Alibaba Cloud Anti-DDoS Basic

New Anti-DDoS Pro Service

Issue: 20190412

Legal disclaimer

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

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

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

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

Generic conventions

Table -1: Style conventions

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

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

Contents

Legal disclaimer..... I
Generic conventions..... I
1 Product Introduction..... 1
1.1 What is Anti-DDoS Pro..... 1
2 Pricing..... 4
2.1 Billing methods..... 4
2.2 Buy Anti-DDoS Pro instances..... 7
2.3 Upgrade Anti-DDoS Pro instance configurations..... 8
3 Quick Start..... 10
3.1 Set up Anti-DDoS Pro to protect your business..... 10
4 User Guide..... 16
4.1 Use NS records to set up Anti-DDoS Pro..... 16
4.2 Configure layer 4 protection..... 18
4.2.1 Configure layer 4 anti-DDoS protection settings..... 18
4.2.2 Configure layer 4 smart defense settings..... 20
4.3 Configure layer 7 protection..... 25
4.3.1 Configure HTTP flood protection..... 25
4.3.2 Configure the blacklist and whitelist..... 28
4.3.3 Deactivate the black hole status..... 30
4.3.4 Block traffic flow..... 31
4.3.5 Change the IP of an ECS instance..... 33
4.4 New protection policies..... 34
4.5 View security reports..... 36
4.6 Log queries..... 38
4.6.1 Full log..... 38
4.6.2 Fields..... 40
4.7 Anti-DDoS packages..... 45
4.8 Import and export configurations..... 49
4.9 Managed Security Service..... 56
4.10 New protection policies..... 57

1 Product Introduction

1.1 What is Anti-DDoS Pro

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

Anti-DDoS Pro provides the following benefits:

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

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

Differences between older and current versions of Anti-DDoS Pro

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

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

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

Scenarios

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

- Reliable networking that supports minimal latency, quick disaster recovery, and multiple ISP networks.
- Basic protection that offers 20 Gbit/s or more BGP bandwidth.
- Capability to mitigate DDoS attacks peaking at more than 300 Gbit/s.

2 Pricing

2.1 Billing methods

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

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

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

Basic protection (monthly subscription)

Protection capability (peak attack bandwidth)	Network	Price
30 Gbit/s	Eight BGP-line	USD 3,220 per month
60 Gbit/s	Eight BGP-line	USD 7,250 per month
100 Gbit/s	Eight BGP-line	Special offer: USD 4,240 per year
300 Gbit/s	Eight BGP-line	Special offer: USD 6,820 per year
400 Gbit/s	Eight BGP-line	Special offer: USD 12,490 per month
500 Gbit/s	Eight BGP-line	Special offer: USD 48,420 per month
600 Gbit/s	Eight BGP-line	Special offer: USD 57,630 per month
700 Gbit/s	Eight BGP-line	Special offer: USD 65,780 per month
800 Gbit/s	Eight BGP-line	Special offer: USD 73,680 per month
900 Gbit/s	Eight BGP-line	Special offer: USD 81,570 per month
1 Tbit/s	Eight BGP-line	Special offer: USD 89,470 per month

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

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

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

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

Notes:

- No additional fee is charged if the peak attack bandwidth does not exceed the basic bandwidth.
- No additional fee is charged if the peak attack bandwidth exceeds the burstable bandwidth. This means if the Anti-DDoS Pro instance enters the black hole status, no additional fee is charged.
- The additional fee for the current day is usually generated between 8 am to 9 am the next day.

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

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

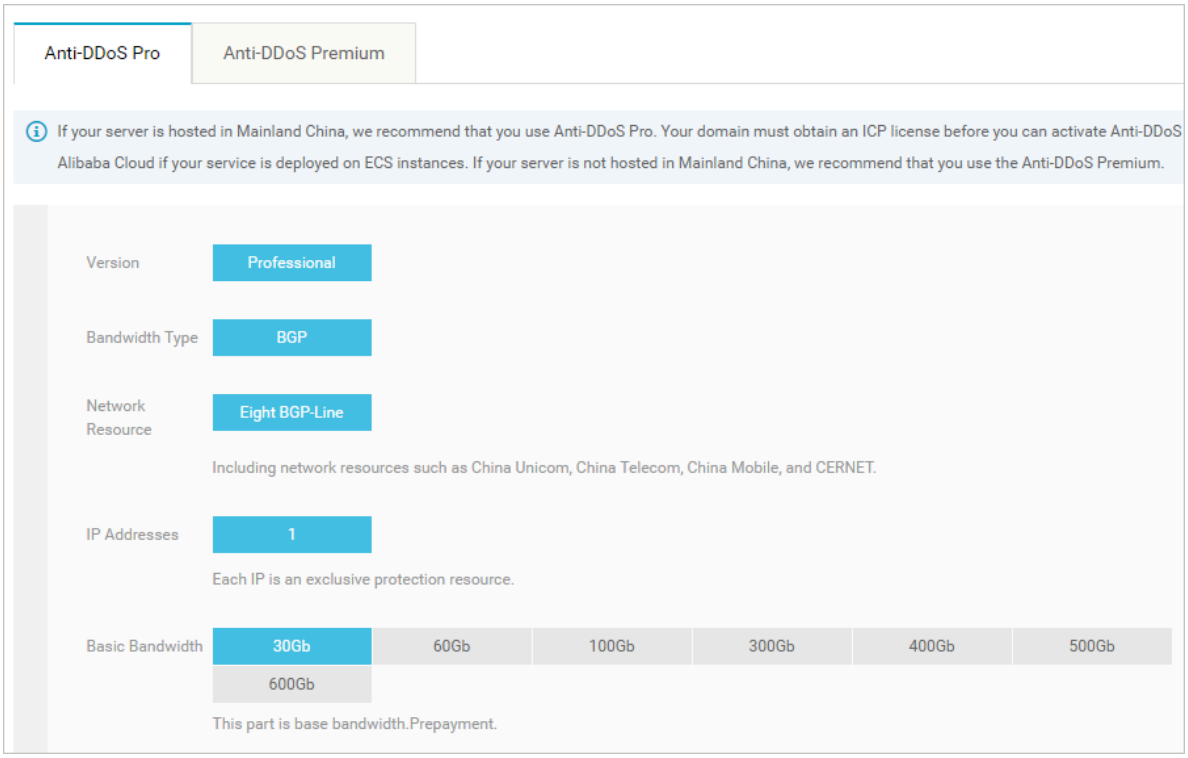
Bandwidth difference	Fees
1,100 Gbit/s < Bandwidth difference ⩽ 1,200 Gbit/s	USD 18,580 per day
1,200 Gbit/s < Bandwidth difference ⩽ 1,300 Gbit/s	USD 20,130 per day
1,300 Gbit/s < Bandwidth difference ⩽ 1,400 Gbit/s	USD 21,670 per day
1,400 Gbit/s < Bandwidth difference ⩽ 1,500 Gbit/s	USD 23,220 per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

2.2 Buy Anti-DDoS Pro instances

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

Procedure

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



2. Select the Basic Bandwidth, Burstable Bandwidth, Ports, and Service Bandwidth based on your needs.
   - Basic Bandwidth: The minimum bandwidth provided by the Anti-DDoS Pro instance during protection. Your subscription fee is calculated based on the basic bandwidth and subscription duration.
   - Burstable Bandwidth: The maximum bandwidth provided by the Anti-DDoS Pro instance during protection. When the attack bandwidth exceeds the basic bandwidth, the burstable bandwidth is consumed to defend against the attack. Additional fees will be charged based on the difference between the peak attack bandwidth and basic bandwidth.

     Note:
     If you do not want to consume the burstable bandwidth, you can set the burstable bandwidth and basic bandwidth to the same value. No additional fees will be charged and the maximum bandwidth provided by the Anti-DDoS Pro instance equals the basic bandwidth.
   - Ports: The maximum number of forwarding ports the Anti-DDoS Pro instance can use during port forwarding.
   - Service Bandwidth: The maximum bandwidth provided by the Anti-DDoS Pro instance for normal requests when no attack is in progress.
3. Select the Duration and Quantity, and click Buy Now to make your payment.

Result

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

2.3 Upgrade Anti-DDoS Pro instance configurations

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

Context

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

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

The price for the upgrades is calculated as follows:

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

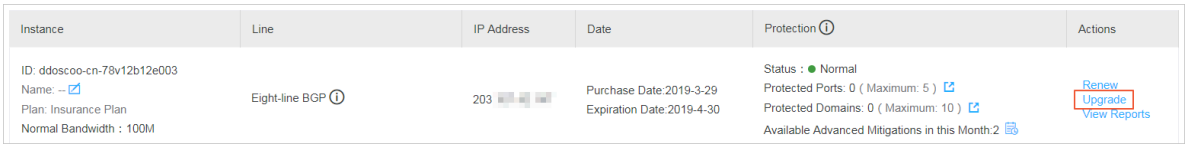
  > **Note:**
  > If your Anti-DDoS Pro instance is associated with 100 domains, Anti-DDoS Pro charges USD 35.16 per month for each domain over the 100 threshold.

- Ports: For each new port, Anti-DDoS Pro charges USD 7.81 per month. This fee is calculated based on your remaining subscription time.
- Service Bandwidth: For each Mbit/s of bandwidth, Anti-DDoS Pro charges additional USD 15.63 per month. This fee is calculated based on your remaining subscription time.

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

Procedure

1. Log on to the *Anti-DDoS Pro console*.
2. In the left-side navigation pane, choose Management > Instances, select an Anti-DDoS Pro instance, and click Upgrade.



3. On the Configuration Upgrade page, specify the basic bandwidth, domains, ports, and service bandwidth.
4. Make your payment and the new configurations take effect immediately.

3 Quick Start

3.1 Set up Anti-DDoS Pro to protect your business

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

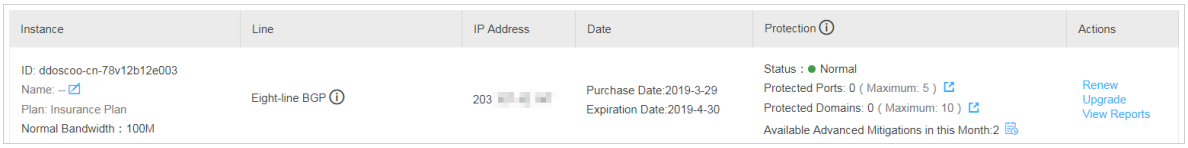
You can set up Anti-DDoS Pro instances by using one of the following methods:

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

Set up Anti-DDoS Pro instances using domains

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

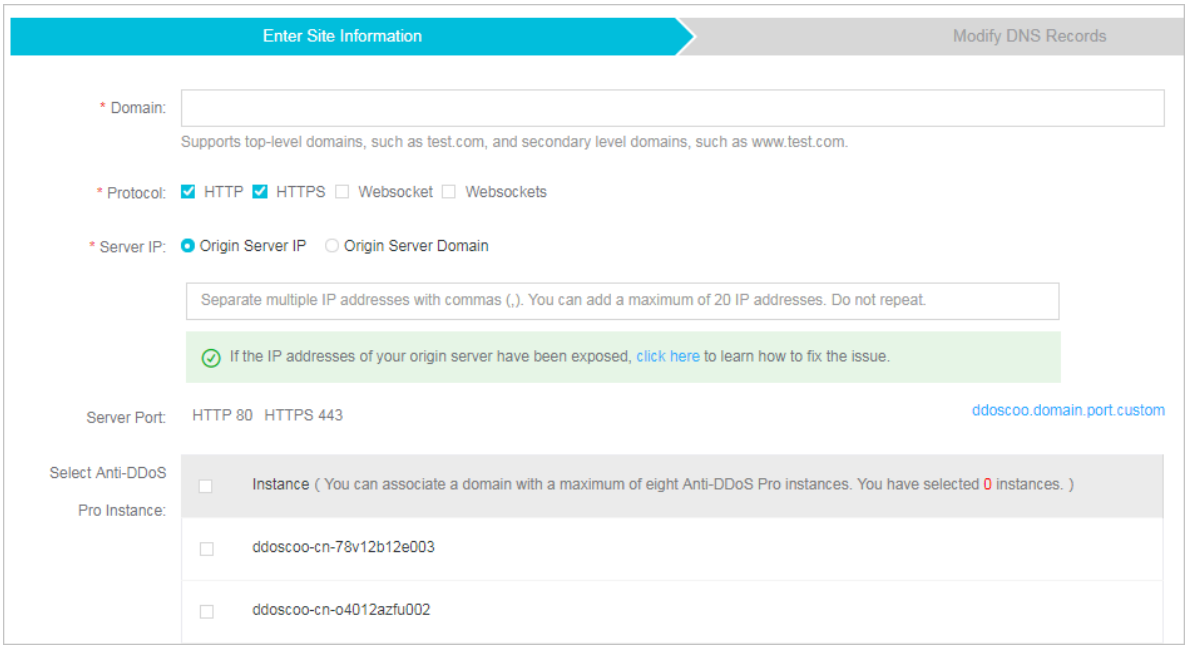
   In the left-side navigation pane, choose Management > Instances to view your Anti-DDoS Pro instances.



2. Choose Management > Websites and click Add Domain.

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

3. You need to configure the following parameters:



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

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

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

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

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

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

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

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

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

- If the forwarding port is 80, the system automatically generates a rule that forwards traffic on TCP port 80 to the origin server. The rule is not generated if the same rule already exists.
- If the forwarding port is 443, the system automatically generates a rule that forwards traffic on TCP port 443 to the origin server. The rule is not generated if the same rule already exists.

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

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

Set up Anti-DDoS Pro instances using IPs and ports

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

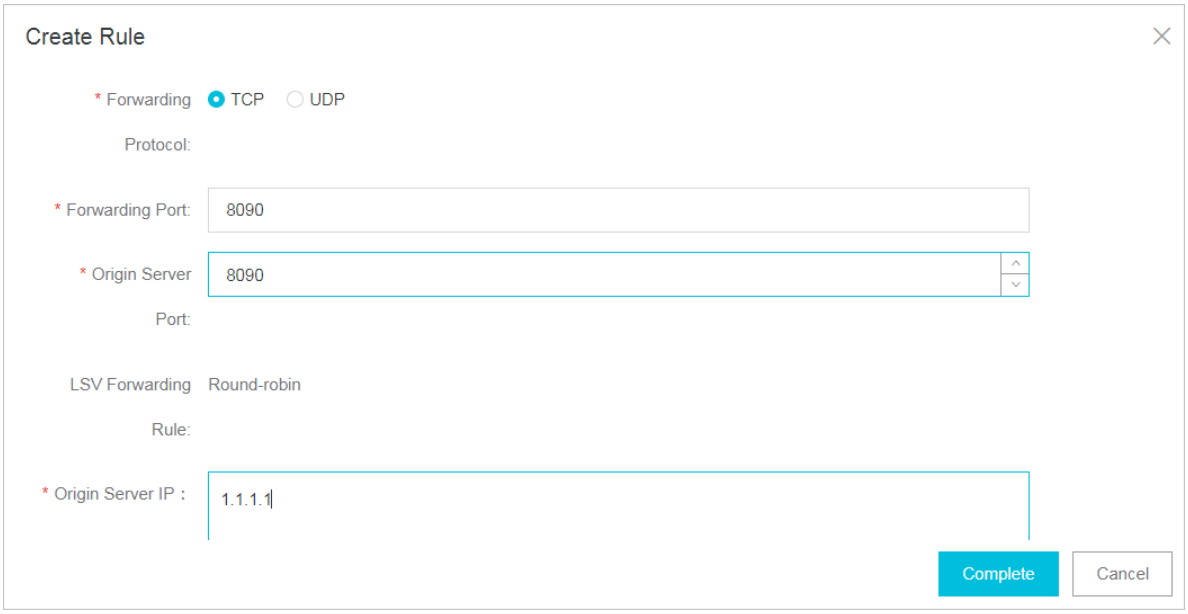
   In the left-side navigation pane, choose Management > Instances to view your Anti-DDoS Pro instances.
2. Choose Management > Port Settings, select an Anti-DDoS Pro instance, and click Create Rule.

   Note:

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

3. You need to configure the following parameters:



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

4. Click Complete.

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

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

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

4 User Guide

4.1 Use NS records to set up Anti-DDoS Pro

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

Prerequisites

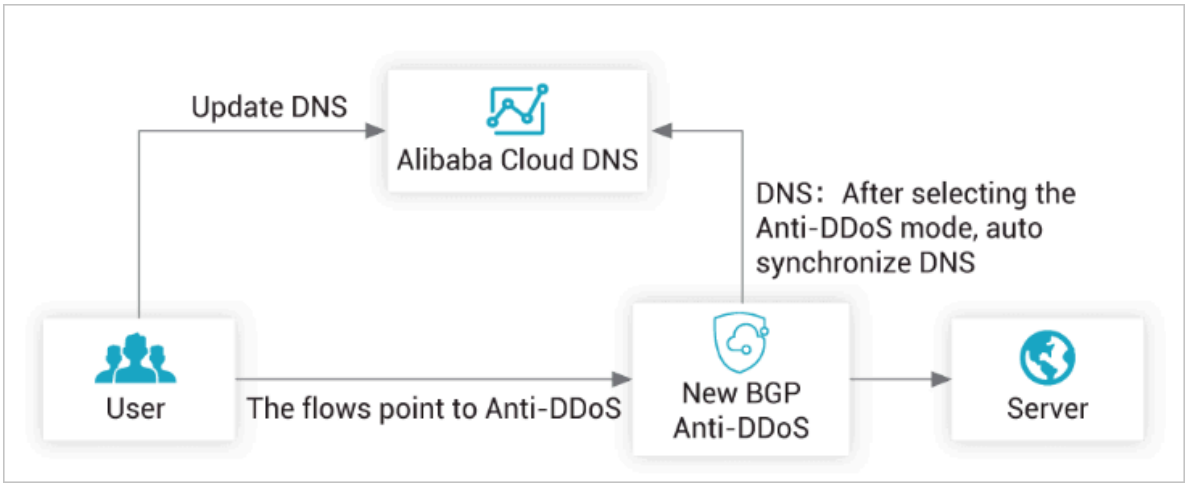
Your domain is managed under a paid version of Alibaba Cloud DNS. Otherwise, you cannot enable NS Mode Access. We recommend that you *activate a paid version of Alibaba Cloud DNS*.

Context

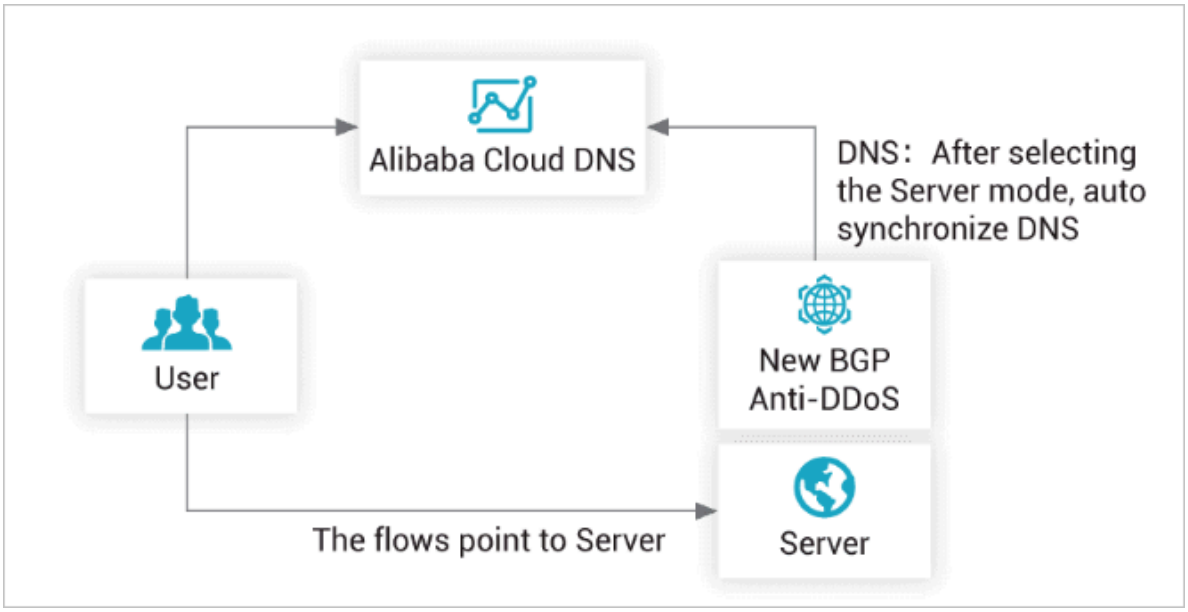
NS Records are nameserver records. You can use NS records to specify which DNS server is used to resolve your domain name.

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

- The Anti-DDoS Pro mode automatically modifies DNS records to forward incoming traffic to your Anti-DDoS Pro instances.



- The Back-to-Origin mode automatically synchronizes DNS records between Anti-DDoS Pro instances and Alibaba Cloud DNS. Incoming traffic is still directed to your origin server.



We recommend that you use the following steps to enable NS Mode Access. If you cannot enable NS Mode Access, you must manually change the DNS records of your domain through your DNS provider.

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

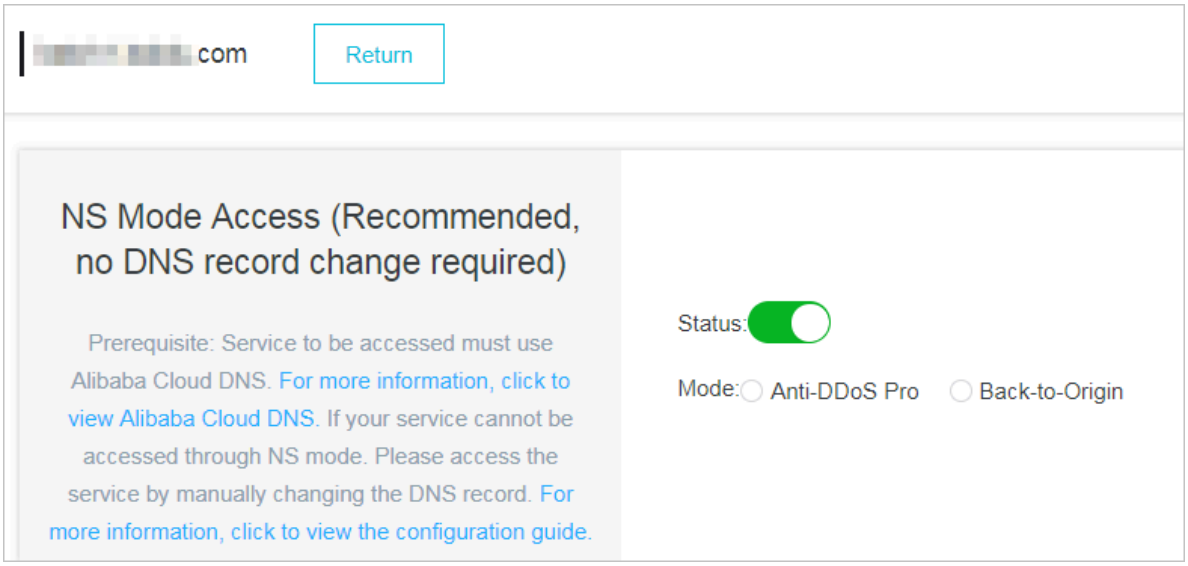
Procedure

1. Log on to the *Anti-DDoS Pro console*.
2. In the left-side navigation pane, choose Management > Websites.
3. Select your domain and click Configure DNS Settings.

4. Enable NS Mode Access.

Note:

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



5. Select the `Anti-DDoS Pro` or `Back-to-Origin` mode based on your needs.
   - When the `Anti-DDoS Pro` mode is selected, Anti-DDoS Pro automatically modifies the DNS records at Alibaba Cloud DNS so that incoming traffic is directed to your Anti-DDoS Pro instances.
   - When the `Back-to-Origin` mode is selected, DNS records are automatically synchronized between Anti-DDoS Pro and Alibaba Cloud DNS. Incoming traffic is still directed to your origin server.
6. After the configuration is complete, you can use DNS testing tools to verify whether the configuration works as expected.

4.2 Configure layer 4 protection

4.2.1 Configure layer 4 anti-DDoS protection settings

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

Context

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

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

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

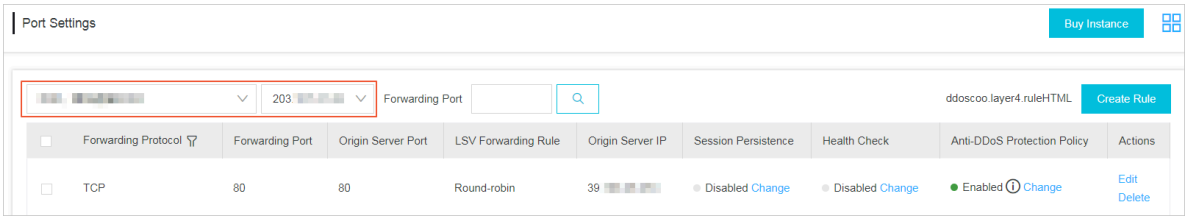
Settings	Description
False Sources	Detects and blocks false source IPs. This setting is only applicable to TCP rules.
Null Session Connections	Detects and blocks null session connections. This setting is only applicable to TCP rules.
New Connection Speed Limits for Source IP	The maximum number of new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

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

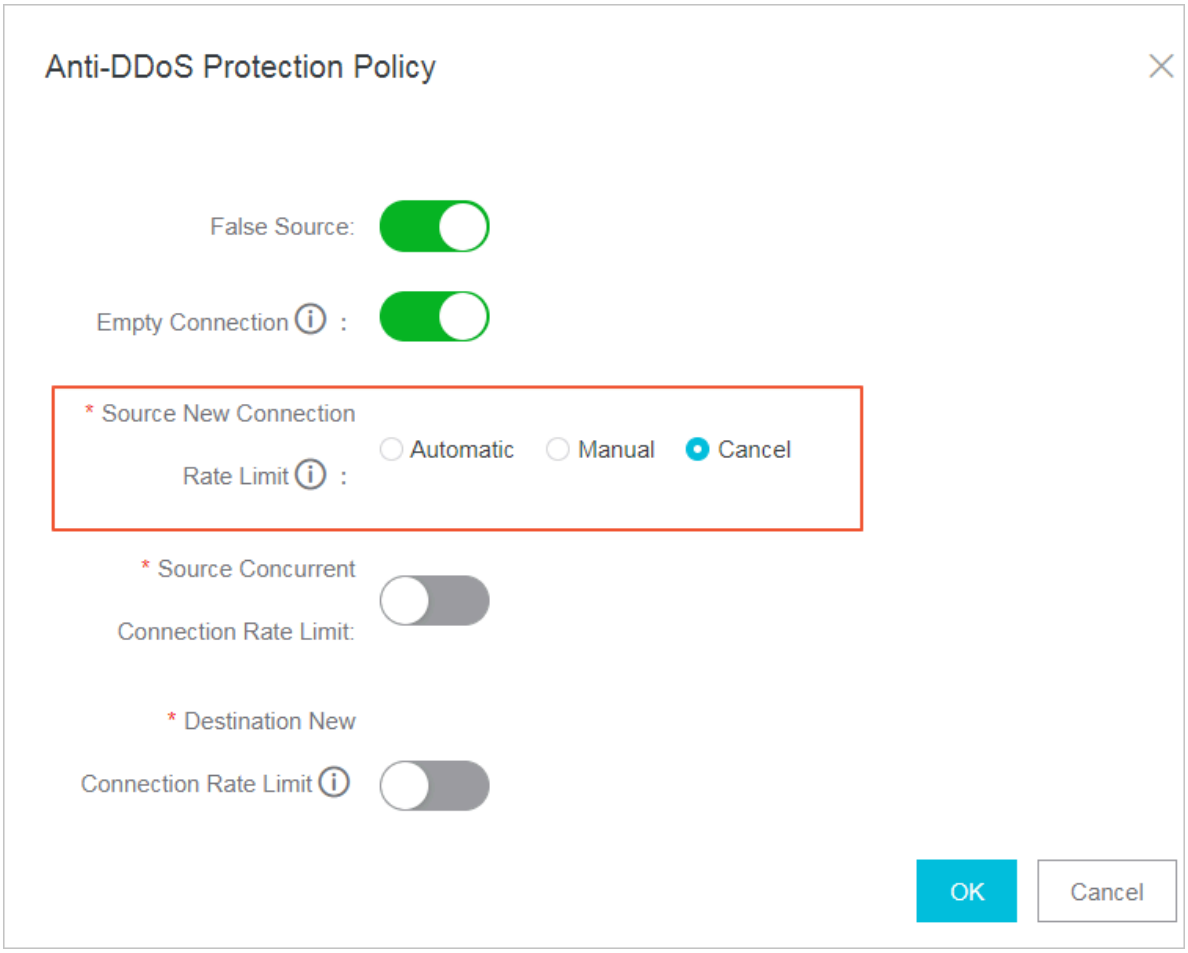
 Note:
Anti-DDoS protection settings take effect for single ports.

Procedure

1. Log on to the *Anti-DDoS Pro console*.
2. In the left-side navigation pane, choose Management > Port Settings, select an Anti-DDoS Pro instance and forwarding rule, and click Configure under the Anti-DDoS Protection Policy column.



3. In the Anti-DDoS Protection Policy dialog box, configure Anti-DDoS protection settings for the selected IP and port.



4.2.2 Configure layer 4 smart defense settings

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

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

The smart defense feature supports the following modes:

- Low: This mode automatically identifies and scrubs traffic that displays common attack patterns based on historical traffic patterns and years of experience defending against Web attacks. The mode is based on an algorithm that automatically identifies malicious IP addresses and adds them to the blacklist. This mode may not be able to block all layer 4 floods but has a low false positive rate.
- Normal: This mode automatically identifies and scrubs traffic that displays common and likely attack patterns based on historical traffic patterns and years of experience defending against Web attacks. We recommend that you use this mode in most situations as it maintains an optimal balance between protection and false positives.
- Strict: This mode provides the most rigorous protection against ongoing attacks based on historical traffic patterns and years of experience defending against Web attacks. The mode may cause false positives.

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

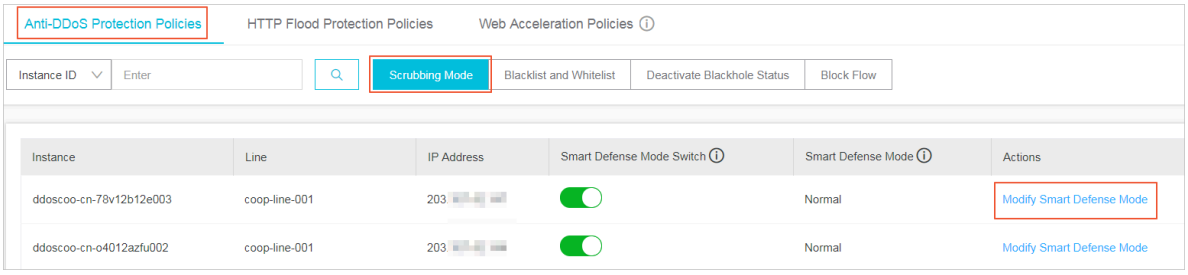
You can view or delete the IP addresses that are automatically added to the blacklist by smart defense. You can also manually add other malicious IP addresses to the blacklist. Meanwhile, you can add specific IP addresses to the whitelist so that Anti-DDoS Pro allows access to these IP addresses without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

Change smart defense modes

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

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

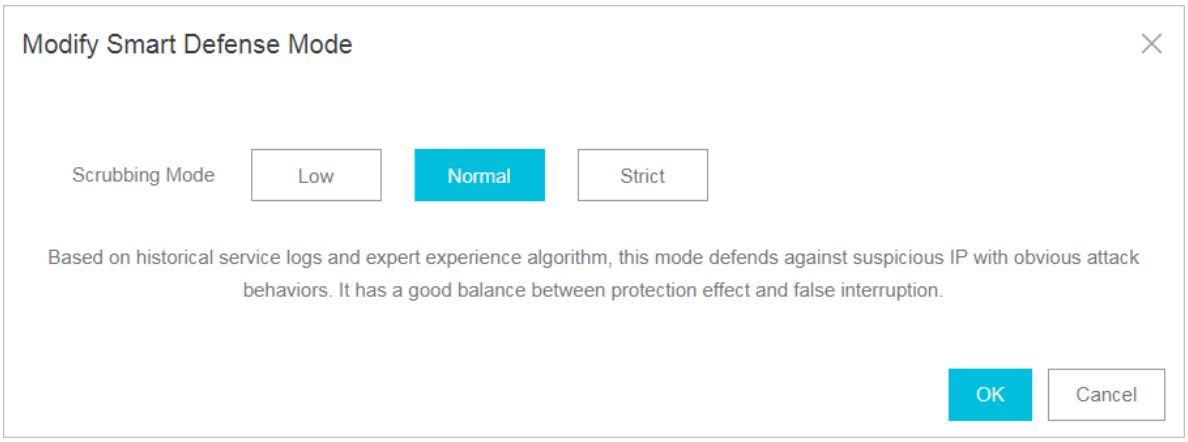
2. Choose Protection > Protection Settings > Anti-DDoS Protection Policies > Scrubbing Mode, select an Anti-DDoS Pro instance, and click Modify Smart Defense Mode.



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

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

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



Manage the blacklist and whitelist

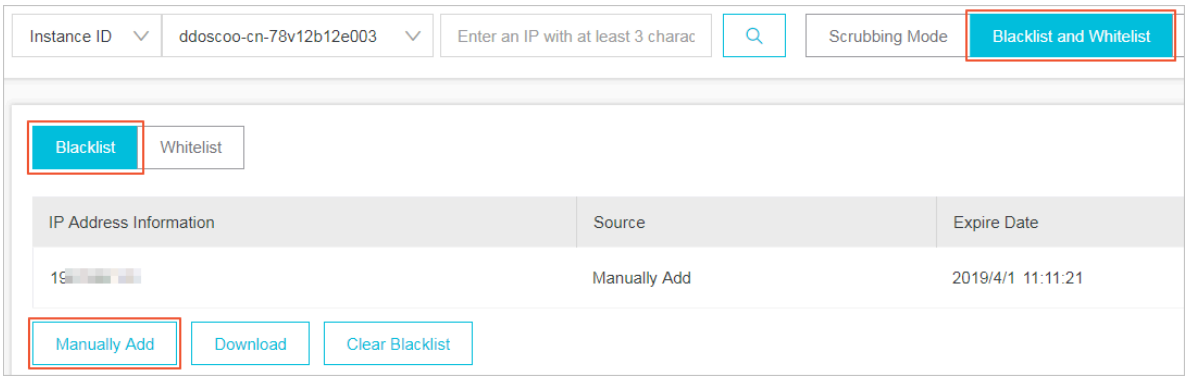
You can view and manage the IP addresses that are added to the blacklist by smart defense. You can also add specific IP addresses to the whitelist so that Anti-DDoS Pro allows access to these IP addresses without further inspection.

- The blacklist

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

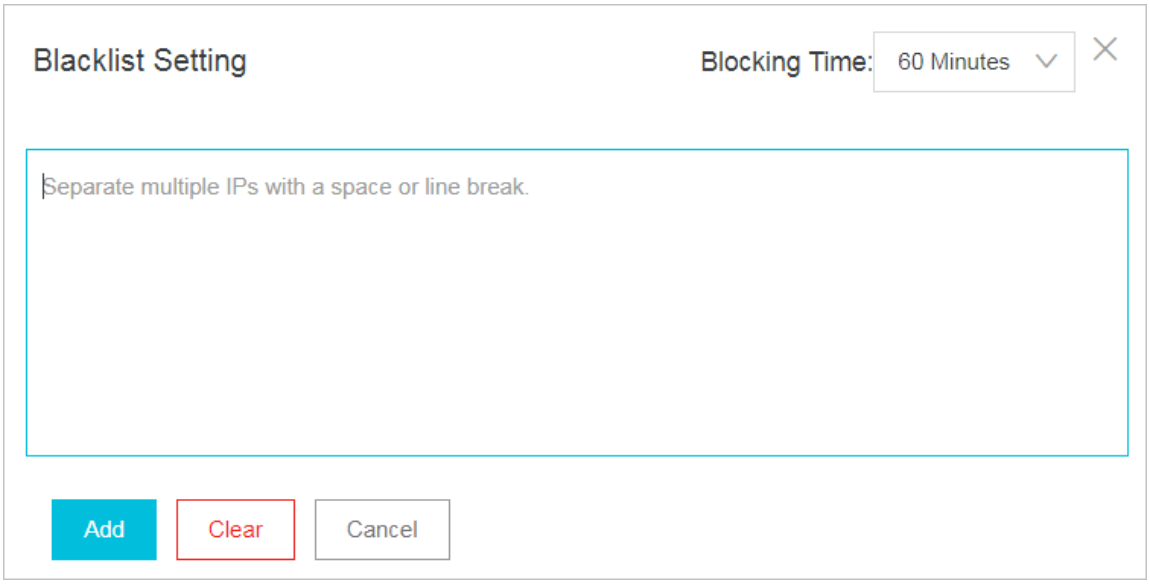
   Note:
  Each IP address in the blacklist has an expiration time. An IP address is automatically removed from the blacklist when its expiration time is reached. Smart defense automatically specifies an expiration time when it adds an IP address to the blacklist. The expiration time ranges from 5 minutes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

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



You can perform the following operations on the blacklist:

- Search by keyword: Enter a keyword in the search box and click the search icon to search for specific IP addresses in the blacklist.
- Download: Click Download to download all blacklisted IP addresses to your local computer.
- Clear Blacklist: Click Clear Blacklist to remove all blacklisted IP addresses.
- Manually Add: Click Manually Add to manually add IP addresses to the blacklist. You need to specify an expiration time for each IP address.



Note:

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

- The whitelist

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

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

  You can perform the following operations on the whitelist:

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

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

4.3 Configure layer 7 protection

4.3.1 Configure HTTP flood protection

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

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

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

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

  The emergency mode provides relatively rigorous protection. This mode can defend against more complicated flood attacks, but may mistakenly block a small number of normal requests.
- Strict: This mode provides rigorous protection against HTTP flood attacks. The mode uses captcha verification to verify the identity of all visitors. Only verified visitors are allowed to access the site.

   Note:
  The strict mode is built on a verification mechanism that verifies whether the request is sent from a browser by a real user. If this mode is enabled for API services and native applications, false positives may occur, disrupting the availability of your service.
- Super Strict: This mode provides the most rigorous protection against HTTP flood attacks. The mode uses captcha verification to verify the identity of all visitors. Only verified visitors are allowed to access the site.

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

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

Procedure

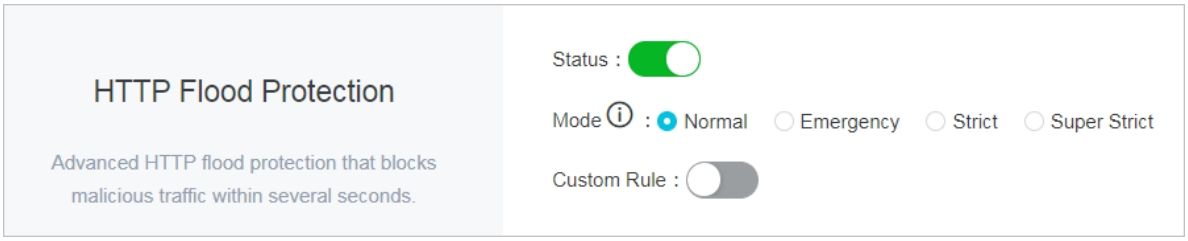
By default, normal HTTP flood protection is used. You can change protection modes based on your needs.

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

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

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

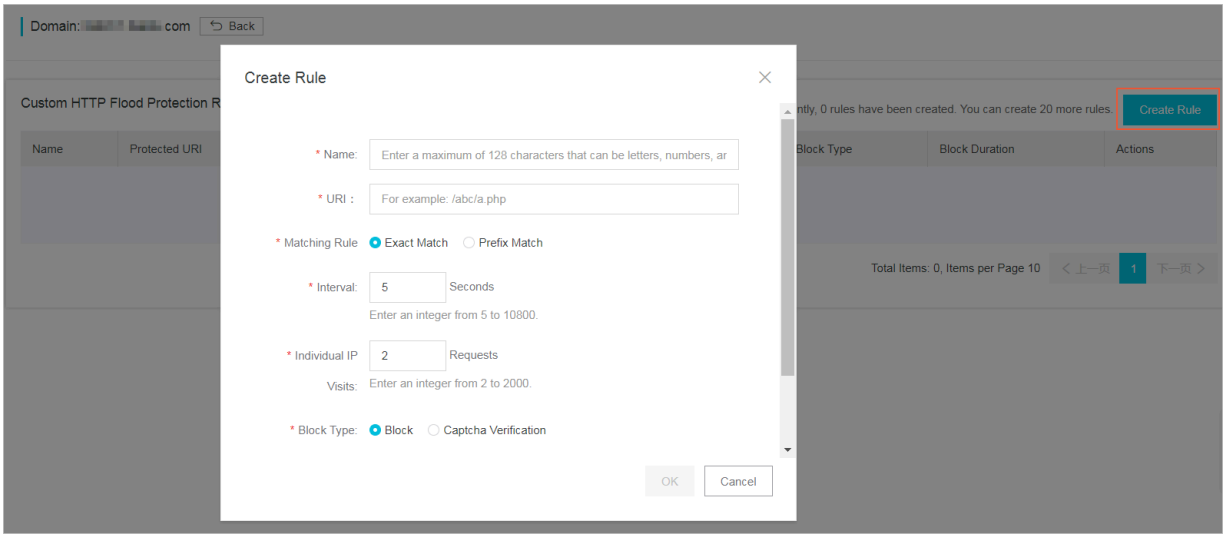
Note:
You can click Status to disable HTTP flood protection.



Custom rules

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

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



Best practices for HTTP flood protection

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

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

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

4.3.2 Configure the blacklist and whitelist

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

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

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

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

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

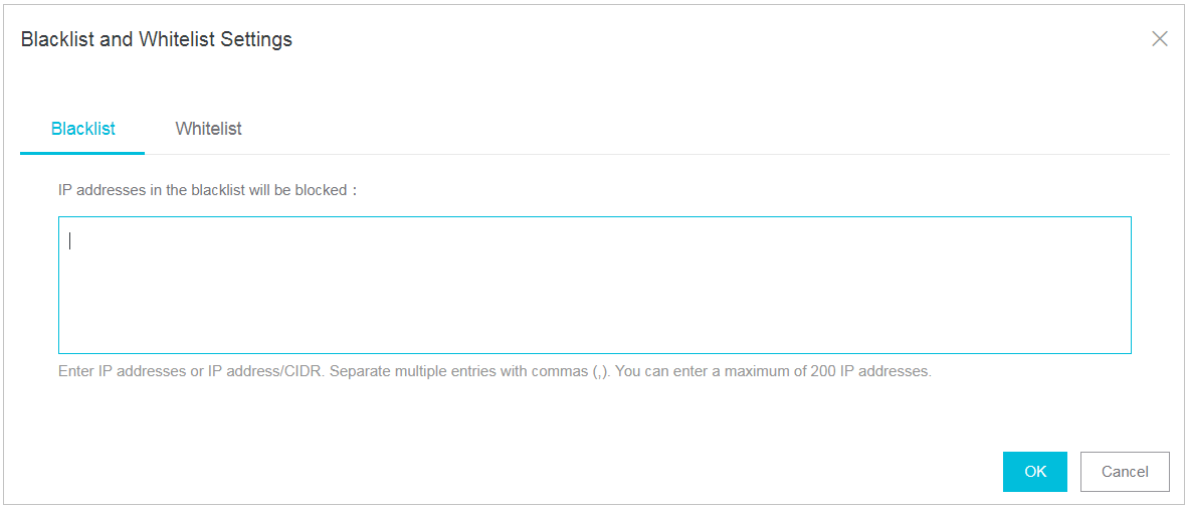
2. In the left-side navigation pane, choose Management > Websites, select a domain, and click Protection Settings.

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

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

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

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



Note:

- The blacklist and whitelist feature is only available in domain configurations.

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

  Notice:
  In some situations, it may take a few minutes for the configurations to take effect. If the configurations of the blacklist and whitelist do not take effect immediately, wait a few minutes.
- You can add 0.0.0.0/0 to the blacklist, which blocks requests from all IP addresses except the ones listed in the whitelist.
- Once created, the configurations of the blacklist and whitelist are effective for all Anti-DDoS Pro instances that are associated with the specified domain.

4.3.3 Deactivate the black hole status

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

Context

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

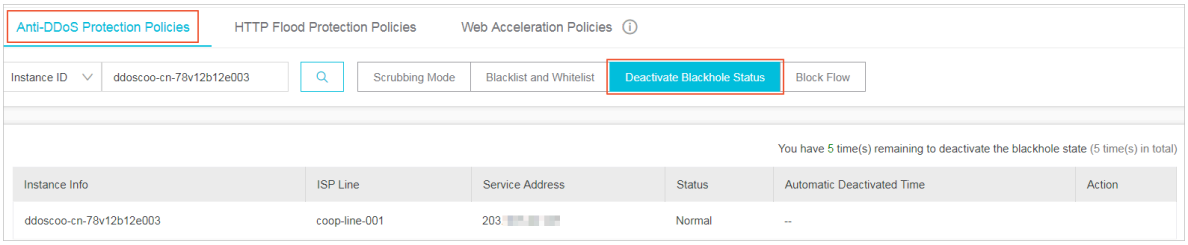
Procedure

1. Log on to the *Anti-DDoS Pro console*.
2. In the left-side navigation pane, choose Protection > Protection Settings.
3. Click Anti-DDoS Protection Policies and select Deactivate Black Hole.

   Note:

   - Each user can deactivate the black hole status up to five times every day. This quota is reduced by one each time the black hole status is successfully lifted.
   - When you deactivate the black hole status for the first time that day, the black hole status is immediately lifted. When you deactivate the black hole status

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



4. Select the Anti-DDoS Pro instance that is in black hole status. Check the time before the black hole status is automatically lifted. You can also click Deactivate under the Actions column to manually deactivate the block hole status.
   - The black hole status is a risk management strategy used by the backend services of Alibaba Cloud. Attempts to deactivate the black hole status may fail , which does not reduce your quota for manually deactivating the block hole status. If an attempt to deactivate the black hole status fails, an error message appears. You can try to deactivate the black hole status later.
   - If the message "Cannot deactivate the black hole status due to risk management. Wait 10 minutes and try again." appears, please wait and try again later.
   - If no error message appears, the black hole status is lifted. You can refresh the page to check if network access is restored.

4.3.4 Block traffic flow

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

Context

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

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

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

Procedure

1. Log on to the *Anti-DDoS Pro console*.
2. In the left-side navigation pane, choose Protection > Protection Settings.
3. On the Anti-DDoS Protection Policies page, click Block Flow.

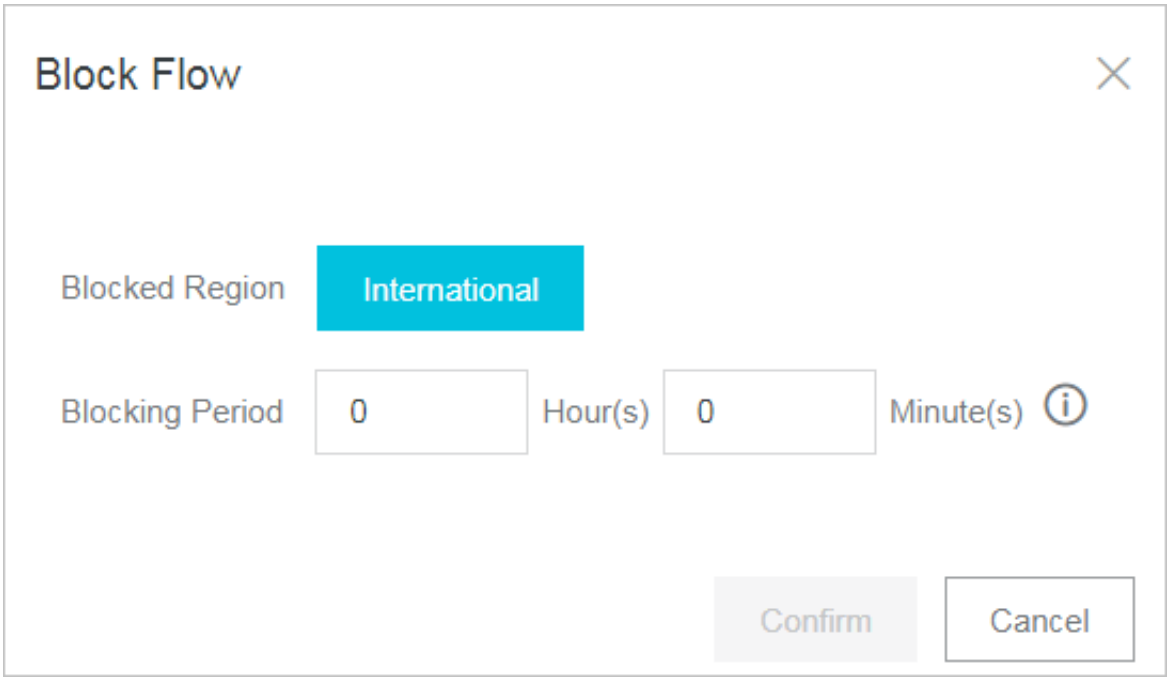
4. Select the Anti-DDoS Pro instance and network type, and click Block.

> **Note:**
>
> - You can block overseas traffic transmitted through China Telecom and China Unicom networks. We recommend that you block traffic transmitted through China Telecom networks first and observe the trend of attacks. If the attack bandwidth is still increasing, you can then block traffic transmitted through China Unicom networks.
> - Each user can block overseas traffic up to 10 times. This quota is reduced by one each time you block traffic transmitted through China Telecom or China Unicom networks.

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

> **Note:**

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



6. Click Confirm.
   - If an error occurs when blocking overseas traffic, an error message appears. Resolve the issue and try again later.
   - If no error message appears, overseas traffic is blocked. Refresh the page and you can find the blocked region and blocking duration. The block button is replaced by Unblock. To immediately unblock traffic, click Unblock under the Actions column.

4.3.5 Change the IP of an ECS instance

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

Context

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

Procedure

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

2. In the left-side navigation pane, choose Management > Websites.
3. Click Change ECS IP.

   Notice:
   When you change the IP of an ECS instance, your service deployed on the instance is interrupted for a few minutes. We recommend that you back up your data in advance.
4. You must stop an ECS instance if you want to change its IP address. If the target ECS instance is stopped, go to step 6. In the Change ECS IP dialog box, click Go to ECS to stop the target ECS instance in the ECS console.
   a) In the instances list, select the target ECS instance and click its instance ID.
   b) On the instance details page, click Stop in the upper-right corner.
   c) Select a stop method and click OK.

      Notice:
      To stop the instance, you must pass SMS verification.
   d) Wait until the target ECS instance is Stopped.
5. Return to the Change ECS IP dialog box, enter the ID of the target ECS instance, and click Next.
6. Make sure you have selected the right ECS instance and click Release IP.
7. After the original IP address is released, click Next and the system assigns a new IP address to the instance.
8. Click OK.

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

4.4 New protection policies

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

Note:

Currently, new protection policies are in beta testing until May 31, 2019.

Enable new protection policies

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

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

1. Log on to the *Anti-DDoS Pro console*.
2. In the left-side navigation pane, choose Protection > Protection Settings, select your domain, and click Try out New Protection Policies.
3. In the dialog box that appears, read the note and click OK.

Note:

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

Introduce new protection policies

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

- Geo-blocking: This feature enables you to block traffic based on geographical location. Chinese regions are divided into 34 provincial regions and international regions are divided into 7 continents. The Anti-DDoS scrubbing center directly discards traffic originating from blocked regions.
- Accurate Access Control: This feature allows you to customize access control rules to filter requests based on the client IP, request URL, and common HTTP header fields, such as the referer, user-agent, and parameter. You can handle matching requests with different actions, such as clear, block, and challenge.

- Intelligent Protection: Based on a big data analysis engine, this feature can analyze your traffic patterns to preemptively detect and block DDoS attacks.
- Web Acceleration Policies: Integrated with Web caching techniques, this feature uses the scrubbing center to speed up your site and protect it from DDoS attacks You can add custom rules to cache specific URLs. Meanwhile, you can select from two cache modes:
  - Standard: Only caches static files on the page, such as .css, .js, and .txt files.
  - Enhanced: Caches all contents on the page.

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

Cipher suites supported by the new protection policies

New protection policies support the following cipher suites:

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

4.5 View security reports

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

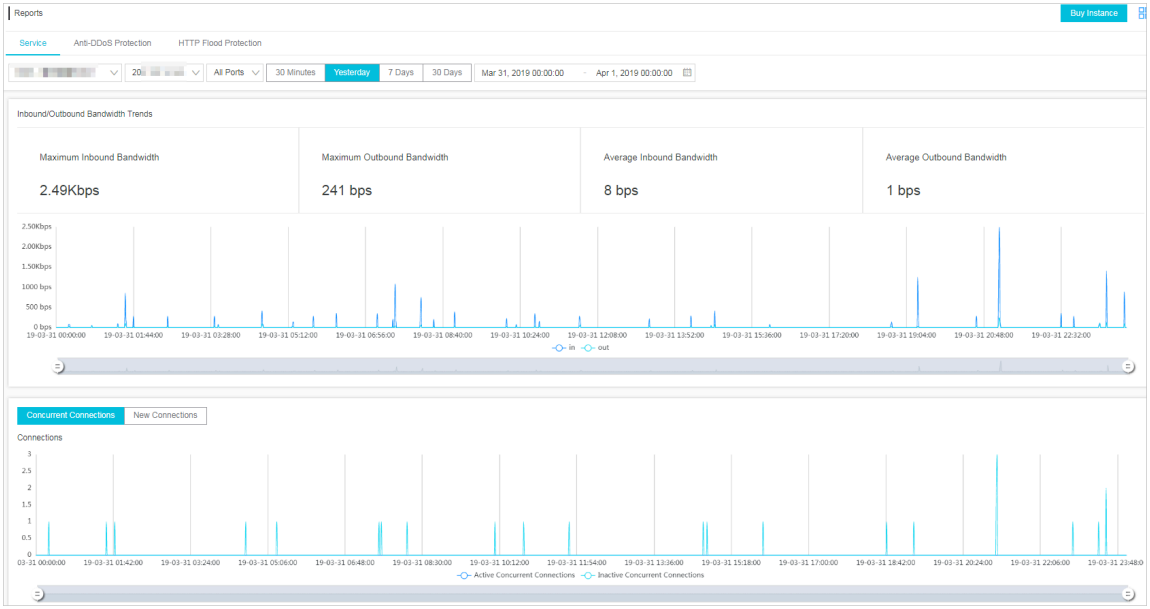
Procedure

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

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

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

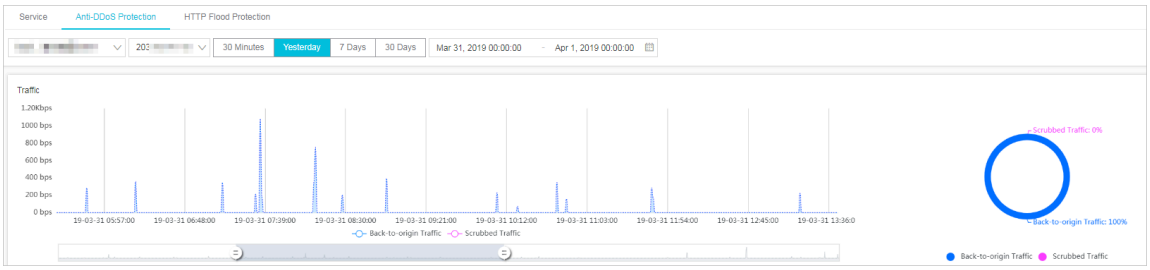
     Note:
     You can query traffic and connection data for up to 30 days.



     You can drag the slider to quickly change time ranges.

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

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



     Note:

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

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

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

4.6 Log queries

4.6.1 Full log

Integrated with Log Service, Alibaba Cloud Anti-DDoS Pro now supports real-time analysis of access logs and attack logs, and provides a report center with a variety of reports.

According to the *2017 APNIC DDoS threat landscape* report, more than 80% of DDoS attacks are combined with HTTP flood attacks, which can be quite difficult to detect. It is especially important to analyze access logs in real time to identify attack behavior and apply a protection policy in a timely manner.

After you set up Anti-DDoS Pro for your website, Log Service collects access logs and attack logs in real time, allows you to query and analyze log data, and displays query results in dashboards.

Enable full log

To enable full log for your website, perform the following steps:

Note:
By default, full log retains log data for 30 days with a maximum of 3 TB storage capacity for free. More storage configurations will be available soon. You may upgrade to a higher storage configuration based on your needs. Additional fees will be charged for higher storage configurations.

Notice:

- When the maximum storage capacity is reached, new log data is not saved. You have three chances to delete all log data. You can also choose not to save log data from unnecessary websites.
- The free storage configuration retains log data for 30 days by default. Log data that is more than 30 days old is automatically overwritten by new log data.

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

    Note:
   If you have not enabled full log, the following message appears when you log on to the Anti-DDoS Pro console. You can click View Details to enable full log.

2. Click Enable Now and authorize Anti-DDoS Pro to save your log data to your exclusive logstore in Log Service.

    Note:
   If you have not activated Log Service, you can activate Log Service for free when you enable full log.

3. On the Full Log page, select a domain and click Status to enable full log for the selected domain.

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

Scenarios

After full log is enabled, you can use it in the following scenarios.

- Troubleshoot exceptions

  You can query and analyze log data 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 exceptions, and view information about read/write latency and the distribution of ISPs.

  For example, you can use the following statement to view access logs on your website:

  ```
  __topic__ : DDoS_acces s_log
  ```

- Track attack sources

  Access logs record information about the source and distribution of HTTP flood attacks. You can query and analyze access logs in real time to track attack sources, helping you select the most effective protection strategy.

  - For example, you can use the following statements to analyze the geographical distribution of HTTP flood attacks:

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

  - For example, use the following statement to view PVs:

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

- Analyze site 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 find the most visited webpages, the source IPs of the clients, the browsers that initiated the requests, and the distribution of client devices, which can help you analyze site operations.

  For example, you can use the following statements to view the distribution of traffic by ISP:

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

4.6.2 Fields

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

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

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

Field	Description	Example
real_client_ip	The actual IP address of the client. If the actual IP address is unavailable, - is displayed.	1.2.3.4
isp_line	The network 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
request_uri	The request path.	/answers/377971214/banner
server_name	The domain name in the request. If this field is empty, `default` is displayed.	api.abc.com
status	The HTTP status code.	200
time	The time when the log entry is written.	2018-05-02T16:03:59+08:00
cc_action	The action that is used to handle the request, such as none, challenge, pass, close, captcha, wait, login, and n.	close

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

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

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

4.7 Anti-DDoS packages

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

What is an anti-DDoS package

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

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

bandwidth and basic bandwidth. Click here to view *billing methods*. This method involves increased cost to maintain the security of your service.

- If you set the burstable bandwidth and basic bandwidth to the same value, when the attack bandwidth exceeds the basic bandwidth, the black hole is triggered and your service is interrupted till the black hole status is lifted. This method may affect the performance of your service but does not incur additional fees.

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

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

Notes

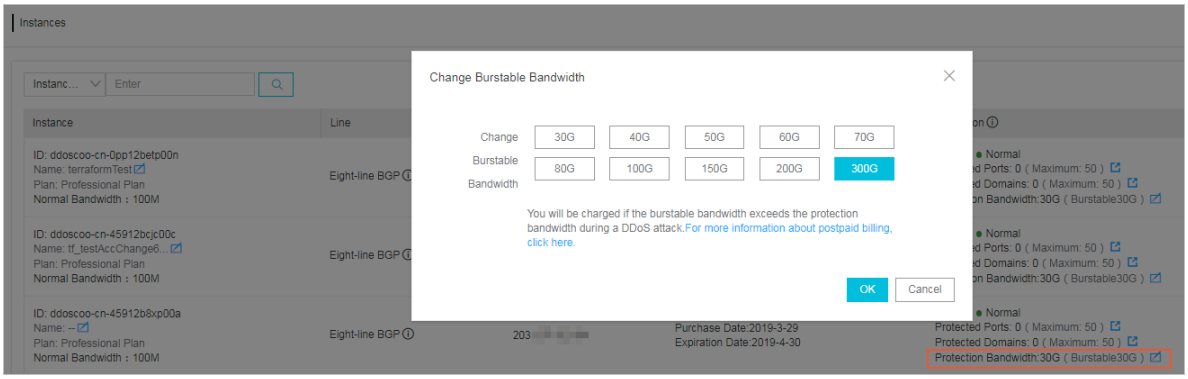
Note the following details when you use anti-DDoS packages:

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

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

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

For example, if your basic bandwidth is 30 Gbit/s and you have an anti-DDoS package with 300 Gbit/s bandwidth, we recommend that you set the burstable bandwidth to 330 Gbit/s.



- You can only use anti-DDoS packages to offset additional fees when the peak attack bandwidth is no greater than the sum of the basic bandwidth and anti-DDoS package bandwidth.
- When the number of available protections of your anti-DDoS package is reduced to zero, we recommend that you set the burstable bandwidth to the same as the basic bandwidth to avoid additional fees.
- You can only use anti-DDoS packages to offset additional fees that are billed no earlier than the day you obtained the anti-DDoS packages.

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

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

How to obtain anti-DDoS packages

Currently, anti-DDoS packages are provided to qualified users as a value-added service. If you meet one of the following conditions, you can contact customer service to obtain anti-DDoS packages for free:

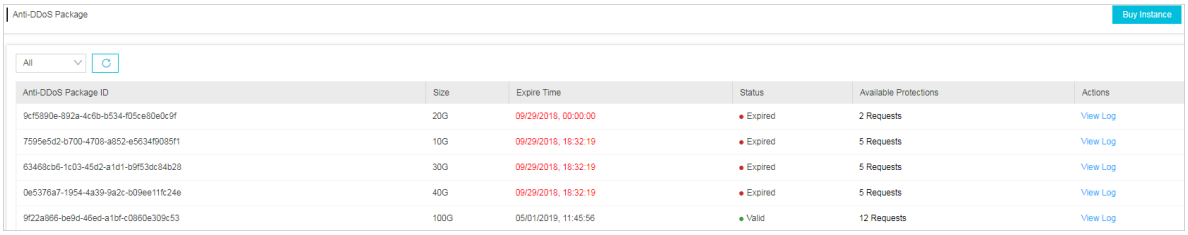
- It is the first time that you activated Anti-DDoS Pro.
- You have been continuously using Anti-DDoS Pro for three months or more.
- You have purchased a yearly subscription.

How to use anti-DDoS packages

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

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

1. Log on to the *Anti-DDoS Pro console*.
2. In the left-side navigation pane, choose Management > Anti-DDoS Package to view all anti-DDoS packages.
   - Anti-DDoS Package ID: The unique identifier of the anti-DDoS package.
   - Size: The bandwidth of the anti-DDoS package.
   - Expire Time: The expiration time of the anti-DDoS package.
   - Status: The anti-DDoS package status, including valid, exhausted, and expired.
   - Available Protections: The number of times you can use the anti-DDoS package.



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

4.8 Import and export configurations

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

- You can import and export layer 4 forwarding rules in TXT files.
- You can import and export domain configurations in XML files, which offer better compatibility. The XML format also provides better readability and extensibility than the TXT format. Meanwhile, you can import and export the configurations of websites that only have their origin server domain names specified.

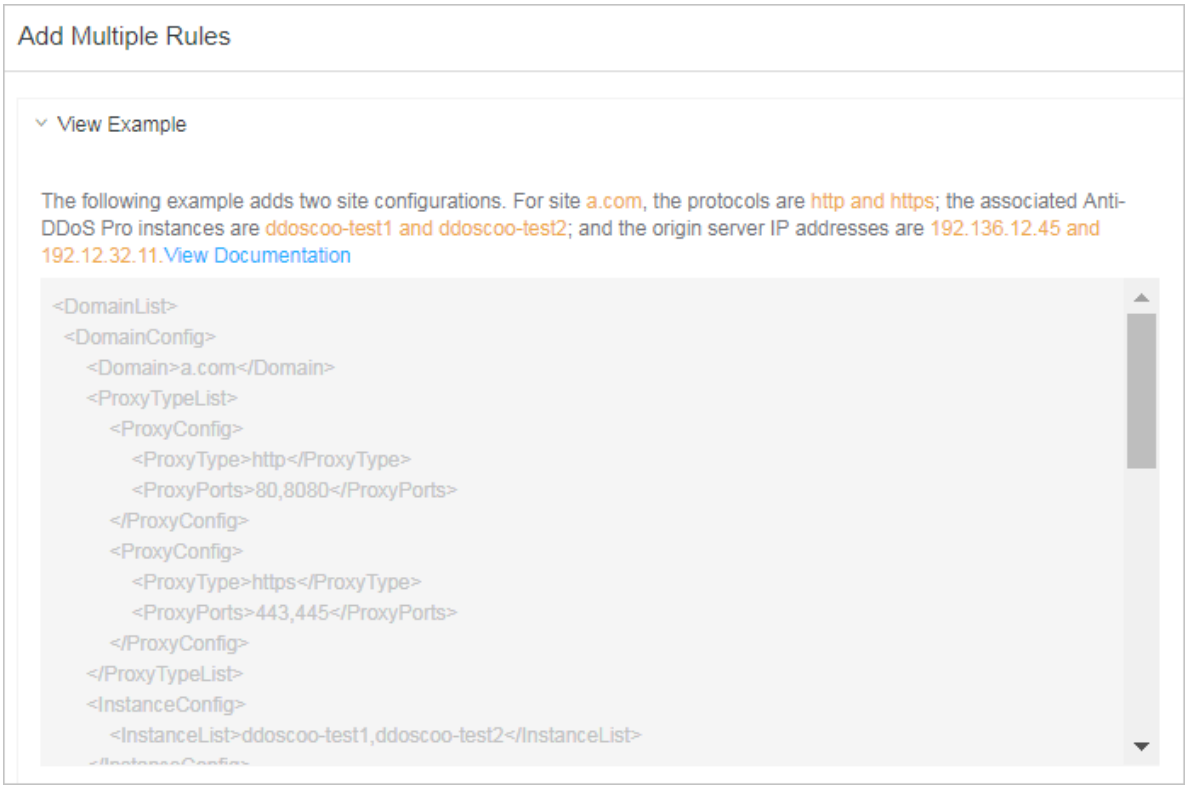
Batch import domain configurations

1. Log on to the *Anti-DDoS Pro console*.
2. In the left-side navigation pane, choose Management > Websites and click Batch Domains Import at the end of the website list to add multiple domain configurations.

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

Note:

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



XML format

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

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

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

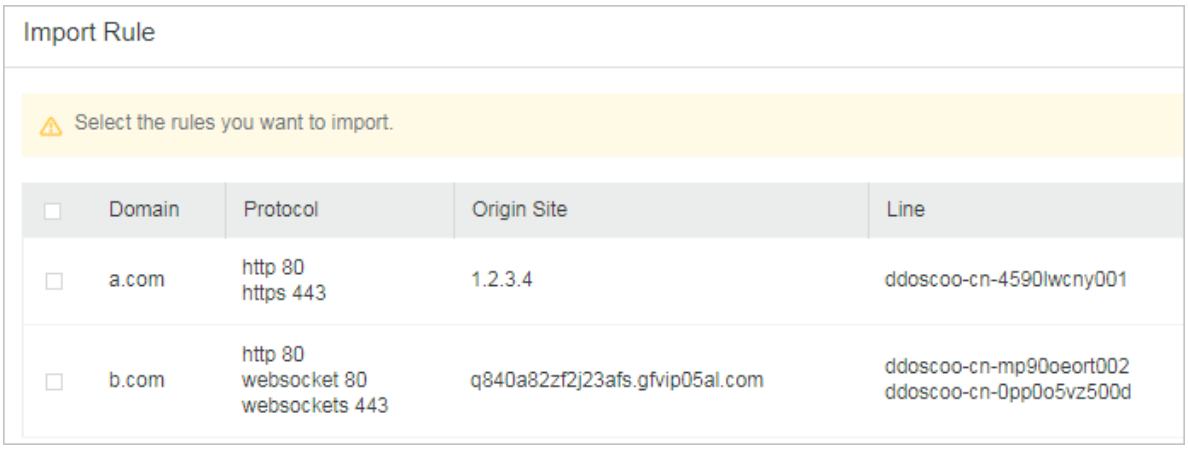
`< InstanceCo nfig >< InstanceLi st > ddoscoo - cn - 4590lwcny0 01 </ InstanceLi st ></ InstanceCo nfig >`	The Anti-DDoS Pro instance that is configured for the domain. **Note:** Each Anti-DDoS Pro instance has only one IP address. You can just enter the instance ID. Separate multiple instance IDs with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

Sample

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

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

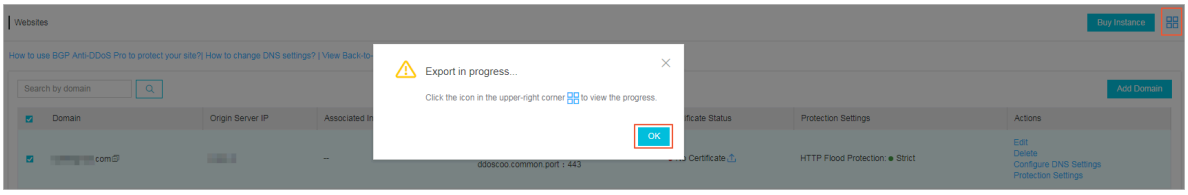
4. Click Next. If the XML file is correctly formatted, the domain configurations you have entered are displayed.



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

Batch export domain configurations

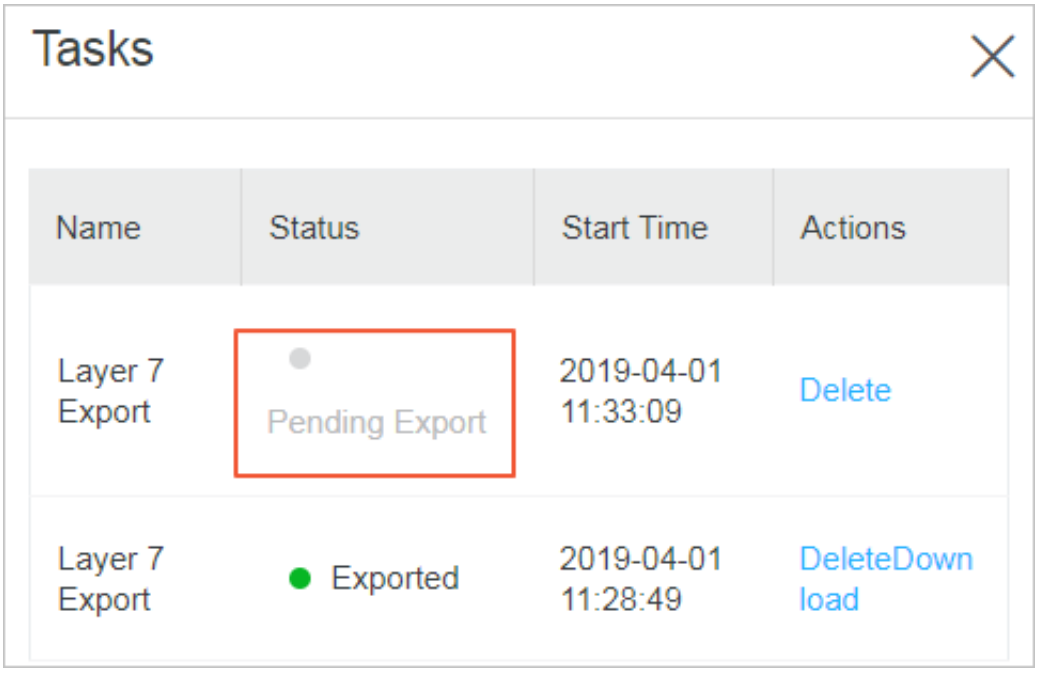
1. In the left-side navigation pane, choose Management > Websites and click Batch Domains Export at the end of the website list. In the dialog box that appears, click OK to export domain configurations.
2. On the Websites page, click the button in the upper-right corner to view the progress of the export task.



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

Note:

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

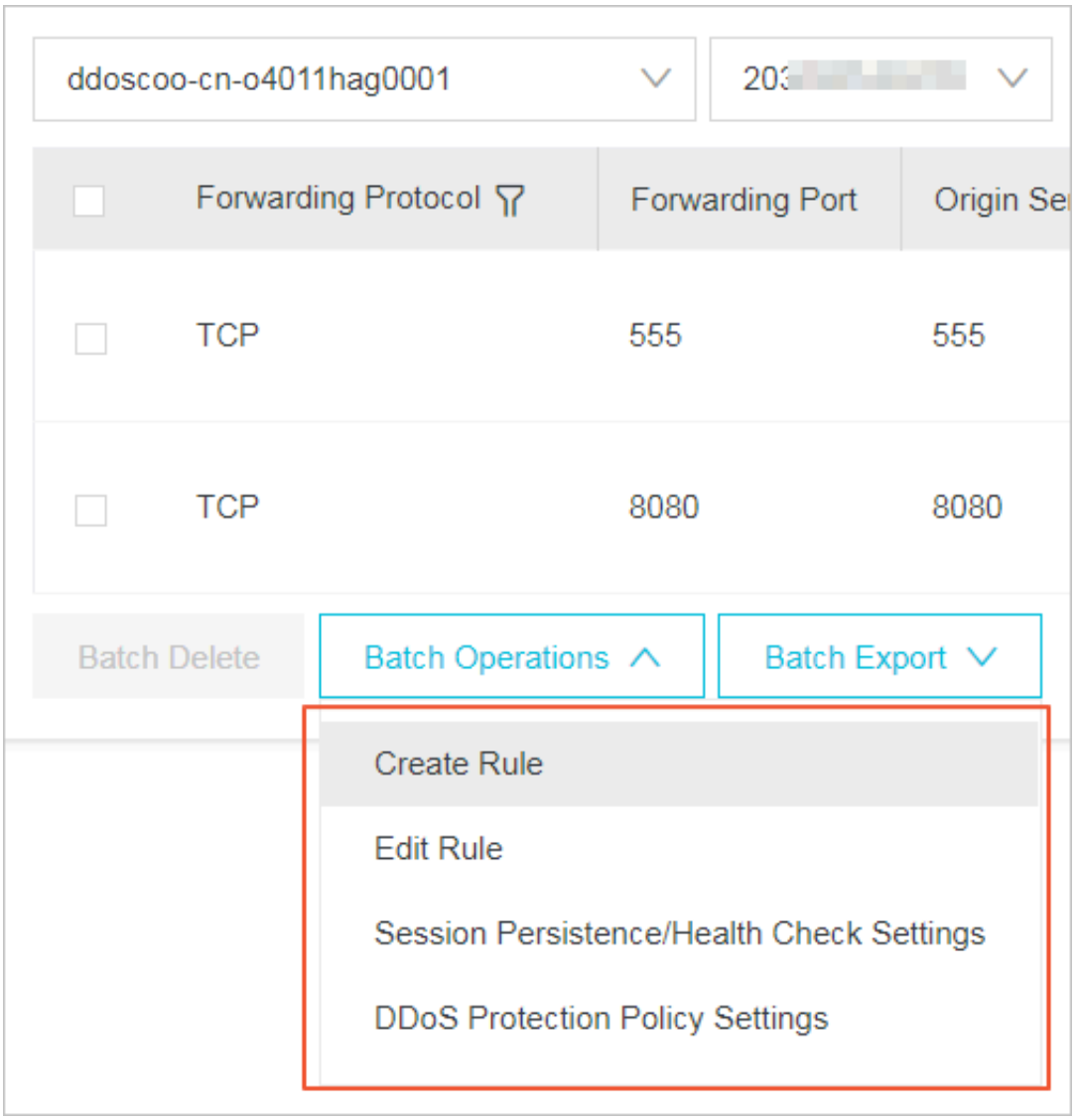


Batch import forwarding rules

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

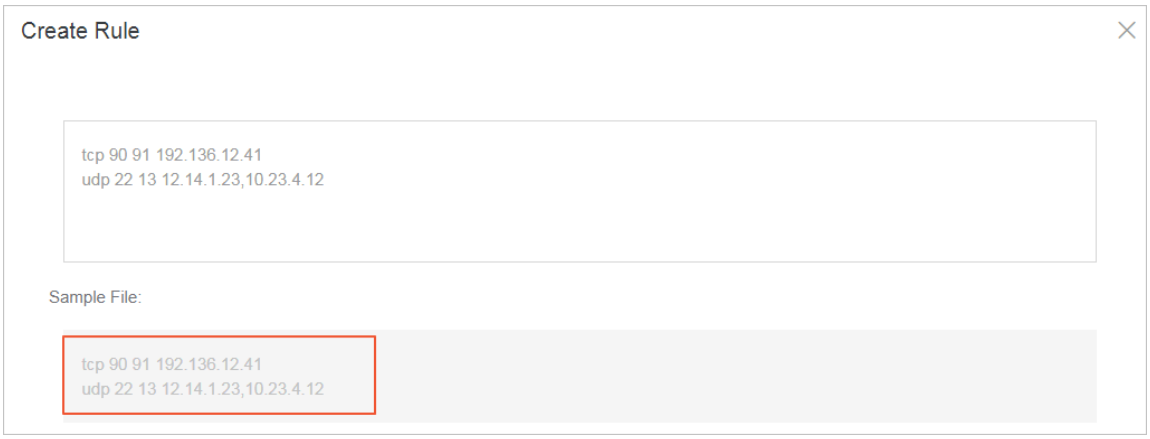
   Note:

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

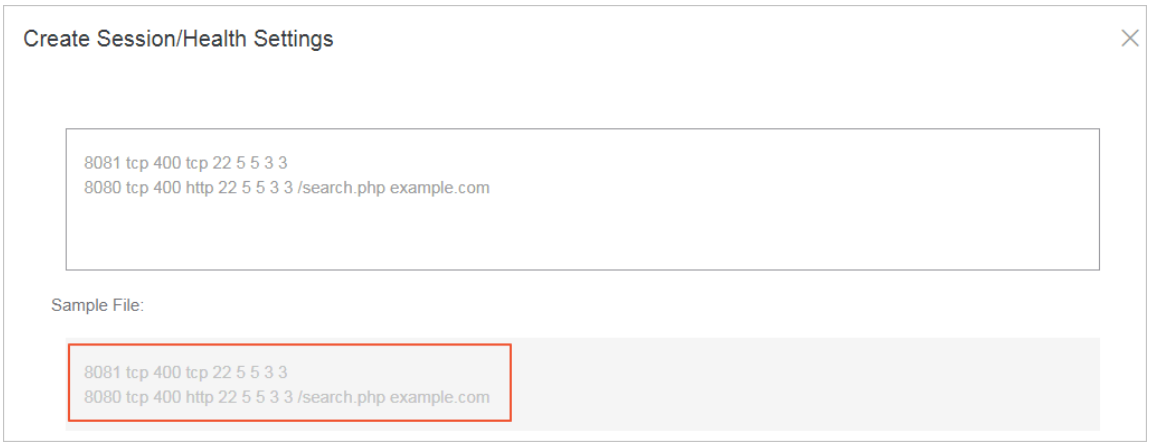


2. Follow the given examples to enter rules.

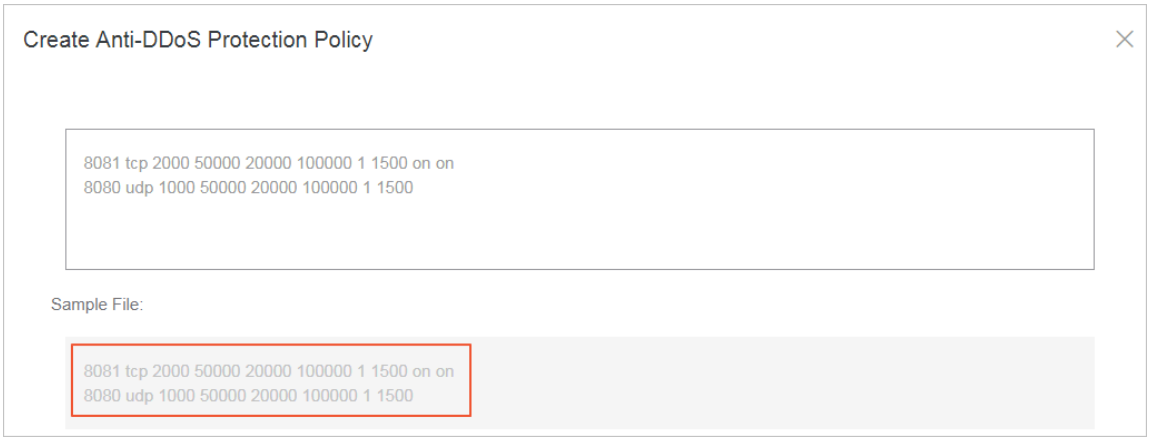
   - Create forwarding rules



   - Create session persistence/health check settings



   - Create anti-DDoS protection policies

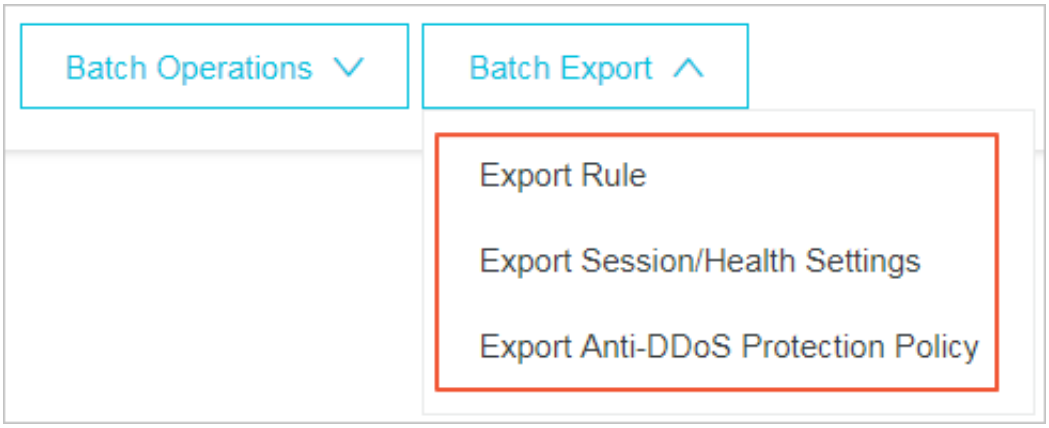


3. Click OK to add settings.

Batch export forwarding rules

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

   Note:
   You can also choose Export Session/Health Settings or Export Anti-DDoS Protection Policy to export corresponding settings.

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

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

4.9 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

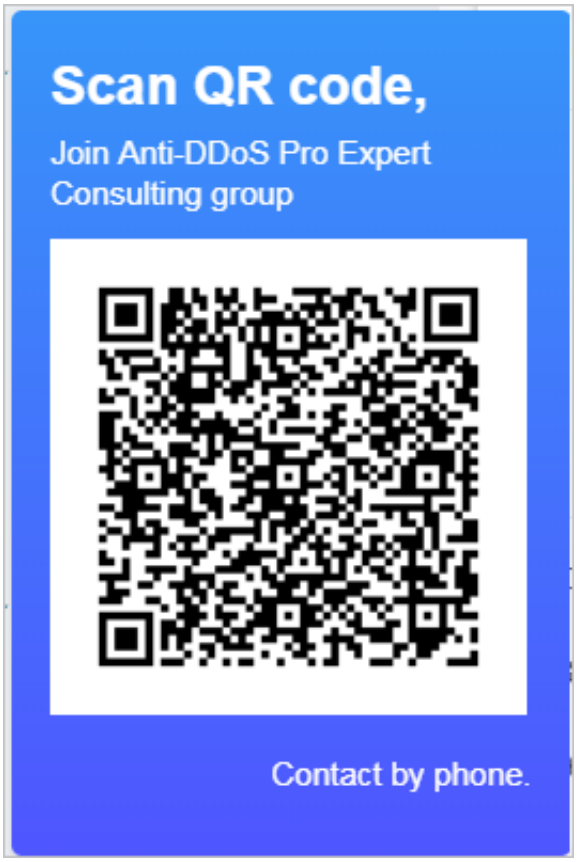
If you have any issues using Anti-DDoS Pro, join the Anti-DDoS Pro consulting group in DingTalk through the Anti-DDoS Pro console.

Our experienced secruity 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.

4.10 New protection policies