Anti-DDoS

FAQs

Copyright Notice

Trademark Notice

Tencent Cloud

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

FAQs
Block Related Issues

Last updated: 2026-03-11 18:01:49

What Should I Do If the IP Protected By DDoS Anti -DDoS Is Blocked?

You have three self-service unlocking chances per day. If you exceed three times in a day, you won't be able to unlock. The system will reset the self-service unlocking count at midnight every day, and the unused unlocking chances won't be carried over to the next day.

If the Number Of Unblocking Times Is Used Up:

- For users who have not purchased DDoS high defense, it is recommended to purchase Anti-DDoS Pro. The device can be unblocked upon first binding.
- For users who have purchased DDoS high defense, it is recommended to upgrade the protection package to unblock in advance.

For details, see: Business is blocked due to large-scale traffic attacks .

Why Is Blocking Carried Out?

Tencent Cloud reduces cloud costs by sharing infrastructure. All users share Tencent Cloud's public egress IP address. When a large-scale traffic attack occurs, it may not only affect the targeted object but also the entire Tencent Cloud network. To prevent the attack from affecting other unattacked users and ensure the stability of the entire cloud platform network, blocking is necessary.

How Long Will It Be Blocked?

The default blocking duration is 2 hours. The actual blocking duration is related to the blocking trigger count and the attack peak value, and can last up to 24 hours.
The blocking duration is mainly affected by the following factors:

- Whether the attack is continuous: If the attack continues, the blocking time will be extended, and the blocking time will be recalculated from the moment of extension.
- Whether the attack is frequent: Users who are frequently attacked have a higher probability of continuous attacks, and the blocking time will be automatically extended.
- The size of attack traffic: Users who are attacked by extremely large traffic will have their blocking time automatically extended.

> **Note:**

> For users who are blocked too frequently, Tencent Cloud reserves the right to extend the blocking duration and lower the blocking threshold.

Regarding viewing the unblocking time, please see View Blocking Time.

Why Can'T the Block Be Lifted Immediately?

Typically, a DDoS attack will last for a certain duration and will not stop immediately after being blocked. The specific duration is uncertain. Tencent Cloud's security team will set the default blocking duration based on the results of big data analysis.

Since blocking is effective in part of the ISP network, once the attacked public IP is blocked, Tencent Cloud cannot monitor whether the attack traffic has stopped. If the block is lifted while the attack has not ceased, the attacked public IP will be blocked again. Moreover, during the time from unblocking to the effectiveness of reblocking, the attack traffic will directly enter Tencent Cloud's basic network, which may affect other users within the cloud. Additionally, blocking is a service purchased by Tencent Cloud from the ISP, and there are limitations on the number of unblocking times and frequency.

Why Is There a Times Limit For Self -Service Unlocking? What Are the Limits?

Blocking is a service purchased by Tencent Cloud from the ISP, and the ISP has clear unblocking time and frequency limitations, so the blocking status cannot be manually lifted frequently.

- Users of Anti-DDoS Pro (excluding the lightweight edition and inclusive edition) and Anti-DDoS Advanced will have three self-service unlocking opportunities per day. If the number exceeds three in a day, unlocking operations will not be available. The system will reset the self-service unlocking count at midnight every day, and the unused unlocking opportunities will not be carried over to the next day.
- Users of the lightweight edition of Anti-DDoS Pro are provided with three self-service unlocking capabilities per month, which can only be used to unlock lightweight server resources.
- Users of the 10Gbps specification of Anti-DDoS Pro (inclusive edition) are provided with three self-service unlocking capabilities per month. If the number exceeds three in a month, unlocking operations will not be available.

Can the Server IP Be Replaced If the IP Is Blocked?

Server IP replacement is not supported during blocking; it can only be done after unblocking.

When your server is blocked due to a DDoS attack, it is not recommended to immediately change the IP. Changing the server IP does not resolve the risk of your server being attacked by DDoS. Frequent IP changes can affect the detection and analysis of the backend protection system and also impact the stability of the cloud platform. Therefore, when your business encounters multiple DDoS attacks, it is recommended to use DDoS high-defense products to improve the protection capability of your business and resolve DDoS security risks.

Attack-Related Issues

Last updated: 2026-03-11 17:59:02

Will There Be a Notification If There Is a DDoS Attack?

After a DDoS attack, the backend will push alarm notifications. Users can also customize the alarm threshold according to their needs. When the traffic reaches the user-set alarm threshold, notifications will be sent. For specific operations, see Setting Security Event Notifications.

Why Does the Server Get a DDoS Attack Even If It Is Not In Use?

- A DDoS attack refers to hackers using DDoS attackers to control multiple machines to attack simultaneously to achieve the purpose of "hindering normal users from using services". Generally, it is mainly aimed at your business, rather than the IP and domain name corresponding to the server.
- If your business connects to public network communication, there is a risk of DDoS attacks.

Why Am I Still Attacked After Purchasing DDoS High-Defense Products?

- If your business communicates with the external network, there is a risk of DDoS attacks.
- DDoS high-defense products protect your business from as little loss as possible under DDoS attacks.

What Is Being Attacked When the Server Is Attacked?

When a server is attacked, it is generally your IP or business that is targeted.

What Are the Common Attack Types?

- Network layer attacks: Common attack types include UDP reflection attacks, SYN flood attacks and connection attacks; These attacks aim to consume server bandwidth resources and connection resources to achieve the purpose of denial of service.
- Application layer attacks: Common attack types include DNS floods, HTTP flood, and CC attacks; These attacks aim to consume server processing performance to achieve the purpose of denial of service.

Where Can I View the Logs Of Server Attacks?

On the Protection Overview page, you can view the attack logs of the server across different time dimensions.

Where Can I View the Attack Source IP?

On the Protection Overview page, select the attack event you want to view, click **View Details**, and you can view the attack source information, attack source region, generated attack traffic, and the size of the attack packet volume.

What Should I Do If My Lightweight Server Is Attacked By DDoS?

Users within Tencent Cloud can effectively resist DDoS attacks and ensure the normal operation of your servers and business by purchasing Anti-DDoS Advanced.

How Much Attack Traffic Will Be Judged As an Attack?

As long as the traffic is detected to contain attack traffic, it is judged to be under attack, regardless of the size. However, users can set alarms based on the size of the attack traffic.

When the Business Is Under DDoS Attack, a Certain Source IP Has Been Added To the Blacklist Of Anti-DDoS Pro, but This IP Can Still Access the Business. Is the DDoS Protection Not Working?

After being added to the blocklist, access sources on the blocklist will not be restricted immediately. When the traffic exceeds the threshold-clearing, only accesses from IPs in the blocklist will be directly blocked.

Features

Last updated: 2026-03-11 17:42:37

Anti-DDoS Pro Package

Does Anti-DDoS Pro Support Off-Cloud IP Connection Protection?

Not supported. Anti-DDoS Pro only provides DDoS protection for public IPs within Tencent Cloud. For protection outside of the cloud, please purchase high-protection IP, which supports the protection of website domains and business ports.

Does Anti-DDoS Pro Support Protection For VPN Gateways?

It is supported.

Does Anti-DDoS Pro Support Protection For Anycast EIP?

AnycastEIP does not support connection to Anti-DDoS packages. If you need DDoS protection, please purchase Anti-DDoS Advanced (Global Enterprise Edition) first and then bind it in the Anti-DDoS IP.

What Happens If the Bound Resource Has Expired but the Anti-DDoS Pro Instance Has Not?

Anti-DDoS Pro instances are purchased monthly and provide protection capabilities through IP. If the protected resource expires and the IP bound to the Anti-DDoS Pro instance is not replaced in time, the Anti-DDoS Pro instance will continue to provide protection for the bound IP during the validity period, but the resource corresponding to that IP may not be yours. It is recommended that you renew your cloud services in time or replace the new protected object IP.

If the Protection Bandwidth Of Anti-DDoS Basic Does Not Exceed 2Gbps, and a Package Of Anti-DDoS Pro Is Purchased, Will the Final Protection Peak Value Be Stacked?

No, the final protection peak value enjoyed by users is based on the protection capability in the Anti-DDoS Pro package purchased, and it will not stack with the default protection bandwidth of Anti-DDoS Basic.
Assuming that a Cloud Virtual Machine's IP originally enjoys free protection bandwidth of no more than 2Gbps. Due to frequent attacks, the user purchased an Anti-DDoS Pro package for the IP, then the maximum protection capability is the maximum protection capability of the current local Anti-DDoS Pro resources.

What Is the Difference Between Anti-DDoS Pro and Anti-DDoS Advanced?

- Protection Object:
  - Anti-DDoS Pro only enhances DDoS protection capabilities for services within Tencent Cloud.
  - Anti-DDoS Advanced is aimed at users both on and off the cloud, supporting website domain names and business port integration protection.
- Integration:
  - The connection configuration of Anti-DDoS Pro is more convenient, and there is no need to change the public IP address.
  - Anti-DDoS Advanced requires modification of DNS Resolution or business IP before integration for protection.

What Is the Difference Between Anti-DDoS Pro and Three-Network High Defense?

Differences	Anti-DDoS Pro Package	Three-Network High Defense
Integration Cost	No need to change the server IP, directly enhance the defense capability of cloud products, take effect immediately, and the access cost is low.	The server IP needs to be changed to a CTCC/CUCC/CMCC IP, and the domain name and port information need to be filled in. The configuration is quite complicated.
Access Quality	By adopting BGP bandwidth, cross-network access delay is reduced, and access speed is increased by more than 30%.	Without BGP bandwidth, there is a large network delay and poor quality.
Pricing Strategy	Sold based on "number of protected IPs + protection times" and provides full protection without additional elastic fees.	Billing is complex and requires payment for traffic fees.

What Does Managed IP Refer To?

Managed IP refers to a customized network routing solution, which is not provided by DDoS high-defense packages, but DDoS high-defense packages support the protection of such products.
If there is a demand for managed IP, you can submit a ticket to apply for use.

What Is the Impact If the Anti-DDoS Pro Exceeds the Protection Threshold?

There is no concept of threshold in Anti-DDoS Pro.

Does Anti-DDoS Pro (Light) Provide 3 Self-Service Unlocking Capabilities?

Provide, Anti-DDoS Pro (Light) offers self-service unlocking capability three times a month.

Does Anti-DDoS Pro (Light)'S Self-Unblock Feature Support Unblocking Non-Lighthouse Resources?

Not supported. Only supports unblocking Lighthouse resources.

Which Version Of Anti-DDoS Pro Needs To Be Purchased When Using a Lightweight Server?

Both versions of Anti-DDoS Pro can be purchased to protect lightweight servers. The difference lies in the protection capability and discount intensity. For details, see Purchase Guide.

DDoS Protective IP

Does Anti-DDoS Advanced Support Integration and Protection For Users Outside Tencent Cloud?

Supported. Anti-DDoS Advanced can protect any public network server, including but not limited to those on Tencent Cloud, other clouds, IDCs, etc.

> ⚠ **Note:**
> Domain names connected in the Chinese mainland must be registered with the ICP in accordance with the requirements of the Ministry of Industry and Information Technology. If a domain name is not registered, Anti-DDoS services cannot be provided.

Does Anti-DDoS IP Support Wildcard Domain Names?

In the website business forwarding rule configuration of Anti-DDoS Advanced, protection for wildcard domain names is supported.
Wildcard domain name resolution refers to using a wildcard (*) as a secondary domain name to ensure all secondary domain names point to the same IP. For example, supporting configuration of *.tencent.com.

What Specific Behavior Patterns Does Behavior Pattern Analysis In DDoS Anti-DDoS IP Security Protection Policy Refer To?

Behavior pattern analysis mainly includes checking for messages with attack patterns, messages that do not conform to protocol specifications, and features of abnormal connection attacks, etc. You can set flexibly according to business characteristics to cope with constantly changing attack methods. For setting details, see Protection Configuration.

Will the Anti-DDoS Advanced Service Automatically Add the Origin-Pull IP Address To the Security Group?

No. Users need to manually add the origin-pull IP range to the CVM security group. If the user has deployed a firewall or other host security protection software at the origin server, the origin-pull IP range also needs to be added to the corresponding allowlist to prevent the high-protection origin-pull IP from being blocked or speed-limited, causing business traffic damage.

Can a Private IP Address Be Filled As the Origin Server IP In the Anti-DDoS High-Defense IP?

Anti-DDoS Advanced pulls from the public network and cannot directly fill in the private network IP.

What Is the Anti-DDoS Origin-Pull IP Address?

After the user business is integrated, the system automatically allocates multiple origin-pull IP addresses. The origin-pull IP address is used as the egress IP of the high-protection IP, directing the clean and filtered normal access traffic to the user's origin server. The egress IP address used is the source IP address of the business traffic seen from the origin server.

Is There a Delay When Modifying the Origin Server IP Of the Anti-DDoS Advanced Service?

There is no delay. Modifying the protected origin server IP of the high-protection IP service can take effect in seconds.

How Long Does It Take For Configuration Changes In the Anti-DDoS IP Service Console To Take Effect?

Changes to the Anti-DDoS IP service configuration take effect in seconds.

Does the Anti-DDoS Advanced Support IPv6 Protocol For IP Origin-Pull?

IPv6 protocol is not supported yet.

Does Anti-DDoS Advanced Support HTTPS Mutual Authentication?

- Website integration does not support HTTPS two-way verification.
- Non-website integration using TCP forwarding supports HTTPS two-way verification.

Does the Anti-DDoS Advanced IP Service Have Packet Capture Files?

Currently, the new Anti-DDoS Advanced IP service does not support downloading attack packet files.

How Does the Anti-DDoS Advanced Load Balance When Configuring Multiple Origin Server IPs?

- Website business uses default round-robin for Cloud Load Balancer.
- Non-website business uses weighted round-robin for sequential forwarding.

How Does Anti-DDoS Advanced IP Distinguish Between Layer-4 and Layer-7 Forwarding?

The Anti-DDoS Advanced IP distinguishes between layer-4 and layer-7 forwarding methods as follows:

- **Layer 4 forwarding**: Uses the method of IP + Port, that is, "port access".
- **Layer 7 forwarding**: Uses the method of domain name access.

What Does the Protection Bandwidth Of DDoS High Defense IP Refer To?

Protection bandwidth is divided into baseline protection bandwidth and elastic protection bandwidth.

- **Baseline protection bandwidth**: Refers to the baseline protection capability of the high-defense IP instance, with the guaranteed part being annual/monthly prepayment.
- **Elastic protection bandwidth**: Refers to the maximum elastic protection capability of the high-defense IP instance, with the elastic part being postpaid by day.
  - If elastic protection is not enabled, the baseline protection bandwidth is the highest protection capability of the high-defense IP instance.
  - If elastic protection is enabled, the elastic protection bandwidth serves as the highest protection capability of the high-defense IP instance.

Blocking is triggered when the attack traffic exceeds the maximum protection capability of the high-defense IP instance.

How Many Forwarding Ports and Domain Names Are Supported By One Anti-DDoS IP?

- Forwarding ports: The total number of forwarding rule entries supported by the TCP/UDP protocol, with 60 provided for free by default, and up to 500 supported at most.
- Number of supported domain names: The total number of forwarding rule entries supported by the HTTP/HTTPS protocol, with 60 provided for free by default, and up to 500 supported at most.

What Is the Quota For IP Allowlist and Blocklist In CC Protection, and Does It Support Scale-Out?

CC protection supports setting 50 IP allowlists and blocklists respectively. If you need to set more IP allowlists and blocklists, you can submit a ticket to apply for scale-out.

What Is Business Bandwidth, and What Impact Will There Be If It Is Exceeded?

The purchased business bandwidth is for the entire high-defense IP instance, referring to the traffic in the IN or OUT direction of all normal services of the instance.
If the user's business traffic exceeds the given specification, traffic speed limit will be triggered, which may cause random packet loss. If this situation persists, please adjust to a larger business bandwidth in time.

> **Note:**
> Tencent Cloud users whose business is in the Chinese mainland will be given a default 100 Mbps forwarding business bandwidth when purchasing Anti-DDoS Advanced services; there is no giveaway outside the Chinese mainland.

Does the Anti-DDoS Pro IP Service Support Session Persistence?

Anti-DDoS Advanced service supports session persistence, which is not enabled by default. Non-website services can be configured through the console. See Configuring session persistence.

Does Anti-DDoS Advanced Support Health Check?

Non-website services enable health check by default. It is recommended to use the default value. If modification is needed, see the operation step Configuring Health Check.

After the User'S Business Is Bound To Anti-DDoS Advanced, Why Is the Access To the Origin Server Slow When the Window Scaling (WS) Is Not Enabled On the Origin Server?

Anti-DDoS server enables Window Scaling (WS) by default. If the origin server does not enable it, receiving slightly larger files may quickly fill up the sliding window and cause delay. It is recommended that users enable WS on all origin servers. For the concept and examples of WS, visit Tencent Community Slow TCP Speed? Pay Attention to WS Window Factor.

FAQs About Billing

Last updated: 2025-03-20 09:54:06

Anti-DDoS Pro Package

Does an Anti-DDoS Pro Instance Take Effect Immediately After Purchase?

Takes effect immediately upon successful purchase and integration.

How Is the Monthly Peak Traffic Value Of 95% Calculated?

Sampling is performed at a granularity of 5 minutes, with one natural month as the statistical duration. At the end of the month, all sampling points are sorted from high to low based on peak values, the top 5% highest peak sampling points are removed, and the 95th percentile highest peak is used as the 95 billing point bandwidth.

For example: Take one traffic point every 5 minutes within a month, 12 points per hour, 12 × 24 points per day, and 12 × 24 × 30 = 8640 points for a month (calculated as 30 days). Remove the top 5% highest points, and the remaining highest bandwidth is the billing value for 95% billing.

What Is the Difference Between the Billing Modes Of Full Protection For Anti-DDoS Pro and Elastic Protection For Anti-DDoS Advanced?

When an attack occurs, the maximum DDoS protection capability of Tencent Cloud in the region of the Anti-DDoS Pro instance will be automatically called to provide full protection, which is included in the instance and will not incur additional resilient protection fees.
The resilient protection of Anti-DDoS Advanced is billed by the bandwidth of the resilient protection range corresponding to the maximum attack traffic generated on the day.

Anti-DDoS IP

How To Bind IP After Purchasing Anti-DDoS Advanced?

You can refer to Website Business Access or Non-website Business Access documentation to bind IP.

How To Select a Circuit?

When purchasing a DDoS high-protection IP, if your server is in mainland China, choose CTCC/CUCC/CMCC; generally, for servers outside mainland China, choose BGP.

How Many Anti-DDoS Advanced Can Be Purchased At the Same Time With a Tencent Cloud Account?

There is currently no limitation on the purchase quantity; generally, all purchase quantities are supported. If you have a particularly large demand and cannot complete the purchase successfully, please submit a ticket to contact us for help.

Is the Elastic Protection Billing Mode Of the Advanced Anti-DDoS Service the Same? How Is It Calculated?

Similarly, after triggering elastic protection, billing is based on the corresponding elastic protection interval after deducting the baseline protection from the highest attack peak of the day. For billing details, see Billing Overview.

For example, if the Anti-DDoS Advanced instance you purchased has a specification of 30Gbps baseline protection bandwidth + 60Gbps elastic protection bandwidth, and if there is a DDoS attack event on that day with the highest attack traffic peak at 45Gbps, since 45Gbps exceeds the baseline protection bandwidth range and triggers elastic protection, it falls into the billing interval of 10Gbps ≤ (attack peak 45Gbps − baseline protection bandwidth 30Gbps = 15Gbps) < 20Gbps. The elastic fee incurred on that day is charged according to the billing interval of 10Gbps ≤ elastic peak < 20Gbps.

If the IP Protected By Anti-DDoS Advanced Is Blocked Due To a Large-Scale Attack, Will That Part Of the Attack Traffic Be Included In the Billing?

The elastic protection billing rule of the Anti-DDoS Advanced service is for attack traffic that exceeds the base protection bandwidth cap and is less than or equal to the elastic protection peak. Blocked means that the attack traffic has exceeded the set elastic protection, so the part of the attack traffic that exceeds the elastic protection is not within the billing range.

After Purchasing Elastic Protection, If No Attack Occurs In a Month, Is There a Fee?

In this case, you only need to pay the monthly fee for the baseline protection, and no other additional fees will be incurred.

Is It Possible To Upgrade the Elastic Protection Bandwidth During an Attack On the Business?

Supported. The elastic protection bandwidth of the Anti-DDoS Advanced service supports both increase and decrease. Different regions support different protection capabilities, and

the range of elastic protection bandwidth can be referred to on the purchase interface.

> **Note:**
> If an attack that occurs on the day has already generated billing, it will be billed based on the latest elastic protection bandwidth the next day after modification.

If a Protected IP Suffers Multiple Attacks Within One Day, Will Multiple Fees Be Charged?

The Anti-DDoS Advanced IP service is billed based on the peak attack traffic bandwidth during the day, and only one fee is charged.

If Two Anti-DDoS Packages Are Purchased and the Attack Traffic Received By Both Anti-DDoS Instances Exceeds the Baseline Protection, How Will the Elastic Protection Fees Be Calculated?

The elastic protection fee is calculated based on the product instance. If two Anti-DDoS instances exceed the baseline protection, the elastic protection fees of the two Anti-DDoS instances need to be charged separately.

How To Get a Refund For Anti-DDoS Advanced?

The Anti-DDoS Advanced service does not support advance unsubscribe and is not applicable for five-day unconditional refunds. If you have used the Anti-DDoS Advanced instance, refunds are not supported at all.