ALIBABA CLOUD

Alibaba Cloud

Anti-DDoS

Pricing

Document Version: 20220111

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	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.
Warning	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.
Notice	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.
Note	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 `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Billing methods of Anti-DDoS Origin

Anti-DDoS Origin is offered in two editions: Anti-DDoS Origin Basic and Anti-DDoS Origin Enterprise. Anti-DDoS Origin Basic provides a protection capability of up to 5 Gbit/s for the Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, elastic IP addresses (EIPs), and Web Application Firewall (WAF) instances under your Alibaba Cloud account. It is enabled by default and free of charge. Anti-DDoS Origin Enterprise provides unlimited protection against DDoS attacks for all your assets. It is billed on a yearly subscription basis. Protection is provided after you purchase an Anti-DDoS Origin Enterprise instance.

Instance specifications of Anti-DDoS Origin Enterprise

By default, Anti-DDoS Origin Enterprise provides shared and unlimited protection. Unlimited protection provides defense against DDoS attacks. The unlimited protection capability is based on the total number of available resources and strengthens with the increase of the overall network capability of Alibaba Cloud. The increased protection capability is provided free of charge.

Anti-DDoS Origin Enterprise supports the following subscription durations: one year, two years, and three years. The unit price of a yearly subscription Anti-DDoS Origin Enterprise instance varies based on the specific business scale and the number of IP addresses that you choose. Before you use Anti-DDoS Origin Enterprise, you must select instance specifications based on your business scale and complete the payment.

- **Business Scale**: specifies the scale of your business that you want to protect. The business scale is measured in bit/s based on the 95th percentile per month. Valid values: 100 Mbit/s, 300 Mbit/s, 500 Mbit/s, 800 Mbit/s, 1 Gbit/s, 1.5 Gbit/s, 2 Gbit/s, 2.5 Gbit/s, and 3 Gbit/s. For more information about how to determine your business scale, see Business scale estimation.
- **IP Addresses**: specifies the number of IP addresses that you want to protect. The default value is 100. Valid values range from 100 to 255.

Billing methods of Anti-DDoS Origin Enterprise

If you want to protect 100 IP addresses in a single region, the subscription fee for an Anti-DDoS Origin Enterprise instance in the region is calculated by using the following formula: Monthly unit price for the specific business scale × 12 (months) × Subscription duration (years)

If you want to protect more than 100 IP addresses in a single region, the subscription fee for an Anti-DDoS Origin Enterprise instance in the region is calculated by using the following formula: [Monthly unit price for the specific business scale + (Number of IP addresses that you want to protect - 100) × USD 30 per month] × 12 (months) × Subscription duration (years).

The following table lists the monthly unit prices for different business scales.

> **Note** By default, an Anti-DDoS Origin Enterprise instance provides protection for 100 IP addresses in a single region. If you want to protect more than 100 IP addresses, the unit price will be increased by USD 30 per month for each added IP address. If you want to protect IP addresses across regions, you must create multiple instances or submit a ticket to create an Anti-DDoS Origin Enterprise instance with custom specifications.

Prices that are listed in the following table may be different from those on the Anti-DDoS Origin buy page. The prices on the Anti-DDoS Origin buy page prevail.

Note The monthly price unit for an Anti-DDoS Origin Enterprise instance remains unchanged no matter whether IPv4 or IPv6 is used.

Business scale	Unit price (USD per month)
100 Mbit/s	7,016
300 Mbit/s	9,025
500 Mbit/s	11,034
800 Mbit/s	14,047
1 Gbit/s	16,056
1.5 Gbit/s	21,079
2 Gbit/s	26,101
2.5 Gbit/s	31,124
3 Gbit/s	36,146

Note The minimum business scale is 100 Mbit/s, which is also the default value. The maximum business scale is 3 Gbit/s. If the business scale that you specify exceeds 3 Gbit/s, we recommend that you submit a ticket to create an Anti-DDoS Origin Enterprise instance with custom specifications.

Business scale estimation

You can estimate a business scale or clean bandwidth by using the following method:

Sample inbound and outbound bandwidth at five-minute intervals. Calculate the average inbound and outbound bandwidth. Use the greater average value as the bandwidth of the sample point. At the end of each month, sort all sample points in descending order, ignore the top 5% of sample points, and use the first value of the remaining 95% of sample points is as the 95th percentile bandwidth.

Assume that the actual business bandwidth exceeds the clean bandwidth of an Anti-DDoS Origin Enterprise instance that you purchase.

Anti-DDoS Origin Enterprise allows your clean bandwidth to exceed the purchased business scale for a short period of time. If the period exceeds 36 hours, unlimited protection becomes invalid. Anti-DDoS Origin Enterprise imposes no limit on your clean bandwidth but provides only basic protection.

Refunds

Anti-DDoS Origin instances do not support the 5-day money-back guarantee refund.

Contact us

You can submit a ticket or contact your service manager to create an Anti-DDoS Origin Enterprise instance with custom specifications.

2.Billing methods of Anti-DDoS Pro

This topic describes the billing methods of Anti-DDoS Pro.

Overview

Anti-DDoS Pro provides **basic protection** and **burstable protection** to protect your services that are deployed in regions in mainland China against DDoS attacks. You are charged for these protection services based on the following billing methods:

- Basic protection: subscription (billed monthly)
  Before you use Anti-DDoS Pro, you must purchase an Anti-DDoS Pro instance. When you purchase an Anti-DDoS Pro instance, you must specify the specifications and the subscription period and complete the payment. The Anti-DDoS Pro instance provides basic protection within the specified subscription period.
  For example, if you purchase a basic protection bandwidth of 30 Gbit/s for an Anti-DDoS Pro instance and the peak bandwidth of DDoS attacks is no greater than 30 Gbit/s, basic protection is triggered, and no additional fees are generated.
- Burstable protection: pay-as-you-go (billed daily)
  You can enable burstable protection based on your business needs. To enable burstable protection, specify a burstable protection bandwidth that is greater than the basic protection bandwidth. If the bandwidth of DDoS attacks is greater than the basic protection bandwidth but is less than the burstable protection bandwidth, burstable protection is triggered to mitigate the DDoS attacks. You are charged for the usage of burstable protection.
  For example, the basic protection bandwidth of your Anti-DDoS Pro instance is 30 Gbit/s and the burstable protection bandwidth is 100 Gbit/s. If the peak bandwidth of DDoS attacks is no greater than 30 Gbit/s or exceeds 100 Gbit/s, burstable protection is not triggered, and no fees are generated for burstable protection. If the peak bandwidth of DDoS attacks is between 30 Gbit/s and 100 Gbit/s, burstable protection is triggered, and fees are generated for burstable protection.

For more information, visit the Anti-DDoS pricing page.

Basic protection: subscription (billed monthly)

The following table lists the prices of an Anti-DDoS Pro instance based on different basic protection bandwidths when the default specifications are used. Anti-DDoS Pro provides the Standard and Enhanced function plans. The prices vary based on the function plan. For more information about the Standard and Enhanced function plans, see Function plan.

> **Note** If the protection bandwidths listed in the following table cannot meet your business needs, submit a ticket.

Basic protection bandwidth	Line	Unit price for the Standard function plan	Unit price for the Enhanced function plan
30 Gbit/s		USD 3,120/month	USD 4,320/month
60 Gbit/s		USD 7,020/month	USD 8,220/month
100 Gbit/s		USD 49,230/year (including yearly subscription discount)	USD 63,630/year (including yearly subscription discount)

Basic protection bandwidth	Line Eight BGP lines	Unit price for the Standard function plan	Unit price for the Enhanced function plan
300 Gbit/s		USD 79,260/year (including yearly subscription discount)	USD 93,660/year (including yearly subscription discount)
400 Gbit/s		USD 145,300/year (including yearly subscription discount)	USD 159,700/year (including yearly subscription discount)
500 Gbit/s		USD 563,430/year (including yearly subscription discount)	USD 577,830/year (including yearly subscription discount)
600 Gbit/s		USD 670,610/year (including yearly subscription discount)	USD 685,010/year (including yearly subscription discount)

The following table lists the default specifications of an Anti-DDoS Pro instance and the prices for upgrades. If the default specifications cannot meet your business needs, you can choose higher specifications when you purchase the instance. You can also upgrade the instance after you purchase it.

Item	Description	Default value	Price for upgrades
Number of protected ports	The number of TCP and UDP ports that the instance can protect	50	Price for every five ports: USD 37.5/month
Number of protected domain names	The number of HTTP and HTTPS domain names that the instance can protect	50 **Note** The domain names that you add to an instance can belong to a maximum of five second-level domain names.	• Price for every 10 domain names in the Standard function plan: USD 45/month • Price for every 10 domain names in the Enhanced function plan: USD 75 /month **Note** For every 10 additional domain names, the total number of second-level domain names that are supported is increased by one.

Item	Description	Default value	Price for upgrades
Clean bandwidth	The maximum bandwidth that the instance uses to manage service traffic if no attacks occur	100 Mbit/s	Price for every Mbit/s:USD 15 /month Note If your clean bandwidth exceeds 600 Mbit/s, you are charged for the bandwidth over 600 Mbit/s. The additional fees are added to your regular monthly fee. The unit price per additional Mbit/s is USD 11 per month.
Queries per second (QPS)	The maximum number of HTTP and HTTPS requests that the instance can concurrently process per second if no attacks occur	3,000 QPS	Price for every 100 QPS: USD 150/month

Burstable protection: pay-as-you-go (billed daily)

Anti-DDoS Pro provides burstable protection to protect your services when the peak bandwidth of DDoS attacks exceeds the basic protection bandwidth but is less than the burstable protection bandwidth. The usage of burstable protection is charged based on the difference between the peak bandwidth of DDoS attacks on the day and the basic protection bandwidth.

> **Note** If you specify the same value for the burstable protection bandwidth and the basic protection bandwidth, your Anti-DDoS Pro instance does not provide burstable protection, and no additional fees are generated.

Billing:

- If the peak bandwidth of DDoS attacks on the day is no greater than the basic protection bandwidth, burstable protection is not triggered, and no fees are generated for burstable protection.

- If the peak bandwidth of DDoS attacks on the day is greater than the burstable protection bandwidth, burstable protection is not triggered, and no fees are generated for burstable protection. In this case, if DDoS attacks on the day trigger blackhole filtering for the IP address that is protected by an Anti-DDoS Pro instance, no fees are generated for burstable protection.
- The bill for burstable protection each day is generated between 08:00 to 09:00 the following day.

For example, the basic protection bandwidth of your Anti-DDoS Pro instance is 30 Gbit/s and the burstable protection bandwidth is 100 Gbit/s. Two DDoS attacks are launched against the instance on the same day. The peak bandwidths of the two DDoS attacks are 80 Gbit/s and 40 Gbit/s, both of which exceed the basic protection bandwidth. You are charged for the usage of burstable protection based on the higher peak bandwidth (80 Gbit/s). The difference between the peak bandwidth and basic protection bandwidth (30 Gbit/s) is 50 Gbit/s. Based on the pricing tiers listed in the following table, the fee generated for burstable protection on the day is USD 960.

The following table lists prices of burstable protection based on different pricing tiers.

Pricing tier	Price for burstable protection (Unit: USD/day)
0 Gbit/s < Bandwidth difference ≤ 5 Gbit/s	120
5 Gbit/s < Bandwidth difference ≤ 10 Gbit/s	180
10 Gbit/s < Bandwidth difference ≤ 20 Gbit/s	330
20 Gbit/s < Bandwidth difference ≤ 30 Gbit/s	540
30 Gbit/s < Bandwidth difference ≤ 40 Gbit/s	730
40 Gbit/s < Bandwidth difference ≤ 50 Gbit/s	960
50 Gbit/s < Bandwidth difference ≤ 60 Gbit/s	1,170
60 Gbit/s < Bandwidth difference ≤ 70 Gbit/s	1,380
70 Gbit/s < Bandwidth difference ≤ 80 Gbit/s	1,590
80 Gbit/s < Bandwidth difference ≤ 100 Gbit/s	1,770
100 Gbit/s < Bandwidth difference ≤ 150 Gbit/s	2,190
150 Gbit/s < Bandwidth difference ≤ 200 Gbit/s	3,240

Pricing tier	Price for burstable protection (Unit: USD/day)
200 Gbit/s < Bandwidth difference ≤ 300 Gbit/s	4,200
300 Gbit/s < Bandwidth difference ≤ 400 Gbit/s	6,000
400 Gbit/s < Bandwidth difference ≤ 500 Gbit/s	7,510
500 Gbit/s < Bandwidth difference ≤ 600 Gbit/s	9,010
600 Gbit/s < Bandwidth difference ≤ 700 Gbit/s	10,510
700 Gbit/s < Bandwidth difference ≤ 800 Gbit/s	12,010
800 Gbit/s < Bandwidth difference ≤ 900 Gbit/s	13,510
900 Gbit/s < Bandwidth difference ≤ 1,000 Gbit/s	15,010
1,000 Gbit/s < Bandwidth difference ≤ 1,100 Gbit/s	16,510
1,100 Gbit/s < Bandwidth difference ≤ 1,200 Gbit/s	18,010
1,200 Gbit/s < Bandwidth difference ≤ 1,300 Gbit/s	19,510
1,300 Gbit/s < Bandwidth difference ≤ 1,400 Gbit/s	21,010
1,400 Gbit/s < Bandwidth difference ≤ 1,500 Gbit/s	22,520

Instance expiration

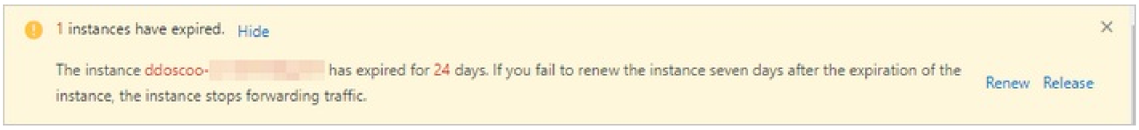
If you do not renew your Anti-DDoS Pro instance in time after the instance expires, your services are adversely affected. The following table describes the impacts.

Time period	Protection capability	Traffic forwarding	Instance configuration
From the expiration date to 7 calendar days (excluded) after the expiration date	The instance provides only the basic protection against attacks of 5 Gbit/s. If you renew your instance within this time period, the instance continues to provide the protection capabilities based on the plan that you purchased.	The instance still forwards service traffic.	Instance configurations are retained.

Time period	Protection capability	Traffic forwarding	Instance configuration
7 calendar days (included) after the expiration date to 15 calendar days (excluded) after the expiration date	The instance provides only the basic protection against attacks of 5 Gbit/s.	The instance no longer forwards service traffic. **Warning** If you no longer need Anti-DDoS Pro, you must switch service traffic from the Anti-DDoS Pro instance to the origin server seven calendar days before the expiration date. Otherwise, access to your services may be adversely affected. If you want to switch service traffic, make sure that the domain name of your website does not map to the CNAME assigned by Anti-DDoS Pro. You must also make sure that your non-website service does not use an exclusive IP address provided by the instance. If you renew your instance within this time period, the instance continues to forward service traffic, and you do not need to configure the instance again.	Instance configurations are retained.

Time period	Protection capability	Traffic forwarding	Instance configuration
15 calendar days (included) after the expiration date to later points in time	The instance provides only the basic protection against attacks of 5 Gbit/s.	The instance no longer forwards service traffic.	The Anti-DDoS Pro instance is released. **Warning** After all Anti-DDoS Pro instances that are created by using your Alibaba Cloud account are released, the configurations that are added to Anti-DDoS Pro, such as website access configurations, port access configurations, mitigation settings, and reports, are deleted and cannot be restored. If you want to use Anti-DDoS Pro again, you must purchase and configure another Anti-DDoS Pro instance.

Notice We recommend that you carefully read the instance expiration prompt that is displayed in the Anti-DDoS Pro console. Then, renew the instance in time or set auto-renewal for the instance to prevent negative impacts on your services.



1 instances have expired.

The instance ddoscoo-[redacted] has expired for 24 days. If you fail to renew the instance seven days after the expiration of the instance, the instance stops forwarding traffic.

Refunds

The subscription of a subscription Anti-DDoS Pro instance cannot be canceled before the expiration date. The 5-day money-back guarantee is not provided for the subscription. After an Anti-DDoS Pro instance is created, the fees you paid cannot be refunded.

References

- Purchase an Anti-DDoS Pro instance
- Upgrade an instance
- Renew an instance

3.Anti-DDoS premium billing methods

3.1. Billing methods of the Insurance and Unlimited mitigation plans

This topic describes the billing methods of the Anti-DDoS Premium Insurance and Unlimited mitigation plans.

Overview

Anti-DDoS Premium provides **advanced mitigation**[1] to protect your services that are deployed in regions outside the Chinese mainland against DDoS attacks. The number of advanced mitigation sessions that you can use varies based on the mitigation plan that you purchase. You can purchase the **Insurance**[2] or **Unlimited**[3] mitigation plan.

Anti-DDoS Premium supports only the **subscription** billing method. Before you use Anti-DDoS Premium, you must purchase an Anti-DDoS Premium instance. When you purchase an Anti-DDoS Premium instance, you must specify the mitigation plan, instance specifications, and subscription period and complete the payment. The Anti-DDoS Premium instance provides advanced mitigation within the subscription period that you specify.

[1] *Advanced mitigation*

Advanced mitigation integrates with all Alibaba Cloud Anti-DDoS scrubbing centers outside the Chinese mainland to protect your services against DDoS attacks. Advanced mitigation provides unlimited protection.

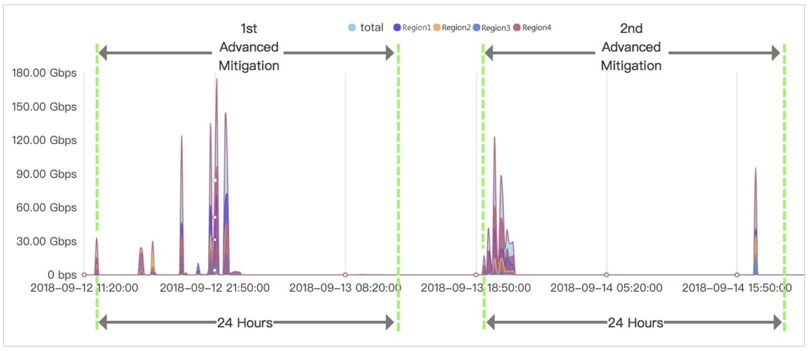
Services that are protected by Anti-DDoS Premium are less vulnerable to DDoS attacks. In most cases, the goal of DDoS attacks is to disrupt your services. The cost of launching a DDoS attack is relatively high. If attackers cannot achieve their goal within the time frame, they stop their attacks. Anti-DDoS Premium provides unlimited advanced mitigation and integrates with all Alibaba Cloud Anti-DDoS scrubbing centers outside the Chinese mainland to protect your services.

> **Notice** If the attacks that are launched against your services threaten the infrastructure of the Anti-DDoS scrubbing centers, Alibaba Cloud reserves the rights to throttle network traffic. If throttling is triggered for your Anti-DDoS Premium instance, your services may be adversely affected. For example, the network traffic may be throttled or blackhole filtering may be triggered.

[2] *Insurance mitigation plan*

The Insurance mitigation plan is a basic mitigation plan of Anti-DDoS Premium. The Insurance mitigation plan provides two advanced mitigation sessions per month and is suitable for users who are less likely to be targeted. If DDoS attacks are detected, advanced mitigation is triggered and one advanced mitigation session is consumed to provide unlimited protection over the next 24 hours. The number of advanced mitigation sessions that are available is automatically reset to two on the first day of each month.

For example, a volumetric DDoS attack was detected on a protected IP address at 11:20:00 on September 12 (UTC+8), and advanced mitigation was triggered. One advanced mitigation session was consumed to provide unlimited protection for the IP address over the next 24 hours. Then, another volumetric DDoS attack was detected on the same IP address at 18:50:00 on September 13 (UTC+8), and advanced mitigation is triggered. Another advanced mitigation session was consumed because this attack happened 24 hours after the first attack. In this case, the two sessions included in the Insurance mitigation plan for September were exhausted. The number of advanced mitigation sessions that are available is reset to two on October 1.



Note If the two advanced mitigation sessions that are provided per month cannot meet your business requirements, we recommend that you purchase global advanced mitigation. For more information, see Billing methods of global advanced mitigation sessions.

[3]Unlimited mitigation plan

The Unlimited mitigation plan provides unlimited advanced mitigation sessions. If you purchase the Unlimited mitigation plan, Anti-DDoS Premium provides unlimited protection to protect your services against DDoS attacks at all times.

Pricing

The following table describes the prices of an Anti-DDoS Premium instance with default specifications at different **clean bandwidths**[4]. Anti-DDoS Premium provides the Standard and Enhanced function plans. The prices vary based on the function plan. For more information about the Standard and Enhanced function plans, see Function plan.

[4]Clean bandwidth

Clean bandwidth specifies the maximum bandwidth that an Anti-DDoS Premium instance can use to manage service traffic if no attacks occur. The clean bandwidth of an instance must be greater than the peak volume between the inbound and outbound traffic of protected services.

Warning If the actual bandwidth exceeds the clean bandwidth of the instance, throttling and packet loss may occur. In this case, your services may become unavailable, respond slowly, or have high latency for a period of time.

Note If the clean bandwidths that are listed in the following table cannot meet your business requirements, submit a ticket.

Mitigation plan	Clean bandwidth	Unit price of the Standard function plan (USD/month)	Unit price of the Enhanced function plan (USD/month)
Insurance Two advanced mitigation sessions per month **Note** You can purchase global advanced mitigation sessions to obtain more advanced mitigation sessions. For more information, see Billing methods of global advanced mitigation sessions.	100 Mbit/s	2,630	3,830
	150 Mbit/s	3,420	4,620
	200 Mbit/s	4,210	5,410
	250 Mbit/s	5,000	6,200
	300 Mbit/s	5,570	6,770
Unlimited Unlimited advanced mitigation sessions	100 Mbit/s	11,560	12,760
	150 Mbit/s	12,610	13,810
	200 Mbit/s	13,660	14,860
	250 Mbit/s	14,720	15,920
	300 Mbit/s	15,770	16,970

The following table describes the default specifications of an Anti-DDoS Premium instance and the prices for upgrades. If the default specifications cannot meet your business requirements, you can select higher specifications when you purchase the instance. You can also upgrade the instance after you purchase it.

Item	Description	Default value	Price for upgrades
Number of protected ports	The number of TCP and UDP ports that the instance can protect	5	Price for every five ports: USD 150/month
Number of protected domain names	The number of HTTP and HTTPS domain names that the instance can protect	10 **Note** You can add one second-level domain name and nine subdomains of this second-level domain name. Alternatively, you can add 10 domain names that belong to a second-level domain name.	- Price for every 10 domain names in the Standard function plan: USD 45/month - Price for every 10 domain names in the Enhanced function plan: USD 75 /month **Note** For every 10 additional domain names, the total number of second-level domain names that are supported is increased by one.
Queries per second (QPS)	The maximum number of HTTP and HTTPS requests that the instance can concurrently process per second if no attacks occur	- Insurance mitigation plan: 500 - Unlimited mitigation plan: 1,000	Price for every 100 QPS: USD 150/month

Instance expiration

If you do not renew your Anti-DDoS Premium instance in time after the instance expires, your services are adversely affected. The following table describes the impacts.

Time period	Protection capability	Traffic forwarding	Instance configuration
From the expiration date to 30 (excluded) calendar days after the expiration date	The instance provides only the basic protection against attacks of 5 Gbit/s. If you renew your instance within this time period, the instance continues to provide the protection capabilities based on the plan that you purchased.	The instance still forwards service traffic.	Instance configurations are retained.

Time period	Protection capability	Traffic forwarding	Instance configuration
30 (included) calendar days after the expiration date to later points in time	The instance provides only the basic protection against attacks of 5 Gbit/s.	The instance no longer forwards service traffic. 🔔 **Warning** If you no longer need Anti-DDoS Premium, you must switch service traffic from the Anti-DDoS Premium instance to the origin server 30 calendar days before the expiration date. Otherwise, access to your services may be adversely affected. If you want to switch service traffic, make sure that the domain name of your website does not map to the CNAME assigned by Anti-DDoS Premium. You must also make sure that your non-website service does not use an exclusive IP address provided by the instance.	The Anti-DDoS Premium instance is released. 🔔 **Warning** After all Anti-DDoS Premium instances that are created by using your Alibaba Cloud account are released, the configurations that are added to Anti-DDoS Premium, such as website access configurations, port access configurations, mitigation settings, and reports, are deleted and cannot be restored. If you want to use Anti-DDoS Premium again, you must purchase and configure another Anti-DDoS Premium instance.

Refunds

You cannot cancel the subscription of an Anti-DDoS Premium instance before the expiration date. The 5-day money-back guarantee does not apply to subscription Anti-DDoS Premium instances. After you create an Anti-DDoS Premium instance, you cannot request a refund of the fees that you paid.

Related information

- Purchase an Anti-DDoS Premium instance of the Insurance or Unlimited plan
- Purchase global advanced mitigation sessions
- Upgrade an instance
- Renew an instance

3.2. Mainland China Acceleration billing methods

This topic describes the billing methods of Anti-DDoS Premium Mainland China Acceleration (MCA). Before you use MCA, you must purchase an Anti-DDoS Premium instance. You can purchase an Anti-DDoS Premium instance to defend against DDoS attacks for services that are deployed outside mainland China. If no attacks are launched, you can use MCA to accelerate service delivery to users in mainland China.

Overview

MCA is suitable for services that are deployed in regions outside mainland China and are protected by Anti-DDoS Premium. If no attack is launched against your Anti-DDoS Premium instance, you can use MCA to accelerate service delivery to users in mainland China.

> **Notice** An MCA instance does not offer any protection and must be used with an Anti-DDoS Premium Insurance Plan or Unlimited Plan instance.

MCA instances support only the **subscription** billing method. Before you use MCA, you must purchase an MCA instance, and specify the specifications and the subscription period. An MCA instance provides acceleration for services that are added to Anti-DDoS Premium within the subscription period.

Pricing

The following table lists the prices of an MCA instance based on different **clean bandwidths**[1].

[1] *Clean bandwidth*

Clean bandwidth refers to the maximum bandwidth that an MCA instance can use to accelerate service delivery if no attacks are launched. The clean bandwidth of an MCA instance must be greater than the peak volume of the inbound and outbound traffic of the protected services.

> **Warning** If the actual bandwidth exceeds the clean bandwidth of the instance, throttling and packet loss can occur. In some cases, your services become unavailable or slow down within a period of time.

Clean bandwidth	Unit price (USD/month)
10 Mbit/s	1,548

Clean bandwidth	Unit price (USD/month)
20 Mbit/s	3,096
30 Mbit/s	4,643
40 Mbit/s	6,191
50 Mbit/s	7,739
60 Mbit/s	9,287
70 Mbit/s	10,834
80 Mbit/s	12,382
90 Mbit/s	13,930
100 Mbit/s	15,478

Instance expiration

Instance status	Description
Before expiration	Alibaba Cloud sends you text messages and emails seven days, three days, and one day before your instance expires to remind you to renew your subscription.
Within 30 days after expiration	• Impact on acceleration: You must renew the subscription of your MCA instance before the expiration date. After the MCA instance expires, it stops accelerating service delivery. • Impact on instance configurations: The configurations of an expired MCA instance are retained for 30 days. To continue using the MCA instance with the retained configurations, renew the subscription of your MCA instance within 30 days after the expiration date.
30 days after expiration	If you do not renew the subscription of your MCA instance within 30 days after the instance expires, the instance and the instance configurations are automatically released. To continue using the acceleration service, you must purchase another MCA instance.

References

- Purchase an Anti-DDoS Premium instance of the MCA plan
- Configure Anti-DDoS Premium MCA

3.3. Sec-MCA billing methods

This topic describes the billing methods of the Anti-DDoS Premium Secure Mainland China Acceleration (Sec-MCA) mitigation plan.

Overview

The Sec-MCA mitigation plan of Anti-DDoS Premium supports only the **subscription** billing method. Before you use the Sec-MCA mitigation plan, you must purchase an Anti-DDoS Premium instance. When you purchase an Anti-DDoS Premium instance, you must select the Sec-MCA mitigation plan, instance specifications, and subscription period and complete the payment. An Anti-DDoS Premium instance of the Sec-MCA mitigation plan provides access acceleration and DDoS mitigation services within the subscription period.

Pricing

The following table describes the prices of an Anti-DDoS Premium instance of the Sec-MCA mitigation plan with the default specifications at different An Anti-DDoS Premium instance of the Sec-MCA mitigation plan provides the Standard and Enhanced function plans. The prices vary based on the function plan. For more information about the Standard and Enhanced function plans, see Function plan. clean bandwidths

Warning The clean bandwidth of an instance must be greater than the peak volume between the inbound and outbound traffic of protected services.

If the actual bandwidth exceeds the clean bandwidth of the instance, throttling and packet loss may occur. In this case, your services may become unavailable, respond slowly, or have high latency for a period of time.

If the clean bandwidths listed in the following table cannot meet your business requirements, submit a ticket.

Mitigation plan	Clean bandwidth	Unit price of the Standard function plan (USD/month)	Unit price of the Enhanced function plan (USD/month)
Sec-MCA Two advanced mitigation sessions per calendar month **Note** You can purchase global advanced mitigation sessions to obtain more advanced mitigation sessions. For more information, see Billing methods of global advanced mitigation sessions.	10 Mbit/s	15,480	16,680
	20 Mbit/s	17,028	18,228
	30 Mbit/s	18,576	19,776
	40 Mbit/s	20,124	21,324
	50 Mbit/s	21,672	22,872
	60 Mbit/s	23,220	24,420
	70 Mbit/s	24,768	25,968
	80 Mbit/s	26,316	27,516
	90 Mbit/s	27,864	29,064
	100 Mbit/s	29,412	30,612
	150 Mbit/s	37,152	38,352
	200 Mbit/s	44,892	46,092

The following table describes the default specifications of an Anti-DDoS Premium instance of the Sec-MCA mitigation plan and the prices for upgrades. If the default specifications cannot meet your business requirements, you can select higher specifications when you purchase the instance. You can also upgrade the instance after you purchase it.

Item	Description	Default value	Price for upgrades
Number of protected ports	The number of TCP and UDP ports that the instance can protect	5	Price for every five ports: USD 150/month
Number of protected domain names	The number of HTTP and HTTPS domain names that the instance can protect	10 **Note** You can add one second-level domain name and nine subdomains of this second-level domain name. Alternatively, you can add 10 domain names that belong to a second-level domain name.	• Price for every 10 domain names in the Standard function plan: USD 45/month • Price for every 10 domain names in the Enhanced function plan: USD 75 /month **Note** For every 10 additional domain names, the total number of second-level domain names that are supported is increased by one.
Queries per second (QPS)	The maximum number of HTTP and HTTPS requests that the instance can concurrently process per second if no attacks occur	500 QPS	Price for every 100 QPS: USD 150/month

Instance expiration

If you do not renew your Anti-DDoS Premium instance in time after the instance expires, your services are adversely affected. The following table describes the impacts.

Time period	Protection capability	Traffic forwarding	Instance configuration
From the expiration date to 30 (excluded) calendar days after the expiration date	The instance provides only the basic protection against attacks of 5 Gbit/s. If you renew your instance within this time period, the instance continues to provide the protection capabilities based on the plan that you purchased.	The instance still forwards service traffic.	Instance configurations are retained.

Time period	Protection capability	Traffic forwarding	Instance configuration
30 (included) calendar days after the expiration date to later points in time	The instance provides only the basic protection against attacks of 5 Gbit/s.	The instance no longer forwards service traffic. **Warning** If you no longer need Anti-DDoS Premium, you must switch service traffic from the Anti-DDoS Premium instance to the origin server 30 calendar days before the expiration date. Otherwise, access to your services may be adversely affected. If you want to switch service traffic, make sure that the domain name of your website does not map to the CNAME assigned by Anti-DDoS Premium. You must also make sure that your non-website service does not use an exclusive IP address provided by the instance.	The Anti-DDoS Premium instance is released. **Warning** After all Anti-DDoS Premium instances that are created by using your Alibaba Cloud account are released, the configurations that are added to Anti-DDoS Premium, such as website access configurations, port access configurations, mitigation settings, and reports, are deleted and cannot be restored. If you want to use Anti-DDoS Premium again, you must purchase and configure another Anti-DDoS Premium instance.

Refunds

You cannot cancel the subscription of an Anti-DDoS Premium instance before the expiration date. The 5-day money-back guarantee does not apply to subscription Anti-DDoS Premium instances. After you create an Anti-DDoS Premium instance, you cannot request a refund of the fees that you paid.

Related information

- Purchase an Anti-DDoS Premium instance of the Sec-MCA plan
- Configure Anti-DDoS Premium Sec-MCA
- Purchase global advanced mitigation sessions

3.4. Billing methods of global advanced mitigation sessions

This topic describes the billing methods of global advanced mitigation sessions of Anti-DDoS Premium.

Global advanced mitigation session

Global advanced mitigation sessions are used to increase the number of advanced mitigation sessions of an Anti-DDoS Premium instance of the Insurance mitigation plan or of the Secure Mainland China Acceleration (Sec-MCA) mitigation plan.

An Anti-DDoS Premium instance of the Insurance mitigation plan or of the Sec-MCA mitigation plan provides two advanced mitigation sessions free of charge per month. If the two advanced mitigation sessions that are provided each month cannot meet your business requirements, we recommend that you purchase global advanced mitigation sessions. The following table describes the types of global advanced mitigation sessions.

Type	Protection scope	Validity period	Number of advanced mitigation sessions
Global advanced mitigation session for the Insurance mitigation plan	Services protected by all valid Anti-DDoS Premium instances of the Insurance mitigation plan within your Alibaba Cloud account	One year	Each Alibaba Cloud account can use advanced mitigation sessions up to 20 times per month. The advanced mitigation sessions include the advanced mitigation sessions that are provided free of charge and the global advanced mitigation sessions that you purchase.
Global advanced mitigation session for the Sec-MCA mitigation plan	Services protected by all valid Anti-DDoS Premium instances of the Sec-MCA mitigation plan within the Alibaba Cloud account	One year	

For more information about global advanced mitigation sessions, see Method to use global advanced mitigation sessions.

Overview

Global advanced mitigation sessions use the subscription billing method.

You must specify the number of global advanced mitigation sessions when you purchase the sessions. After you complete the payment, you can use the global advanced mitigation sessions that you purchase within the validity period of the sessions.

By default, the validity period is one year.

Pricing

The unit prices of global advanced mitigation sessions vary based on the types of global advanced mitigation sessions.

- Global advanced mitigation session for the Insurance mitigation plan: USD 1,580 per session
- Global advanced mitigation session for the Sec-MCA mitigation plan: USD 7,790 per session

Refunds

After you purchase global advanced mitigation sessions, you cannot request a refund of the fees that you paid.

Related information

- Purchase global advanced mitigation sessions
- Billing methods of the Insurance and Unlimited mitigation plans
- Sec-MCA billing methods

4.Function plan

Both Anti-DDoS Pro and Anti-DDoS Premium provide standard and enhanced function plans. The enhanced function plan provides the following features in addition to all the features of the standard function plan: static page caching, non-standard ports support, and blocked regions. These features enhance connection capabilities of instances and the ability of Anti-DDoS Pro and Anti-DDoS Premium to prevent DDoS attacks. You can select a mitigation plan as required.

When you purchase Anti-DDoS Pro or Anti-DDoS Premium instances, the standard function plan is selected by default. You can select the enhanced function plan to obtain advanced anti-DDoS protection. The price for each instance that uses the enhanced function plan is USD 1,145 per month.

For a purchased instance that uses the standard function plan, you can scale up the specification to obtain enhanced anti-DDoS protection. For more information, see Upgrade an instance.

> **Note** After you purchase an instance that uses the enhanced function plan or upgrade an instance to the enhanced function plan, you need to configure the domain names to enable the enhanced capabilities.

Comparison of the standard and enhanced function plans

The following table describes feature differences between the standard and enhanced function plans.

Category	Feature	Description	Standard function plan	Enhanced function plan
Protection algorithm	Protection against volumetric DDoS attacks	Supports protection against volumetric DDoS attacks such as malformed packet attacks and flood attacks.	✓	✓
	Protection against resource exhaustion DDoS attacks	Supports protection against common HTTP flood attacks at the transport layer, such as HTTP GET floods and HTTP POST floods. For more information, see Configure frequency control.	✓	✓

Category	Feature	Description	Standard function plan	Enhanced function plan
	Intelligent protection	• Supports intelligent protection against application-layer floods and mitigates HTTP flood attacks. • Supports intelligent protection against transport-layer floods and mitigates TCP flood attacks. For more information, see Use the intelligent protection feature.	✓	✓
Protection rule	Black lists and white lists	A blacklist and whitelist for each protected domain name can each contain a maximum of 200 IP addresses. For more information, see Configure blacklists and whitelists for domain names.	✓	✓
	Accurate access control	Supports fine-grained access control based on HTTP. For more information, see Configure accurate access control rules.	For each protected domain name, you can configure a maximum of five rules based on the following fields: IP, URL, Referer, and User-Agent.	For each protected domain name, you can configure a maximum of 10 rules.
	Blocked regions	Blocks traffic based on geographic locations. For more information, see Configure blocked regions for domain names.	✗	✓
	Standard HTTP ports (80 and 8080) and HTTPS ports (443 and 8443)	Supports anti-DDoS protections based on standard HTTP ports (80 and 8080) and HTTPS ports (443 and 8443).	✓	✓

Category	Feature	Description	Standard function plan	Enhanced function plan
Connection methods	Non-standard HTTP and HTTPS ports	Supports DDoS prevention based on non-standard HTTP and HTTPS ports. **Note** For each instance, you can configure a maximum of 10 port forwarding rules that use non-standard ports.	✗	✓
Other	Static page caching	Supports static page caching to reduce page loading time. **Note** Static page caching is in the public preview stage. For each protected domain name, you can configure a maximum of three rules. For more information, see Configure static page caching.	✗	✓

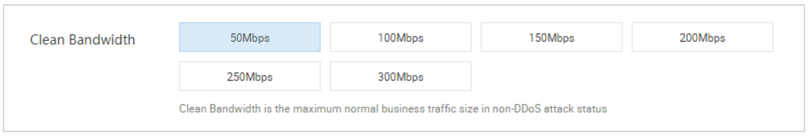
5.Billing of the burstable clean bandwidth feature

This topic describes the billing of the burstable clean bandwidth feature that is provided by Anti-DDoS Pro and Anti-DDoS Premium.

Burstable clean bandwidth

Clean bandwidth refers to the peak bandwidth of normal service traffic that can be protected by an Anti-DDoS Pro or Anti-DDoS Premium instance. Clean bandwidth is measured in Mbit/s. In the following sections, the peak bandwidth of normal service traffic is referred to as the peak traffic. The normal service traffic refers to the sum of the normal service traffic of all services that are protected by the Anti-DDoS Pro or Anti-DDoS Premium instance.

When you purchase an Anti-DDoS Pro or Anti-DDoS Premium instance, you must select a value for the **clean bandwidth** based on your normal service traffic. The normal service traffic is determined based on the inbound traffic or outbound traffic, whichever is larger. The fee for the clean bandwidth is included in the subscription fee for the Anti-DDoS Pro or Anti-DDoS Premium instance. The larger the clean bandwidth, the higher the subscription fee of the Anti-DDoS Pro or Anti-DDoS Premium instance.



Clean Bandwidth: 50Mbps

Clean Bandwidth is the maximum normal business traffic size in non-DDoS attack status

The burstable clean bandwidth feature provides extra clean bandwidth for your Anti-DDoS Pro or Anti-DDoS Premium instance. When the peak traffic of your service exceeds the clean bandwidth of the instance during peak hours, the burstable clean bandwidth feature prevents your service from being throttled.

By default, the burstable clean bandwidth feature is disabled. After you purchase an Anti-DDoS Pro or Anti-DDoS Premium instance, you can enable the burstable clean bandwidth feature. When you enable the burstable clean bandwidth feature, you must specify a value for the burstable clean bandwidth. You can specify a value that is up to nine times the clean bandwidth of the Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Configure burstable clean bandwidth.

The burstable clean bandwidth feature uses the pay-as-you-go billing method. After you enable the burstable clean bandwidth feature, you are charged for the burstable clean bandwidth when the peak traffic exceeds the specified clean bandwidth. For more information, see Billing of the burstable clean bandwidth feature.

Billing of the burstable clean bandwidth feature

Item	Description

Item	Description
Billing scope	The billing scope refers to the usage of the burstable clean bandwidth. If the burstable clean bandwidth feature is disabled, you are not charged for the feature. Anti-DDoS Pro or Anti-DDoS Premium generates monthly bills for the usage of the burstable clean bandwidth only if the burstable clean bandwidth feature is enabled. The burstable clean bandwidth that can be used within a calendar month does not exceed the value that you specify for the burstable clean bandwidth. The actual usage of the burstable clean bandwidth is determined based on the actual peak traffic. • Actual peak traffic ≤ Clean bandwidth: The burstable clean bandwidth is not used, and you are not charged for the burstable clean bandwidth. • Clean bandwidth < Actual peak traffic ≤ Sum of the clean bandwidth and the burstable clean bandwidth: The burstable clean bandwidth is billed based on the difference between the actual peak traffic and the clean bandwidth. • Actual peak traffic > Sum of the clean bandwidth and the burstable clean bandwidth: The burstable clean bandwidth is billed based on the burstable clean bandwidth that you specify. **Notice** In this case, your service may be throttled. To prevent service throttling, you must increase the burstable clean bandwidth or increase the clean bandwidth at the earliest opportunity. For more information, see Configure burstable clean bandwidth and Upgrade an instance.
Metering method (monthly 95th percentile bandwidth)	The actual peak traffic is calculated based on the monthly 95th percentile bandwidth. The following list describes how to calculate the actual peak traffic based on the monthly 95th percentile bandwidth: 1. Calculate the daily 95th percentile bandwidth values within a calendar month. To calculate the 95th percentile bandwidth value of a calendar day, collect the valid bandwidth values of your Anti-DDoS Pro or Anti-DDoS Premium instance every 5 minutes within the day, sort the collected bandwidth values in descending order, and then exclude the top 5% of the bandwidth values. The largest bandwidth value among the remaining 95% of the bandwidth values is used as the 95th percentile bandwidth value of the day. For example, if you collect a bandwidth value every 5 minutes, you can collect 12 bandwidth values within an hour and 288 bandwidth values within a day, which is calculated based on the following formula: 12 × 24 = 288. Then, you can sort the bandwidth values in descending order and exclude the top 5% of the bandwidth values. In this example, the number of the top 5% of the bandwidth values is 14, which is calculated based on the following formula and is rounded down to the nearest integer: 288 ×5% = 14.4. Therefore, the 15th bandwidth value is used as the 95th percentile bandwidth value of the day. 2. Use the largest daily 95th percentile bandwidth value within a calendar month as the actual peak traffic of the month.

Item	Description
Pricing	After you enable the burstable clean bandwidth feature, the fee of the burstable clean bandwidth within a calendar month is calculated based on the usage of the burstable clean bandwidth multiplied by the monthly unit price of the burstable clean bandwidth feature of your Anti-DDoS Pro or Anti-DDoS Premium instance. The billing cycle of the burstable clean bandwidth feature is calculated from 00:00:00 on the first day of the month to 23:59:59 on the last day of the month. The usage of the burstable clean bandwidth is measured in Mbit/s. The monthly unit price of the burstable clean bandwidth is measured in (USD per month per Mbit/s). The monthly unit price of the burstable clean bandwidth feature varies based on the mitigation plan of your Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see the Monthly unit price of the burstable clean bandwidth feature section of this topic. For more information about billing examples, see the Billing examples section of this topic.
Bill generation time and settlement time	Bill generation time: A bill is generated at 10:00 the first day of the next calendar month after the current billing cycle ends. For example, the bill for the usage of the burstable clean bandwidth in January is generated on February 1. The January bill is generated for the usage of the burstable clean bandwidth from 00:00:00 on January 1 to 23:59:59 on January 31. After a bill is generated, the bill is not immediately issued. You can query and check the details about the usage of the burstable clean bandwidth of the previous calendar month on the **System logs** page. If you have questions about the bill, submit a ticket. If the usage of the burstable clean bandwidth that is indicated by the bill is different from your actual usage, the bill is terminated, and you do not need to pay for the bill. Settlement time: If you do not have concerns about a bill, Alibaba Cloud deducts the fee of the burstable clean bandwidth from your account balance at 10:00 on the tenth day of the current calendar month. For example, Alibaba Cloud deducts the fee of January on February 10. You must make sure that the balance of your Alibaba Cloud account is sufficient. Otherwise, the burstable clean bandwidth feature becomes unavailable due to overdue payments. You can query the issued bills on the **System Log** page.

Pricing of the burstable clean bandwidth feature

Mitigation plan	Unit price for the monthly 95th percentile bandwidth (USD per month per Mbit/s)
Anti-DDoS Pro instance of the Profession mitigation plan	15
Anti-DDoS Premium instance of the Insurance mitigation plan	16
Anti-DDoS Premium instance of the Unlimited mitigation plan	21

Mitigation plan	Unit price for the monthly 95th percentile bandwidth (USD per month per Mbit/s)
Anti-DDoS Premium instance of the Mainland China Acceleration (MCA) plan	155
Anti-DDoS Premium instance of the Secure Mainland China Acceleration (Sec-MCA) plan	155

Billing examples

You purchase an Anti-DDoS Pro instance and select 100 Mbit/s for the clean bandwidth. You also enable the burstable clean bandwidth feature and set the value of the burstable clean bandwidth to 400 Mbit/s.

- Example 1: The actual peak traffic within a month is 300 Mbit/s. How is the burstable clean bandwidth billed?
  In this example, the actual peak traffic within the month is 300 Mbit/s and the clean bandwidth that you select is 100 Mbit/s. Therefore, the usage of the burstable clean bandwidth is 200 Mbit/s, which is calculated based on the following formula: 300 - 100 = 200. The monthly unit price of the burstable clean bandwidth feature is CNY 100. Therefore, the fee of the burstable clean bandwidth is CNY 20,000, which is calculated based on the following formula: 200 × 100 = 20,000.
- Example 2: The actual peak traffic within a month is 800 Mbit/s. How is the burstable clean bandwidth billed?
  In this example, the actual peak traffic within the month exceeds the sum of the clean bandwidth that you select and the burstable clean bandwidth that you specify. The burstable clean bandwidth is billed based on the usage of the burstable clean bandwidth. The usage of the burstable clean bandwidth is the burstable clean bandwidth that you specify, which is 400 Mbit/s. The monthly unit price of the burstable clean bandwidth feature is CNY 100. Therefore, the fee of the burstable clean bandwidth is CNY 40,000, which is calculated based on the following formula: 400 × 100 = 40,000.

  > **Notice** If the actual peak traffic exceeds the sum of the clean bandwidth and the burstable clean bandwidth, packet loss may occur. We recommend that you increase the burstable clean bandwidth at the earliest opportunity. In this example, you must set the burstable clean bandwidth to a value that is no less than 700 Mbit/s to prevent packet loss.

- Example 3: The actual peak traffic within a month is 1,200 Mbit/s. How is the burstable clean bandwidth billed?
  The fee of the burstable clean bandwidth in this example is the same as the fee in Example 2.

  > **Notice** In this example, the actual peak traffic is more than ten times the clean bandwidth that you select. To prevent packet loss, you must upgrade your instance to increase the clean bandwidth. For example, you can increase the clean bandwidth to 200 Mbit/s and set the burstable clean bandwidth to a value that is no less than 1,000 Mbit/s.