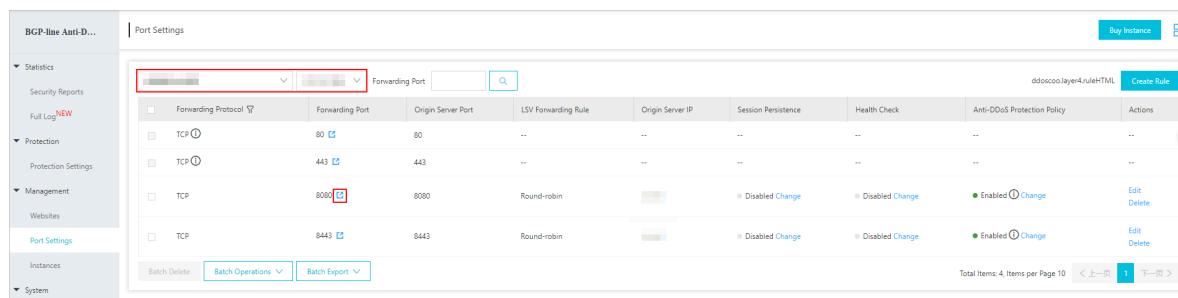
After you set up an Anti-DDoS Pro instance to protect your service, you can view the traffic that goes through your service in the Anti-DDoS Pro console.

Prerequisites

You have added port forwarding rules. For more information, see [Step 1: Create a port forwarding rule](#).

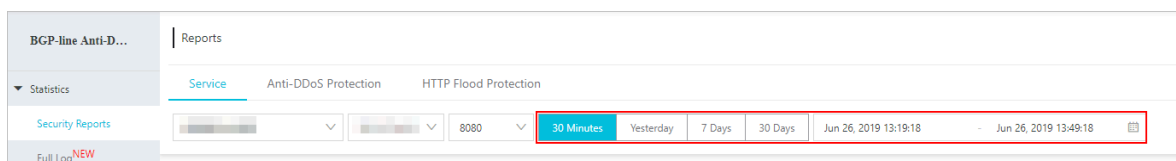
Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose **Management > Port Settings**.
3. On the Port Settings page, select an Anti-DDoS Pro instance.
4. Select a port forwarding rule and click the redirect icon in the Forwarding Port column.

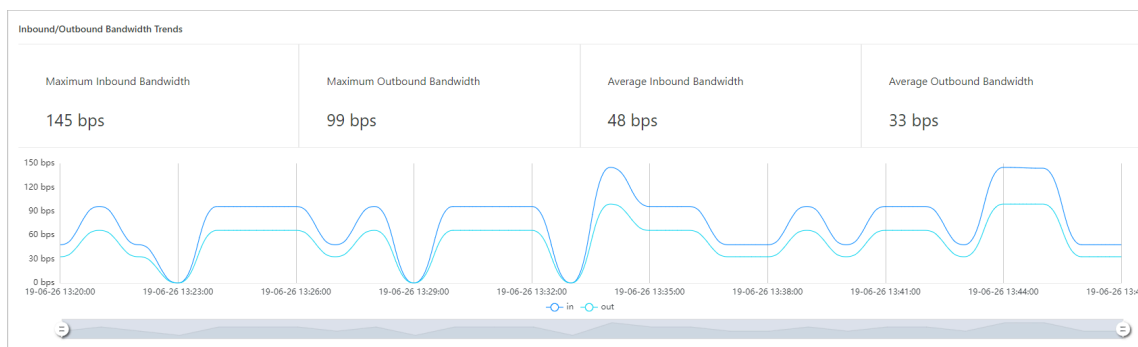


5. On the Reports page, click the **Service** tab and select a time period to view traffic data. You can select from the following time periods: 30 minutes, yesterday, 7

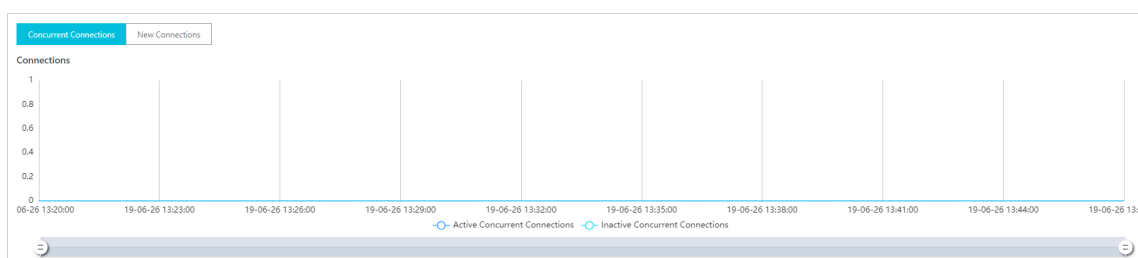
days, 30 days, or a custom period within the last 30 days. The traffic data includes the following information:



- **Inbound/Outbound bandwidth:** The maximum and average inbound/outbound bandwidth represented by curves.



- **Connections:** The number of concurrent connections and new connections represented by curves.



4 Deploy Anti-DDoS Pro

4.1 Websites

4.1.1 Custom non-standard ports

The standard package of Anti-DDoS Pro provides DDoS protection based on standard HTTP ports (80, 8080) and HTTPS ports (443, 8443). The enhanced package supports non-standard HTTP and HTTPS ports. However, the number of ports used by each protected domain is subject to a limit.

**Note:**

To add non-standard HTTP or HTTPS ports, make sure that your domain is associated with an Anti-DDoS Pro instance of the enhanced package.

Port limit

The domains associated with each Anti-DDoS Pro instance of the enhanced package can use a maximum of 10 ports.

Supported ports

**Note:**

Anti-DDoS Pro only protects supported HTTP and HTTPS ports. The service does not protect or forward traffic from non-supported ports. For example, if an Anti-DDoS Pro instance receives a packet on port 4444, the packet will be directly discarded.

- For HTTP and WebSocket, the enhanced package of Anti-DDoS Pro supports the following ports:

80, 83, 84, 88, 89, 800, 808, 1000, 1090, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7060, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8106, 8181, 8334, 8336, 8800, 8686, 8787, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9999, 10000, 10001, 10080, 12601, 86, 9021,

9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, and 33702.

- For HTTPS and WebSockets, the enhanced package of Anti-DDoS Pro supports the following ports:

443, 4443, 5443, 6443, 7443, 8443, 9443, 8553, 8663, 9553, 9663, and 18980.

4.1.2 Upload SSL certificates

To use Anti-DDoS Pro to filter HTTPS traffic, you must select HTTPS in the domain settings and upload the SSL certificate. When your SSL certificate expires, you must update the certificate in the Anti-DDoS Pro console in a timely manner.

Prerequisites

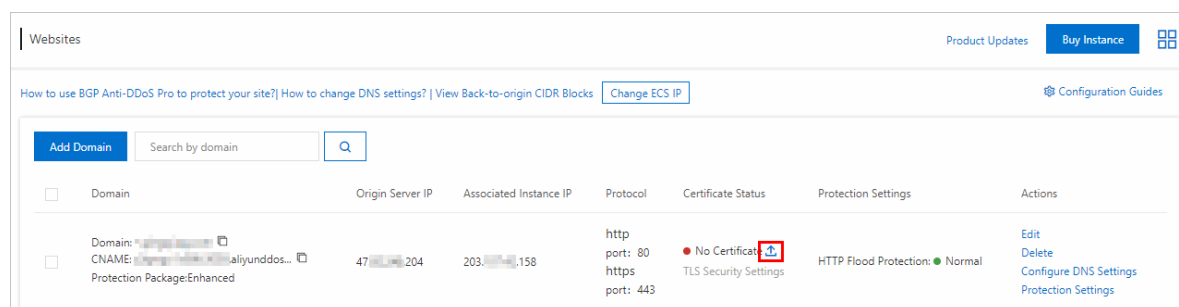
- You have added your domain in the Anti-DDoS Pro console and your site supports HTTPS. For more information about adding domains, see [Step 1: Add a website](#).
- You have prepared the certificate files.

If you have uploaded your certificate files to [Alibaba Cloud SSL Certificates Service](#), you can select the certificate directly. Otherwise, you need to prepare the certificate files for upload. Generally, the following files are required:

- The public key file in CRT format or the certificate file in PEM format.
- The private key file in KEY format.

Procedure

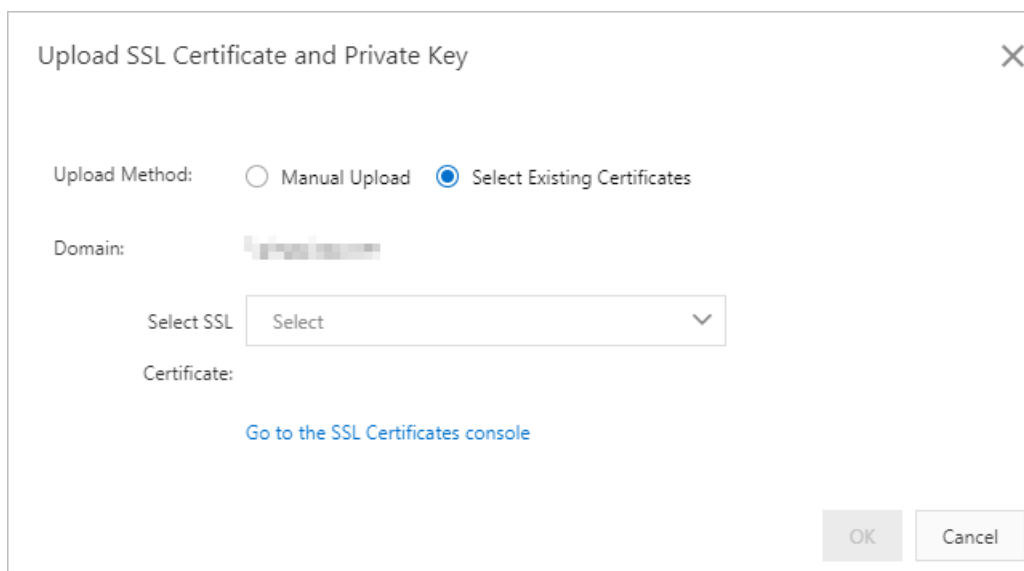
1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose Management > Websites.
3. In the Websites list, select your domain and click the upload icon in the Certificate Status column.



4. In the Upload SSL Certificate and Private Key dialog box, select an Upload Method and specify the parameters. You can select from one of the following methods to upload your certificate.

- **Select Existing Certificates (Recommended)**

If you have uploaded your SSL certificate to Alibaba Cloud SSL Certificates Service, you can directly select an existing certificate for upload.



If your certificate is not hosted on SSL Certificates Service, you can click **Go to the SSL Certificates console** to upload your certificate first. For more information about uploading certificates to SSL Certificates Service, see [#unique_44](#).

- **Manual Upload**

Enter a Certificate Name, and copy the contents of the certificate file and private key file to the Certificate File field and Private Key field respectively.



Note:

- For certificate files in common formats, such as PEM, CER, and CRT, you can use a text editor to open the file and copy its contents. For certificate files in other formats, such as PFX and P7B, you need to convert the file into PEM format first.

- If your SSL certificate includes multiple certificate files, such as a certificate chain, you need to combine the contents of multiple certificate files and paste them into the Certificate File field.

Certificate file example

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxvs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+
j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir
+g92cL8IG0kjgvlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nx
Jf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiN
Y7yZIo2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

Private key file example

```
-----BEGIN RSA PRIVATE KEY-----
xxxxxxxxxxxxxZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThL
yvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQ
ra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/
3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

Upload SSL Certificate and Private Key

Upload Method:

☒ Manual Upload
 ☐ Select Existing Certificates

Domain:

Certificate Name:

* Certificate File ⓘ

62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+

1M+j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS

5NIL5ir+g92cL8IG0kjgvlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUek

C2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv

4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg==

-----END CERTIFICATE-----

* Private Key ⓘ

DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDG

M9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ

+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+

D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04Rt

KadOw==

-----END RSA PRIVATE KEY-----

OK

Cancel

5. Click OK.

Result

After the upload is complete, the certificate status is updated.

4.1.3 Custom TLS security settings

The new Anti-DDoS Pro supports custom TLS security settings and allows you to choose TLS protocols based on your business needs.

Prerequisites

- Your website has been associated with an Anti-DDoS Pro instance of the enhanced package.
- You have added your domain in the Anti-DDoS Pro console and your website supports HTTPS. For more information about adding domains, see [Step 1: Add a website](#).
- You have uploaded the corresponding SSL certificates in the console. For more information, see [Upload SSL certificates](#).

Context

If one of your service needs to implement an authentication mechanism that is compliant with PCI DSS 3.2, TLS 1.0 must be disabled. However, if your clients only support TLS 1.0, your service must also support TLS 1.0. Anti-DDoS Pro allows you to configure different TLS security settings for different services.

Procedure

1. Log on to the [new Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose Management > Websites.
3. Select a domain and click TLS Security Settings under the Certificate Status column.

Domain	Origin Server IP	Associated Instance ID	Protocol	Certificate Status	Protection Settings	Actions
<div>Domain</div> <div>Clicked: alividdos.com</div> <div>Protection Package Enhanced</div>			http: 80 https: 443	<div>Normal</div> <div>TLS Security Settings</div>	HTTP Flood Protection: Normal	<div>Edit</div> <div>Delete</div> <div>Configure DNS Settings</div> <div>Protection Settings</div>

4. In the TLS Security Settings dialog box, select TLS Versions and Cipher Suites based on your needs.

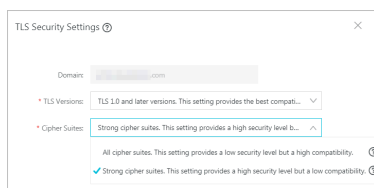
- **TLS Versions:** Default is TLS 1.0 and later versions. This setting provides the best compatibility but a low security level. You can choose to support TLS 1.1 or TLS 1.2 and later versions based on your needs.
- **Cipher Suites:**
 - **Strong cipher suites.** This setting provides a high security level but a low compatibility.

Supported strong cipher suites are as follows:

- 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
- **All cipher suites.** This setting provides a low security level but a high compatibility.

The following weak cipher suites are also supported in addition to above strong cipher suites.

- RSA-AES256-CBC-SHA
- RSA-AES128-CBC-SHA
- ECDHE-RSA-3DES-EDE-CBC-SHA
- RSA-3DES-EDE-CBC-SHA



4.1.4 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.

Add Multiple Rules

▼ View Example

The following example adds two site configurations. For site **a.com**, the protocols are **http** and **https**; the associated Anti-DDoS Pro Instances are **ddoscoo-test1** and **ddoscoo-test2**; and the origin server IP addresses are **192.136.12.45** and **192.12.32.11**. [View Documentation](#)

```
<DomainList>
  <DomainConfig>
    <Domain>a.com</Domain>
    <ProxyTypeList>
      <ProxyConfig>
        <ProxyType>http</ProxyType>
        <ProxyPorts>80,8080</ProxyPorts>
      </ProxyConfig>
      <ProxyConfig>
        <ProxyType>https</ProxyType>
        <ProxyPorts>443,445</ProxyPorts>
      </ProxyConfig>
    </ProxyTypeList>
    <InstanceConfig>
      <InstanceList>ddoscoo-test1,ddoscoo-test2</InstanceList>
    </InstanceConfig>
  </DomainConfig>
</DomainList>
```

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 `<DomainConfig>` and end with `</DomainConfig>`. 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 `<DomainConfig>..... </DomainConfig>` tag pair.

XML parameter	Description
<Domain>a.com</Domain>	The domain to be configured. You can only enter one domain.
<ProtocolConfig><ProtocolList>http,https</ProtocolList></ProtocolConfig>	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.

<pre><InstanceConfig><InstanceList>ddoscoo-cn-4590lwcny001</InstanceList></InstanceConfig></pre>	<p>The Anti-DDoS Pro instance that is configured for the domain.</p> <div data-bbox="868 297 1433 537">  Note: Each Anti-DDoS Pro instance has only one IP address. You can just enter the instance ID. Separate multiple instance IDs with commas (,). </div>
<pre><RealServerConfig><ServerType>0</ServerType><ServerList>1.2.3.4</ServerList></RealServerConfig></pre>	<p>Information about the origin server .</p> <ul style="list-style-type: none"> • <code><ServerType>0</ServerType></code> indicates that the IP address of the origin server is specified. • <code><ServerType>1</ServerType></code> indicates that the domain of the origin server is specified. <p><code><ServerList>1.2.3.4</ServerList></code> indicates the address of the origin server. Separate multiple addresses with commas (,).</p> <div data-bbox="868 1093 1433 1332">  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. </div>

Sample

```
<DomainList>
  <DomainConfig>
    <Domain>a.com</Domain>
    <ProtocolConfig>
      <ProtocolList>http,https</ProtocolList>
    </ProtocolConfig>
    <InstanceConfig>
      <InstanceList>ddoscoo-cn-4590lwcny001</InstanceList>
    </InstanceConfig>
    <RealServerConfig>
      <ServerType>0</ServerType>
      <ServerList>1.2.3.4</ServerList>
    </RealServerConfig>
  </DomainConfig>
  <DomainConfig>
    <Domain>b.com</Domain>
    <ProtocolConfig>
      <ProtocolList>http,websocket,websockets</ProtocolList>
    </ProtocolConfig>
  </DomainConfig>
```

```
<InstanceList>ddoscoo-cn-mp90oeort002,ddoscoo-cn-0pp0o5vz500d</InstanceList>
</InstanceConfig>
<RealServerConfig>
<ServerType>1</ServerType>
<ServerList>q840a82zf2j23afs.gfvip05al.com</ServerList>
</RealServerConfig>
</DomainConfig>
</DomainList>
```

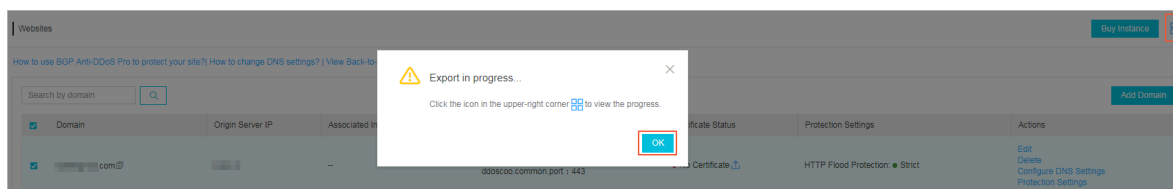
4. Click Next. If the XML file is correctly formatted, the domain configurations you have entered are displayed.

Import Rule				
⚠ Select the rules you want to import.				
<input type="checkbox"/>	Domain	Protocol	Origin Site	Line
<input type="checkbox"/>	a.com	http 80 https 443	1.2.3.4	ddoscoo-cn-4590lwny001
<input type="checkbox"/>	b.com	http 80 websocket 80 websockets 443	q840a82zf2j23afs.gfvip05al.com	ddoscoo-cn-mp90oeort002 ddoscoo-cn-0pp0o5vz500d

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.

Tasks ×			
Name	Status	Start Time	Actions
Layer 7 Export	<div><div></div><div>Pending Export</div></div>	2019-04-01 11:33:09	Delete
Layer 7 Export	<div><div></div><div>Exported</div></div>	2019-04-01 11:28:49	DeleteDown load

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.


ddoscoo-cn-o4011hag0001

203

<input type="checkbox"/>	Forwarding Protocol 	Forwarding Port	Origin Se
<input type="checkbox"/>	TCP	555	555
<input type="checkbox"/>	TCP	8080	8080

Batch Delete

Batch Operations 

Batch Export 

Create Rule

Edit Rule

Session Persistence/Health Check Settings

DDoS Protection Policy Settings

2. Follow the given examples to enter rules.

- **Create forwarding rules**

Create Rule

tcp 90 91 192.136.12.41
udp 22 13 12.14.1.23,10.23.4.12

Sample File:

tcp 90 91 192.136.12.41
udp 22 13 12.14.1.23,10.23.4.12

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

Create Session/Health Settings

8081 tcp 400 tcp 22 5 5 3 3
8080 tcp 400 http 22 5 5 3 3 /search.php example.com

Sample File:

8081 tcp 400 tcp 22 5 5 3 3
8080 tcp 400 http 22 5 5 3 3 /search.php example.com

- **Create anti-DDoS protection policies**

Create Anti-DDoS Protection Policy

8081 tcp 2000 50000 20000 100000 1 1500 on on
8080 udp 1000 50000 20000 100000 1 1500

Sample File:

8081 tcp 2000 50000 20000 100000 1 1500 on on
8080 udp 1000 50000 20000 100000 1 1500

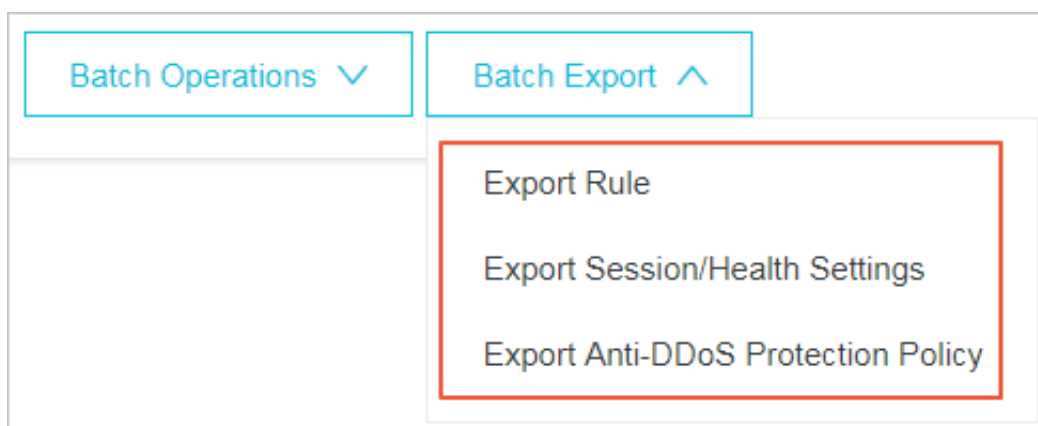
3. Click OK to add settings.

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.

4.2 Provisioning settings

4.2.1 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

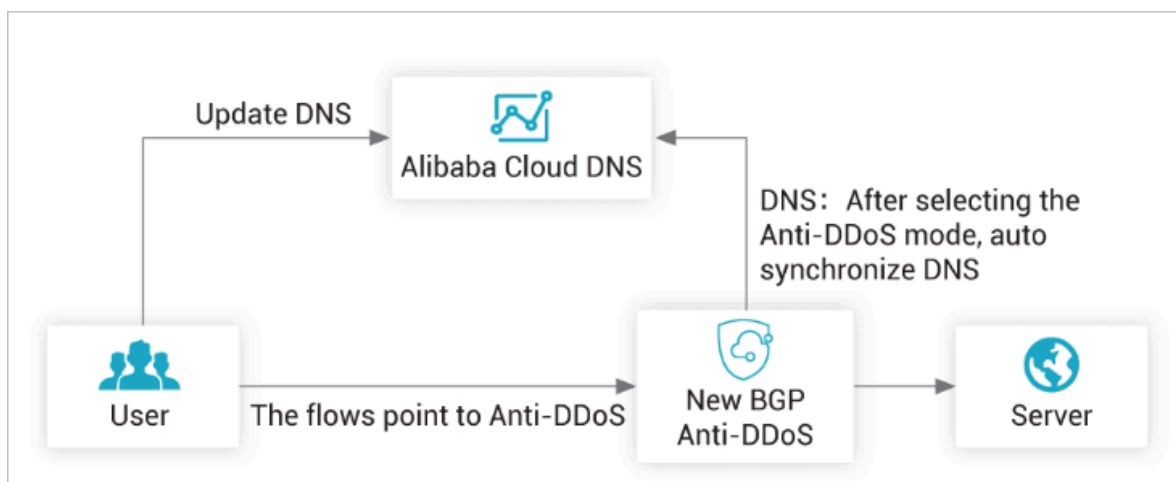
Your domain is managed under a paid version of Alibaba Cloud DNS. Otherwise, you cannot enable NS Mode Access. We recommend that you [activate a paid version of Alibaba Cloud DNS](#).

Context

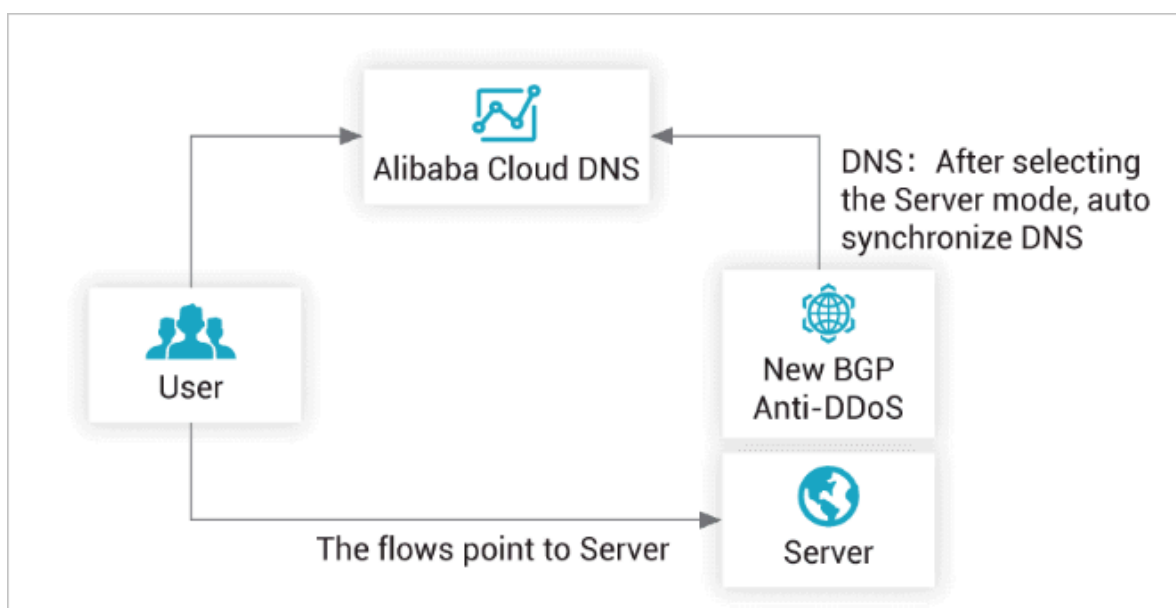
NS Records are nameserver records. You can use NS records to specify which DNS server is used to resolve your domain name.

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.

<input type="checkbox"/>	Domain	Origin Server IP	Associated Instance IP	Protocol	Certificate Status	Protection Settings	Actions
<input type="checkbox"/>	example.com	1.1.1.1	203.10.10.10	http ddoscoo.common.port : 80 https ddoscoo.common.port : 443	No Certificate ⬇	HTTP Flood Protection: Disabled	Edit Delete Configure DNS Settings Protection 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.

example.com

Return

NS Mode Access (Recommended, no DNS record change required)

Prerequisite: Service to be accessed must use Alibaba Cloud DNS. [For more information, click to view Alibaba Cloud DNS](#). If your service cannot be accessed through NS mode. Please access the service by manually changing the DNS record. [For more information, click to view the configuration guide](#).

Status: ☒

Mode: ☐ Anti-DDoS Pro ☐ Back-to-Origin

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.

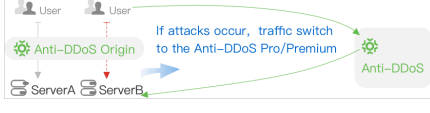

4.3 Security traffic manager

Anti-DDoS Pro provides security traffic manager to set the interaction rules between Anti-DDoS Pro and other cloud resources. You can set rules to enable Anti-DDoS Pro in specific scenarios only. This guarantees smooth workloads if no DDoS attacks occur and more effective protection when DDoS attacks are detected. Security traffic manager provides features such as cloud service interaction, tiered protection, and CDN interaction. This topic describes the application scenarios and configuration procedures of these features.

Scenarios

The following table lists the application scenarios of the features provided by security traffic manager.




Feature	Scenario	How the feature works
Cloud service interaction	Anti-DDoS Pro is required only if the cloud service instances are attacked.	<p>If no DDoS attacks occur, Anti-DDoS Pro is disabled to avoid a longer latency. If DDoS attacks are detected, Anti-DDoS Pro is enabled.</p>  <pre> graph TD User1[User] --> ServerA[ServerA] User2[User] --> ServerB[ServerB] ServerA -- "If attacks occur, traffic switch to the Anti-DDoS Pro/Premium" --> AntiDDoS[Anti-DDoS] ServerB -- "If attacks occur, traffic switch to the Anti-DDoS Pro/Premium" --> AntiDDoS </pre>

Feature	Scenario	How the feature works
Tiered protection	Anti-DDoS Protection Package is required to protect your cloud resources. Anti-DDoS Pro is required only if the cloud resources encounter high-volume DDoS attacks.	<p>Anti-DDoS Protection Package is used to protect your workloads against low-volume DDoS attacks. This does not increase network latency. If high-volume DDoS attacks are detected, Anti-DDoS Pro is enabled.</p> 
CDN interaction	The website requires Content Delivery Network (CDN) for network acceleration. Anti-DDoS Pro is required if DDoS attacks are detected.	<p>If no DDoS attacks occur, the website uses the CDN node nearest to the client for acceleration. When DDoS attacks are detected, the workloads are switched from CDN to Anti-DDoS Pro.</p> 

Limits

The following table lists the limits of the features provided by security traffic manager.

Feature	Limits	Description
Cloud service interaction	Anti-DDoS Pro instance specifications	Make sure that the instance specifications such as the request rate and service bandwidth are large enough to protect your business.
	Anti-DDoS protection configuration	The Anti-DDoS Pro instance must complete the traffic forwarding configuration before the workloads are switched to the instance.
Tiered protection	Anti-DDoS Protection Package edition	Anti-DDoS Protection Package Enterprise edition is required.
	Anti-DDoS Protection Package instance specification	The service bandwidth of the protection packages must meet the protection requirements.

Feature	Limits	Description
	Anti-DDoS protection configuration	The Anti-DDoS Pro instance must complete the traffic forwarding configuration before the workloads are switched to the instance.
	Anti-DDoS Protection Package configuration	Your cloud resources must be included in the objects protected by Anti-DDoS Protection Package.
CDN interaction	Domain status in CDN	<p>This feature is unavailable for domain names in the sandbox.</p> <div>  Note: If a domain name has been added to the sandbox by CDN, we recommend that you use Anti-DDoS Pro without enabling this feature. </div>
	Attack frequency	This feature does not apply to websites that are attacked more than three times per week.
	Time required for Anti-DDoS protection to take effect	<p>This feature does not apply to scenarios where Anti-DDoS protection is required to take effect in a short time.</p> <div>  Note: After the workloads are switched to Anti-DDoS Pro, the time required for Anti-DDoS protection to take effect depends on the TTL in the DNS records of the protected domain. </div>
	Website bandwidth	<p>This feature does not apply to websites with a high bandwidth or high request rate.</p> <div>  Note: If the bandwidth exceeds 3 Gbit/s or the queries received per second exceeds 10,000, submit a ticket to request an analysis on whether the feature applies to this website. </div>

Feature	Limits	Description
	Request type	This feature applies to HTTP and HTTPS requests only. ApsaraVideo Live is not supported.
	Anti-DDoS Pro function plan	This feature is supported by the enhanced function plan only.

To enable CDN interaction, you must set the request rate threshold that triggers the workloads to switch between CDN and Anti-DDoS Pro. The workloads switchover between CDN and Anti-DDoS Pro is subject to the following conditions and limits:


- From CDN to Anti-DDoS Pro
 - If the request rate exceeds the threshold three times within three minutes or more than six times within 10 minutes, a switchover is triggered.
 - The bandwidth of the workloads on CDN must be lower than or equal to 10 Gbit/s.



**Note:**

The maximum bandwidth that an Anti-DDoS Pro instance can protect is lower than 10 Gbit/s.

- From Anti-DDoS Pro to CDN
 - If the request rate remains lower than 80% of the threshold and the HTTP flood protection success rate remains lower than 10% for more than 12 hours in a row, workloads switch back from Anti-DDoS Pro to CDN.
 - The IP address of the Anti-DDoS Pro instance cannot be in the black hole and no traffic is scrubbed or blackholed during the past 60 minutes.
 - A switchback can be triggered only from 8:00 to 23:00.

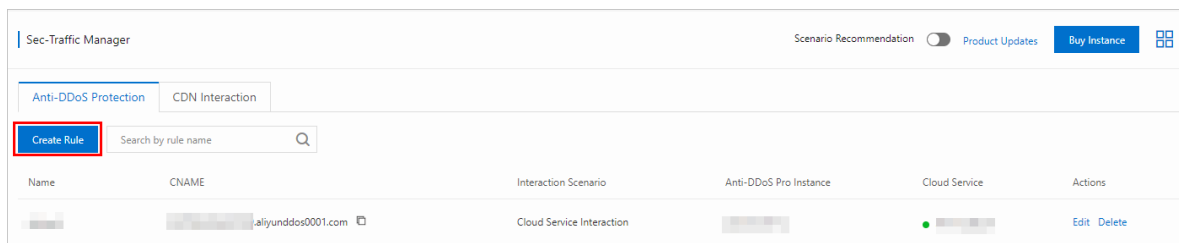
Configure Anti-DDoS Pro features

Feature	Description
Cloud service interaction	<p>Cloud service interaction switches workloads between one or more cloud service instances and an Anti-DDoS Pro instance. The configuration procedure is as follows:</p> <ol style="list-style-type: none"> 1. Configure traffic forwarding for Anti-DDoS Pro. For more information, see Add website configuration. 2. Verify that the Anti-DDoS Pro instance can forward traffic to the origin server. For more information, see Verify configuration. 3. Configure security traffic manager. <ul style="list-style-type: none"> • Switch workloads from a single cloud service instance to an Anti-DDoS Pro instance. For more information, see Create anti-DDoS rules. • Switch workloads from multiple cloud service instances to an Anti-DDoS Pro instance. The configuration methods are described as follows: <ul style="list-style-type: none"> - Switch the workloads to Anti-DDoS Pro only if all cloud service instances are overwhelmed by incoming traffic. Create an anti-DDoS rule in the same way as switching workloads between a single cloud service instance and an Anti-DDoS Pro instance, and specify multiple cloud service instances for interaction. - The cloud service instances share the workloads. If any cloud service instance is attacked, switch the workloads on the instance to Anti-DDoS Pro. For more information, see Configuration example for separate workloads switchovers. 4. Modify the DNS settings of the protected domain. Apply the CNAME resolution, and point the domain to the CNAME assigned by security traffic manager. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;">  Note: For more information about how to modify the CNAME, see Update DNS settings. Use the CNAME assigned by security traffic manager instead of Anti-DDoS Pro. </div>
Tiered protection	<p>Tiered protection switches workloads between one or more cloud service instances protected by Anti-DDoS Protection Package and an Anti-DDoS Pro instance. Configure tiered protection in the same way as configuring cloud service interaction.</p>

Feature	Description
CDN interaction	<p>The configuration procedure is as follows:</p> <ol style="list-style-type: none"> 1. Configure the CDN service, and add the protected domain to CDN. For more information, see Add an CDN domain. <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">  Note: If a security group is configured for the origin server, you must add the back-to-origin IP addresses of CDN to the whitelist of the origin server. </div> <ol style="list-style-type: none"> 2. Configure traffic forwarding for Anti-DDoS Pro. For more information, see Add website configuration. 3. Verify that the Anti-DDoS Pro instance can forward traffic to the origin server. For more information, see Verify configuration. 4. Configure security traffic manager. For more information, see Create a CDN interaction rule. 5. Modify the DNS settings of the protected domain. Apply the CNAME resolution, and point the domain to the CNAME assigned by security traffic manager. <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">  Note: For more information about how to modify the CNAME, see Update DNS settings. Use the CNAME assigned by security traffic manager instead of Anti-DDoS Pro. </div>

Create an anti-DDoS rule

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose Anti-DDoS Pro > Sec-Traffic Manager.
3. On the Anti-DDoS Protection tab, click Create Rule.



4. In the Create Rule pane that appears, configure the rule, and click Next. The following table lists the parameters in an interaction rule.

Parameter	Description
Interaction Scenario	The scenario where the rule is applied. Valid values: <ul style="list-style-type: none"> Cloud Service Interaction Tiered Protection (Only cloud resources that are protected by Anti-DDoS Protection Package are supported, such as ECS, EIP, SLB, and WAF instances.)
Name	The name of the rule. The rule name must be no more than 128 characters in length and can contain letters, digits, and underscores (_).
Anti-DDoS Pro Instance	The IP address of the target Anti-DDoS Pro instance.
Cloud Resource	The cloud resources for interaction. Select the region where the target cloud resource is deployed and enter the cloud resource IP address. Click Add Cloud Resource IP to add more cloud resources. You can add up to 20 cloud resources.

After a rule is created, security traffic manager assigns a CNAME to this rule. To apply the rule, you must go to the DNS provider of the cloud resource to modify

the DNS settings. Apply the CNAME resolution, and point the domain to the CNAME assigned by security traffic manager.

Create Rule

Change the DNS settings in the system of your service provider. Point DNS resolution to the Sec-Traffic Manager CNAME.

CNAME: [redacted].aliyunddos0001.com

Add Record

Type: CNAME

Host: www [redacted].aliyunddos0001.com

ISP Line: BEU

* Value: abc.example.com

* TTL: 10 分钟

Record Type : CNAME

Add cname value provided above

Complete

You can view the new rule and the CNAME on the Anti-DDoS Protection tab.

Anti-DDoS Protection		CDN Interaction			
Create Rule		Search by rule name			
Name	CNAME	Interaction Scenario	Anti-DDoS Pro Instance	Cloud Service	Actions
doctest	[redacted].aliyunddos0001.com	Cloud Service Interaction	[Progress Bar]	[Progress Bar]	Edit Delete

Create a CDN interaction rule

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose Anti-DDoS Pro > Sec-Traffic Manager.
3. Click the CDN Interaction tab.

The CDN Interaction tab displays all the domains added to Anti-DDoS Pro.

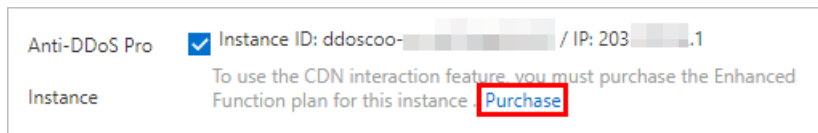
4. Find the target domain, and click Add Interaction.

Sec-Traffic Manager		Scenario Recommendation <input type="checkbox"/> Product Updates <input type="checkbox"/> Buy Instance			
Anti-DDoS Protection		CDN Interaction			
Search by domain					
Domain	CNAME	Anti-DDoS Pro Instance	CDN Interaction	Trigger Condition	Actions
[redacted].com	--	203.[redacted].158	Disabled	--	Add Interaction
[redacted].st.com	--	203.[redacted].224	Disabled	--	Add Interaction

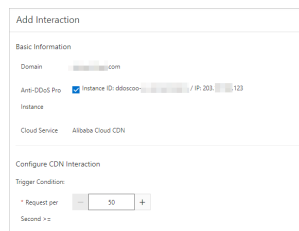
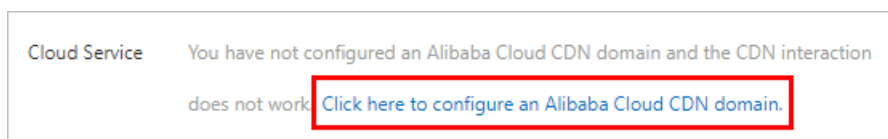
5. In the Add Interaction pane, check whether the Basic Information meets the requirements described as follows. If the requirements are met, set Trigger Condition to the lowest request rate that triggers a switchover. Click Next.

To create a CDN interaction rule, the following requirements must be met:

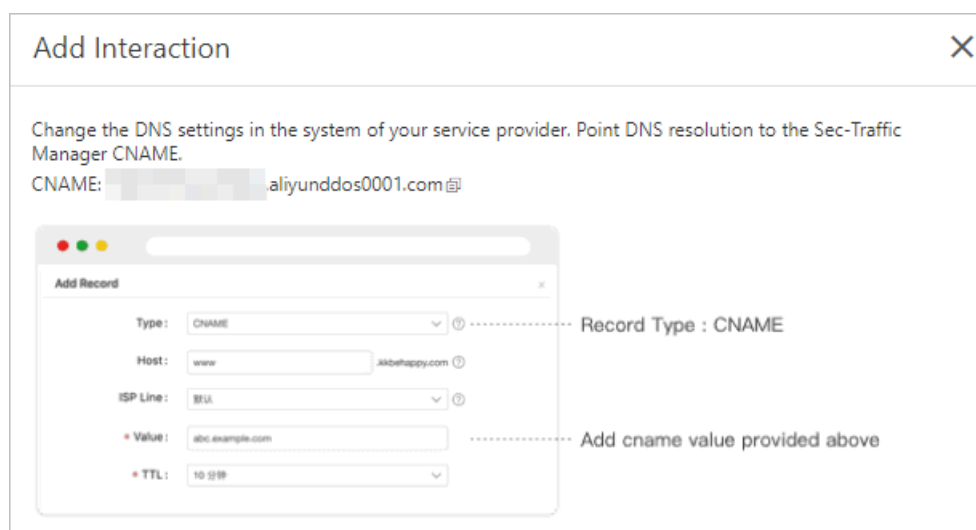
- **Anti-DDoS Pro Instance:** The enhanced function plan is enabled.



- **Cloud Service:** Alibaba Cloud CDN is configured for the domain.



After a rule is created, security traffic manager assigns a CNAME for this rule. To apply the rule, you must go to the DNS provider of the cloud resource to modify the DNS settings. Apply the CNAME resolution, and point the domain to the CNAME assigned by security traffic manager.



On the CDN Interaction tab, CDN Interaction of the target domain changes to **Enabled**. The CNAME is also updated.

Configuration example for separate workloads switchovers

The following example introduces how to configure the switchover between multiple cloud service instances protected by Anti-DDoS Protection Package and an Anti-DDoS Pro instance. In this scenario, the cloud service instances share the workloads. If any instance is attacked, the workloads on the instance are switched to Anti-DDoS Pro. Alibaba Cloud DNS is used in the example figure for modifying the CNAME record.

1. Configure Anti-DDoS Protection Package. Add multiple IP addresses for protection. In the following example, three IP addresses are added.

Add Protected Asset

Enter the IP addresses of assets that you want to protect:

47.193.47.193, 46.120.193.226

You can add 97 IP addresses.

OK Cancel

2. Configure security traffic manager. Create a tiered protection rule for each of the IP addresses added in step 1. Bind the three rules to the same Anti-DDoS IP address.

Create Rule 1

Create Rule 2

Create Rule 3

Anti-DDoS Protection

CDN Interaction

Create Rule

Search by rule name

Name	CNAME	Interaction Scenario	Anti-DDoS Pro Instance	Cloud Service	Actions
slb1	aliyunddos0001.com	Tiered Protection	203.193.39.1	47.193.47.193	Edit Delete
slb2	aliyunddos0001.com	Tiered Protection	203.193.39.1	47.193.46.193	Edit Delete
slb3	aliyunddos0001.com	Tiered Protection	203.193.39.1	120.193.226.193	Edit Delete

3. **Modify the DNS settings. Add three CNAME records that use the same host record. Set the record values to the CNAMEs of the three tiered protection rules created in step 2.**

The screenshot shows three 'Add Record' dialog boxes (labeled 1, 2, and 3) and a 'DNS Settings' table. Each dialog box is for adding a CNAME record with the following fields:

- Type: CNAME - Canonical name
- Host: slbtest
- ISP Line: Default - Return to the default value when the query is not m...
- Value: aliyunddos0001.com
- TTL: 10 minute(s)

The 'DNS Settings' table below shows the existing records:

Host	Type	Line(S)	Value	TTL	Status	Remark	Actions
slbtest	CNAME	Default	aliyunddos0001.com	10 minute(s)	Normal		Edit Disable Delete Remark
slbtest	CNAME	Default	aliyunddos0001.com	10 minute(s)	Normal		Edit Disable Delete Remark
slbtest	CNAME	Default	aliyunddos0001.com	10 minute(s)	Normal		Edit Disable Delete Remark

4. **Verify the DNS settings. Use a DNS checker to check whether the CNAME records added in step 3 take effect.**

4.4 Add Anti-DDoS Pro back-to-origin CIDR blocks to the whitelist

When you use Anti-DDoS Pro to protect your site, we recommend that you add back-to-origin CIDR blocks to the whitelist so that traffic from Anti-DDoS Pro is not mistakenly blocked by security software on your origin server.

Context

After you set up Anti-DDoS Pro to protect your site, all traffic to your site is directed to Anti-DDoS Pro first, which filters out malicious traffic and then forwards the traffic back to the origin server. The process whereby an Anti-DDoS Pro instance forwards traffic back to the origin server is called back-to-origin.

Anti-DDoS Pro acts as a reverse proxy and supports Full NAT mode.

Before Anti-DDoS Pro is used to protect the origin server, client IP addresses are widely distributed. The number of requests from each client IP address is relatively small under normal circumstances.

After Anti-DDoS Pro is used, a limited number of back-to-origin CIDR blocks are used to forward traffic to the origin server. For the origin server, all incoming requests originate from these back-to-origin CIDR blocks. The number of requests from each back-to-origin IP address can be quite large, which makes it appear

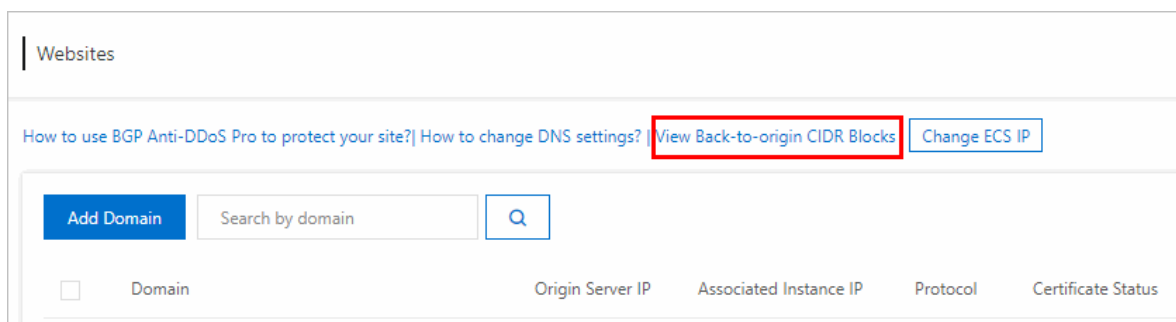
that these IP addresses are attacking the origin server. If other DDoS protection policies are configured on the origin server, these back-to-origin CIDR blocks may be blocked or subject to bandwidth limits.

For example, the most commonly found 502 error indicates that when Anti-DDoS Pro forwards requests to the origin server, the server is not responding. The reason may be that the back-to-origin IP address is blocked by the firewall on the origin server.

Therefore, we recommend that you disable the firewall and other security software on the origin server after you configure forwarding rules. This ensures that Anti-DDoS back-to-origin CIDR blocks are not affected by the protection policies on the origin server. Alternatively, you can use the following steps to find the back-to-origin CIDR blocks used by Anti-DDoS Pro and add them to the whitelist of the security software on the origin server. We recommend that you create security groups or use whitelists to protect your origin server. For more information, see [Protect origin servers](#).

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose Management > Websites.
3. On the Websites page, click View Back-to-origin CIDR Blocks on the top of the page.



4. In the Back-to-origin CIDR Block dialog box, copy the back-to-origin CIDR blocks used by Anti-DDoS Pro.



5. Modify the whitelist of the security software on your origin server and add these back-to-origin CIDR blocks to the whitelist.

4.5 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.

5 Security overview

After you associate your domain with an Anti-DDoS Pro instance and forward incoming traffic to the instance, you can view business metrics and DDoS events in real time on the Security Overview page in the console.

Context

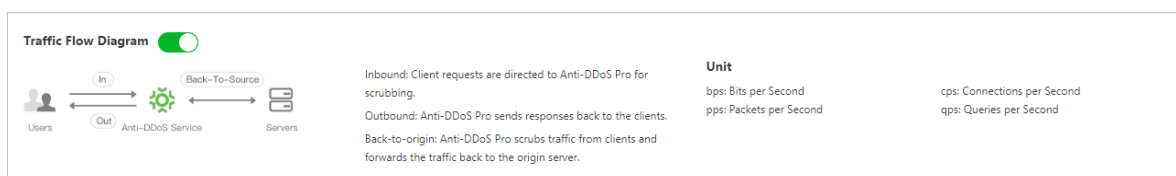
The Security Overview page provides an overview of the following business metrics and DDoS events:

- **Business metrics:** service bandwidth, request rate (QPS), connection rate (CPS), protected domains, and protected ports.
- **DDoS events:** volume based attacks, application layer attacks and protocol attacks.

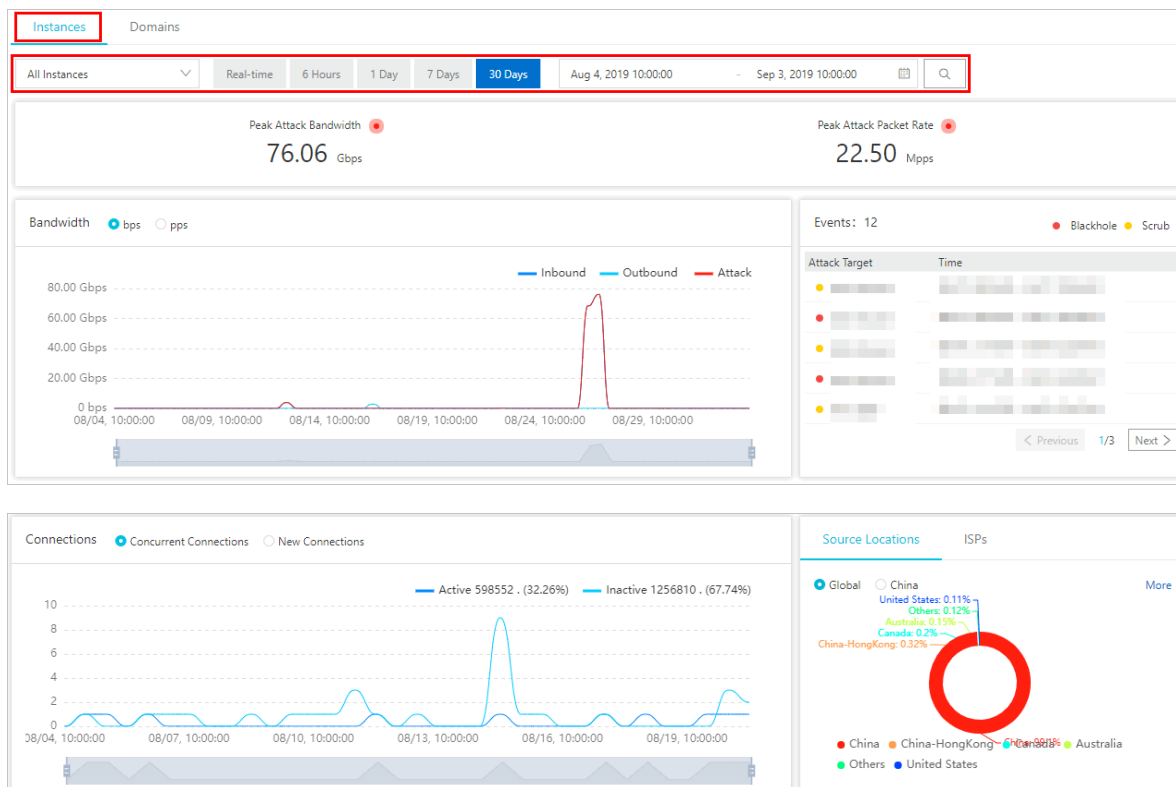
Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, select **Statistics > Security Overview**. You can learn basic terms and concepts about Anti-DDoS Pro.

In the top section of the Security Overview page, you can learn how incoming traffic flows between Anti-DDoS Pro and backend servers, and commonly used terms and units.



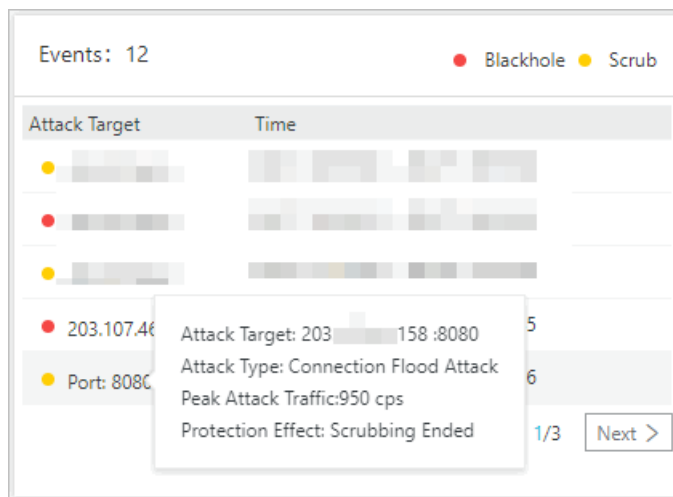
3. Click the **Instances** tab, select one or multiple instances, and specify a time period to view the corresponding business metrics.



You can view the following information about selected instances:

- **Peak Attack Bandwidth and Peak Attack Packet**
- **Trend of Traffic Bandwidth, including inbound traffic, outbound traffic, and attack traffic.**
- **Attack Events**

Hover over an IP address to view attack details, such as the attack type, peak attack traffic, and protection effect.

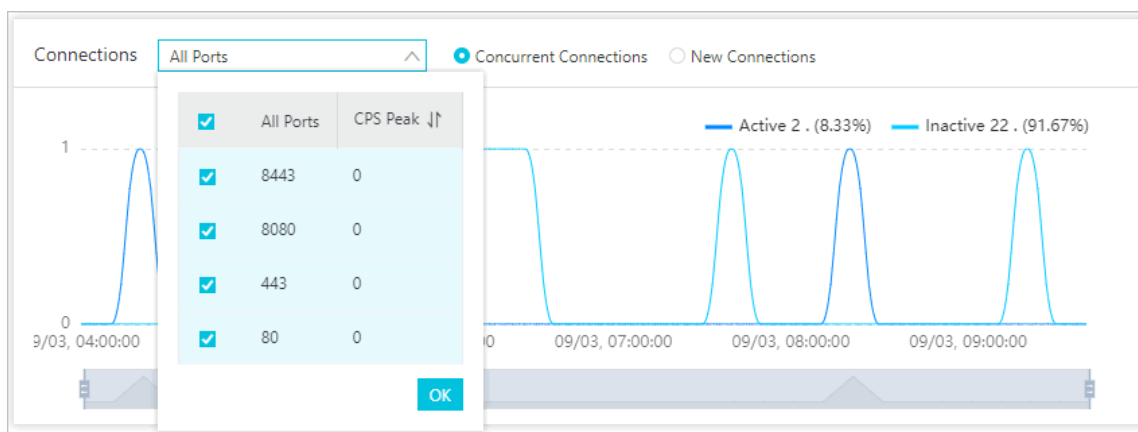


- **Port Connections**

- **Concurrent Connections:** number of TCP connections established between the client and anti-DDoS pro at the same time.
- **New Connections:** number of TCP connections added by the client to communicate with anti-DDoS pro per second.

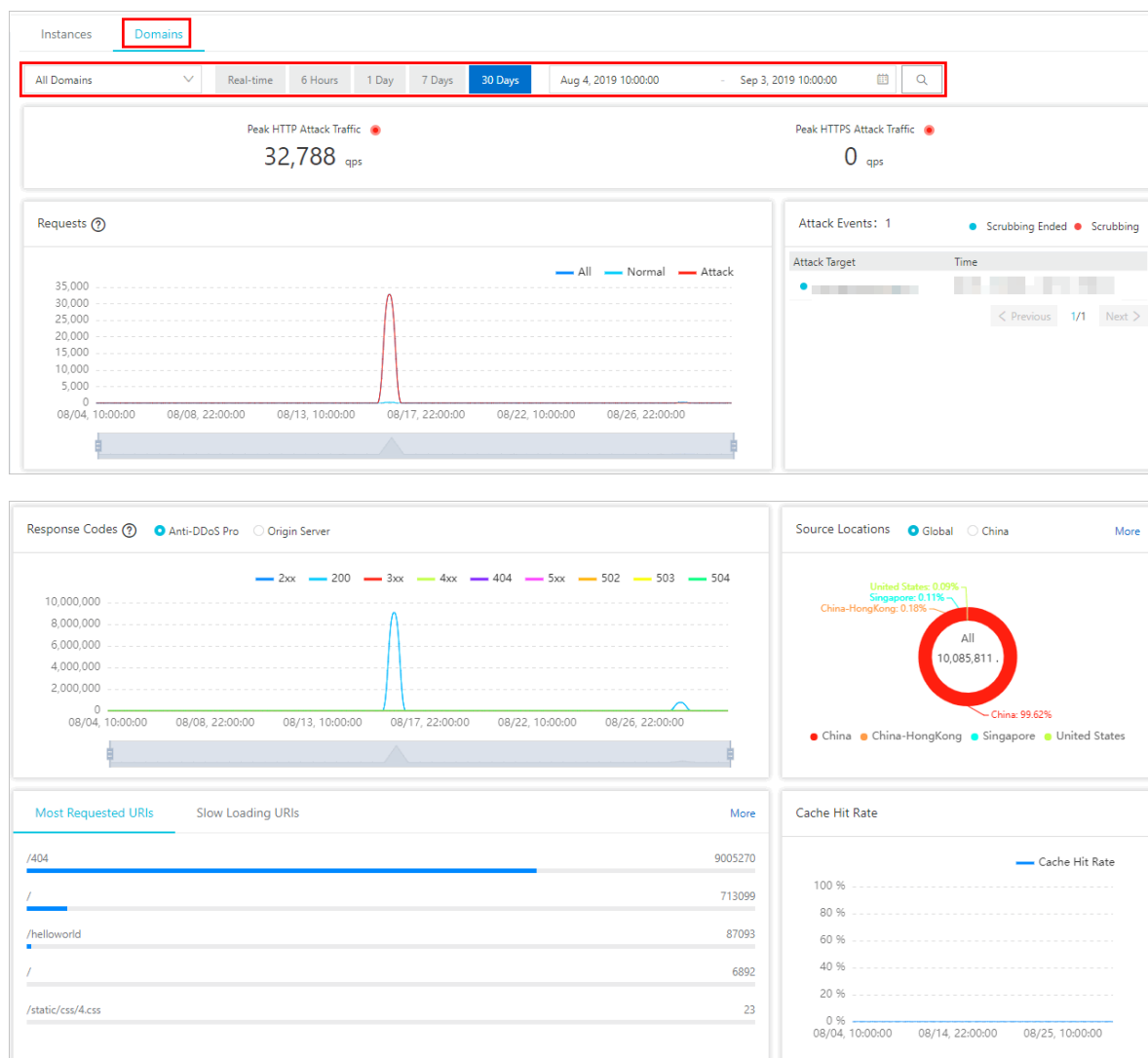
**Note:**

When only one instance is selected, the chart displays the numbers of different port connections to the instance. When two or more instances are selected, the chart displays the total number of port connections to the selected instances.



- **Traffic Source Locations and ISPs**

4. Click the Domains tab, select one or multiple domains, and specify a time period to view the corresponding business metrics.



You can view the following information about selected domains:

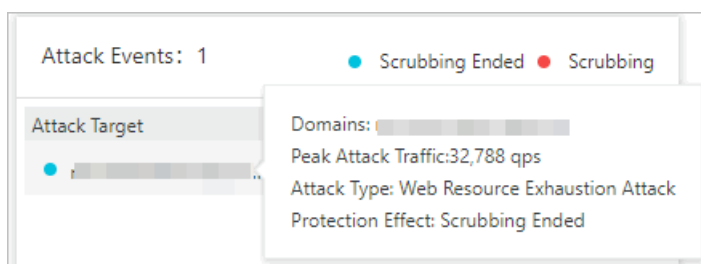
- Peak HTTP Attack Traffic and Peak HTTPS Attack Traffic
- Trend of Requests

The trend of requests is displayed based on the peak values during specific time intervals. The time interval varies according to the search time period.

- If the search time period is less than an hour, the time interval is one minute.
- If the search time period is between 1 to 6 hours, the time interval is 10 minutes.
- If the search time period is between 6 to 24 hours, the time interval is 30 minutes.

- If the search time period is between 1 to 7 days, the time interval is one hour.
 - If the search time period is between 7 to 15 days, the time interval is 4 hours.
 - For other search time periods, the time interval is 12 hours.
- **Application Layer Attack Events**

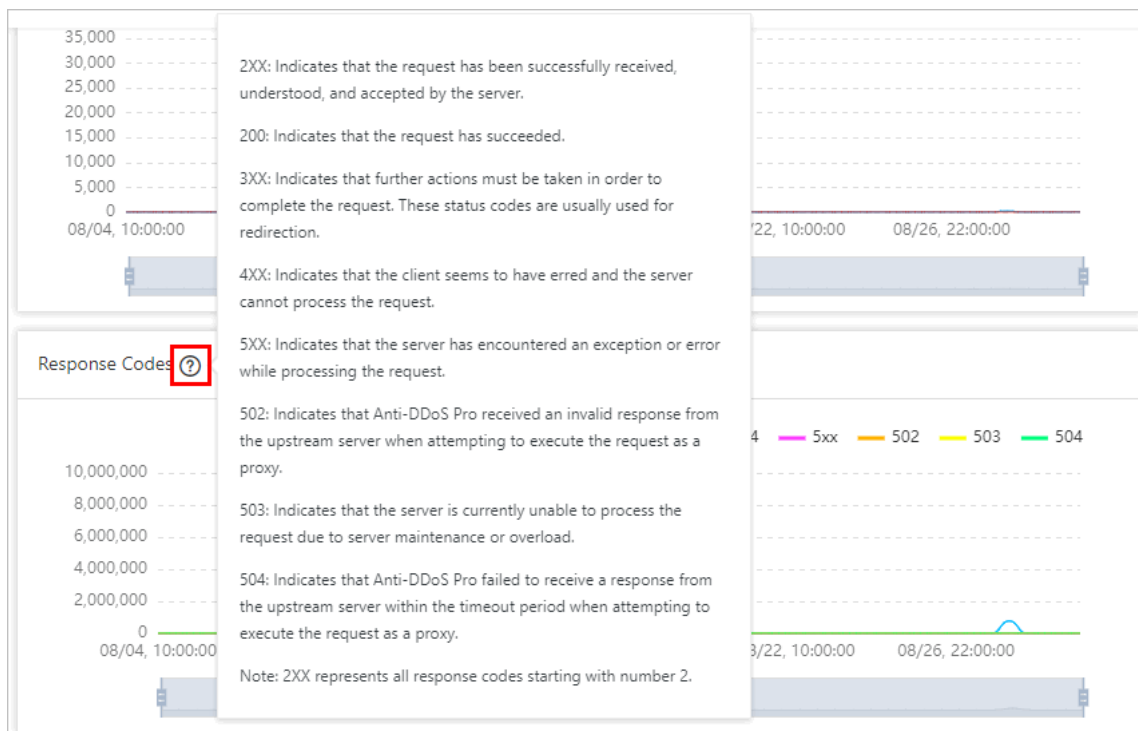
Hover over a domain to view attack details, such as the attack type and peak attack traffic.



- **Response Codes**

The trend of response codes displays the accumulated numbers of response codes within the search time period, which is the same as the time period used

in the trend of requests. You can hover over the question mark icon to find what the response codes mean.



- Traffic Source Locations
- The Most Requested URIs and Slow Loading URIs
- Trend of Cache Hit Rate



Note:

To view the trend of cache hit rate, you must enable the static page caching feature first. For more information, see [Configure static page caching rules](#).

6 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.

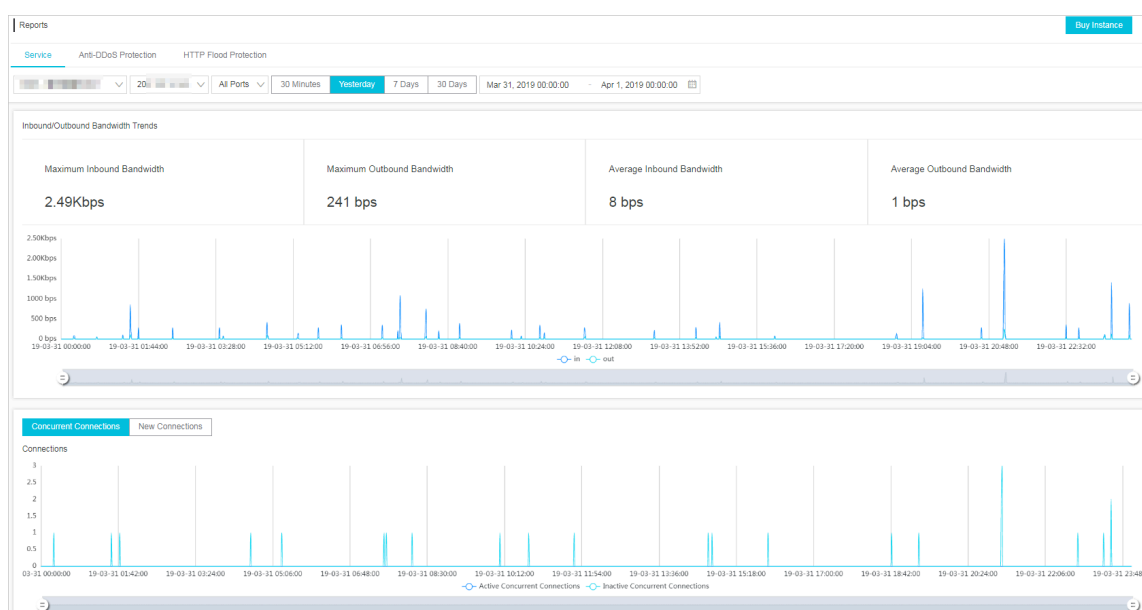
Procedure

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.



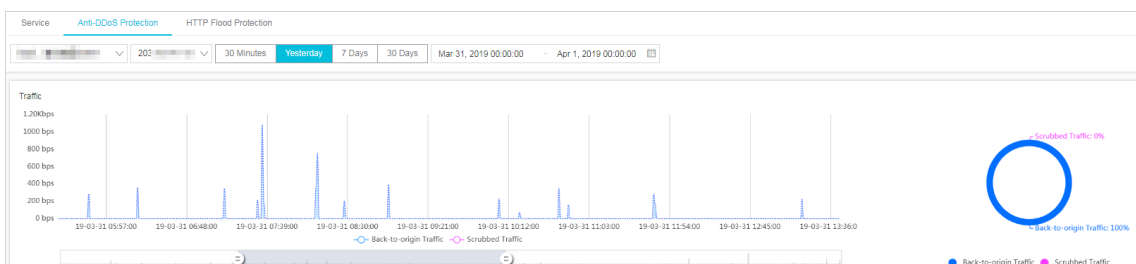
You can drag the slider to quickly change time ranges.

- 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.

7 Configure protection policies

7.1 Protection for Infrastructure

7.1.1 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.

Anti-DDoS Protection Policies HTTP Flood Protection Policies Web Acceleration Policies ⓘ

Instance ID: ddoscoo-cn-78v12b12e003 Search Scrubbing Mode Blacklist and Whitelist Deactivate Blackhole Status **Block Flow**

You have 9952 time(s) remaining to deactivate the blackhole state (15 time(s) in total)

Instance Info	ISP Line	Service Address	Status	ISP	Blocked Region	Blocking Period	Deactivated Time	Blocked Time	Action
ddoscoo-cn-78v12b12e003	coop-line-001	203.113.113.113	Normal	China Telecom	International	--	--	--	Blocked
			Normal	China Unicom (Beta)		--	--	--	Blocked

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.

7.1.2 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.

The screenshot shows the 'Anti-DDoS Protection Policies' tab selected. Below the tabs, there's a search bar and several buttons: 'Scrubbing Mode', 'Blacklist and Whitelist', 'Deactivate Blackhole Status' (highlighted with a red box), and 'Block Flow'. Below this, a table lists instance information. The first instance is 'ddoscoo-cn-78v12b12e003' with ISP Line 'coop-line-001', Service Address '203.111.111.111', Status 'Normal', and Automatic Deactivated Time '--'. A message at the top right of the table says '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	203.111.111.111	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.

7.2 Configure layer 7 protection

7.2.1 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.



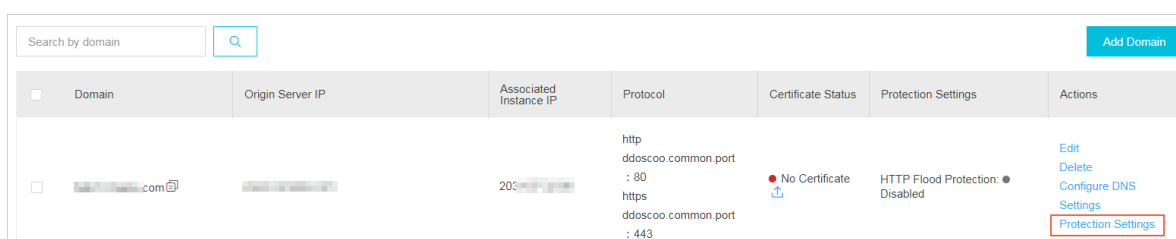
Note:

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.



Domain	Origin Server IP	Associated Instance IP	Protocol	Certificate Status	Protection Settings	Actions
<input type="checkbox"/> [domain].com	[IP]	203.[IP]	http ddoscoo.common.port : 80 https ddoscoo.common.port : 443	No Certificate	HTTP Flood Protection: Disabled	Edit Delete Configure DNS Settings 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 (,).

Blacklist and Whitelist Settings

Blacklist

Whitelist

IP addresses in the blacklist will be blocked :

Enter IP addresses or IP address/CIDR. Separate multiple entries with commas (,). You can enter a maximum of 200 IP addresses.

OK

Cancel

**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.

7.2.2 Block requests from specific regions

Geo-blocking allows you to block access from specific regions based on IP address. For example, you can choose to block requests from 34 Chinese provincial regions and 7 international regions. Currently, this feature is only available to specific domains.

Prerequisites

Before you enable Geo-blocking, make sure that your domain is associated with an Anti-DDoS Pro instance of the enhanced package.

Context

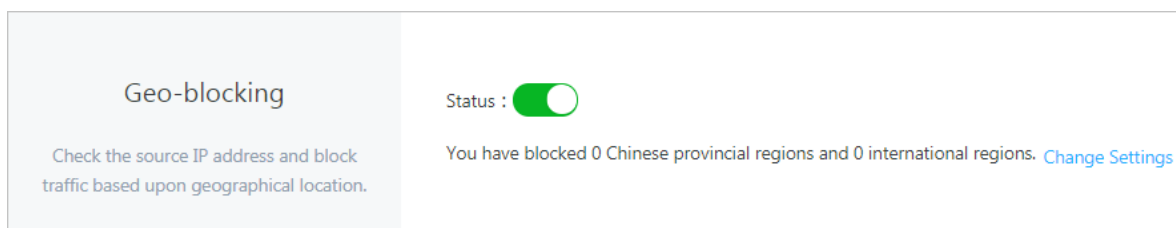
Assume that all normal requests to website `example.aliyundemo.com` are from 34 Chinese provincial regions. You can use Geo-blocking to block requests from international regions.

Notes

- To enable Geo-blocking for multiple domains, you must modify Geo-blocking status for each domain respectively.
- When Geo-blocking is enabled, Anti-DDoS Pro identifies and filters traffic based on the region where the traffic originates. This feature does not reduce the volume of traffic that enters Anti-DDoS Pro scrubbing centers.

Procedure

1. Log on to the [new Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose Protection > Protection Settings > HTTP Flood Protection Policies.
3. Select a domain, for example, `example.aliyundemo.com`. In the Geo-blocking section, click the Status toggle to enable Geo-blocking for the selected domain.



4. Click **Change Settings**. Select the regions that you want to block in the dialog box that appears. You can select regions as follows to block traffic from international regions.

Select Region

☐ Shanghai Municipality ☐ Yunnan Province ☐ Jilin Province

☐ Beijing Municipality ☐ Taiwan Province ☐ Ningxia Hui Autonomous Region

☐ Sichuan Province ☐ Tianjin Municipality ☐ Shaanxi Province

☐ Anhui Province ☐ Shandong Province ☐ Guangxi Zhuang Autonomous Region

☐ Shanxi Province ☐ Guangdong Province ☐ Jiangxi Province

☐ Xinjiang Uyghur Autonomous Region ☐ Jiangsu Province ☐ Zhejiang Province

☐ Hebei Province ☐ Henan Province ☐ Hunan Province

☐ Hainan Province ☐ Hubei Province ☐ Fujian Province

☐ Macau SAR ☐ Gansu Province ☐ Liaoning Province

☐ Tibet Autonomous Region ☐ Guizhou Province ☐ Hong Kong SAR

☐ Chongqing Municipality ☐ Qinghai Province

☐ Heilongjiang Province

International Regions

☒ Select All

☒ Asian (Excluding Chinese Regions) ☒ Europe ☒ North America

☒ South America ☒ Africa ☒ Oceania

☒ Antarctica

OK **Cancel**

5. Click **OK** and the configuration takes effect immediately.

7.2.3 Configure fine-grained access control rules

Fine-grained access control allows you to create custom rules to control access to your business. You can filter requests based on the request IP, URL, and common HTTP header fields, such as the Referer, User-Agent, and parameters. You can handle matching requests with different actions, such as clear, block, and challenge. This feature supports custom business scenarios, such as hotlinking protection and management console protection.

Context

Each access control rule consists of one or more match conditions and an action. When you create a rule, you need to define match conditions by specifying the field

name, logical relation, and field value. You also need to select an action that will be triggered when a matching request is detected.

Match conditions

Each match condition consists of a field name, logical relation, and field value. Currently, field values do not support regular expressions, but can be left empty.

Actions

The following actions are supported:

- **Block:** Requests that meet match conditions are blocked.
- **Clear:** Requests that meet match conditions are allowed to your website.
- **Challenge:** Captcha verification is used to verify the source IP of the requests that meet match conditions.

The order of rules

If multiple rules are configured, requests are compared to these rules based on the order that rules are displayed in the rule list. Anti-DDoS Pro compares requests to the first rule in the list and continues in sequence from top to bottom.

Notes

- The number of access control rules is subject to a limit.
 - **Standard package:** For each protected domain, a maximum of five rules can be configured. Only the request IP, URL, Referer, and User-Agent field can be used to create match conditions.
 - **Enhanced package:** For each protected domain, a maximum of 10 rules can be configured.
- The rule priority is determined by the order that rules are displayed in the rule list. The higher the rule, the higher the priority. If a request meets multiple match conditions of different rules, the action of the rule with the highest priority takes effect.


Procedure

1. Log on to the [new Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose **Protection > Protection Settings > HTTP Flood Protection Policies**.

3. Select a domain, for example, `example.aliyundemo.com`. In the Accurate Access Control section, click the Status toggle to enable fine-grained access control for the selected domain.

Accurate Access Control

Combine common HTTP header fields to create custom access control rules that suit different scenarios.

Status : 

You have set 0 access control rules. [Change Settings](#)

4. Click Change Settings to configure access control rules. In the following example, requests that attempt to access the `/index.php` page and contain MSIE in the User-Agent field are blocked.

Create Rule ×

* Name

* Match

Field Name	Logical Relation	Field Value	
URI	Equals	/index.php	Remove
User-Agent	Contains	MSIE	Remove

+ Add Condition

* Action

* Validity

OK

Cancel

Supported fields



Note:

Anti-DDoS Pro instances of the standard package only support the following fields: request IP, URL, Referer, and User-Agent.

Field	Description	Supported logical relation
IP	The source IP of the request.	<ul style="list-style-type: none"> • Is Part Of • Is Not Part Of
URI	The request URL.	<ul style="list-style-type: none"> • Contains • Does Not Contain • Equals • Does Not Equal • Is Shorter Than • Has a Length Of • Is Longer Than
User-Agent	The information about the browser that sent the request.	<ul style="list-style-type: none"> • Contains • Does Not Contain • Equals • Does Not Equal • Is Shorter Than • Has a Length Of • Is Longer Than
Cookie	The cookie in the request •	<ul style="list-style-type: none"> • Contains • Does Not Contain • Equals • Does Not Equal • Is Shorter Than • Has a Length Of • Is Longer Than • Does Not Exist
Referer	The URL of the site that initiated the request. This URL indicates the page that contained the hyperlink to the currently requested URL.	<ul style="list-style-type: none"> • Contains • Does Not Contain • Equals • Does Not Equal • Is Shorter Than • Has a Length Of • Is Longer Than • Does Not Exist

Field	Description	Supported logical relation
Content-Type	The content type, or MIME type, of the returned content that is specified by the request.	<ul style="list-style-type: none"> • Contains • Does Not Contain • Equals • Does Not Equal • Is Shorter Than • Has a Length Of • Is Longer Than
X-Forwarded-For	The originating IP address of the client that initiated the request.	<ul style="list-style-type: none"> • Contains • Does Not Contain • Equals • Does Not Equal • Is Shorter Than • Has a Length Of • Is Longer Than • Does Not Exist
Content-Length	The byte length of the HTTP body of the request.	<ul style="list-style-type: none"> • Is Smaller Than • Has a Value Of • Is Larger Than
Post-Body	The content of the request.	<ul style="list-style-type: none"> • Contains • Does Not Contain • Equals • Does Not Equal
Http-Method	The request method, such as GET and POST.	<ul style="list-style-type: none"> • Equals • Does Not Equal
Header	The request header. You can specify an HTTP header field and value based on your needs.	<ul style="list-style-type: none"> • Contains • Does Not Contain • Equals • Does Not Equal • Is Shorter Than • Has a Length Of • Is Longer Than • Does Not Exist

Field	Description	Supported logical relation
Params	The parameters in the request URL. The parameter part in the URL usually follows a question mark (?). For example, in the URL <code>www.abc.com/index.html?action=login</code> , the parameter part is <code>action=login</code> .	<ul style="list-style-type: none">• Contains• Does Not Contain• Equals• Does Not Equal• Is Shorter Than• Has a Length Of• Is Longer Than

Examples

The following examples demonstrate how to configure fine-grained access control rules to block specific types of requests.

- **Block specific requests**

Under most circumstances, clients do not send POST requests to the root directory of your website. In an HTTP flood attack, your website may receive a large number of POST requests to the root directory. We recommend that you check the validity of these requests. If it is confirmed that these requests are

not normal requests, you can use access control rules to block them. A sample configuration is provided as follows:

Edit Rule

*

 Name

Aliyun_POSTROOT

*

 Match

Conditions

Field Name	Logical Relation	Field Value	
URI	Equals	/	Remove
Http-Method	Equals	POST	Remove

+ Add Condition

*

 Action

Blocked

*

 Validity

Permanent

OK

Cancel

- **Block Web crawlers**

If your website receives a large volume of crawler traffic, the traffic may originate from malicious bots simulating crawlers, which is one of the

common forms of HTTP flood attacks. You can use access control rules to block crawlers.

Create Rule

* Name

* Match

Field Name	Logical Relation	Field Value	
User-Agent	Contains	spider	Remove

+ Add Condition

* Action

* Validity

OK Cancel

5. Click OK and the rule takes effect immediately.

7.2.4 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**.

Search by domain <input type="text"/>		<input type="button" value="Add Domain"/>				
<input type="checkbox"/>	Domain	Origin Server IP	Associated Instance IP	Protocol	Certificate Status	Protection Settings
<input type="checkbox"/>	example.com		203.107.132.10	http ddoscoo.common.port : 80 https ddoscoo.common.port : 443	No Certificate 	HTTP Flood Protection: Disabled Edit Delete Configure DNS Settings 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.

7.2.5 Enable intelligent protection

Based on Alibaba Cloud's big data capabilities, intelligent protection utilizes an analysis engine to learn the traffic pattern of your business and adjust protection schemes accordingly. This feature can timely detect and block malicious attacks, such as bot attacks and HTTP flood attacks.

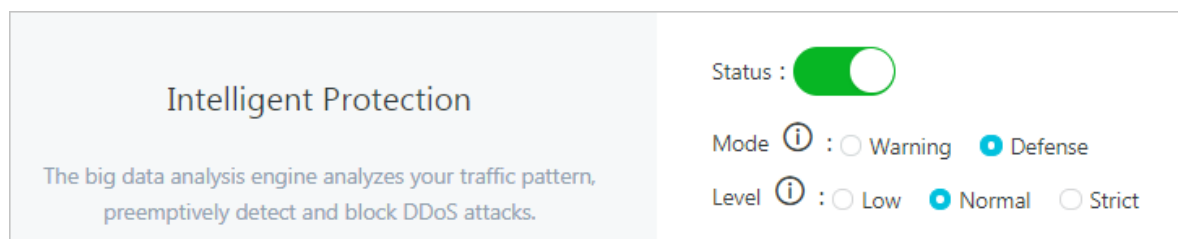
Context

**Notice:**

After intelligent protection is enabled, you cannot delete rules that are automatically created by the system. If you find that the automatically created rules do not suit your business needs, we recommend that you disable intelligent protection. After intelligent protection is disabled, these rules will be deleted instantly.

Procedure

1. Log on to the [new Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose **Protection > Protection Settings > HTTP Flood Protection Policies**.
3. Select a domain, for example, `example.aliyundemo.com`. In the **Intelligent Protection** section, click the **Status** toggle to enable Intelligent Protection for the selected domain.



Result

The system displays the following message: "The operation is successful", indicating that intelligent protection has been enabled.

When intelligent protection is enabled, your Anti-DDoS Pro instance automatically creates protection rules when attacks are detected. You can view these rules in the Accurate Access Control section. The name of these rules all start with string "smartcc_".

**Note:**

Each rule have an expiration time. Once expired, the rule will be invalid and automatically deleted.

7.3 Configure layer 4 protection

7.3.1 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.

Settings	Description
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.

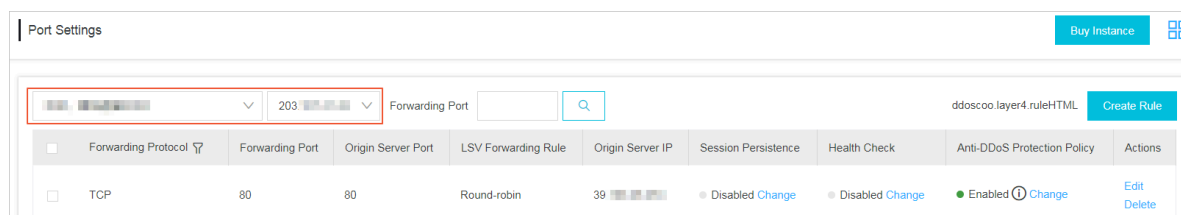


Note:

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.

Anti-DDoS Protection Policy

False Source: ☒

Empty Connection ⓘ : ☒

* Source New Connection

Rate Limit ⓘ : ☐ Automatic ☐ Manual ☒ Cancel

* Source Concurrent

Connection Rate Limit: ☐

* Destination New

Connection Rate Limit ⓘ ☐

OK Cancel

7.3.2 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**.

Anti-DDoS Protection Policies					
Instance ID <input type="text" value="Enter"/>		<input type="text" value="Search"/>	Scrubbing Mode	Blacklist and Whitelist	Deactivate Blackhole Status
Instance	Line	IP Address	Smart Defense Mode Switch ①	Smart Defense Mode ①	Actions
ddoscoo-cn-v6416enj700d	coop-line-shenzhen-CT	203.111.111.111	<input checked="" type="checkbox"/>	Normal	Modify Smart Defense Mode
ddoscoo-cn-mp915qlzv00s	coop-line-001	203.111.111.111	<input checked="" type="checkbox"/>	Normal	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.

Modify Smart Defense Mode

Scrubbing Mode

Low

Normal

Strict

Based on historical service logs and expert experience algorithm, this mode defends against suspicious IP with obvious attack behaviors. It has a good balance between protection effect and false interruption.

OK

Cancel

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.

Instance ID: ddoscoo-cn-78v12b12e003

Enter an IP with at least 3 charac

Scrubbing Mode: Blacklist and Whitelist

Blacklist Whitelist

IP Address Information	Source	Expire Date
192.168.1.1	Manually Add	2019/4/1 11:11:21

Manually Add Download Clear 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.

Blacklist Setting

Blocking Time: 60 Minutes

Separate multiple IPs with a space or line break.

Add Clear Cancel



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.

7.4 Configure static page caching rules

Integrated with Web caching techniques, Anti-DDoS Pro provides a scrubbing center that protects your website from DDoS attacks and also reduces page loading time.

Prerequisites

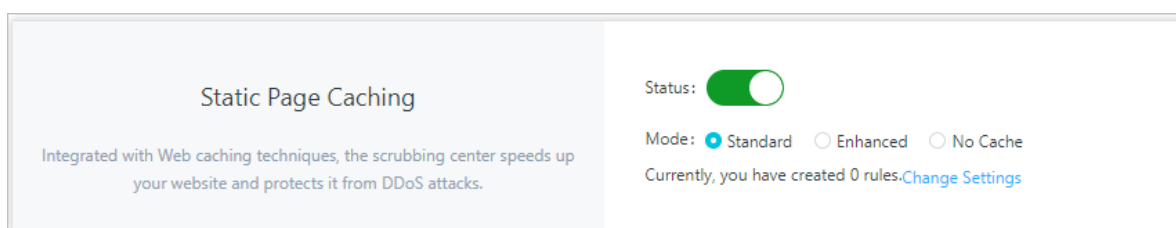
Before you enable the static page caching feature, make sure that your domain is associated with an Anti-DDoS Pro instance of the enhanced package.

Context

You can use the static page caching feature to speed up your website and configure custom rules to reduce the loading time of specific pages.

Procedure

1. Log on to the [new Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose **Protection > Protection Settings > Web Acceleration Policies**.
3. Select a domain and click the Status toggle to enable Static Page Caching for the selected domain.
4. Select the cache mode.
 - **Standard:** This mode will only cache requests that access static resources on the website, such as CSS, JS, and TXT files.
 - **Enhanced:** This mode will try to cache all requests to the website.
 - **No Cache:** This mode will not cache any request to the website.



5. Click **Change Settings** to configure custom rules for specific pages on the website.
 - a) Click **Create Rule**.
 - b) In the **Create Rule** dialog box, specify the URI of the page to be cached, select the cache mode, and specify the time when the cache expires.



Note:

Do not enter parameters or wildcard characters in the URI field. For example, /a/ indicates all pages under path `www.a.com/a/`.

Create Rule

*

Name:

Enter a maximum of 128 characters that can be letters, numbers, and u

*

URI :

For example: /abc/a.php

*

Mode

☒ Standard ☐ Enhanced ☐ No Cache

*

Cache Expires In

Use Origin Server Settings ▼

OK

Cancel

8 Security statistics

8.1 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: $500 \times 60 \times 60 \times 24 \times 2 = 86,400,000$ 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_access_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_access_log and cc_blocks > 0 | SELECT ip_to_country  
(if(real_client_ip='', remote_addr, real_client_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_access_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_access_log | select ip_to_provider(if(real_client_ip
='- ', remote_addr, real_client_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_client_ip='- ', remote_addr, real_client_ip)) <> '' order
by mb_in desc limit 10
```


8.2 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: <code>ddos_access_log</code> . 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.	<code>application/x-www-form-urlencoded</code>
host	The domain of the origin server.	<code>api.abc.com</code>
http_cookie	The request cookie.	<code>k1=v1;k2=v2</code>
http_referer	The referer of the request. If this field is empty, - is displayed.	<code>http://xyz.com</code>

Field	Description	Example
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. <ul style="list-style-type: none"> · 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
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 information, 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

Field	Description	Example
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
cc_blocks	<p>Whether the request is blocked by HTTP flood protection.</p> <ul style="list-style-type: none"> • 1: The request is blocked. • Otherwise, the request is accepted. <div>  Note: In some situations, this field may not exist. The <code>last_result</code> field indicates whether the request is blocked by HTTP flood protection. </div>	1

Field	Description	Example
last_result	<p>Whether the request is blocked by HTTP flood protection.</p> <ul style="list-style-type: none"> · ok: The request is accepted. · failed: The request fails verification or is blocked. <div>  Note: In some situations, this field may not exist. The <code>cc_blocks</code> field indicates whether the request is blocked by HTTP flood protection. </div>	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
ua_browser	<p>The browser that initiated the request.</p> <div>  Note: In some situations, this field may not exist. </div>	ie9
ua_browser_family	<p>The browser type.</p> <div>  Note: In some situations, this field may not exist. </div>	internet explorer

Field	Description	Example
ua_browser_type	<p>Whether the browser is a Web browser, mobile browser, or other.</p> <div>  Note: In some situations, this field may not exist. </div>	web_browser
ua_browser_version	<p>The browser version.</p> <div>  Note: In some situations, this field may not exist. </div>	9.0
ua_device_type	<p>The type of the client device.</p> <div>  Note: In some situations, this field may not exist. </div>	computer
ua_os	<p>The operating system of the client device.</p> <div>  Note: In some situations, this field may not exist. </div>	windows_7
ua_os_family	<p>The family of the operating system.</p> <div>  Note: In some situations, this field may not exist. </div>	windows
upstream_addr	<p>The list of back-to-origin addresses. The format is IP:Port. Multiple addresses are separated by commas (,).</p>	1.2.3.4:443
upstream_ip	<p>The actual back-to-origin IP address.</p>	1.2.3.4

Field	Description	Example
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

8.3 Operation logs

You can view operation logs in the last 30 days on the logs page in the new Anti-DDoS Pro console.



Note:

Operation logs only record important operations in the last 30 days.

Recorded operation	Supported
Change the IP of ECS instances	Yes
Deactivate black holes	Yes
Block or unblock traffic	Yes
Change the scrubbing mode of layer 4 traffic	Yes
Change the HTTP flood protection mode	Yes
Change the burstable bandwidth	Yes

9 Resource management

10 API Reference

10.1 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.
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.

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

Layer 7 rules

API	Description
<i>DescribeDomains</i>	Query layer 7 forwarding rules.
<i>CreateLayer7Rule</i>	Create layer 7 forwarding rules.
<i>ConfigLayer7Rule</i>	Edit layer 7 forwarding rules.
<i>DeleteLayer7Rule</i>	Delete layer 7 forwarding rules.
<i>ConfigLayer7Cert</i>	Configure certificates.
<i>ConfigLayer7BlackWhiteList</i>	Configure the blacklist and whitelist.
<i>DescribeLayer7InstanceRelations</i>	Query instances by domain.
<i>DescribeCertList</i>	Query certificates.
<i>EnableLayer7CC</i>	Enable layer 7 HTTP flood protection.
<i>DisableLayer7CC</i>	Disable layer 7 HTTP flood protection.
<i>EnableLayer7CCRule</i>	Enable layer 7 HTTP flood protection rules.
<i>DisableLayer7CCRule</i>	Disable layer 7 HTTP flood protection rules.
<i>AddLayer7CCRule</i>	Add layer 7 HTTP flood protection rules.
<i>ConfigLayer7CCRule</i>	Edit layer 7 HTTP flood protection rules.
<i>DescribeLayer7CCRules</i>	Query layer 7 HTTP flood protection rules.
<i>DeleteLayer7CCRule</i>	Delete layer 7 HTTP flood protection rules.
<i>ConfigLayer7CCTemplate</i>	Set the mode of layer 7 HTTP flood protection.
<i>DescribeDomainAccessMode</i>	Query the modes that are used to set up instances.

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

Tasks

API	Description
<i>ListAsyncTask</i>	Query asynchronous tasks.
<i>CreateAsyncTask</i>	Create asynchronous tasks.
<i>DeleteAsyncTask</i>	Delete asynchronous tasks.

Logs

API	Description
<i>DescribeOpEntities</i>	Query operation logs.

10.2 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 `DescribeInstances` 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=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&Format=xml
&Version=2017-12-28
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=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.

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/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNWSnsc6v8YG0juE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

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=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-12-28
&SignatureVersion=1.0
```

Perform the following steps to calculate the signature:

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

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeDomainNames&Region%3Dcn&InstanceId%3Dwaf_elasticity-cn-0xldbqtm005&Format%3DXML&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&SignatureVersion%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&.

```
CT9X0VtwR86fNWSnsc6v8YG0juE=
```

3. Add the signature to the request URL:

```
https://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-12-28
&SignatureVersion=1.0
&Signature=CT9X0VtwR86fNWSnsc6v8YG0juE%3D
```

10.3 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): <ul style="list-style-type: none"> 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=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDaxvLU6tFE0DVb
&Version=2017-12-28
&SignatureVersion=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-AC049166F216</RequestId>
    <!--The response data-->
  </API name+Response>
```

- **JSON format**

```
{
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
  /*The response data*/
}
```




}

10.4 Instances

10.4.1 DescribeInstances

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

Request parameters

Name	Type	Required	Description
InstanceIds	String	No	<p>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"].</p> <div>  Note: If this parameter is specified, Ip or Remark is not needed. </div>
Ip	String	No	<p>The IP addresses of Anti-DDoS Pro instances. Exact match is supported.</p> <div>  Note: If this parameter is specified, InstanceIds or Remark is not needed. </div>
Remark	String	No	<p>The remarks on the Anti-DDoS Pro instances. Fuzzy match is supported.</p> <div>  Note: If this parameter is specified, InstanceIds or Ip is not needed. </div>
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 10-1: 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. <ul style="list-style-type: none">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

```
{
  "InstanceIds": "[\"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc\", \"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc\"]",
  "PageNo": 1,
  "PageSize": 1
}
```

Sample responses

```
{
  "Total": 1,
  "Instances": [
    {
      "InstanceId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
      "Remark": "xxx",
      "Status": 1,
      "ExpireTime": 20384032,
      "GmtCreate": 2308402384
    }
  ]
}
```

```
    ],  
    "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"  
}
```

10.4.2 DescribeInstanceDetails

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

Request parameters

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

Response parameters

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

Table 10-2: 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.
EipInfoList	EipInfo	The list of EIPs that are associated with the instance. For more information, see EipInfo .

Table 10-3: EipInfo

Name	Type	Description
Eip	String	The elastic IP address.
Status	String	The status of the EIP. Valid values: <ul style="list-style-type: none">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

```
{
  "InstanceIds": "[\"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc\", \"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc\"]"
}
```

Sample responses

```
{
  "InstanceDetails": [
    {
      "InstanceId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
      "Line": "coop-line-001",
      "EipInfoList": [
        {
          "Eip": "1.1.1.1",
          "Status": "normal"
        }
      ]
    }
  ],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.4.3 DescribeInstanceSpecs

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

Request parameters

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

Response parameters

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

Table 10-4: InstanceSpec

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

Name	Type	Description
BaseBandwidth	Integer	The basic bandwidth of the instance.
ElasticBandwidth	Integer	The burstable bandwidth of the instance.
PortLimit	Integer	The limit on the number of layer 4 forwarding rules on the instance.
DomainLimit	Integer	The limit on the number of layer 7 forwarding rules on the instance.
BandwidthMbps	Integer	The service bandwidth of the instance.

Examples

Sample requests

```
{
  "InstanceIds": "[\"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc\", \"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc\"]"
}
```

Sample responses

```
{
  "InstanceSpecs": [
    {
      "InstanceId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
      "BaseBandwidth": 20,
      "ElasticBandwidth": 10,
      "PortLimit": 10,
      "DomainLimit": 20,
      "BandwidthMbps": 100
    }
  ],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.4.4 DescribeInstanceStatistics

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

Request parameters

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

Response parameters

Name	Type	Description
InstanceStatistics	InstanceStatistic	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 10-5: 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

```
{
  "InstanceIds": "[\"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc\", \"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc\"]"
}
```

Sample responses

```
{
  "InstanceStatistics": [
    {
      "InstanceId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
      "PortUsage": 20,
      "DomainUsage": 10
    }
  ],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

```
}
```

10.4.5 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.
ElasticBandwidthSpec	Integer array	The burstable bandwidth of the instance.

Examples

Sample requests

```
{
  "InstanceId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

Sample responses

```
{
  "ElasticBandwidthSpec": [5,10,20,30],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

```
}
```

10.4.6 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.
ElasticBandwidth	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-d89d6717dxbc",
  "ElasticBandwidth": 50
}
```

Sample responses

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.4.7 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.

Name	Type	Required	Description
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-d89d6717dxbc",
  "Remark": "huadong2"
}
```

Sample responses

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.5 Layer 4 rules

10.5.1 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 10-6: 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.
FrontendPort	Integer	Yes	The port for front-end (client to Anti-DDoS Pro) connections. Valid values: 0-65535.

Name	Type	Required	Description
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-d89d6717dxbc\", \"Protocol\":\"tcp\", \"FrontendPort\":80, \"BackendPort\":5, \"RealServers\":[\"1.1.1.1\", \"2.2.2.2\"]}]"
}
```

Sample responses

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.5.2 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 10-7: 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.

Name	Type	Required	Description
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-d89d6717dxbc\",\"Protocol\":\"tcp\",\"FrontendPort\":80,\"BackendPort\":5,\"RealServers\":[\"1.1.1.1\",\"2.2.2.2\"]}]"
}
```

Sample responses

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.5.3 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 10-8: 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.
FrontendPort	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-d89d6717dxbc\",\"Protocol\":\"tcp\",\"FrontendPort\":80}]"
}
```

Sample responses

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.5.4 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.

Name	Type	Required	Description
Config	String	Yes	The configuration information. You may specify a <code>TcpConfig</code> or <code>UdpConfig</code> object represented as a JSON string. For more information, see TcpConfig and UdpConfig .

Table 10-9: 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 .
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 10-10: UdpConfig

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 .
Slimit	Slimit	Yes	The connection limit on source IPs. For more information, see Slimit .

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

Table 10-11: 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: <ul style="list-style-type: none"> 0: Disabled 1 (Default): Enabled
MaxconnEnable	Integer	No	Indicates whether Maxconnection is enabled. Valid values: <ul style="list-style-type: none"> 0: Disabled 1 (Default): Enabled

Table 10-12: 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: <ul style="list-style-type: none"> 0: Disabled 1 (Default): Enabled

Name	Type	Required	Description
MaxconnEnable	Integer	No	Indicates whether Maxconnection is enabled. Valid values: <ul style="list-style-type: none"> 0: Disabled 1 (Default): Enabled

Table 10-13: 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-d89d6717dxbc",
  "ForwardProtocol": "tcp",
  "FrontendPort": 80,
  "Config": "{\"PersistenceTimeout\":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-d89d6717dxbc"
}
```

10.5.5 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.

Name	Type	Required	Description
ForwardProtocol	String	Yes	The forwarding protocol. Valid values: <ul style="list-style-type: none"> TCP (Layer 4) UDP (Layer 4) HTTP (Layer 7)
FrontendPort	Integer	Yes	The port for front-end connections.
HealthCheck	String	Yes	The HealthCheck objects represented as a JSON string. For more information, see HealthCheck .

Table 10-14: HealthCheck

Name	Type	Required	Description
Type	String	Yes	The listener protocol. Valid values: <ul style="list-style-type: none"> TCP: Layer 4 HTTP: Layer 7
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-d89d6717dxbc",
  "ForwardProtocol": "tcp",
  "FrontendPort": 80,
  "HealthCheck": "{\"Type\":\"tcp\",\"Timeout\":10,\"Port\":80,\"Interval\":10,\"Up\":10,\"Down\":40}"
}
```


Sample responses

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.5.6 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. <div>  Note: If not specified, all result records are returned. </div>
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.

Name	Type	Description
Listeners	Listener []	The array of listeners. For more information, see Listener .
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Table 10-15: 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.
BackendPort	Integer	The port for back-end (Anti-DDoS Pro to origin server) connections. Valid values: 0-65535.
RealServers	JSON array	The IP addresses of the origin servers.
IsAutoCreate	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-d89d6717dxbc",
  "ForwardProtocol": "tcp",
  "FrontendPort": 80,
  "Offset": 1,
  "PageSize": 10
}
```

Sample responses

```
{
  "Total": 1,
  "Listeners": [
    {
      "InstanceId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
      "Protocol": "tcp",
      "FrontendPort": 80,
      "BackendPort": 80,
      "RealServers": [
        "1.1.1.1",
        "2.2.2.2"
      ],
      "IsAutoCreate": true
    }
  ]
}
```

```
    ],  
    "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"  
}
```

10.5.7 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 10-16: 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 10-17: 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 10-18: 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 10-19: 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: <ul style="list-style-type: none"> 0: Disabled 1 (Default): Enabled
MaxconnEnable	Integer	Indicates whether Maxconnection is enabled. Valid values: <ul style="list-style-type: none"> 0: Disabled 1 (Default): Enabled

Table 10-20: 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: <ul style="list-style-type: none"> 0: Disabled 1 (Default): Enabled
MaxconnEnable	Integer	Indicates whether Maxconnection is enabled. Valid values: <ul style="list-style-type: none"> 0: Disabled 1 (Default): Enabled

Table 10-21: 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\", \"FrontendPort\":80}]"
```

```
}
```

Sample responses

```
{
  "Total": 1,
  "Listeners": [
    {
      "InstanceId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
      "Protocol": "tcp",
      "FrontendPort": 80,
      "Config": {
        "PersistenceTimeout": 80,
        "Synproxy": "off",
        "NodataConn": "on",
        "Sla": {
          "Cps": 10,
          "Maxconn": 10,
          "CpsEnable": 1,
          "MaxconnEnable": 1
        },
        "Slimit": {
          "Cps": 10,
          "Maxconn": 10,
          "CpsEnable": 1,
          "MaxconnEnable": 1
        },
        "PayloadLen": {
          "Min": 1,
          "Max": 2
        }
      }
    }
  ],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.5.8 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 10-22: 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 10-23: HealthCheck

Name	Type	Description
Type	String	The protocol type. Valid values: <ul style="list-style-type: none"> 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-d89d6717dxbc\", \"Protocol\":\"tcp\", \"FrontendPort\":80}]"
}
```

Sample responses

```
{
  "Total": 1,
  "HealthCheck": [
    {
      "InstanceId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
      "Protocol": "tcp",
      "FrontendPort": 80,
      "HealthCheck": {
        "Type": "tcp",
        "Timeout": 10,
        "Port": 80,
        "Interval": 10,
        "Up": 10,
        "Down": 20
      }
    }
  ],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.5.9 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 10-24: Listener

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

Name	Type	Required	Description
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 10-25: 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 10-26: 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-d89d6717dxbc\",\"Protocol\":\"tcp\",\"FrontendPort\":80}]"
}
```

Sample responses

```
{
  "HealthCheckStatusList": [
    {
      "InstanceId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
      "Protocol": "tcp",
      "FrontendPort": 80,
      "Status": "normal",
      "RealServerStatusList": [
        {
          "Status": "normal",
          "Address": "1.1.1.1"
        }
      ]
    }
  ],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.6 Layer 7 rules

10.6.1 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.
QueryDomainPattern	String	No	The query mode. Valid values: <ul style="list-style-type: none">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 10-27: Domain

Name	Type	Description
Domain	String	The domain name.
ProxyTypes	[] String	The array of forwarding protocols. Valid values: <ul style="list-style-type: none"> • 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.
BlackList	[] String	The array of IP addresses in the blacklist.
CertName	String	The name of the certificate.
RealSevers	[] Layer7RealServer	The array of origin servers. For more information, see Layer7RealServer .

Table 10-28: Layer7RealServer

Name	Type	Description
RealServer	String	The address of the origin server.

Name	Type	Description
RsType	Integer	The address type. Valid values: <ul style="list-style-type: none">• 0: IP address.• 1: Domain name.

Examples

Sample requests

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

Sample responses

```
{
  "Total": 2,
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "Domains": [
    {
      "Domain": "www.alibaba.com",
      "ProxyTypes": ["https", "http"],
      "RealServers": [{
        "RealServer": "1.1.1.1",
        "RsType": 0
      }, {
        "RealServer": "1.1.1.1",
        "RsType": 1
      }
    ],
    "CcEnabled" : false,
    "CcRuleEnabled" : 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_alibaba_com.pem"
  }, {
    "Domain": "www.alibaba.com",
    "ProxyTypes": ["https", "http"],
    "RealServers": [{
      "RealServer": "1.1.1.1",
      "RsType": 0
    }, {
      "RealServer": "1.1.1.2",
      "RsType": 1
    }
  ],
    "CcEnabled" : false,
    "CcRuleEnabled" : 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_alibaba_com.pem"
  }
]
```

```
]
}
```

10.6.2 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: <ul style="list-style-type: none"> 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, .. <div>  Note: If this parameter is not specified, the domain name is not associated with any Anti-DDoS Pro instance. </div>
Rules	String	Yes	The array of layer 7 rules represented as a JSON string. For more information, see Layer7Rule .

Table 10-29: Layer7Rule

Name	Type	Description
ProxyRules	[] ProxyRule	The array of rule objects. For more information, see ProxyRule .
ProxyType	String	The forwarding protocol. Valid values: <ul style="list-style-type: none"> http https websocket websockets

Table 10-30: 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,
  "InstanceIds. 1": "xxxx",
  "Rules": "[{\"ProxyRules\":{\"ProxyPort\":\"443\",\"RealServers\":[\"1.1.1.1:443\"]},\"ProxyType\":\"https\"},{\"ProxyRules\":{\"ProxyPort\":\"80\",\"RealServers\":[\"1.1.1.1:80\"]},\"ProxyType\":\"http\"}]"
```

Sample responses


```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.6.3 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: <ul style="list-style-type: none">0: IP address.1: Domain name.

Name	Type	Required	Description
InstanceIds.N	String	No	<p>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, ...</p> <div>  Note: If this parameter is not specified, the domain name is not associated with any Anti-DDoS Pro instance. </div>
RealServers.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,
  "RealServers. 1": "1.1.1.1",
  "InstanceIds. 1": "xxxx",
  "ProxyTypes. 1" : "http"
}
```

Sample responses

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
```

```
}
```

10.6.4 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-d89d6717dxbc"
}
```

10.6.5 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.

Name	Type	Required	Description
CertName	String	No	<p>The name of the certificate.</p> <div>  Note: If this parameter is specified, you must also specify Cert and Key. If CertName, Cert, and Key are specified, CertId is not needed. </div>
Cert	String	No	<p>The public key of the certificate.</p> <div>  Note: If this parameter is specified, you must also specify CertName and Key. If CertName, Cert, and Key are specified, CertId is not needed. </div>
Key	String	No	<p>The private key of the certificate.</p> <div>  Note: If this parameter is specified, you must also specify CertName and Cert. If CertName, Cert, and Key are specified, CertId is not needed. </div>

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-d89d6717dxbc"
```



```
}
```

10.6.6 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-d89d6717dxbc"
}
```

```
}
```

10.6.7 DescribeLayer7InstanceRelations

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.
Layer7InstanceRelation	[] Layer7InstanceRelation	The array of domain names and associated Anti-DDoS Pro instances. For more information, see Layer7InstanceRelation .

Table 10-31: Layer7InstanceRelation

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

Table 10-32: 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

```
{
  "Layer7InstanceRelations": [
    {
      "Domain": "1.aliyun.com",
      "InstanceDetails": [
        {
          "EipList": [
            "203.x.x.0",
            "203.x.x.1"
          ],
          "InstanceId": "xxxxxx"
        },
        {
          "EipList": [
            "203.x.x.0",
            "203.x.x.1"
          ],
          "InstanceId": "xxxxxx"
        }
      ]
    }
  ]
}
```

10.6.8 DescribeCertList

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 .

Table 10-33: 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"
    }
  ]
}
```

10.6.9 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-d89d6717dxbc"
}
```

10.6.10 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-d89d6717dxbc"
}
```

10.6.11 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-d89d6717dxbc"
}
```

10.6.12 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-d89d6717dxbc"
}
```

```
}
```

10.6.13 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. <ul style="list-style-type: none">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. <ul style="list-style-type: none">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-d89d6717dxbc"
}
```

10.6.14 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. <ul style="list-style-type: none">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.

Name	Type	Required	Description
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. <ul style="list-style-type: none">• 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-d89d6717dxbc"
}
```

}

10.6.15 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. <div>  Note: If not specified, all result records are returned. </div>
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.
Layer7CCRules	[] Layer7CCRule	The array of HTTP flood protection rules. For more information, see Layer7CCRule .
Total	Integer	The total number of rules.

Table 10-34: 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. <ul style="list-style-type: none"> close: Block the request. captcha: Enable captcha verification.

Name	Type	Description
Count	Integer	The number of requests. This parameter is used together with the <code>Interval</code> parameter. The rule is triggered when the number of requests sent by an IP address reaches the <code>Count</code> limit during the <code>Interval</code> period.
Interval	Integer	The time interval. This parameter is used together with the <code>Count</code> parameter. The rule is triggered when the number of requests sent by an IP address reaches the <code>Count</code> limit during the <code>Interval</code> period.
Mode	String	The URI matching algorithm. <ul style="list-style-type: none"> <code>match</code>: Exact match. Requests are counted only when the request URI exactly matches the URI that is protected under the rule. <code>prefix</code>: 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-d89d6717dxbc",
  "Total": 10,
  "Layer7CCRules" : [
    {
      "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"
}
```

10.6.16 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-d89d6717dxbc"
}
```

10.6.17 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.

Name	Type	Required	Description
Template	String	Yes	The mode of HTTP flood protection that you want to use. Valid values: <ul style="list-style-type: none">• default: Normal• gf_under_attack: Emergency• gf_sos_verify: Strict• gf_sos_enhance: 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-d89d6717dxbc"
}
```

10.6.18 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.

Name	Type	Description
DomainModeList	[] Object	The list of modes that are used to set up Anti-DDoS Pro. For more information, see DomainModeList .

Table 10-35: 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: <ul style="list-style-type: none">• 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-d89d6717dxbc",
  "DomainModeList":[
    {
      "Domain":"www.alibaba.com",
      "AccessMode":1
    },
    {
      "Domain":"www.aliyun.com",
      "AccessMode":2
    }
  ]
}
```

```
}
```

10.6.19 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: <ul style="list-style-type: none">• 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-d89d6717dxbc",
}
```

```
}
```

10.6.20 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-d89d6717dxbc",
  "CidrList" : ["47.97.128.0/25", "47.97.128.128/25"]
}
```

10.7 Logs

10.7.1 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.

Name	Type	Required	Description
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 10-36: 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.
OpDesc	String	The details of the operation. For more information, see OpDesc .

Table 10-37: 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 10-38: 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,
      "entityObject": "1.1.1.1",
      "opAction": 2,
      "opDesc": {
        "oldValue": {
          "elasticBandwidth": 10
        },
        "newValue": {
          "elasticBandwidth": 30
        }
      },
      "opResult": 1
    }
  ]
}
```



```
}
```

10.8 Tasks

10.8.1 ListAsyncTask

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

Request parameters

Name	Type	Required	Description
TaskType	Integer	No	<p>The type of the task that you want to query. Valid values:</p> <ul style="list-style-type: none">• 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. <div> Note: If this parameter is not specified, all types of tasks are returned.</div>
TaskStatus	Integer	No	<p>The status of the task that you want to query. Valid values:</p> <ul style="list-style-type: none">• 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. <div> Note: If this parameter is not specified, tasks of all statuses are returned.</div>
PageNo	Integer	Yes	The number of the starting page that is displayed. Must be an integer no less than 1.

Name	Type	Required	Description
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 10-39: AsyncTask

Name	Type	Description
TaskId	Long	The ID of the task. You can delete tasks by ID.
TaskType	Integer	The type of the task. Valid values: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 10-40: TaskParam

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

Table 10-41: 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-d89d6717dxbc",
  "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"}
    }
  ]
}
```

```
}
```

10.8.2 CreateAsyncTask

You can call this operation to create asynchronous tasks.

Request parameters

Name	Type	Required	Description
TaskType	Integer	Yes	<p>The type of the task. Valid values:</p> <ul style="list-style-type: none">• 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	<p>The task parameter represented as a JSON string. The parameters vary depending on the task type.</p> <ul style="list-style-type: none">• 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-woieuroi234"}, Layer 7 task: {}, Session and health check task: {"instanceId": "xxxxxxxxxx"}, Anti-DDoS protection policy task: {"instanceId": "xxxxxxxxxx"}
}
```

Sample responses

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

10.8.3 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-d89d6717dxbc"
}
```

}

10.9 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.
InvalidInstanceIdSize	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.

Error code	Error message	Description
ddos_coop12020	illegal timestamp	The error message returned when the timestamp is invalid.
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.

Error code	Error message	Description
ddos_coop13104	eip is released	The error message returned when the specified IP address is released.
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.

Error code	Error message	Description
ddos_coop21005	no action found	The error message returned when the specified operation does not exist.
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.

11 Best Practices

11.1 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.

11.2 Create an Anti-DDoS Pro alert rule

This topic describes how to create Anti-DDoS Pro alert rules and add contact groups in the CloudMonitor console. Anti-DDoS Pro alert notifications provide you with up-to-date information about traffic and connection exceptions. You can troubleshoot errors and restore workloads as soon as possible.

Context

CloudMonitor is a service that monitors applications and Alibaba Cloud resources . It sends you notifications when alerts are triggered. You can customize alert rules

to specify how the alert system checks the monitoring data and when it sends alert notifications. After you set alert rules for important metrics, you are notified when exceptions are detected in these metrics. This enables you to manage exceptions quickly.

The alert feature provided by CloudMonitor is compatible with Anti-DDoS Pro. You can create and customize alert rules in the CloudMonitor console. CloudMonitor supports the following Anti-DDoS Pro metrics.

**Note:**

Anti-DDoS Pro back-to-origin traffic refers to the workload traffic that is scrubbed by Anti-DDoS Pro before it is forwarded to the origin server.

Table 11-1: Anti-DDoS Pro metrics

Metric	Dimension	Unit
Anti-DDoS Pro outbound traffic	Instance and IP address	bit/s
Anti-DDoS Pro inbound traffic	Instance and IP address	bit/s
Anti-DDoS Pro back-to-origin traffic	Instance and IP address	bit/s
Active connections	Instance and IP address	Count
Inactive connections	Instance and IP address	Count
New connections	Instance and IP address	Count

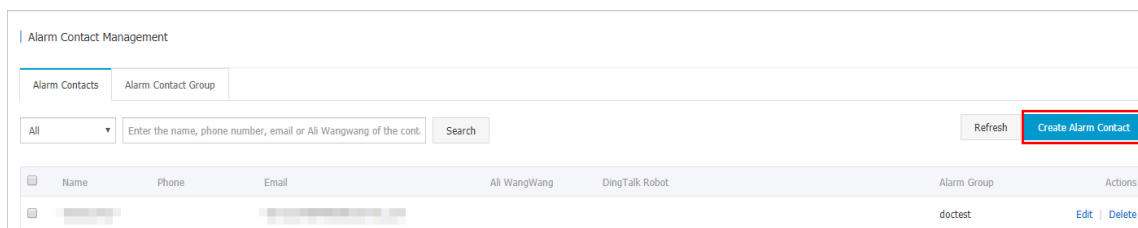
Procedure

1. Log on to the [CloudMonitor console](#).

2. Optional: Add an alert recipient. If you have already specified a recipient, you can skip this step.

a) In the left-side navigation pane, choose Alarms > Alarm Contacts.

b) On the Alarm Contacts tab, click Create Alarm Contact in the upper-right corner.



c) In the Set Alarm Contact dialog box that appears, enter the required contact information. Verify the Phone or Email ID, and then click Save.

The screenshot shows the 'Set Alarm Contact' dialog box. It has a close button (X) in the top right corner. The form contains the following fields and controls:

- Name:** A text input field containing 'doctest_mail'. Below it is a note: 'The name must be 2-40 characters, can include English letters, numbers, ., and underscores, and should start with a Chinese or English character.'
- Phone:** A text input field. To its right is a 'Send verification code.' button.
- Verification code:** A text input field. Below it is a note: 'Fill in the phone verification code.'
- Email ID:** A text input field containing a masked email address. To its right is a 'Send verification code.(48)' button.
- Verification code:** A text input field containing '064170'. Below it is a note: 'Fill in the E-mail verification code.'
- Ali WangWang:** A text input field.
- DingTalk Robot:** A text input field. Below it is a link: 'How to get the DingTalk robot address'.

At the bottom right of the dialog box are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted.

The alert recipient is saved.

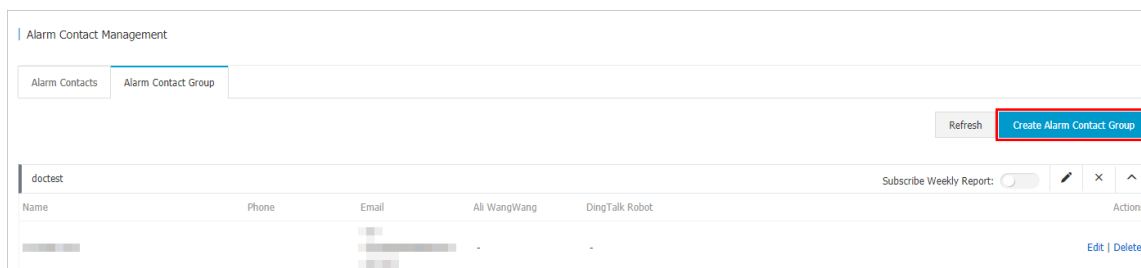
3. Optional: Create an alert contact group. If you have already created an alert contact group, you can skip this step.



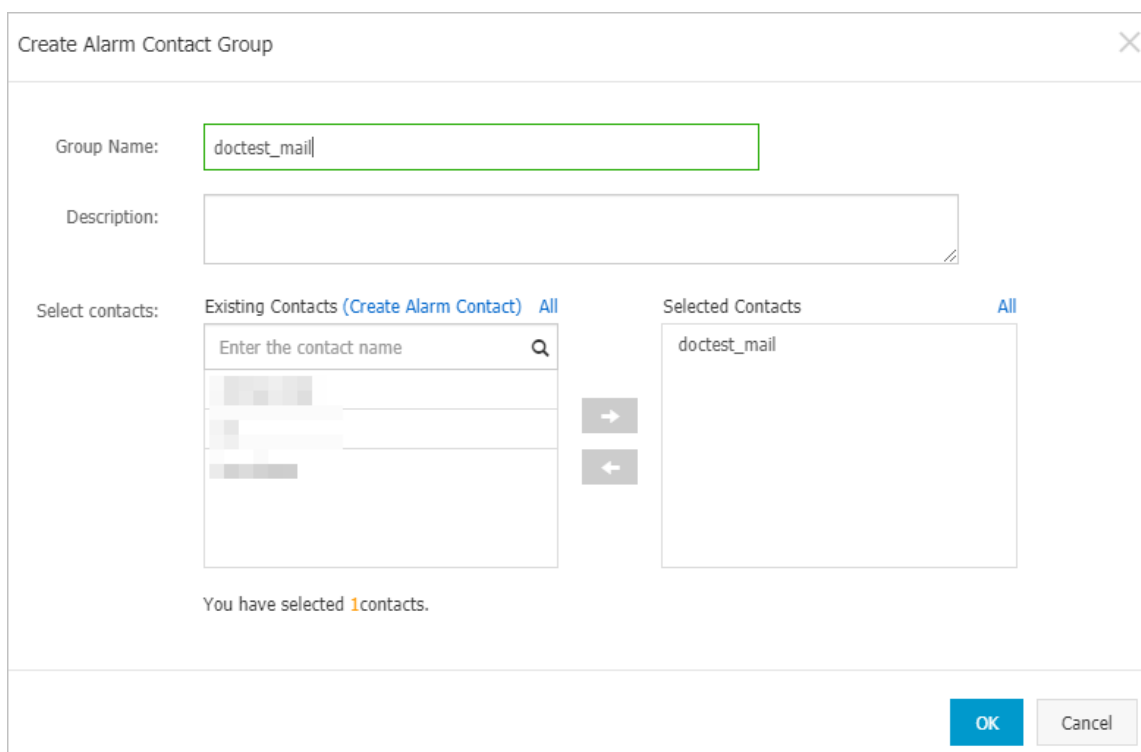
Note:

The recipients of alert notifications must be contact groups. You can add one or more recipients to a contact group.

- a) In the left-side navigation pane, choose **Alarms > Alarm Contacts**.
- b) On the Alarm Contact Group tab, click **Create Alarm Contact Group** in the upper-right corner.



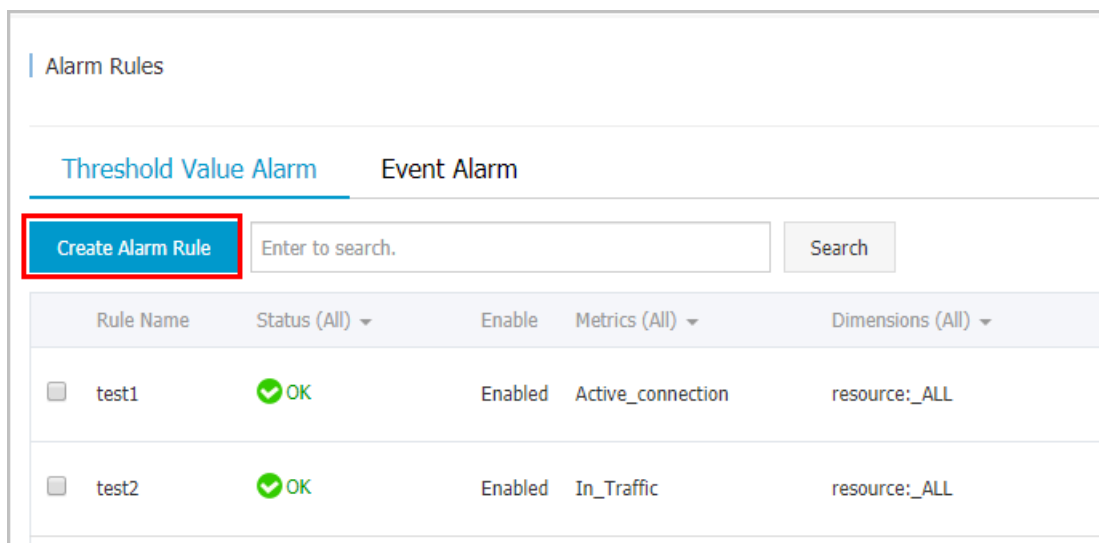
- c) In the Create Alarm Contact Group dialog box that appears, enter a group name in the Group Name field. Select recipients from the left-side Existing Contacts list and add them to the right-side Selected Contacts list. Click OK.



The contact group is created.


4. Create an alert rule


- a) In the left-side navigation pane, choose **Alarms > Alarm Rules**.
- b) On the **Threshold Value Alarm** tab, click **Create Alarm Rule**.



- c) On the **Create Alarm Rule** page, set the parameters and click **Confirm**. The following table lists the parameters and descriptions.

Category	Parameter	Description
Related Resource	Product	Select NewBGPDDoS.
	Resource Range	<p>The resources to which the alert rule is applied. You can select All Resources or Instances.</p> <ul style="list-style-type: none">• All Resources: The alert rule is applied to all Anti-DDoS Pro instances. An alert is triggered when any of the Anti-DDoS Pro instances matches the specified rule.• Instances: The alert rule is applied to selected Anti-DDoS Pro instances. An alert is triggered when one of the selected instances matches the specified rule.

Category	Parameter	Description
Set Alert Rules	Alarm Rule	Specify a name for the alert rule.
	Rule Description	<p>Set the conditions that are used to control how the alert rule is triggered.</p> <div>  Note: We recommend that you set the threshold of metrics based on your actual business requirements. For more information, see Table 11-1: Anti-DDoS Pro metrics. A low threshold may frequently trigger alerts and negatively impact user experience. A high threshold may leave insufficient time for you to manage attacks. </div> <p>Default condition: An Anti-DDoS Pro metric generates a data point every 60 seconds. In the following examples, the Anti-DDoS Pro metrics generate five data points every five-minute detection period.</p> <ul style="list-style-type: none"> • Sample rule description: New connection, 5 minute cycle, 3 periods, once, and > 200 . In this rule, the detection period is set to five minutes. CloudMonitor checks the data points (number of new connections) generated within three detection periods in a row, which are 15 data points in total . If any data point shows that the number of new connections has exceeded 200, an alert is triggered. • Sample rule description: Out traffic, 5 minute cycle, 3 periods, and ≥ 50 Mbit/s . In this rule, the detection period is set to five minutes. CloudMonitor checks the data points (outbound data transfer rate) generated within three detection periods in a row, which are 15 data points in total. If any data point shows that the outbound data transfer rate has exceeded 50 Mbit/s, an alert is triggered.

Category	Parameter	Description
	Mute for	Set a mute period. If the alert is not cleared within the mute period, a new alert notification is sent when the mute period ends. The minimum value is 5 minutes and the maximum value is 24 hours.
	Effective Period	The time period during which the alert rule remains effective. The system only sends alerts within the effective period. The system records alerts if they occur during a non-effective period.
Notification Method	Notification Contact	The contact group that receives alerts.
	Notification Methods	<p>Alert levels include critical, warning, and info. Different levels of alerts are sent by using different methods.</p> <ul style="list-style-type: none"> • Phone + Text Message + Email + DingTalk (Critical) <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">  Note: You can select this notification method only after you purchase a notification plan that supports phone calls. </div> <ul style="list-style-type: none"> • Test Message + Email + DingTalk (Warning) • Email + DingTalk (Info)
	Auto Scaling	After you specify a scaling rule, the specified scaling rule is triggered when an alert occurs. In this example, do not set this parameter.
	Email Remark	Optional. You can add remarks to email notifications. Remarks is included in email notifications.

Category	Parameter	Description
	HTTP Callback	CloudMonitor uses a POST request to push an alert to the specified public URL address. Currently, only HTTP requests are supported.

Create Alarm Rule [← Back to](#)

1

Related Resource

Product: NewBGPDDoS

Resource Range: instance

instance: ddoscoo-cn-001

2

Set Alarm Rules

Alarm Rule: Example-1

Rule Description: New_connection 5Minute cycle Continue for 3 Once >= 200 count

Alarm Rule: Example-2 [Delete](#)

Rule Description: Out_Traffic 5Minute cycle Continue for 3 Once >= 50 Mbit/s

[+Add Alarm Rule](#)

Mute for: 24 h

Effective Period: 00:00 To: 23:59

Out_Traffic-Maximum-ddoscoo-cn-4591euwia001

Warning Line (Value: 52428800)

3

Notification Method

Notification Contact: doctest

Contact Group All

Search Q

[Quickly create a contact group](#)

Selected Groups 1 count All

doctest

Notification Methods:

☐ Phone + Text Message + Email + DingTalk (Critical)

☒ Text Message + Email + DingTalk (Warning)

☐ Email + DingTalk (Info)

☐ Auto Scaling (the corresponding scaling rule will be triggered when the alarm occurs)

Email Subject: The default format of email theme is Product Name + Metric Name + Instance ID.

Email Remark: Optional

HTTP CallBack: for example: http://alert.aliyun.com:8080/callback

Confirm

Cancel

206

Issue: 20200102

The Anti-DDoS Pro alert rule is created. When the Anti-DDoS Pro metric fits the alert rule description, an alert is sent to the specified contact group.

11.3 Monitor black hole events and traffic scrubbing events on Anti-DDoS Pro

This topic describes how to create rules to alert on black hole events and scrubbing events on Anti-DDoS Pro in the CloudMonitor console. The alerts can keep you informed of the latest black hole events and scrubbing events and allow you to troubleshoot errors and restore workloads as early as possible.

Context

CloudMonitor is a service to monitor applications and Alibaba Cloud resources . The event monitoring feature of CloudMonitor provides you with a centralized platform to query and summarize the system events on cloud services. This allows you to track the use of cloud resources.

You can query the black hole events and scrubbing events on Anti-DDoS Pro and create alert rules based on the event level. You can receive notifications or configure alert callbacks through text messages, emails, or DingTalk. CloudMonitor notifies you of critical events at the earliest opportunity. This allows you to handle the events in time. For more information, see [An overview of event monitoring](#).

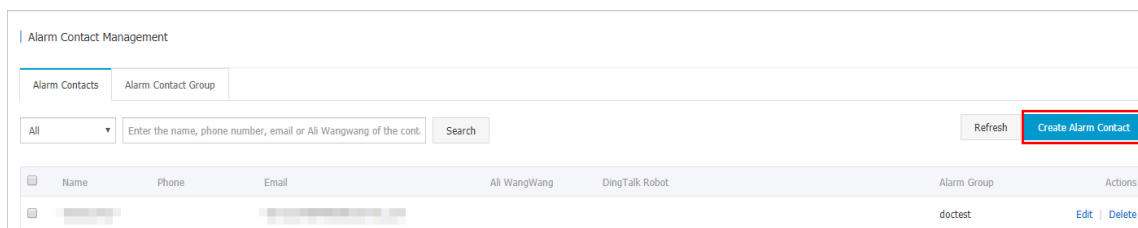
Procedure

- 1. Log on to the [CloudMonitor console](#).**

2. Optional: Add an alert recipient. If you have already specified a recipient, you can skip this step.

a) In the left-side navigation pane, choose Alarms > Alarm Contacts.

b) On the Alarm Contacts tab, click Create Alarm Contact in the upper-right corner.



c) In the Set Alarm Contact dialog box that appears, enter the required contact information. Verify the Phone or Email ID, and then click Save.

The screenshot shows the 'Set Alarm Contact' dialog box. It has a title bar with a close button. The form contains the following fields and controls:

- Name:** A text input field containing 'doctest_mail'. Below it is a note: 'The name must be 2-40 characters, can include English letters, numbers, ., and underscores, and should start with a Chinese or English character.'
- Phone:** A text input field. To its right is a 'Send verification code.' button.
- Verification code:** A text input field. Below it is a note: 'Fill in the phone verification code.'
- Email ID:** A text input field containing a masked email address. To its right is a 'Send verification code.(48)' button.
- Verification code:** A text input field containing '064170'. Below it is a note: 'Fill in the E-mail verification code.'
- Ali WangWang:** A text input field.
- DingTalk Robot:** A text input field. Below it is a link: 'How to get the DingTalk robot address'.

At the bottom right of the dialog box are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted with a blue background.

The alert recipient is saved.

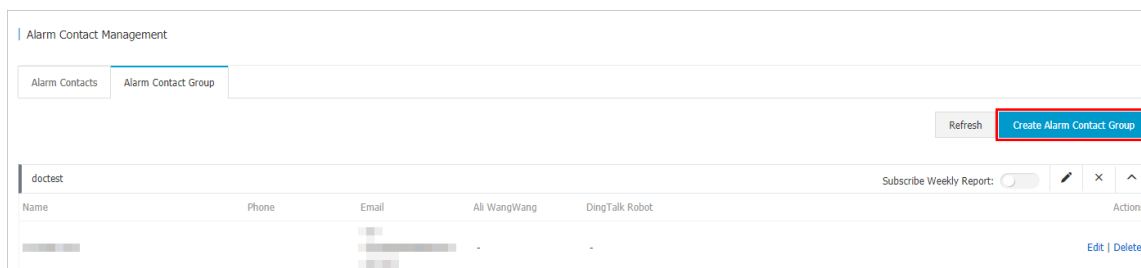
3. Optional: Create an alert contact group. If you have already created an alert contact group, you can skip this step.



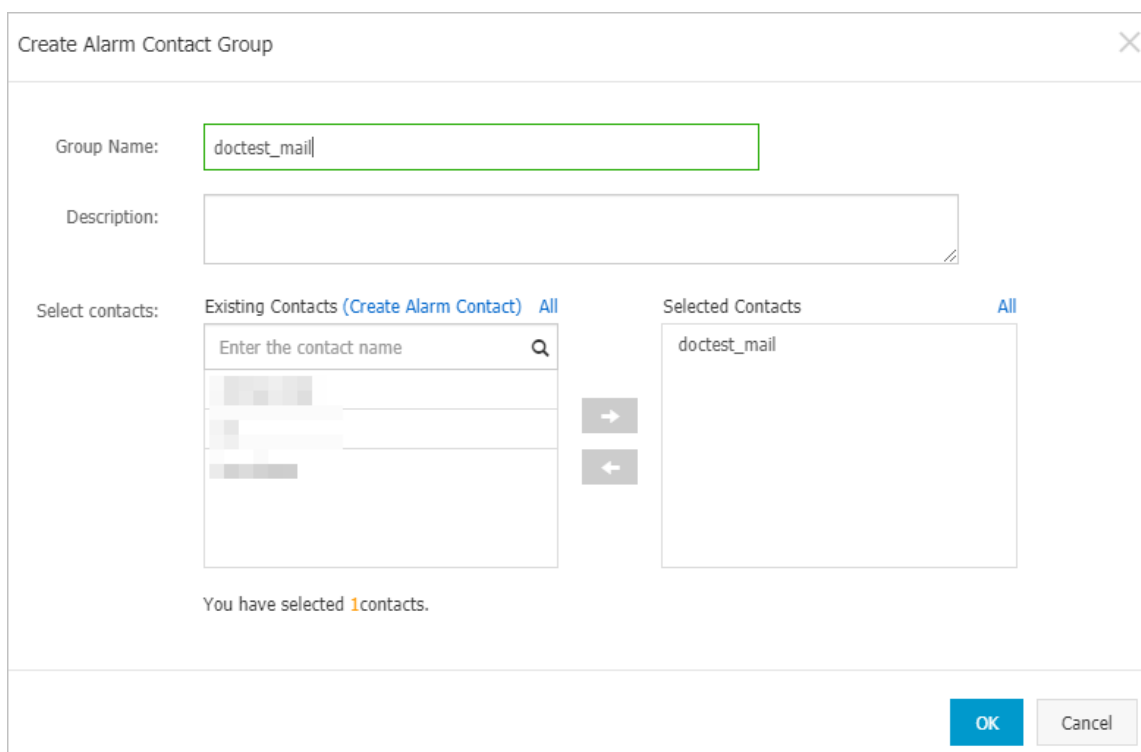
Note:

The recipients of alert notifications must be contact groups. You can add one or more recipients to a contact group.

- a) In the left-side navigation pane, choose **Alarms > Alarm Contacts**.
- b) On the Alarm Contact Group tab, click **Create Alarm Contact Group** in the upper-right corner.



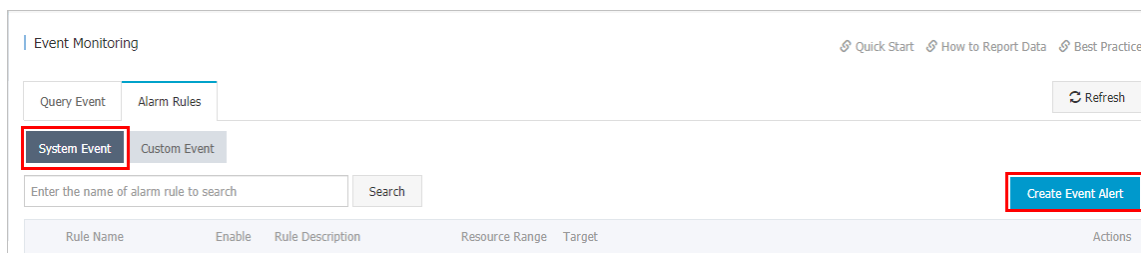
- c) In the Create Alarm Contact Group dialog box that appears, enter a group name in the Group Name field. Select recipients from the left-side Existing Contacts list and add them to the right-side Selected Contacts list. Click OK.



The contact group is created.

4. Create an event alert rule for a cloud service.

- a) In the left-side navigation pane, click Event Monitoring.
- b) On the Alarm Rules tab, select System Event, and click Create Event Alert.



- c) In the Create/Modify Event Alert pane, configure the alert rule, and click OK.
The parameters are described as follows.

Module	Parameter	Description
Basic Information	Alarm Rule Name	Enter the name of the alert rule.
Event alert	Event Type	Select System Event.
	Product Type	Select NewBGPDDoS.
	Event Type	Select the type of the events to alert on. Valid values include Black hole and Traffic scrubbing. You can select multiple event types.
	Event Level	Select the level of events to alert on. Valid values include CRITICAL, WARN, and INFO. You can select multiple levels and must select CRITICAL.
	Event Name	Select one or more events to alert on. <ul style="list-style-type: none"> Black hole events include In black hole and Black hole ended. All black hole events are critical. Traffic scrubbing events include Scrubbing and Scrubbing ended. All scrubbing events are critical.
	Resource Range	Select All Resources.

Module	Parameter	Description
Alarm Type	Alert Notification	Select Alert Notification. Select a Contact Group and a Notification Method. <ul style="list-style-type: none">• Contact Group: Select an existing contact group.• Notification Method: Select Warning (Message+Email ID+DingTalk Robot) or Info (Email ID+DingTalk Robot). You can click Add to add more contact groups and notification methods.
	MNS queue	This option is not required.
	Function service	This option is not required.
	URL callback	This option is not required.

Module	Parameter	Description
	Log Service	This option is not required.

Create / Modify Event Alert

Basic Information

Alarm Rule Name

anti_ddos_event

Event alert

Event Type

☒ System Event

☐ Custom Event

Product Type

NewBGPDDoS

Event Type

All types ✕

Event Level

CRITICAL ✕

WARN ✕

INFO ✕

Event Name

ddoscoo_event_blackhole_add ✕

Resource Range

☒ All Resources

☐ Application Groups

Alarm Type

☒ Alarm Notification

Contact Group

doctest

Delete

Notification Method

Warning (Message+Email ID+DingTalk Robot)

+Add

☐ MNS queue

☐ Function service (Best Practices)

☐ URL callback

OK

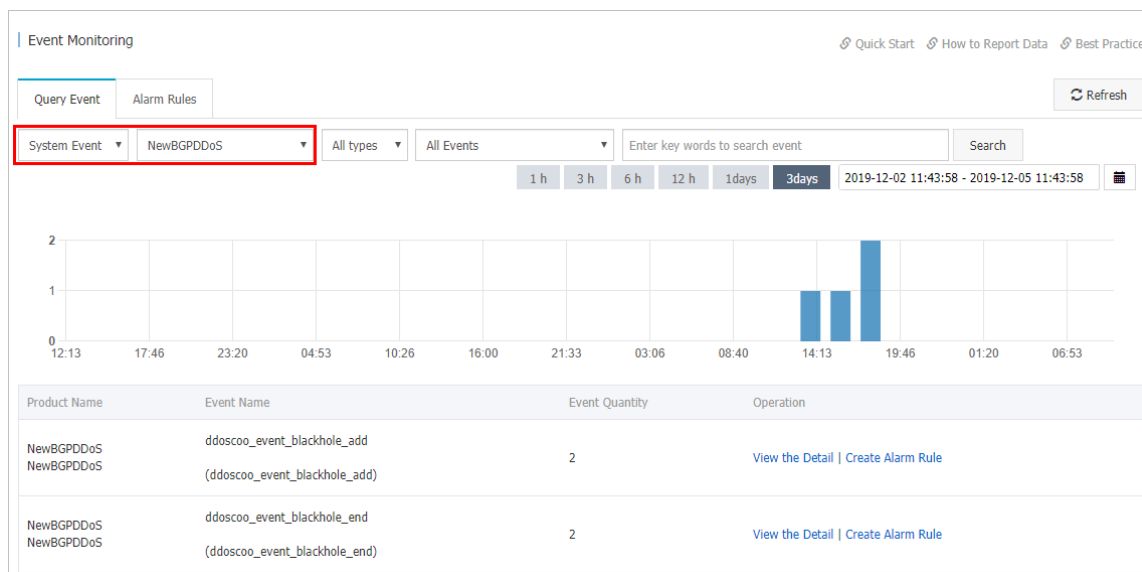
Cancel

The alert rule is created. When a black hole event or traffic scrubbing event occurs on Anti-DDoS Pro, the specified contact group receives an alert.

5. Optional: Query events. You can query the recent black hole events and scrubbing events on Anti-DDoS Pro in the CloudMonitor console.

a) On the Event Monitoring page, click the Query Event tab.

b) Select System Event and NewBGPDDoS, and specify the event type and time period.



c) In the event list, click View Details to view the details of an event.

Time	Product Name	Event Name	Event Level	Status	Region	Resource	Contents	Close Detail
19-12-04 18:30:26	NewBGPDDoS	ddoscoo_event_blackhole_add (ddoscoo_event_blackhole_add)	CRITICAL	blackhole_begin	China East 1 (Hangzhou)	acs:yundun-ddoscoo:cn-hangzhou:1289654106023090:instance/ddoscoo-cn-	<pre>{ "event_time": "2019-12-04 18:30:24", "event_type": "blackhole", "instanceId": "ddoscoo-cn-0pp1eive006", "ip": "203.104", "status": "blackhole_begin", "user_id": "1289654106023090" }</pre>	
19-12-04 15:54:25	NewBGPDDoS	ddoscoo_event_blackhole_add (ddoscoo_event_blackhole_add)	CRITICAL	blackhole_begin	China East 1 (Hangzhou)	acs:yundun-ddoscoo:cn-hangzhou:1289654106023090:instance/ddoscoo-cn-	<pre>{ "event_time": "2019-12-04 15:54:22", "event_type": "blackhole", "instanceId": "ddoscoo-cn-0pp1eive006", "ip": "203.104", "status": "blackhole_begin", "user_id": "1289654106023090" }</pre>	

11.4 Create an Anti-DDoS Pro dashboard

This topic describes how to create a custom Anti-DDoS Pro dashboard and add charts to the dashboard in the CloudMonitor console. Custom Anti-DDoS Pro dashboards and charts help you monitor your workloads.

Context

CloudMonitor is a service that monitors applications and Alibaba Cloud resources . CloudMonitor supports custom dashboards that display monitoring data. On a dashboard, you can view the monitoring data of multiple services and instances . This allows you to monitor the states of different instances that run the same workloads.

The dashboard feature provided by CloudMonitor is compatible with Anti-DDoS Pro. You can create and customize Anti-DDoS Pro dashboards in the CloudMonitor console. CloudMonitor supports the following Anti-DDoS Pro monitor metrics.

**Note:**

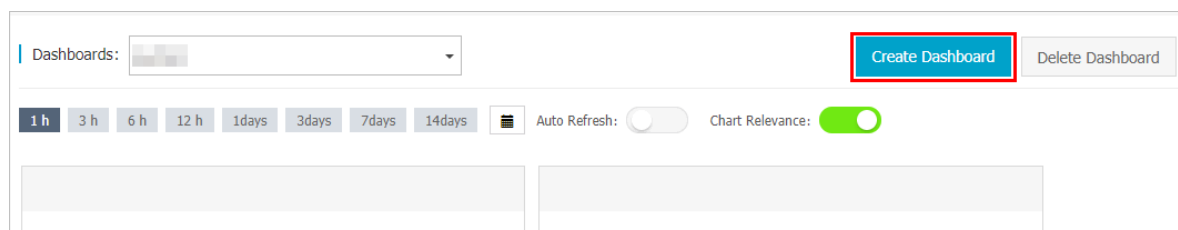
Anti-DDoS Pro back-to-origin traffic refers to the workload traffic that is scrubbed by Anti-DDoS Pro before it is forwarded to the origin server.

Table 11-2: Anti-DDoS Pro metrics

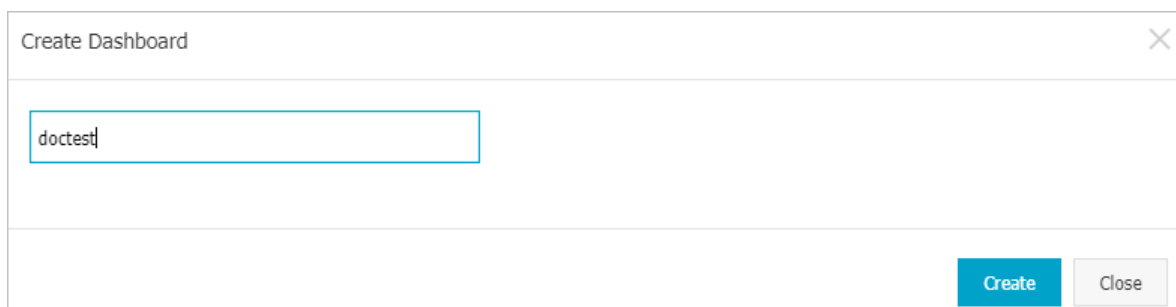
Metric	Dimension	Unit
Anti-DDoS Pro outbound traffic	Instance and IP address	bit/s
Anti-DDoS Pro inbound traffic	Instance and IP address	bit/s
Anti-DDoS Pro back-to-origin traffic	Instance and IP address	bit/s
Active connections	Instance and IP address	Count
Inactive connections	Instance and IP address	Count
New connections	Instance and IP address	Count

Procedure

1. Log on to the [CloudMonitor console](#).
2. Choose Dashboard > Custom Dashboard, and then click Create Dashboard.



3. In the Create Dashboard dialog box that appears, specify a name for the dashboard, and then click Create.

A screenshot of a 'Create Dashboard' dialog box. The dialog has a title bar with the text 'Create Dashboard' and a close button (X) in the top right corner. Below the title bar is a large text input field containing the text 'doctest'. At the bottom right of the dialog, there are two buttons: a blue 'Create' button and a grey 'Close' button.

Create Dashboard

doctest

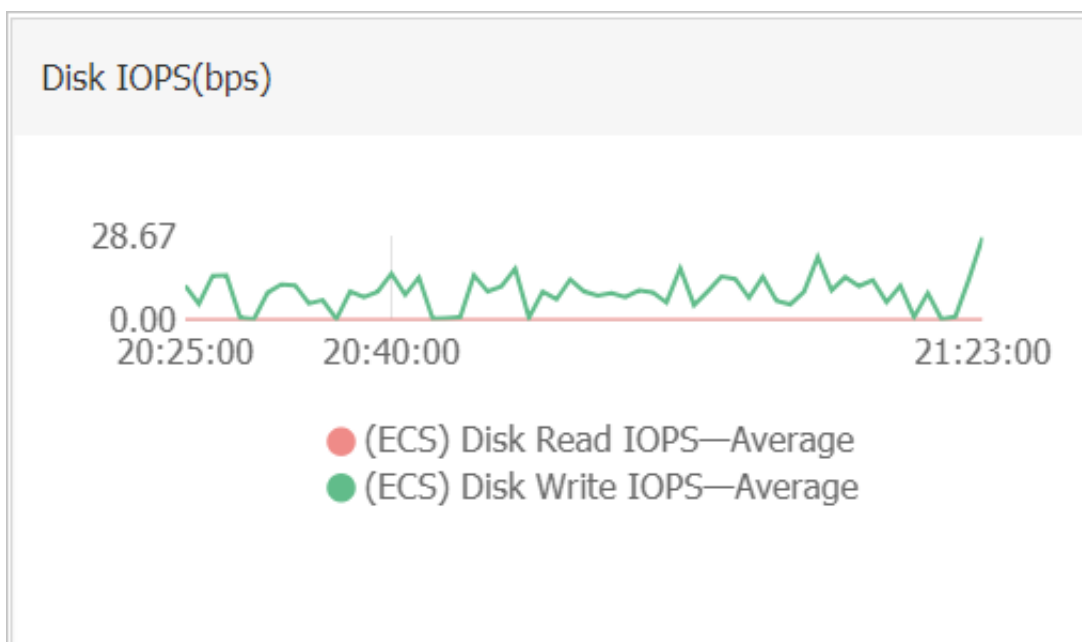
Create Close

After the dashboard is created, you are redirected to the Dashboards page. You can select a dashboard from the Dashboards drop-down list to view or manage the selected dashboard.

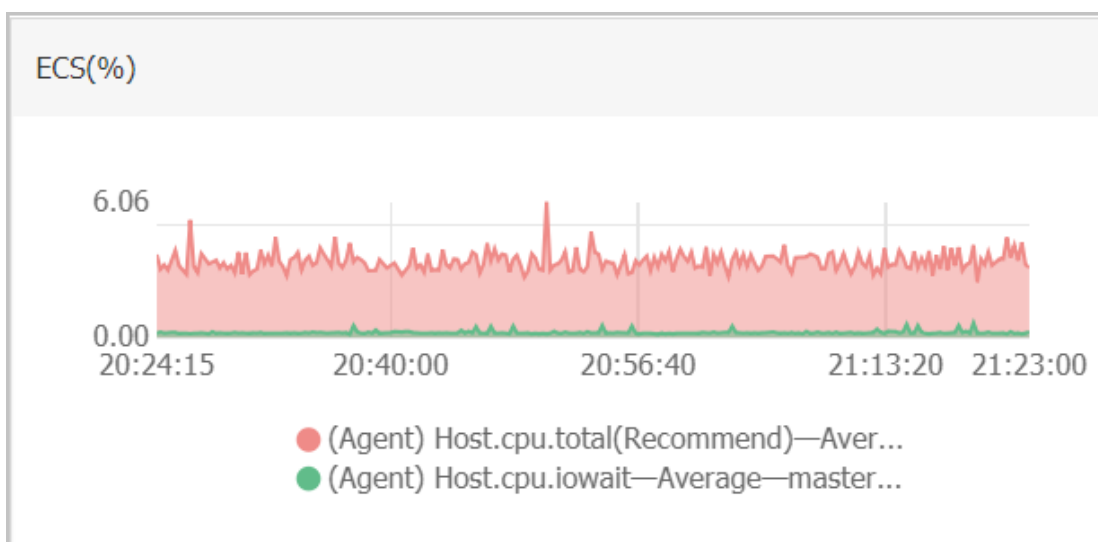
4. Open the dashboard, click Add View, and set the required parameters in the Add View page that appears on the right side to create a custom chart.

a) Select a chart type. Supported chart types include line, area, and pie charts, TopN tables, and heat maps.

- **Line chart:** Displays monitoring data on a basis of time series. Multiple metrics can be added.



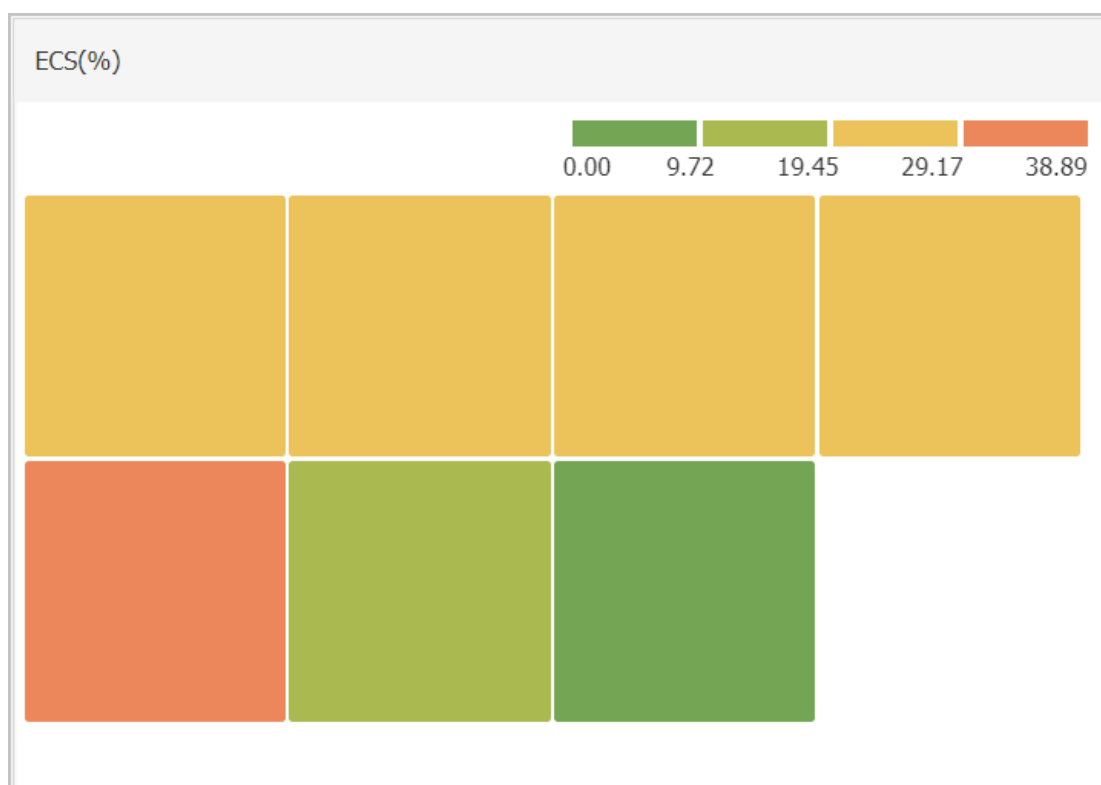
- **Area chart:** Displays monitoring data on a basis of time series. Multiple metrics can be added.



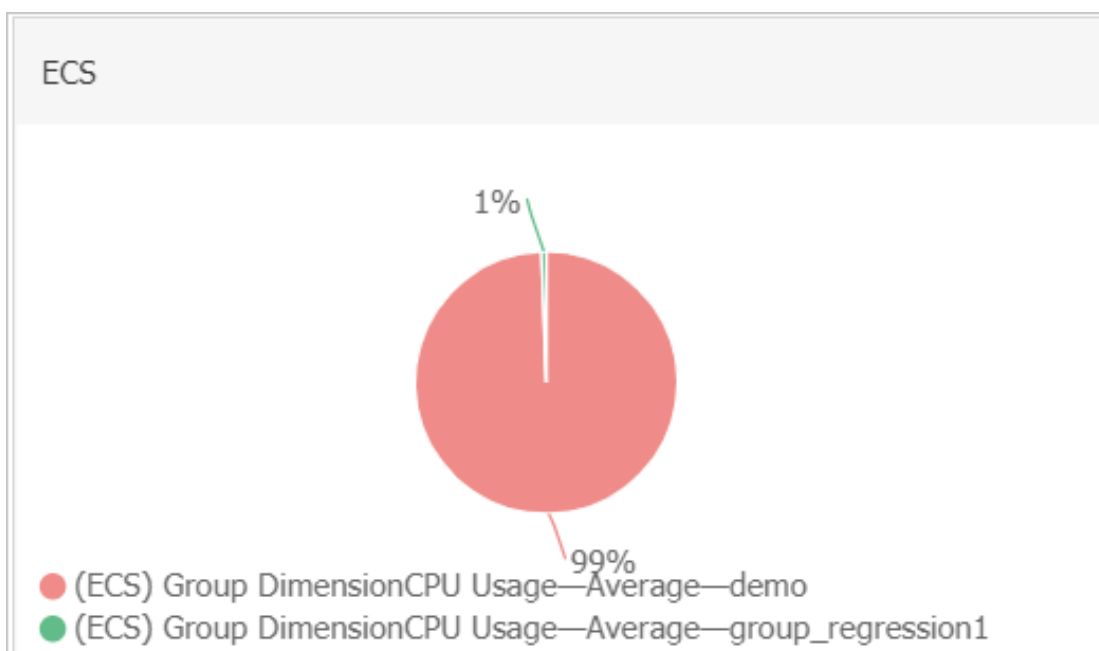
- **Table:** Displays real-time metric data in descending order. Each table displays up to 1,000 data records, which are either the first 1,000 records or the last 1,000 records. Only one metric can be added.

ECS(%)		
Time	Dimensions	Maximum Value
2018-12-06 21:25:00	ESS-asg-yinna_test	100
2018-12-06 21:20:00	node-0003-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	55.56
2018-12-06 21:25:00	master-02-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	38.89
2018-12-06 21:25:00	master-03-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	38.1
2018-12-06 21:00:00	master-01-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	37.5
2018-12-06 21:00:00	node-0001-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	35.29
2018-12-06 21:20:00	node-0002-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	29.41

- **Heat map: Displays real-time metric data. Heat maps show the distribution and comparison of real-time data of a specific metric for multiple instances. Only one metric can be added.**

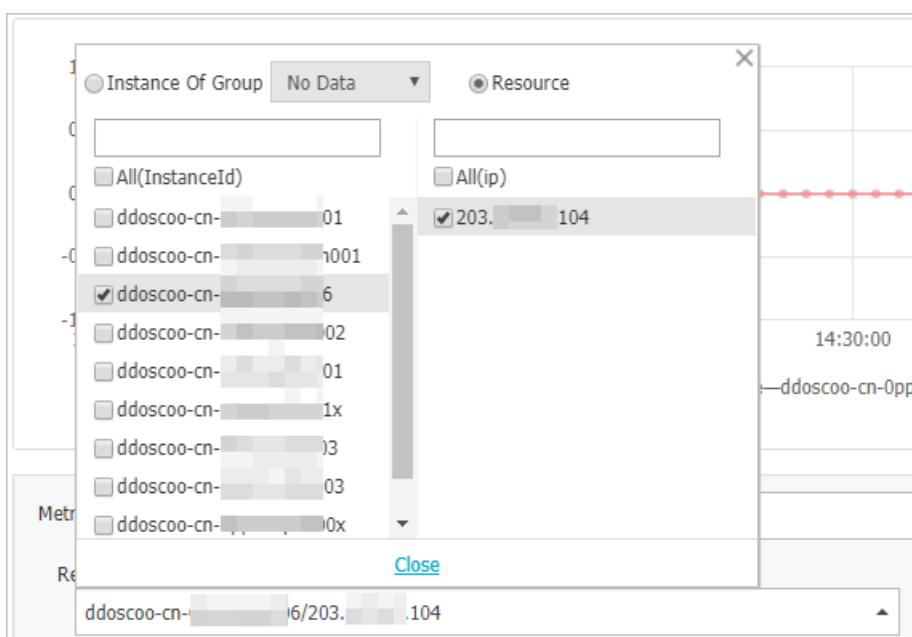


- **Pie chart: Displays real-time metric data and can be used for data comparisons. Only one metric can be added.**



b) Select metrics. Click the Dashboards tab and select NewBGPDDoS. Select metrics and resources from the Metrics and Resource drop-down lists, respectively.

- **Metrics:** Select the Anti-DDoS Pro metrics that you want to monitor. For more information, see [Anti-DDoS Pro metrics](#).
- **Resource:** Select the Anti-DDoS Pro instances and IP addresses that you want to monitor.



You can click Add Metrics to add multiple metrics to the chart.

c) Click Save to create the chart.

Add View

1 Chart Type

Line

Area

Table

Heat Map

Pie Chart

2 Select Metrics

Dashboards

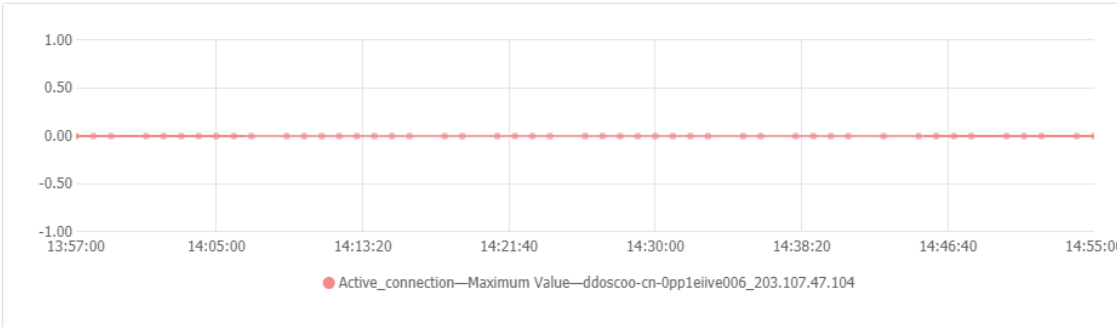
Log Monitoring

Custom

NewBGPDDoS

NewBGPDDoS

Heat Map Gradient Range: 0 auto



Metrics: Active_connection Maximum Value

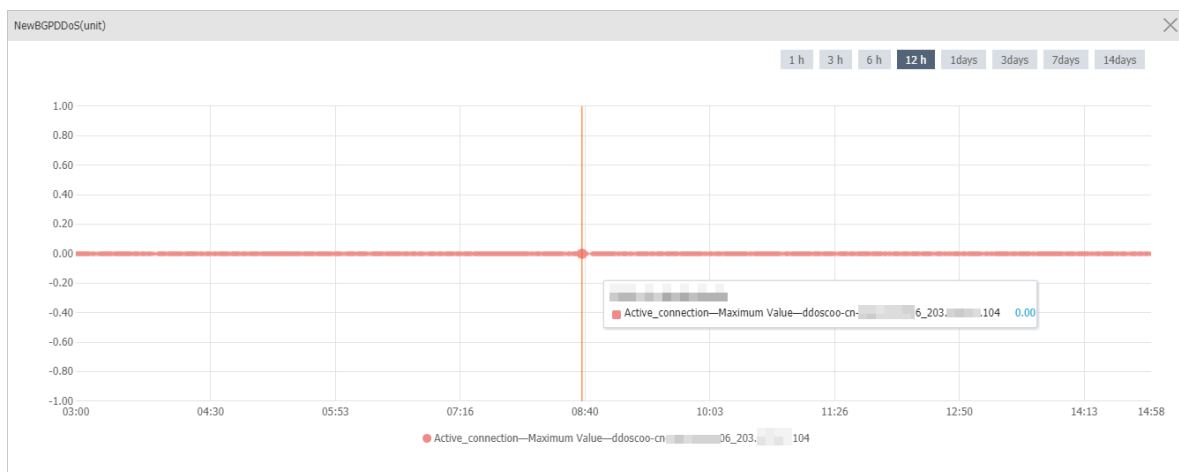
Resource: ddoscoo-cn-0pp1eiive006_203.107.47.104

+AddMetrics

Save

Cancel

You have created a chart that displays monitoring data of Anti-DDoS Pro.



5. To add more charts to the dashboard, repeat step 4. For more information, see [#unique_159](#) and [#unique_160](#).

11.5 Migrate to the latest Anti-DDoS Pro

Overview

It has been three years since Alibaba Cloud released the previous version of Anti-DDoS Pro. To meet your needs for more reliable networking, Alibaba Cloud has been consistently improving Anti-DDoS Pro services.

Currently, Alibaba Cloud has released the latest version of *Anti-DDoS Pro*.

The latest version is built on a new network infrastructure that connects Anti-DDoS Pro with Alibaba Cloud BGP data centers. This version reduces the average latency between Anti-DDoS Pro and any Chinese mainland region to less than 20 ms and offers more reliable networking than China Telecom or China Unicom networks alone. Anti-DDoS Pro adopts an architecture that requires attack traffic to be filtered in the same ISP network where the traffic was first detected. This significantly improves disaster recovery and protection capabilities offered by Anti-DDoS Pro.

Anti-DDoS Pro instance configurations

- **Basic bandwidth:** The minimum basic bandwidth is 30 Gbit/s, which only costs RMB 20,800 per month.
- **Burstable bandwidth:** The maximum burstable bandwidth is 600 Gbit/s. Contact customer service if you need more burstable bandwidth.

Migrate to the latest Anti-DDoS Pro

We recommend that you migrate to the latest version of Anti-DDoS Pro for a more reliable, secure, and faster service. Note the following details:

- The China Telecom data center in Suzhou and China Unicom data center in Dalian will stop providing services after December 30, 2018. If your Anti-DDoS Pro instances are deployed in any of these data centers, you must migrate your service to the latest version of Anti-DDoS Pro before December 30, 2018. If you need help with service migration, contact customer service.



Note:

You must migrate to the latest Anti-DDoS Pro if your Anti-DDoS Pro instances meet the criteria.

- You can keep using your current Anti-DDoS Pro instances if they are not deployed in the China Telecom data center in Suzhou or China Unicom data center in Dalian. To experience the latest version of Anti-DDoS Pro now, you can purchase new Anti-DDoS Pro instances and migrate your service to new instances.

Procedure

You can perform the following steps to migrate your service.

Before you begin

Contact customer service to check whether your Anti-DDoS Pro instances meet the preceding criteria.

If your Anti-DDoS Pro instances meet the criteria, you can contact customer service to create new Anti-DDoS Pro instances for you. The expiration time of new instances is no earlier than that of old instances.

New instances have the same configurations as old instances.



Note:

We recommend that you migrate your service to new Anti-DDoS Pro instances once the new instances are created. During the migration process, both old and new Anti-DDoS Pro instances can forward your traffic and protect the security of your business.



Notice:

We recommend that you back up your configurations in advance. You can read [Import and export configurations](#) to learn how to import and export domain configurations and forwarding rules in the Anti-DDoS Pro console. After you migrate domain configurations to the new Anti-DDoS Pro instances, you cannot view these configurations on old Anti-DDoS Pro instances.

1. Log on to the [Anti-DDoS Pro console](#).

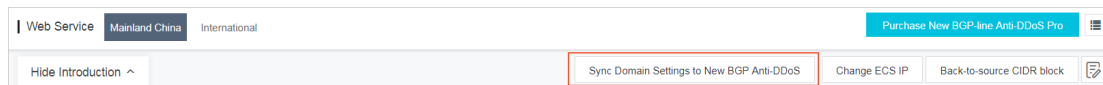
2. Migrate domain configurations and forwarding rules to new Anti-DDoS Pro instances.

- Migrate domain configurations to new Anti-DDoS Pro instances

Notes:

- Do not add forwarding rules on port 80 or 443. Anti-DDoS Pro uses port 80 or 443 by default. If the ports are already in use, you cannot associate your domain to new Anti-DDoS Pro instances.
- If you submitted a ticket to redirect HTTP/2 or HTTPS requests to HTTP, you must disable the redirect feature before you migrate domain configurations to new Anti-DDoS Pro instances.
- If a wildcard subdomain that matches your domain is already configured in other accounts, you cannot associate your domain to new Anti-DDoS Pro instances. If you have multiple Alibaba Cloud accounts, make sure to avoid this conflict.

- a. In the left-side navigation pane, choose Access > Web Service, and click Syn Domain Settings to New BGP Anti-DDoS.



- b. Enter the IP address of the new Anti-DDoS Pro instance and select the domains to be migrated.



Note:

You can select up to 5 domains. If the old Anti-DDoS Pro instance is associated with more than 5 domains, synchronize domain configurations between the old and new instance in batches.

Sync Domain Settings to New BGP Anti-DDoS

Please view corresponding [documentation](#) before doing the synchronization.

IP:

Please enter a New BGP Anti-DDoS IP

Select Domain: ☐ Select All ☐ adf.test.com

Synchronize

Cancel

- c. Click Synchronize to migrate domain configurations to the new Anti-DDoS Pro instance. To view the domain configurations that are already migrated to new Anti-DDoS Pro instances, log on to the [New BGP Anti-DDoS console](#) and select **Management > Websites**.



Note:

At this point, your traffic is still forwarded by the old Anti-DDoS Pro instance.

Domain synchronization notes:

- If you have only one old Anti-DDoS Pro instance, perform the preceding steps to synchronize all domain configurations between the old and new Anti-DDoS Pro instance.
- If you have multiple old Anti-DDoS Pro instances and some domains are associated with multiple instances, you must identify the domains to be synchronized and the Anti-DDoS Pro instances associated with these domains. If you want to keep using some of the old Anti-DDoS Pro instances, we recommend that you dissociate the domains to be synchronized from these instances and perform the preceding steps to synchronize domain configurations between old and new Anti-DDoS Pro instances.



Notice:

After you synchronize domain configurations, you cannot view these configurations on old Anti-DDoS Pro instances. However, the domains are still associated with old Anti-DDoS Pro instances. You can choose Management > Websites in the New BGP Anti-DDoS console to view domain configurations that are already migrated to new Anti-DDoS Pro instances. To prevent mistakes to these domain configurations, you cannot view these configurations in the old Anti-DDoS Pro console.

- d. After you synchronize domain configurations, we recommend that you log on to the [New BGP Anti-DDoS console](#), choose Management > Websites, and compare the domain configurations in the Websites list with your backup configurations. If you find any differences, you can manually change the domain configurations according to your backup configurations.

Notes:

- The new and old Anti-DDoS Pro instances use different CIDR blocks to forward traffic back to your origin server. If you set access control rules on your origin server, make sure to add the back-to-origin CIDR blocks used by new Anti-DDoS Pro instances to the whitelist. You can select Management > Websites and click View Back-to-origin CIDR

Blocks to view all back-to-origin CIDR blocks used by new Anti-DDoS Pro instances.

- If your domain has not obtained an ICP license, you can submit a ticket or contact customer service for help. We recommend that you obtain an ICP license as soon as possible.
- Migrate forwarding rules to the new Anti-DDoS Pro instances
 - a. In the left-side navigation pane, choose Access > Non-Web Service and select an Anti-DDoS Pro instance and IP address.
 - b. Click Export Rules and select Export rules to export forwarding rules in a TXT file to your local computer.
 - c. In the *New BGP Anti-DDoS console*, choose Management > Port Settings, select an Anti-DDoS Pro instance, click Batch Operations, and select Create Rule.
 - d. Copy the contents of the TXT file to the edit area in the Create Rule dialog box, and click Create to migrate the forwarding rules to the selected Anti-DDoS Pro instance.



Note:

For more information about importing and exporting multiple forwarding rules, see *Import and export configurations*. After you migrate forwarding rules to the new instance, you can follow a similar procedure to migrate session persistence and health check settings to the new instance.

3. You can modify the hosts file on your machine to test if the domain configurations and forwarding rules work as expected. For more information, see *Test configurations on local machines*.
4. After you pass the tests, change DNS resolution settings and modify A record values through your DNS provider to forward traffic to your Anti-DDoS Pro instances.



Note:

If you use IPs and ports to set up the Anti-DDoS Pro instance, replace your service IP with the IP address of the Anti-DDoS Pro instance to forward traffic to Anti-DDoS Pro.

5. After you migrate your service to new Anti-DDoS Pro instances, your old Anti-DDoS Pro instances will be released when their subscription period ends.

You can also submit a ticket or contact customer service to release your old instances.



Note:

When both old and new Anti-DDoS Pro instances are in use, you cannot delete the domain configurations that were migrated from the old instances in the new BGP Anti-DDoS console. You can only delete these domain configurations when the associated old Anti-DDoS Pro instances are released.

Notes

- The migration process will not affect your service. If you need to roll back the configurations, submit a ticket or contact customer service.
- To avoid additional fees during the migration process and when both new and old Anti-DDoS Pro instances are in use, we recommend that you set the basic bandwidth and burstable bandwidth to the same value on your old Anti-DDoS Pro instances.
- If your Anti-DDoS Pro instances do not meet the preceding criteria, you can purchase new Anti-DDoS Pro instances by yourself and follow the preceding steps to migrate your service to new Anti-DDoS Pro instances. After the migration process is complete, and your old Anti-DDoS Pro instances have subscription time left, you can submit a ticket to request a refund.



Note:

If your Anti-DDoS Pro instances meet the preceding criteria, you cannot request a refund because your new Anti-DDoS Pro instances are created by Alibaba Cloud free of charge.

FAQ

What benefits does the latest Anti-DDoS Pro have?

For more information about the benefits offered by Anti-DDoS Pro, see [What is Anti-DDoS Pro](#).

Where can I find detailed pricing information?

For more information about pricing, see [Billing methods](#).

How fast is the network used by Anti-DDoS Pro?

You can use third-party testing tools to test the latency of Anti-DDoS Pro instances. For example, <http://ping.chinaz.com/203.107.32.57>.

Test IP address: 203.107.32.57

Do I need to buy new Anti-DDoS Pro instances during the migration process?

No. After you confirm the configurations of your new Anti-DDoS Pro instances with customer service, Alibaba Cloud creates new Anti-DDoS Pro instances for you free of charge.

How can I tell where my Anti-DDoS Pro instance is deployed?

Your Anti-DDoS Pro instance is deployed in the China Telecom data center in Suzhou or China Unicom data center in Dalian if its IP address is within one of the following CIDR blocks:

- 180.97.164.128/26
- 180.97.164.0/25
- 180.97.163.0/24
- 180.97.162.0/24
- 180.97.161.0/24
- 180.97.89.0/24
- 180.101.207.0/24
- 180.101.208.0/24
- 218.94.232.0/24
- 218.60.113.0/24
- 218.60.114.0/24
- 218.60.115.0/25
- 218.60.115.128/26
- 218.60.112.0/24
- 218.60.121.0/24
- 218.60.82.0/24
- 218.60.83.0/24
- 211.93.149.0/24

How long does it take to migrate my service to new Anti-DDoS Pro instances?

- If you use domains to set up Anti-DDoS Pro instances, it takes one to three days because you need to update DNS records through your DNS provider.
- If you use IPs and ports to set up Anti-DDoS Pro instances, it depends on your service status.

Will my service be interrupted during the migration process?

In most situations, migrating to new Anti-DDoS Pro instances does not affect your service. The actual situation may vary according to the service status. Alibaba Cloud allows you to keep both old and new Anti-DDoS Pro instances in use for a period of time. Old Anti-DDoS Pro instances are not released until Alibaba Cloud confirms that all your traffic is forwarded to your new Anti-DDoS Pro instances.

Your service availability is the highest priority of Alibaba Cloud during the entire migration process.

What else do I need to know when migrating to the latest Anti-DDoS Pro?

- The latest version of Anti-DDoS Pro is based on BGP networks and supports quick disaster recovery. This version provides faster and more reliable networks compared with older versions. To set up the latest Anti-DDoS Pro to protect your business, you need to change A records instead of CNAME records.
- The latest Anti-DDoS Pro uses different back-to-origin CIDR blocks than older versions of Anti-DDoS Pro. You need to manually update back-to-origin CIDR blocks if you have set access control rules to protect your origin server.