ALIBABA CLOUD

Alibaba Cloud

Anti-DDoS

FAQ

Document Version: 20200930

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.FAQ overview

This topic lists commonly asked questions about Alibaba Cloud Anti-DDoS, which provides Anti-DDoS Origin Basic, Anti-DDoS Origin Enterprise, Anti-DDoS Pro, and Anti-DDoS Premium.

Type	Question
售前常见问题	• 售前常见问题 • 售前常见问题 • 售前常见问题 • 售前常见问题 • 售前常见问题 • 售前常见问题 • 售前常见问题 • 售前常见问题 • 售前常见问题 • 售前常见问题 • 售前常见问题
FAQ for the billing of burstable protection	• Are burstable protection fees charged when no attacks are detected? • What is the maximum mitigation capacity if I purchase an Anti-DDoS instance with a basic protection bandwidth of 20 Gbit/s and a burstable protection bandwidth of 50 Gbit/s? • What happens if the size of the DDoS attacks exceeds the burstable protection bandwidth? • How burstable protection is charged if the basic protection bandwidth is 30 Gbit/s, the burstable protection bandwidth is 50 Gbit/s, and the size of the DDoS attacks is 45 Gbit/s? • Can I change the burstable protection bandwidth from 100 Gbit/s to 200 Gbit/s? • Can I increase the protection bandwidth anytime when the basic protection bandwidth of 30 Gbit/s provided by the Anti-DDoS Pro instance cannot meet the requirements? • How is the mitigation fee calculated if a domain name has been attacked multiple times in a day? • How do I prevent an Anti-DDoS Pro instance from providing burstable protection?

Type	Question
FAQ about Anti-DDoS Origin	**Basic** • Can Anti-DDoS Origin Basic provide protection against SYN flood attacks? • Why does Anti-DDoS Origin Basic not protect my Elastic Compute Service (ECS) instance against an attack of 20 Mbit/s? • Why cannot I manually deactivate blackhole filtering for an Anti-DDoS Origin Basic instance? • Why the traffic data in the Anti-DDoS Origin console differs from that in Cloud Monitor and other cloud services? • What is the billing difference between unlimited protection of Anti-DDoS Origin Enterprise and burstable protection of Anti-DDoS Pro? • What do I do if blackhole filtering is activated for an IP address that is protected by Anti-DDoS Origin Enterprise? • What do I do if I deployed an Anti-DDoS Origin Enterprise instance in the wrong region? • What do I do if the error message "The IP address does not belong to your account" is displayed when I add an IP address to Anti-DDoS Origin? **Enterprise** • What is the billing difference between unlimited protection of Anti-DDoS Origin Enterprise and burstable protection of Anti-DDoS Pro? • What do I do if blackhole filtering is activated for an IP address that is protected by Anti-DDoS Origin Enterprise? • What do I do if I deployed an Anti-DDoS Origin Enterprise instance in the wrong region? • When I add the IP address of a service, the system prompts that the number of IP addresses reaches the upper limit. What do I do? • What do I do if the error message "The IP address does not belong to your account" is displayed when I add an IP address to Anti-DDoS Origin?

Type	Question
Anti-DDoS Pro and Anti-DDoS Premium FAQ	• What happens if an Anti-DDoS Pro or Anti-DDoS Premium instance expires? • What is the clean bandwidth of an Anti-DDoS Pro or Anti-DDoS Premium instance? • What happens if the actual bandwidth exceeds the clean bandwidth of an Anti-DDoS Pro or Anti-DDoS Premium instance? • Can I manually deactivate the black hole status? • What are the back-to-origin CIDR blocks for Anti-DDoS Pro and Anti-DDoS Premium? • Are the back-to-origin CIDR blocks of Anti-DDoS Pro and Anti-DDoS Premium automatically added to a security group? • Can I use an internal IP address as the origin server IP address for an Anti-DDoS Pro or Anti-DDoS Premium instance? • Does the configuration of the origin server IP address for an Anti-DDoS Pro or Anti-DDoS Premium instance take effect immediately? • How do I identify which website is under attack when multiple website services are protected by an Anti-DDoS Pro or Anti-DDoS Premium instance? • Do Anti-DDoS Pro and Anti-DDoS Premium support the health check feature? • How is traffic distributed to multiple origin servers protected by an Anti-DDoS Pro or Anti-DDoS Premium instance? • Can I configure session persistence in Anti-DDoS Pro and Anti-DDoS Premium? • How does session persistence work for an Anti-DDoS Pro or Anti-DDoS Premium instance? • What is the default TCP timeout period for an Anti-DDoS Pro or Anti-DDoS Premium instance? • What are the default HTTP and HTTPS timeout periods for an Anti-DDoS Pro or Anti-DDoS Premium instance? • Do Anti-DDoS Pro and Anti-DDoS Premium support IPv6? • Do Anti-DDoS Pro and Anti-DDoS Premium support WebSocket? • Does Anti-DDoS Pro or Anti-DDoS Premium support mutual HTTPS authentication? • Why am I unable to access HTTPS websites by using the browsers of earlier versions or from an Android mobile client? • Which SSL protocols and cipher suites are supported by Anti-DDoS Pro or Anti-DDoS Premium? • What are the limits on the numbers of ports and domain names protected by an Anti-DDoS Pro or Anti-DDoS Premium instance? • Why does the traffic chart show a traffic scrubbing event even though the size of the traffic received by the server does not exceed the traffic scrubbing threshold? • Do Anti-DDoS Pro and Anti-DDoS Premium protect websites that use NTLM authentication?

Type	Question
Hot FAQ about Anti-DDoS Pro and Anti-DDoS Premium	**Configuration** • How do I enable WebSocket? • How do I configure Anti-DDoS Pro or Anti-DDoS Premium by using different Alibaba Cloud accounts? • What are the proactive detection IP addresses of Anti-DDoS Pro and Anti-DDoS Premium? **Service exception** • How do I handle the issues of slow response, high latency, and access failure on websites that are protected by an Anti-DDoS Pro or Anti-DDoS Premium instance? • 502 error reported after configuring Anti-DDoS Pro • How do I resolve 504 errors on websites that are protected by Anti-DDoS Pro or Anti-DDoS Premium? • How do I handle the issue of slow connection establishment after I configure Anti-DDoS Pro or Anti-DDoS Premium? • How do I handle the issue of slow access to services protected by an Anti-DDoS Pro or Anti-DDoS Premium instance? • How do I handle the issue that session persistence cannot be implemented after I configure Anti-DDoS Pro or Anti-DDoS Premium? • How do I handle the issue that I cannot ping websites protected by an Anti-DDoS Pro or Anti-DDoS Premium instance? • How do I handle the issue that large files fail to upload to websites that are protected by Anti-DDoS Pro or Anti-DDoS Premium? • How do I handle the issue that large files fail to upload over HTTP and HTTPS after I configure Anti-DDoS Pro or Anti-DDoS Premium? **Protection analysis** • What are the differences between website protection and non-website protection? • How do I identify the types of attacks against an Anti-DDoS Pro or Anti-DDoS Premium instance? • How do I mitigate NTP-based DDoS attacks? **HTTPS service** • What are the errors returned for HTTPS service exceptions? • How do I handle the error "The specified parameter is invalid" reported when I upload an HTTPS certificate? • How do I convert an HTTPS certificate to the PEM format? • How do I handle HTTPS access exceptions that occur when clients do not support SNI? • How do I handle the issue that HTTP status code 413 is returned for GET requests?

2.Pre-sales FAQ

This topic lists the frequently asked questions about pre-sales of Anti-DDoS services provided by Alibaba Cloud.

Does Alibaba Cloud provide free Anti-DDoS services?

Yes. Alibaba Cloud automatically activates Anti-DDoS Origin Basic for Alibaba Cloud users. This service can mitigate DDoS attacks of up to 5 Gbit/s. Anti-DDoS Origin Basic is free of charge. You do not need to purchase, activate, or configure this service. For more information, see What is Anti-DDoS Origin.

Alibaba Cloud does not provide unlimited mitigation free of charge. Bandwidth resources are essential to DDoS attack mitigation. Bandwidth usage takes the highest proportion in mitigation service billing. Alibaba Cloud pays for bandwidth resources provided by Internet Service Providers (ISPs), such as China Telecom, China Unicom, and China Mobile. The bandwidth costs include bandwidth usage caused by mitigating DDoS attacks. Alibaba Cloud Security helps users mitigate DDoS attacks of up to 5 Gbit/s free of charge. When the size of the DDoS attacks exceeds 5 Gbit/s, Alibaba Cloud Security automatically blocks all network traffic sent to the attacked domain name in case a large number of mitigation fees are incurred.

Can Anti-DDoS Pro and Anti-DDoS Premium be billed only when they are triggered to mitigate DDoS attacks?

No. Anti-DDoS Pro and Anti-DDoS Premium are billed on a subscription basis. You must purchase Anti-DDoS instances and complete the payment before you can use the instances to mitigate DDoS attacks within the subscription duration.

Do Anti-DDoS services have trial mitigation plans?

- Anti-DDoS Origin: Anti-DDoS Origin Basic is a free migration plan that is used to mitigate DDoS attacks of up to 5 Gbit/s for public IP addresses of Alibaba Cloud. Anti-DDoS Origin Enterprise is a charged mitigation plan and no free trial is available.

> **Note** We recommend that you use Anti-DDoS Origin Basic to test your network and then upgrade your service to Anti-DDoS Origin Enterprise. The upgrading process is completely transparent and does not add any changes to the network and connections.

- Anti-DDoS Pro/Premium: Anti-DDoS Pro and Anti-DDoS Premium work with scrubbing centers built on Anti-DDoS-exclusive servers to mitigate volumetric DDoS attacks. The mitigation cost is high. No free trial service is provided.

Can Anti-DDoS services protect external servers?

Yes. Anti-DDoS Pro and Anti-DDoS Premium can protect Alibaba Cloud Elastic Compute Service (ECS) instances and external servers against DDoS attacks. Anti-DDoS Pro and Anti-DDoS Premium instances redirect requests to origin servers over the Internet. Therefore, Anti-DDoS instances can protect servers that can be accessed over the Internet, such as external servers, servers deployed on Alibaba Cloud, and on-premises servers. For more information, see What are Anti-DDoS Pro and Anti-DDoS Premium.

Can Anti-DDoS Pro and Anti-DDoS Premium protect external servers that serve a domain name registered with Alibaba Cloud?

Yes. Anti-DDoS Pro and Anti-DDoS Premium can protect Alibaba Cloud ECS instances and external servers that serve domain names registered with Alibaba Cloud or third-party domain name service providers.

Is Internet Content Provider (ICP) filing required for domain names that require the protection of Alibaba Cloud Anti-DDoS services?

You must complete ICP filing for domain names that require the protection of Anti-DDoS Pro. ICP filing is not required when you use Anti-DDoS Premium to protect domain names. For more information, see ICP filing application overview.

What are the regions supported by Anti-DDoS services?

- Anti-DDoS Pro: protects workloads deployed in mainland China.
- Anti-DDoS Premium: protects workloads deployed outside mainland China, including China (Hong Kong).

Do Anti-DDoS Pro and Anti-DDoS Premium have limits on the number of protected domain names?

Yes.

- By default, each Anti-DDoS Pro instance can protect up to 50 domain names, including subdomains and wildcard domains. The subdomains and wildcard domains must not belong to more than five top-level domains.
- By default, each Anti-DDoS Premium instance can protect up to 10 domain names, including subdomains and wildcard domains. The subdomains and wildcard domains must not belong to more than one top-level domain.

Note You can increase domain name quota when you purchase an Anti-DDoS instance. Each Anti-DDoS Pro or Anti-DDoS Premium instance can protect a maximum of 200 domain names. For more information, see 开通DDoS高防（新BGP&国际）.

Do Anti-DDoS instances support wildcard domains?

Yes. You can add wildcard domains on the **Website Config** page. For more information, see Add a website.

A wildcard DNS record is specified by using an asterisk (*) as the leftmost part of a domain name. The record points all matching subdomains to the domain name. For example, a wildcard DNS record specified by using *.taobao.com points all subdomains that match *.taobao.com to www.taobao.com.

What are the prerequisites for setting up protection with Anti-DDoS Premium?

If you want to use Anti-DDoS Premium to protect a website, you must add the domain name of the website to Anti-DDoS Premium. If you want to use Anti-DDoS Premium to protect a non-website service, you only need to connect the service port to your Anti-DDoS Premium instance.

Does the basic protection bandwidth provided by an Anti-DDoS Pro instance indicate the maximum mitigation capacity?

The basic protection bandwidth provided by an Anti-DDoS Pro instance is the guaranteed bandwidth for handling both normal and malicious traffic of the workloads protected by the Anti-DDoS Pro instance. All network traffic from the public network must first pass through the Anti-DDoS traffic scrubbing centers. Malicious traffic is filtered out, and only normal traffic is forwarded to the origin server.

3.FAQ about Anti-DDoS Origin

This topic provides answers to some commonly asked questions about Anti-DDoS Origin Basic and Enterprise.

Basic

- Can Anti-DDoS Origin Basic provide protection against SYN flood attacks?
- Why does Anti-DDoS Origin Basic not protect my Elastic Compute Service (ECS) instance against an attack of 20 Mbit/s?
- Why cannot I manually deactivate blackhole filtering for an Anti-DDoS Origin Basic instance?
- Why the traffic data in the Anti-DDoS Origin console differs from that in Cloud Monitor and other cloud services?

Enterprise

- What is the billing difference between unlimited protection of Anti-DDoS Origin Enterprise and burstable protection of Anti-DDoS Pro?
- What do I do if blackhole filtering is activated for an IP address that is protected by Anti-DDoS Origin Enterprise?
- What do I do if I deployed an Anti-DDoS Origin Enterprise instance in the wrong region?
- When I add the IP address of a service, the system prompts that the number of IP addresses reaches the upper limit. What do I do?
- What do I do if the error message "The IP address does not belong to your account" is displayed when I add an IP address to Anti-DDoS Origin?

Can Anti-DDoS Origin Basic provide protection against SYN flood attacks?

Yes, Anti-DDoS Origin Basic can provide protection against SYN flood attacks.

Why does Anti-DDoS Origin Basic not protect my Elastic Compute Service (ECS) instance against an attack of 20 Mbit/s?

If the size of attacks is lower than 100 Mbit/s, Anti-DDoS Origin Basic is free of charge. Anti-DDoS Origin Basic does not provide protection. We recommend that you optimize your server or install a host-based firewall, such as Yunsuo, to protect against attacks lower than 100 Mbit/s.

Why cannot I manually deactivate blackhole filtering for an Anti-DDoS Origin Basic instance?

In most cases, blackhole filtering lasts 30 minutes to 24 hours. If your services are under frequent volumetric DDoS attacks, Alibaba Cloud may extend the blackhole filtering duration.

Alibaba Cloud purchases blackhole filtering from Internet Service Providers (ISPs), who preset the duration of blackhole filtering. You cannot manually deactivate blackhole filtering for Anti-DDoS Origin Basic before the duration ends. if you want to deactivate blackhole filtering, we recommend that you purchase Anti-DDoS Origin Enterprise, Anti-DDoS Pro, or Anti-DDoS Premium instances. For more information, see What is Anti-DDoS Origin and What are Anti-DDoS Pro and Anti-DDoS Premium?.

Why the traffic data in the Anti-DDoS Origin console differs from that in Cloud Monitor and other cloud services?

In most cases, the traffic in the Anti-DDoS Origin console is higher than that in Cloud Monitor and other cloud services.

Assume that your ECS instance is under DDoS attacks, which triggers traffic scrubbing when the traffic reaches 2.5 Gbit/s. Alibaba Cloud notifies you that the traffic scrubbing provided by Anti-DDoS Origin Basic instance is triggered. However, the Cloud Monitor console shows that the inbound bandwidth of the elastic IP address (EIP) associated with your ECS instance is 1.2 Gbit/s during the traffic scrubbing.

The reasons for this difference include:

- Anti-DDoS Origin collects traffic data before traffic scrubbing is triggered, whereas Cloud Monitor collects traffic data after traffic scrubbing is triggered.
- Anti-DDoS Origin monitors all network traffic destined for your ECS instance, including malicious traffic, whereas Cloud Monitor monitors only normal traffic.
- Anti-DDoS Origin and Cloud Monitor collect traffic data at different intervals. Anti-DDoS Origin collects traffic data at intervals of seconds so that DDoS attacks can be detected at the earliest opportunity. Cloud Monitor collects the traffic data of EIPs at intervals of minutes and displays the data in charts in the Cloud Monitor console.
- Anti-DDoS Origin and Cloud Monitor collect traffic data from different sources. Anti-DDoS Origin collects the traffic data of EIPs from the border gateway devices between Alibaba Cloud and the Internet, whereas Cloud Monitor collects the traffic data of EIPs from the devices that forward traffic.

> **Note** The difference in traffic data can happen to Alibaba Cloud services, such as ECS, Server Load Balancer (SLB), EIP, and NAT Gateway, that are Infrastructure as a Service (IaaS) and support Internet access.

What is the billing difference between unlimited protection of Anti-DDoS Origin Enterprise and burstable protection of Anti-DDoS Pro?

- Anti-DDoS Origin Enterprise provides the unlimited protection capability. If DDoS attacks are detected, the Anti-DDoS Origin Enterprise instance uses all the protection capacity for the region where it resides to defend against the DDoS attacks. Unlimited protection is included in the Anti-DDoS Origin Enterprise instance that you have purchased. No additional fee is charged for unlimited protection.
- Burstable protection of Anti-DDoS Pro is charged based on the peak value of the burstable protection bandwidth on the current day. For more information, see Burstable protection (pay-as-you-go on a daily basis).

What do I do if blackhole filtering is activated for an IP address that is protected by Anti-DDoS Origin Enterprise?

You can manually deactivate blackhole filtering.

- For more information about how to manually deactivate blackhole filtering for a protected IP address, see 解除黑洞.
- You can also configure automated response to and deactivation of blackhole filtering. For more information, see Best practices for automatic deactivation of black holes.

What do I do if I deployed an Anti-DDoS Origin Enterprise instance in the wrong region?

If the IP address that you want to protect is not in the same region as the purchased Anti-DDoS Origin Enterprise instance, submit a submit a ticket to apply for a refund. After you receive the refund, you can purchase a new instance to protect the IP address.

When I add the IP address of a service, the system prompts that the number of IP addresses reaches the upper limit. What do I do?

If the number of protected IP addresses reaches the value of **Protected IP Addresses** that you specify on the Anti-DDoS Origin Enterprise buy page, increase the value of **Protected IP Addresses** or purchase a new Anti-DDoS Origin Enterprise instance. For more information, see Upgrade instance types and 开通DDoS原生防护企业版.

What do I do if the error message "The IP address does not belong to your account" is displayed when I add an IP address to Anti-DDoS Origin?

If you receive the error message **The IP address does not belong to your account** when you add an IP address in the Anti-DDoS Origin console, perform the following steps to troubleshoot the error:

1. Verify that you have entered the correct IP address.
2. Verify that the IP address is located in the same region as the purchased Anti-DDoS Origin Enterprise instance.
3. If you want to protect the IP address of a WAF instance, verify that Anti-DDoS Origin Enterprise is available in the region of the WAF instance. For more information about regions where you can activate Anti-DDoS Origin Enterprise, see Limits.

4.Anti-DDoS Pro and Anti-DDoS Premium FAQ

This topic provides answers to some commonly asked questions about Anti-DDoS Pro and Anti-DDoS Premium.

What happens if an Anti-DDoS Pro or Anti-DDoS Premium instance expires?

An expired instance no longer protects your services.

- The instance still forwards your traffic for seven days after it expires. If the actual bandwidth exceeds the clean bandwidth of the instance, throttling is triggered and packet loss may occur.
- The instance stops forwarding traffic seven days after it expires. If the IP addresses of your services are mapped to the instance, your services become inaccessible.

For more information, see Instance expiration.

What is the clean bandwidth of an Anti-DDoS Pro or Anti-DDoS Premium instance?

The clean bandwidth of an instance is equal to the peak value of the inbound or outbound traffic of the protected service, whichever is greater. Unit: Mbit/s.

You can increase the **clean bandwidth** of an instance on the **Instances** page in the Anti-DDoS Pro console. For more information, see Upgrade the specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance.

What happens if the actual bandwidth exceeds the clean bandwidth of an Anti-DDoS Pro or Anti-DDoS Premium instance?

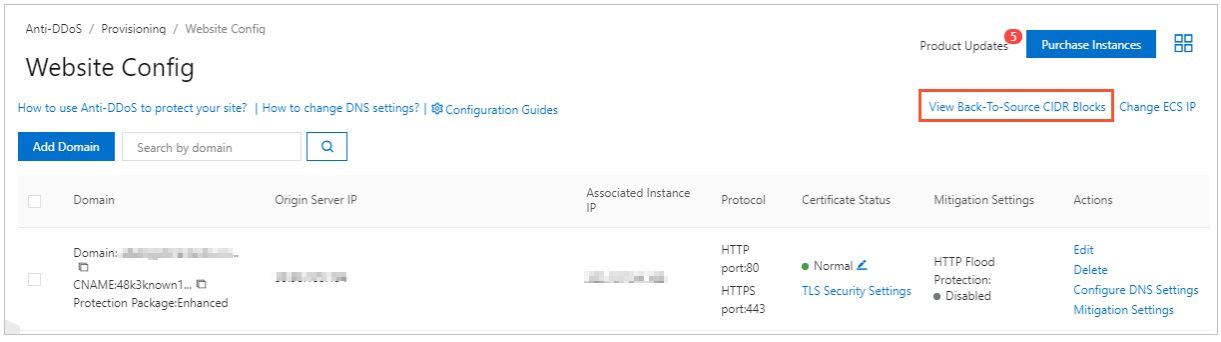
If the actual bandwidth exceeds the clean bandwidth of the instance, throttling is triggered and packet loss may occur.

Can I manually deactivate the black hole status?

- You can manually deactivate the black hole status for an Anti-DDoS Pro instance. Each Alibaba Cloud account can deactivate the black hole status up to five times a day. The limit is reset at 00:00:00 (UTC+8) the next day. For more information, see 黑洞解封.
- You cannot manually deactivate the black hole status for an Anti-DDoS Premium instance.

What are the back-to-origin CIDR blocks for Anti-DDoS Pro and Anti-DDoS Premium?

You can view the back-to-origin CIDR blocks on the **Website Config** page in the Anti-DDoS Pro console. For more information, see Allow back-to-origin IP addresses to access the origin server.



Are the back-to-origin CIDR blocks of Anti-DDoS Pro and Anti-DDoS Premium automatically added to a security group?

No. If you deploy Web Application Firewall (WAF) or a third-party security service on your origin server, you must manually add the back-to-origin CIDR blocks of Anti-DDoS Pro to the whitelist of the security software. For more information, see Allow back-to-origin IP addresses to access the origin server.

Can I use an internal IP address as the origin server IP address for an Anti-DDoS Pro or Anti-DDoS Premium instance?

No, you cannot use internal IP addresses because Anti-DDoS Pro and Anti-DDoS Premium support forwarding traffic to origin servers only over the Internet.

Does the configuration of the origin server IP address for an Anti-DDoS Pro or Anti-DDoS Premium instance take effect immediately?

No, the configuration does not immediately take effect. The configuration requires about five minutes to take effect. We recommend that you perform this operation during off-peak hours. For more information, see Change the public IP address of an ECS origin server.

How do I identify which website is under attack when multiple website services are protected by an Anti-DDoS Pro or Anti-DDoS Premium instance?

When website services are targeted by volumetric DDoS attacks, you cannot identify which website is under attack from the dimension of data packets. We recommend that you connect your website services to multiple instances. This way, you can view the monitoring data of the website services separately.

Do Anti-DDoS Pro and Anti-DDoS Premium support the health check feature?

Yes, Anti-DDoS Pro and Anti-DDoS Premium instance support the health check feature.

- The health check feature is enabled for website services by default.
- The health check feature is disabled for non-website services by default. You can enable the health check feature in the Anti-DDoS Pro console. For more information, see Configure a health check.

For more information about the health check feature, see Health check overview.

How is traffic distributed to multiple origin servers protected by an Anti-DDoS Pro or Anti-DDoS Premium instance?

- Traffic destined for website services is distributed to origin servers by using the IP hash policy.
- Traffic destined for non-website services is distributed to origin servers by using the weighted round robin policy.

Can I configure session persistence in Anti-DDoS Pro and Anti-DDoS Premium?

Yes, you can configure session persistence for non-website services in the console. For more information, see Configure session persistence.

How does session persistence work for an Anti-DDoS Pro or Anti-DDoS Premium instance?

After you configure session persistence for an instance, the instance forwards requests from the same IP address to the same origin server within a specific time period. If you change the network from a wired network or 4G network to a wireless network, the change in the client IP address results in a session persistence failure.

What is the default TCP timeout period for an Anti-DDoS Pro or Anti-DDoS Premium instance?

The default timeout period is 900 seconds. You can set the timeout period for non-website services in the Anti-DDoS Pro console. For more information, see Configure session persistence.

What are the default HTTP and HTTPS timeout periods for an Anti-DDoS Pro or Anti-DDoS Premium instance?

The default timeout periods are 120 seconds.

Do Anti-DDoS Pro and Anti-DDoS Premium support IPv6?

No, Anti-DDoS Pro and Anti-DDoS Premium do not support IPv6.

Do Anti-DDoS Pro and Anti-DDoS Premium support WebSocket?

Yes, Anti-DDoS Pro and Anti-DDoS Premium support WebSocket. For more information, see How do I enable WebSocket?.

Does Anti-DDoS Pro or Anti-DDoS Premium support mutual HTTPS authentication?

- Website services that are added to Anti-DDoS Pro or Anti-DDoS Premium do not support mutual HTTPS authentication.
- Non-website services that are added to Anti-DDoS Pro or Anti-DDoS Premium and use TCP port forwarding support mutual HTTPS authentication.

Why am I unable to access HTTPS websites by using the browsers of earlier versions or from an Android mobile client?

This issue occurs because the browser or client does not support Server Name Indication (SNI). Make sure that the browser or client supports SNI. For more information, see How do I handle HTTPS access exceptions that occur when clients do not support SNI?.

Which SSL protocols and cipher suites are supported by Anti-DDoS Pro or Anti-DDoS Premium?

Supported SSL protocols:

- TLS v1.0
- TLS v1.1
- TLS v1.2

Supported cipher suites:

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- AES128-GCM-SHA256
- AES256-GCM-SHA384
- AES128-SHA256
- AES256-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-ECDSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA
- AES128-SHA
- AES256-SHA
- DES-CBC3-SHA
- RSA+3DES

What are the limits on the numbers of ports and domain names protected by an Anti-DDoS Pro or Anti-DDoS Premium instance?

- Maximum number of protected ports:
  - An Anti-DDoS Pro instance protects 50 ports by default. You can upgrade the instance to protect a maximum of 400 ports.
  - An Anti-DDoS Premium instance protects 5 ports by default. You can upgrade the instance to protect a maximum of 400 ports.
- Maximum number of protected domain names:
  - An Anti-DDoS Pro instance protects 50 domain names by default. You can upgrade the instance to protect a maximum of 200 domain names.
  - An Anti-DDoS Premium instance protects 10 domain names by default. You can upgrade the instance to protect a maximum of 200 domain names.

Why does the traffic chart show a traffic scrubbing event even though the size of the traffic received by the server does not exceed the traffic scrubbing threshold?

An Anti-DDoS Pro or Anti-DDoS Premium instance automatically filters out malformed packets, such as small SYN packets and packets that do not meet TCP requirements, and invalid SYN flags for protected services. This way, your servers do not allocate resources to manage these malformed packets. These filtered malformed packets are counted in the scrubbed traffic statistics. This indicates that the traffic chart may show a traffic scrubbing event even though the size of the traffic received by the server does not exceed the traffic scrubbing threshold.

Do Anti-DDoS Pro and Anti-DDoS Premium protect websites that use NTLM authentication?

No, Anti-DDoS Pro and Anti-DDoS Premium do not protect websites that use NTLM authentication. The website request forwarded by an Anti-DDoS Pro or Anti-DDoS Premium instance cannot pass the NTLM authentication of the origin server. The client encounters repeated authentication requests. We recommend that you use other authentication methods for your website.

5.FAQ for the billing of burstable protection

This topic lists the frequently asked questions about the billing of burstable protection provided by Anti-DDoS Pro.

Are burstable protection fees charged when no attacks are detected?

No. Only subscription fees for basic protection are charged.

What is the maximum mitigation capacity if I purchase an Anti-DDoS instance with a basic protection bandwidth of 20 Gbit/s and a burstable protection bandwidth of 50 Gbit/s?

The maximum mitigation capacity is determined by the burstable protection bandwidth, which is 50 Gbit/s in this example. If you purchase a burstable protection bandwidth of 20 Gbit/s that equals to the basic protection bandwidth, the maximum mitigation capacity is 20 Gbit/s. In this case, the Anti-DDoS instance does not provide burstable protection.

What happens if the size of the DDoS attacks exceeds the burstable protection bandwidth?

If the size of the DDoS attacks exceeds the burstable protection bandwidth, network traffic destined for the domain names protected by your Anti-DDoS Pro instance is routed to the black hole.

How burstable protection is charged if the basic protection bandwidth is 30 Gbit/s, the burstable protection bandwidth is 50 Gbit/s, and the size of the DDoS attacks is 45 Gbit/s?

Burstable protection is charged based on the difference between the peak volume of the DDoS attacks and the basic protection bandwidth. In this example, burstable protection is charged based on the difference of 15 Gbit/s.

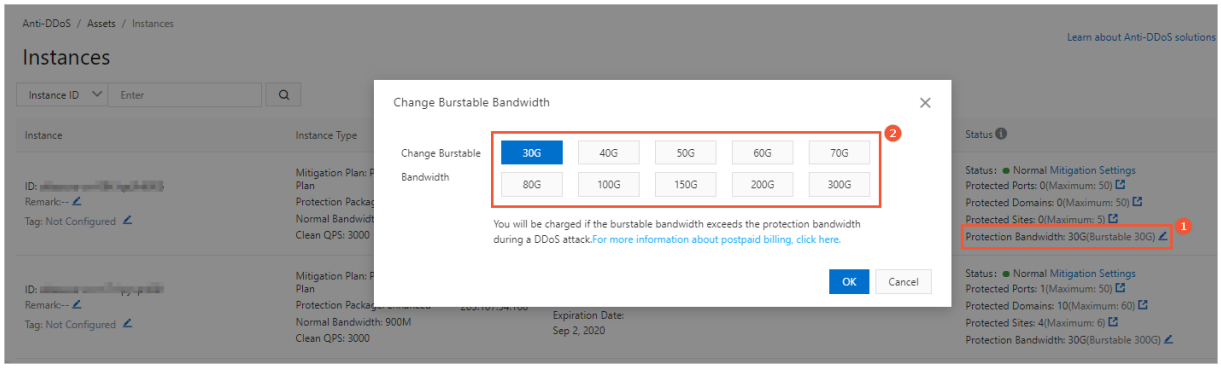
For more information about the price of burstable protection, see Pricing for Anti-DDoS. In this example, 15 Gbit/s is charged at a unit price of USD 330/day.

Exceed Attack Bandwidth of Committed Mitigation Capacity	Price(USD/Day)
0-5 Gbps	120
5-10 Gbps	180
10-20 Gbps	330
20-30 Gbps	540

Can I change the burstable protection bandwidth from 100 Gbit/s to 200 Gbit/s?

Yes.

You can manage **burstable protection** for an Anti-DDoS Pro instance on the **Instances** page in the Anti-DDoS Pro console. **Mainland China** is selected by default.



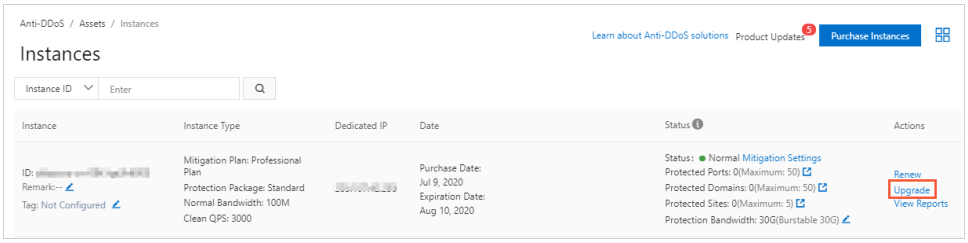
Note If burstable protection on the day when you change the burstable protection bandwidth is already charged, the system starts to charge burstable protection based on the newly selected bandwidth the next day.

Can I increase the protection bandwidth anytime when the basic protection bandwidth of 30 Gbit/s provided by the Anti-DDoS Pro instance cannot meet the requirements?

Yes. You can increase the basic protection bandwidth or burstable protection bandwidth.

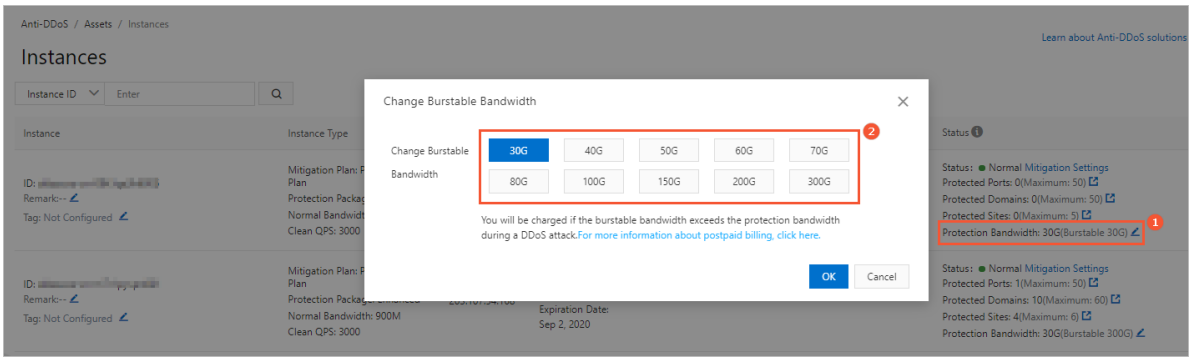
- Increase the basic protection bandwidth

  You can manage **basic protection** for an Anti-DDoS Pro instance on the **Instances** page in the Anti-DDoS Pro console and complete the payment. **Mainland China** is selected by default. For more information, see Upgrade the specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance.



- Increase the burstable protection bandwidth

You can manage **burstable protection** for an Anti-DDoS Pro instance on the **Instances** page in the Anti-DDoS Pro console. **Mainland China** is selected by default. Burstable protection is billed on a pay-as-you-go basis and charged based on the difference between the peak volume of the DDoS attacks and the basic protection bandwidth. For more information, see Burstable protection (pay-as-you-go on a daily basis).



How is the mitigation fee calculated if a domain name has been attacked multiple times in a day?

Burstable protection is charged only once based on the peak volume of DDoS attacks on the same day (from 00:00 to 24:00). For example, if three DDoS attacks are launched to a protected domain name, and the peak volumes of the three DDoS attacks are 50 Gbit/s, 100 Gbit/s, and 200 Gbit/s, burstable protection is charged based on the highest peak volume (200 Gbit/s).

How do I prevent an Anti-DDoS Pro instance from providing burstable protection?

You can set the burstable protection bandwidth and basic protection bandwidth to the same value. When DDoS attacks exhaust the basic protection bandwidth, no burstable protection is provided to mitigate the attacks and no bills are generated.

You can manage **burstable protection** for an Anti-DDoS Pro instance on the **Instances** page in the Anti-DDoS Pro console. **Mainland China** is selected by default.