

Alibaba Cloud

Anti-DDoS

FAQ

Document Version: 20220419

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 .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.FAQ overview	05
2.Pre-sales FAQ	09
3.FAQ about Anti-DDoS Origin	12
4.FAQ about Anti-DDoS Pro and Anti-DDoS Premium	15
5.FAQ about the billing of burstable protection	22

1.FAQ overview

This topic lists frequently asked questions about Alibaba Cloud Anti-DDoS.

Category	Question
Pre-sales FAQ	<ul style="list-style-type: none"> • Does Alibaba Cloud Anti-DDoS provide free services? • Can Anti-DDoS Pro and Anti-DDoS Premium be billed only when they mitigate DDoS attacks? • Does Anti-DDoS have trial mitigation plans? • Can Anti-DDoS Pro and Anti-DDoS Premium protect servers that are not deployed on Alibaba Cloud? • Can Anti-DDoS Pro and Anti-DDoS Premium protect servers that are not deployed on Alibaba Cloud but have domain names registered with Alibaba Cloud? • Is ICP filing required for domain names that you want Anti-DDoS Pro or Anti-DDoS Premium to protect? • What are the regions supported by Anti-DDoS Pro and Anti-DDoS Premium? • Do Anti-DDoS Pro and Anti-DDoS Premium have limits on the number of protected domains? • Do Anti-DDoS instances support wildcard domains? • What are the limits for the ports that can be added to Anti-DDoS Pro? • What are the prerequisites for activating Anti-DDoS Premium? • Does the basic protection bandwidth provided by Anti-DDoS Pro apply to all traffic or only attack traffic?
FAQ about the billing of burstable protection	<ul style="list-style-type: none"> • If no attacks are detected, are burstable protection fees charged? • 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 is the maximum mitigation capacity? • What happens if the size of DDoS attacks exceeds the burstable protection bandwidth? • If the basic protection bandwidth is 30 Gbit/s, the burstable protection bandwidth is 50 Gbit/s, and the size of DDoS attacks is 45 Gbit/s, how is burstable protection charged? • Can I change the burstable protection bandwidth from 100 Gbit/s to 200 Gbit/s? • If the basic protection bandwidth of 30 Gbit/s provided by the Anti-DDoS Pro instance cannot meet my requirements, can I increase the protection bandwidth anytime? • If an IP address is attacked multiple times in a day, how is the mitigation fee calculated? • How do I prevent an Anti-DDoS Pro instance from providing burstable protection?

Category	Question
FAQ about Anti-DDoS Origin	Anti-DDoS Origin Basic <ul style="list-style-type: none"> • 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?
	Anti-DDoS Origin Enterprise <ul style="list-style-type: none"> • 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?

Category	Question
FAQ about Anti-DDoS Pro and Anti-DDoS Premium	<ul style="list-style-type: none"> • 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 traffic volume exceeds the clean bandwidth of an Anti-DDoS Pro or Anti-DDoS Premium instance? • Can I manually deactivate blackhole filtering? • What are the back-to-origin CIDR blocks of an Anti-DDoS Pro or Anti-DDoS Premium instance? • Are the back-to-origin CIDR blocks of an Anti-DDoS Pro or Anti-DDoS Premium instance automatically added to a whitelist? • Can I use an internal IP address as the IP address of the origin server for an Anti-DDoS Pro or Anti-DDoS Premium instance? • I have changed the IP address of the origin server for an Anti-DDoS Pro or Anti-DDoS Premium instance. Does the change immediately take effect? • How do I identify which website is under attack when multiple websites 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 that are protected by an Anti-DDoS Pro or Anti-DDoS Premium instance? • Can I configure session persistence in the Anti-DDoS Pro or Anti-DDoS Premium console? • 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? • Do Anti-DDoS Pro and Anti-DDoS Premium support mutual HTTPS authentication? • Why am I unable to access HTTPS websites by using a browser of an earlier version or from an Android mobile client? • Which SSL protocols and cipher suites are supported by Anti-DDoS Pro and Anti-DDoS Premium? • How do Anti-DDoS Pro and Anti-DDoS Premium ensure the security of an uploaded certificate and its private key? Do Anti-DDoS Pro and Anti-DDoS Premium decrypt HTTPS traffic and record the content of HTTPS requests? • What are the limits on the numbers of ports and domain names that can be protected by an Anti-DDoS Pro or Anti-DDoS Premium instance? • Why does the traffic chart show a traffic scrubbing event even though the volume of the traffic received by the server does not exceed the traffic scrubbing threshold? • Can Anti-DDoS Pro and Anti-DDoS Premium protect websites that use NTLM authentication?

Category	Question
Hot issues about Anti-DDoS Pro and Anti-DDoS Premium	Configuration <ul style="list-style-type: none"> How do I configure Anti-DDoS Pro or Anti-DDoS Premium by using different Alibaba Cloud accounts? How do I enable WebSocket? What are the proactive detection IP addresses of Anti-DDoS Pro and Anti-DDoS Premium?
	Service exception <ul style="list-style-type: none"> 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? How do I resolve error 502 on websites protected by Anti-DDoS Pro or Anti-DDoS Premium? How do I resolve the "504 Gateway Timeout" error on websites protected by Anti-DDoS Pro or Anti-DDoS Premium? How do I handle slow connection establishment after I configure Anti-DDoS Pro or Anti-DDoS Premium? How do I handle slow access to services protected by Anti-DDoS Pro or Anti-DDoS Premium? 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 the IP address of an Anti-DDoS Pro or Anti-DDoS Premium instance? How do I handle the issue that large files fail to be uploaded over HTTP and HTTPS after I add my service to Anti-DDoS Pro or Anti-DDoS Premium?
	Protection analysis <ul style="list-style-type: none"> 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? What are the differences between website protection and non-website protection?
	HTTPS service <ul style="list-style-type: none"> The certificate uploaded for HTTPS services does not match its private key. What do I do? How do I convert an HTTPS certificate file into the PEM format? How do I handle HTTPS access exceptions that occur if clients do not support SNI? How do I handle the mismatch between a certificate and its private key?

2.Pre-sales FAQ

This topic provides answers to some frequently asked questions about pre-sales of Alibaba Cloud Anti-DDoS.

- Does Alibaba Cloud Anti-DDoS provide free services?
- Can Anti-DDoS Pro and Anti-DDoS Premium be billed only when they mitigate DDoS attacks?
- Does Anti-DDoS have trial mitigation plans?
- Can Anti-DDoS Pro and Anti-DDoS Premium protect servers that are not deployed on Alibaba Cloud?
- Can Anti-DDoS Pro and Anti-DDoS Premium protect servers that are not deployed on Alibaba Cloud but have domain names registered with Alibaba Cloud?
- Is ICP filing required for domain names that you want Anti-DDoS Pro or Anti-DDoS Premium to protect?
- What are the regions supported by Anti-DDoS Pro and Anti-DDoS Premium?
- Do Anti-DDoS Pro and Anti-DDoS Premium have limits on the number of protected domains?
- Do Anti-DDoS instances support wildcard domains?
- What are the limits for the ports that can be added to Anti-DDoS Pro?
- What are the prerequisites for activating Anti-DDoS Premium?
- Does the basic protection bandwidth provided by Anti-DDoS Pro apply to all traffic or only attack traffic?

Does Alibaba Cloud Anti-DDoS provide free services?

Yes, Alibaba Cloud Anti-DDoS provides free services. Anti-DDoS Origin Basic is activated for every Alibaba Cloud user. Anti-DDoS Origin Basic mitigates DDoS attacks of up to 5 Gbit/s free of charge. 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 protection 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 charges incurred from mitigating DDoS attacks. Anti-DDoS Origin Basic mitigates DDoS attacks of up to 5 Gbit/s free of charge. When the volume of the DDoS attacks exceeds 5 Gbit/s, Anti-DDoS Origin Basic blocks all traffic to the victim to avoid additional mitigation fees.

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

No, Anti-DDoS Pro and Anti-DDoS Premium are still billed when they are not working. Anti-DDoS Pro and Anti-DDoS Premium are billed on a subscription basis. You must purchase Anti-DDoS Pro or Anti-DDoS Premium instances and complete the payment before you can use the instances to mitigate DDoS attacks. The protection takes effect for the duration of your subscription.

Does Anti-DDoS have trial mitigation plans?

- Anti-DDoS Origin: Anti-DDoS Origin Basic is a free mitigation plan and provides up to 5 Gbit/s protection for public IP addresses of Alibaba Cloud resources. Anti-DDoS Origin Enterprise is a paid mitigation plan, and no free trials are provided.

 **Notice** We recommend that you use Anti-DDoS Origin Basic to test the mitigation capability of Anti-DDoS Origin and then upgrade your service to Anti-DDoS Origin Enterprise. The upgrade process is completely transparent and does not affect your network and connections.

- Anti-DDoS Pro and Anti-DDoS Premium: Anti-DDoS Pro and Anti-DDoS Premium rely on dedicated data centers to provide traffic scrubbing services. This incurs high costs. No free trials are provided.

Can Anti-DDoS Pro and Anti-DDoS Premium protect servers that are not deployed on Alibaba Cloud?

Yes, Anti-DDoS Pro and Anti-DDoS Premium can protect servers that are not deployed on Alibaba Cloud. Anti-DDoS Pro and Anti-DDoS Premium can protect servers that are assigned public IP addresses. If your service uses a public IP address and is accessible over the Internet, you can use Anti-DDoS Pro or Anti-DDoS Premium to protect your service. For more information, see [What are Anti-DDoS Pro and Anti-DDoS Premium?](#).

Can Anti-DDoS Pro and Anti-DDoS Premium protect servers that are not deployed on Alibaba Cloud but have domain names registered with Alibaba Cloud?

Yes, Anti-DDoS Pro and Anti-DDoS Premium can protect servers that are not deployed on Alibaba Cloud but have domain names registered with Alibaba Cloud. If you want to use Anti-DDoS Pro to protect the domain names, you must ensure that Internet Content Provider (ICP) filing is completed for the domain names.

Is ICP filing required for domain names that you want Anti-DDoS Pro or Anti-DDoS Premium to protect?

If you use Anti-DDoS Pro to protect domain names, you must complete ICP filing for the domain names. If you use Anti-DDoS Premium to protect domain names, ICP filing is not required. However, your service must be legal.

For more information, see [ICP filing application overview](#).

What are the regions supported by Anti-DDoS Pro and Anti-DDoS Premium?

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

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

Yes, Anti-DDoS Pro and Anti-DDoS Premium have limits on the number of protected domains.

- By default, each Anti-DDoS Pro instance supports a maximum of 50 domains, only 5 of which can be second-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 the number of domains when you purchase an Anti-DDoS Pro or Anti-DDoS Premium instance. Each Anti-DDoS Pro or Anti-DDoS Premium instance supports a maximum of 200 domains. For more information, see [Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance](#).

Do Anti-DDoS instances support wildcard domains?

Yes, Anti-DDoS Pro and Anti-DDoS Premium support wildcard domains. 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 left most part of a domain name. The record resolves all matching subdomains to the domain. For example, when you specify *.aliyundoc.com as a DNS record, all subdomains that match *.aliyundoc.com are resolved to www.aliyundoc.com.

What are the limits for the ports that can be added to Anti-DDoS Pro?

No limits are imposed on the ports that can be added to Anti-DDoS Pro. You can add web services by using ports that range from 80 to 65535 to Anti-DDoS Pro instances that use the **Enhanced function plan**. For more information, see [Specify custom ports](#).

However, security risks may be caused by vulnerable ports, and ISPs block service traffic that is destined for the vulnerable ports. Vulnerable TCP ports include ports 42, 135, 137, 138, 139, 445, 593, 1025, 1434, 1068, 3127, 3128, 3129, 3130, 4444, 5554, 5800, 5900, and 9996.

If your website that is protected by Anti-DDoS Pro uses the preceding vulnerable ports, your website may be inaccessible in some regions. Therefore, before you add your web service to Anti-DDoS Pro, make sure that the website does not use the vulnerable ports.

What are the prerequisites for activating 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. ICP filing is not required for the domain name but your website must be legal. If you want to use Anti-DDoS Premium to protect a non-website service, you need only to add the service port to your Anti-DDoS Premium instance.

Does the basic protection bandwidth provided by Anti-DDoS Pro apply to all traffic or only attack traffic?

The basic protection bandwidth provided by an Anti-DDoS Pro instance is the guaranteed bandwidth for handling both normal and attack traffic of the workloads protected by the instance. All traffic must first pass through the Anti-DDoS traffic scrubbing centers. Attack 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 (billed daily)**.

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 **Deactivate blackhole filtering**.
- You can also configure automated response to and deactivation of blackhole filtering. For more information, see **Best practices for automatic deactivation of blackhole filtering**.

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 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 an Anti-DDoS Origin Enterprise instance](#) and [Purchase an Anti-DDoS Origin Enterprise instance](#).

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 [What is Anti-DDoS Origin?](#).

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

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

- [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 traffic volume exceeds the clean bandwidth of an Anti-DDoS Pro or Anti-DDoS Premium instance?](#)
- [Can I manually deactivate blackhole filtering?](#)
- [What are the back-to-origin CIDR blocks of an Anti-DDoS Pro or Anti-DDoS Premium instance?](#)
- [Are the back-to-origin CIDR blocks of an Anti-DDoS Pro or Anti-DDoS Premium instance automatically added to a whitelist?](#)
- [Can I use an internal IP address as the IP address of the origin server for an Anti-DDoS Pro or Anti-DDoS Premium instance?](#)
- [I have changed the IP address of the origin server for an Anti-DDoS Pro or Anti-DDoS Premium instance. Does the change immediately take effect?](#)
- [How do I identify which website is under attack when multiple websites 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 that are protected by an Anti-DDoS Pro or Anti-DDoS Premium instance?](#)
- [Can I configure session persistence in the Anti-DDoS Pro or Anti-DDoS Premium console?](#)
- [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?](#)
- [Do Anti-DDoS Pro and Anti-DDoS Premium support mutual HTTPS authentication?](#)
- [Why am I unable to access HTTPS websites by using a browser of an earlier version or from an Android mobile client?](#)
- [Which SSL protocols and cipher suites are supported by Anti-DDoS Pro and Anti-DDoS Premium?](#)
- [How do Anti-DDoS Pro and Anti-DDoS Premium ensure the security of an uploaded certificate and its private key? Do Anti-DDoS Pro and Anti-DDoS Premium decrypt HTTPS traffic and record the content of HTTPS requests?](#)
- [What are the limits on the numbers of ports and domain names that can be protected by an Anti-DDoS Pro or Anti-DDoS Premium instance?](#)
- [Why does the traffic chart show a traffic scrubbing event even though the volume of the traffic received by the server does not exceed the traffic scrubbing threshold?](#)
- [Can Anti-DDoS Pro and Anti-DDoS Premium protect websites that use NTLM authentication?](#)
- [Do the ports that are enabled in Anti-DDoS Pro or Anti-DDoS Premium affect my service security?](#)

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

An expired instance can no longer protect your services.

- After the instance expires, the instance continues to forward your traffic for seven days. If the traffic volume exceeds the clean bandwidth of the instance, throttling is triggered, and random packet loss may occur.
- After the instance expires seven days, the instance stops forwarding traffic. 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 inbound or outbound traffic of the protected services, 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 an instance](#).

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

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

Can I manually deactivate blackhole filtering?


The answer to this question varies based on the instance that you use.

- If you use an Anti-DDoS Pro instance, you can manually deactivate blackhole filtering.

Each Alibaba Cloud account can deactivate blackhole filtering up to five times a day. The limit is reset at 00:00 the next day. For more information, see [Deactivate blackhole filtering](#).

- If you use an Anti-DDoS Premium instance, you cannot manually deactivate blackhole filtering.

Unlike an Anti-DDoS Pro instance, which has a fixed protection bandwidth, an Anti-DDoS Premium instance mitigates DDoS attacks with all the capabilities that are available. You do not need to manually deactivate blackhole filtering for an Anti-DDoS Premium instance.

 **Note** If you use an Anti-DDoS Premium instance with the **Insurance** plan, and the quota for advanced mitigation sessions in the current month is exhausted, blackhole filtering is triggered after your service is attacked. In this case, we recommend that you upgrade your instance to the **Unlimited** plan, which provides unlimited protection capabilities. After you upgrade your instance to the **Unlimited** plan, blackhole filtering is automatically deactivated.

What are the back-to-origin CIDR blocks of an Anti-DDoS Pro or Anti-DDoS Premium instance?

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 an Anti-DDoS Pro or Anti-DDoS Premium instance automatically added to a whitelist?

No, the back-to-origin CIDR blocks are not automatically added to a whitelist. If you deploy a firewall or third-party security software on your origin server, you must add the back-to-origin CIDR blocks of your Anti-DDoS Pro or Anti-DDoS Premium instance to the whitelist of the firewall or 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 IP address of the origin server for an Anti-DDoS Pro or Anti-DDoS Premium instance?

No, you cannot use an internal IP address as the IP address of the origin server. This is because Anti-DDoS Pro and Anti-DDoS Premium forward traffic to origin servers only over the Internet.

I have changed the IP address of the origin server for an Anti-DDoS Pro or Anti-DDoS Premium instance. Does the change immediately take effect?

No, the change takes effect about 5 minutes later. 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 websites are protected by an Anti-DDoS Pro or Anti-DDoS Premium instance?

If websites are targeted by volumetric DDoS attacks, you cannot identify which website is under attack from the dimension of data packets. We recommend that you add your websites to different instances. This way, you can separately view the monitoring data of each website.

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

Yes, Anti-DDoS Pro and Anti-DDoS Premium 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 for non-website services in the Anti-DDoS Pro or Anti-DDoS Premium 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 that are protected by an Anti-DDoS Pro or Anti-DDoS Premium instance?

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

Can I configure session persistence in the Anti-DDoS Pro or Anti-DDoS Premium console?

Yes, you can configure session persistence for non-website services in the Anti-DDoS Pro or Anti-DDoS Premium 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 period. If the network of a client is changed from a wired network or 4G network to a wireless network, session persistence fails because the IP address of the client changes.

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


The default timeout period is 900 seconds.

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?

The answer to this question varies based on the instance that you use. If you use an Anti-DDoS Pro instance of the Enhanced function plan, IPv6 is supported. If you use an Anti-DDoS Premium instance, IPv6 is not supported.

 **Note** By default, an Anti-DDoS Pro instance uses IPv4 addresses to forward access requests. If you require an instance to forward access requests by using IPv6 addresses, submit a or contact sales personnel. Before you apply for such an instance, you must purchase an Anti-DDoS Pro instance of the Enhanced function plan.

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?](#).

Do Anti-DDoS Pro and 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 a browser of an earlier version or from an Android mobile client?

You are unable to access HTTPS websites because the browser or client may 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 and Anti-DDoS Premium?

The following SSL protocols are supported: TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.

The following cipher suites are supported:

- 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


For more information, see [Customize a TLS policy](#).

How do Anti-DDoS Pro and Anti-DDoS Premium ensure the security of an uploaded certificate and its private key? Do Anti-DDoS Pro and Anti-DDoS Premium decrypt HTTPS traffic and record the content of HTTPS requests?

If you use Anti-DDoS Pro or Anti-DDoS Premium to protect HTTPS services, you must upload the required HTTPS certificate and its private key. This way, Anti-DDoS Pro and Anti-DDoS Premium can decrypt HTTPS traffic to detect attacks and analyze the characteristics of attacks. Alibaba Cloud uses a dedicated key server to store and manage private keys. The key server is based on Alibaba Cloud Key Management Service (KMS) and can ensure the data security, integrity, and availability of both certificates and private keys. This helps meet the requirements for regulation, classified protection, and compliance. For more information about KMS, see [What is Key Management Service?](#).

Anti-DDoS Pro and Anti-DDoS Premium use an uploaded certificate and its private key to decrypt HTTPS traffic only when they detect attacks in real time. Anti-DDoS Pro and Anti-DDoS Premium record only specific content of request payloads. The content is determined based on attack characteristics. Then, Anti-DDoS Pro and Anti-DDoS Premium can provide attack reports and data statistics based on the content. Anti-DDoS Pro and Anti-DDoS Premium can record the full content of requests or responses only when they are authorized.

Anti-DDoS Pro and Anti-DDoS Premium have been accredited against authoritative standards, including ISO 9001, ISO 20000, ISO 27001, ISO 27017, ISO 27018, ISO 22301, ISO 27701, ISO 29151, BS 10012, CSA STAR, MLPS level 3, Service Organization Control (SOC) 1, SOC 2, SOC 3, Cloud Computing Compliance Criteria Catalogue (C5), Outsourced Service Providers Audit Report (OSPAR), ISO 27001 (Indonesia), and Payment Card Industry Data Security Standard (PCI DSS). The standards also include those that prove the effectiveness of Anti-DDoS Pro and Anti-DDoS Premium across financial sectors in Hong Kong (China) and the Philippines. In addition, Anti-DDoS Pro and Anti-DDoS Premium provide the same security and compliance qualifications as Alibaba Cloud. For more information, visit [Alibaba Cloud Trust Center](#).

 **Note** If you use Anti-DDoS Pro or Anti-DDoS Premium to protect HTTPS services, you can use a dual-certificate method. This method allows you to independently use a set of certificate and private key on both your Anti-DDoS Pro or Anti-DDoS Premium instance and the origin server. The two sets of certificates and private keys must be valid. This way, the key server can separately manage the certificates and private keys.

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

- The following list describes the maximum number of ports that can be protected:
 - 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.
- The following list describes the maximum number of domain names that can be protected:
 - 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 volume 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. The packets include small SYN packets and packets that do not meet TCP requirements due to specific reasons, such as invalid SYN flags. In this case, your server does not allocate resources to manage these malformed packets. These malformed packets are counted in the scrubbed traffic statistics. Therefore, the traffic chart may show a traffic scrubbing event even though the volume of the traffic received by the server does not exceed the traffic scrubbing threshold.

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

No, Anti-DDoS Pro and Anti-DDoS Premium cannot protect websites that use New Technology LAN Manager (NTLM) authentication. The website requests forwarded by an Anti-DDoS Pro or Anti-DDoS Premium instance cannot pass the NTLM authentication of the origin server. In this case, the clients receive repeated authentication requests. We recommend that you use other authentication methods for your website.

Do the ports that are enabled in Anti-DDoS Pro or Anti-DDoS Premium affect my service security?

No, the back-to-origin CIDR blocks are not automatically added to a whitelist. the ports enabled in Anti-DDoS Pro or Anti-DDoS Premium do not affect your service security.

Anti-DDoS Pro and Anti-DDoS Premium provide traffic access and forwarding. Ports are predefined in a protection cluster. You can use the predefined ports to protect your services after you add your websites to an Anti-DDoS Pro and Anti-DDoS Premium instance. The traffic destined for each domain name or port that is added to the instance is forwarded to the origin server only by using the specified ports. You can specify the ports when you add a domain name or port to the instance. Only the access requests over the ports that are specified in an Anti-DDoS Pro or Anti-DDoS Premium instance are forwarded to the origin server. If you enable the ports that are not specified in an Anti-DDoS Pro or Anti-DDoS Premium instance, no security risks or threats are imposed on your origin server.

5. FAQ about the billing of burstable protection

This topic provides answers to some commonly asked questions about the billing of burstable protection provided by Anti-DDoS Pro.

- If no attacks are detected, are burstable protection fees charged?
- 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 is the maximum mitigation capacity?
- What happens if the size of DDoS attacks exceeds the burstable protection bandwidth?
- If the basic protection bandwidth is 30 Gbit/s, the burstable protection bandwidth is 50 Gbit/s, and the size of DDoS attacks is 45 Gbit/s, how is burstable protection charged?
- Can I change the burstable protection bandwidth from 100 Gbit/s to 200 Gbit/s?
- If the basic protection bandwidth of 30 Gbit/s provided by the Anti-DDoS Pro instance cannot meet my requirements, can I increase the protection bandwidth anytime?
- If an IP address is attacked multiple times in a day, how is the mitigation fee calculated?
- How do I prevent an Anti-DDoS Pro instance from providing burstable protection?

If no attacks are detected, are burstable protection fees charged?

No, if no attacks are detected, no burstable protection fees are charged. Only subscription fees for basic protection are charged.

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 is the maximum mitigation capacity?

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 the basic protection bandwidth, the maximum mitigation capacity is 20 Gbit/s. In this case, your Anti-DDoS instance does not provide burstable protection.

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

If the size of DDoS attacks exceeds the burstable protection bandwidth, the traffic that is destined for the protected IP addresses is forwarded by using null routes.

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

Burstable protection is charged based on the difference between the peak traffic throughout of DDoS attacks and the basic protection bandwidth. In this example, you are charged only for the burstable protection bandwidth of 15 Gbit/s.

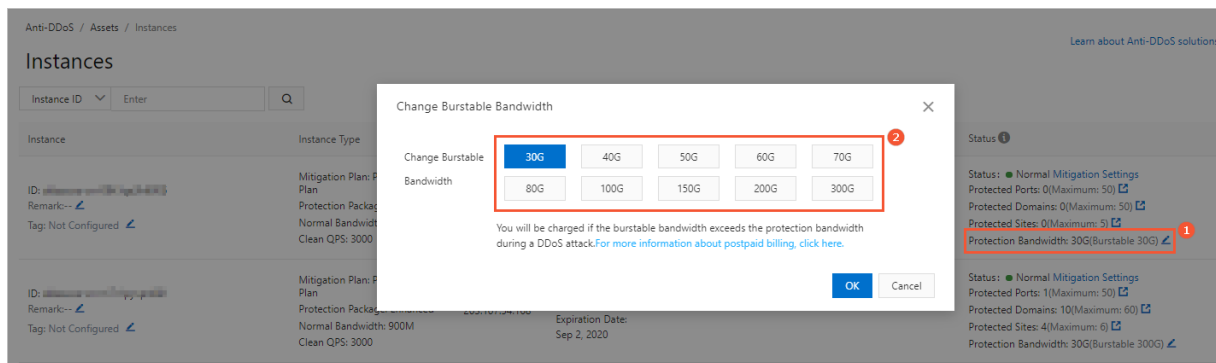
For more information about the pricing of burstable protection, visit the [Anti-DDoS Pricing page](#). In this example, you are charged based on the burstable protection bandwidth of 15 Gbit/s at the price of USD 330/day.

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 change the burstable protection bandwidth from 100 Gbit/s to 200 Gbit/s.

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.



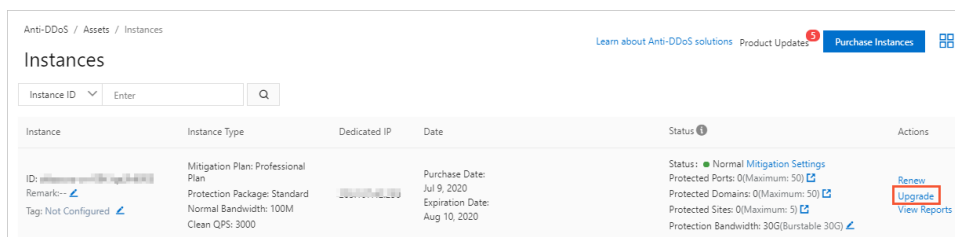
Note If burstable protection on the day when you change the burstable protection bandwidth is already charged, the system starts to charge burstable protection based on the newly selected bandwidth the next day.

If the basic protection bandwidth of 30 Gbit/s provided by the Anti-DDoS Pro instance cannot meet my requirements, can I increase the protection bandwidth anytime?

Yes, you can increase the basic protection bandwidth or burstable protection bandwidth.

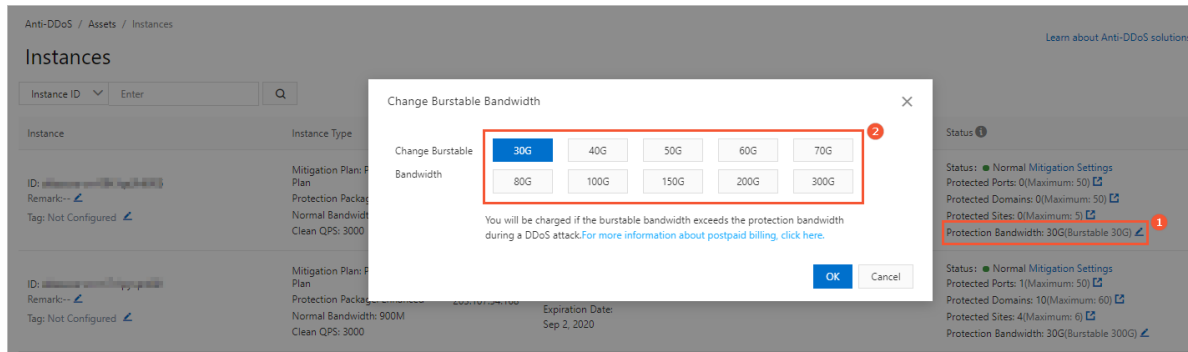
- Increase the basic protection bandwidth

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 an 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 traffic throughout of DDoS attacks and the basic protection bandwidth. For more information, see **Burstable protection: pay-as-you-go (billed daily)**.



If an IP address is attacked multiple times in a day, how is the mitigation fee calculated?

Burstable protection is charged only once based on the peak traffic throughout of DDoS attacks on the same day (from 00:00 to 24:00). For example, if three DDoS attacks are launched to a protected IP address, and the peak traffic throughout 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 traffic throughput (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. If 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.

