Anti-DDoS

FAQs

Product Documentation

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

FAQs

Blocking

Last updated：2024-07-01 11:41:51

What should I do if the IP protected by Anti-DDoS is blocked?

Each user has three chances of manual unblocking every day. The system resets the chance counter daily at 00:00 midnight. Unused chances will not be carried over to the next day.

If the manual unblocking chances are used up:

If you haven't purchased any Anti-DDoS service, we recommend you purchase Anti-DDoS Pro. Then, you can perform unblocking when binding devices for the first time.

If you have already purchased Anti-DDoS, we recommend you upgrade your protection package so that you can perform unblocking earlier.

For more information, see Business IPs Blocked Due to High-traffic Attacks.

Why is my IP blocked?

Tencent Cloud reduces the costs of cloud services by sharing the infrastructure, with one public IP shared by many users. When a high-traffic attack occurs, the entire Tencent Cloud network may be affected, not only the target servers. To protect other users and ensure network stability, the target server IP needs to be blocked.

How long will blocking last?

An attacked IP is blocked for two hours by default. The actual duration can be up to 24 hours depending on how many times the IP is blocked and how high the peak attack bandwidth is.

The blocking duration is subject to the following factors:

Continuity of the attack: The blocking duration will extend if an attack continues. Once the duration extends, a new blocking cycle will start.

Frequency of the attack: Users who are frequently attacked are more likely to be attacked continuously. In such a case, the blocking duration extends automatically.

Traffic volume of the attack: The blocking duration extends automatically in case of ultra-large volume of attack traffic.

Note:

For IPs that are blocked extra frequently, Tencent Cloud reserves the right to extend the duration and lower the threshold.

To view the unblocking time, see Viewing Blocking Time.

Why can't I unblock my IP immediately?

A DDoS attack usually does not stop immediately after the target IP is blocked and the attack duration varies. Tencent Cloud security team sets the default blocking duration based on big data analysis.

Since IP blocking takes effect in the ISP's network, Tencent Cloud is unable to monitor whether the attack traffic has stopped after the attacked IP is blocked. If the IP is recovered while the attack is still going on, the IP will be blocked again. During the gap between the recovery and re-blocking, Tencent Cloud's classic network will be exposed to the attack traffic, which may affect other Tencent Cloud users. In addition, IP blocking is a service Tencent Cloud purchases from ISPs with limitations on the number of times and the frequency of unblocking.

Why is there a limit on the number of times of manual unblocking? What are the restrictions?

Tencent Cloud pays ISPs for blocking attacked IPs, and ISPs impose limits on the number of times and frequency of unblocking.

Each Anti-DDoS user has three chances of manual unblocking every day. The system resets the chance counter daily at 00:00 midnight. Unused chances will not be carried over to the next day.
This limit also applies to Anti-DDoS Pro (Light) users, who can only use the three chances to unblock Lighthouse resources.

Can I change the server IP if it is blocked?

You can change the server IP only after it is unblocked.
We don't recommend you change the server IP immediately after your server is blocked due to DDoS attacks. Changing the server IP does not eliminate the risk of your server being hit by DDoS attacks. Frequent IP changes will impact the detection and analysis of the backend protection system and the stability of the cloud platform. Therefore, if your business suffers DDoS attacks, we recommend you use Anti-DDoS products to enhance your business's protection capabilities against DDoS attacks.

Attacks

Last updated：2024-07-01 11:41:51

Will I receive alerts for DDoS attacks?

Yes. You will get alert notifications when the inbound traffic exceeds a specified threshold. To learn how to set thresholds, see Configuring Security Event Notifications.

Why does my business suffer DDoS attacks without my business running on the server?

A DDoS attack is an attack involving multiple devices attempting to make your business, rather than the IP or domain name of the server, inaccessible for users.
Your business may be at risk of DDoS attacks if it communicates over the public network.

Why is my business attacked again after I have Anti-DDoS products deployed?

Your business may be at risk of DDoS attacks if it communicates over the public network.
Your business may still be targeted even though it is protected by Anti-DDoS products, but the attacks are less likely to cause losses.

What are the targets when the server is attacked?

DDoS attacks target your IP or business by attacking the server.

What are the common types of attacks?

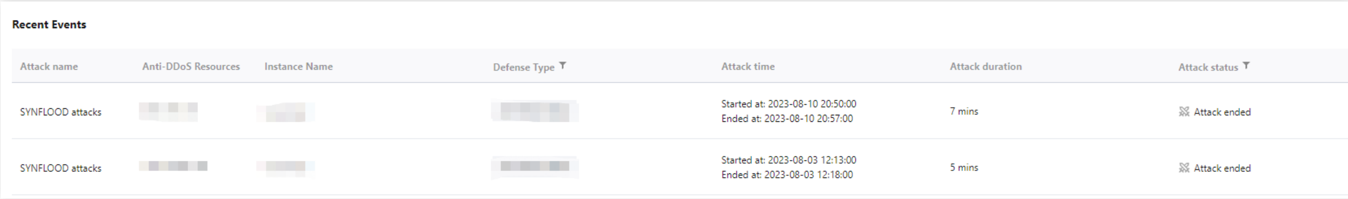
Network layer attacks: include UDP reflection attacks, SYN floods, and connection attacks. Attacks of this type cause a denial of service by consuming server bandwidth and connection resources.
Application layer attacks: include DNS floods, HTTP floods, and CC attacks. Attacks of this type cause a denial of service by exhausting server performance.

Where can I view the logs of attacks on the server?

On the Overview page, you can view the attack logs for different time ranges.

Where can I view the details of the attack source IP?

On the Overview page, select the attack event you want to view, and then click **View details** to check the information and region of the attack source, attack traffic, and attack packet size.



Recent Events

Attack name	Anti-DDoS Resources	Instance Name	Defense Type	Attack time	Attack duration	Attack status
SYNFLOOD attacks	[redacted]	[redacted]	[redacted]	Started at: 2023-08-10 20:50:00 Ended at: 2023-08-10 20:57:00	7 mins	Attack ended
SYNFLOOD attacks	[redacted]	[redacted]	[redacted]	Started at: 2023-08-03 12:13:00 Ended at: 2023-08-03 12:18:00	5 mins	Attack ended

What should I do when my Lighthouse server is under DDoS attacks?

We recommend you purchase an Anti-DDoS Advanced to defend against DDoS attacks and guarantee the availability of your server and business.

How should I identify an attack by the amount of attack traffic?

An attack is identified as long as attack traffic is detected. You can set an alert threshold based on the amount of attack traffic.

I have added the access source IP to the blocklist configured for the Anti-DDoS Pro instance when my business is attacked, but the IP still has access to my business. Is the instance not working?

The access restriction for the IP will not take effect right after it is added to the blocklist. Only when the incoming traffic exceeds the cleansing threshold, the IP will be denied directly from accessing your business.

Features

Last updated：2024-07-01 11:41:51

Anti-DDoS Pro

Does Anti-DDoS Pro support non-Tencent Cloud IPs?

No. Anti-DDoS Pro only provides DDoS protection for public IPs in Tencent Cloud. If you need protection for IPs off Tencent Cloud, purchase Anti-DDoS Advanced, which supports protection for website domain names and service ports.

Does Anti-DDoS Pro provide protection for VPN gateways?

Yes.

Does Anti-DDoS Pro provide protection for Anycast EIPs?

Anycast EIPs cannot be connected to Anti-DDoS Pro. However, you can purchase an Anti-DDoS Advanced (Global Enterprise) instance and bind it to your Anycast EIP for protection.

What if the bound resource has expired but the Anti-DDoS Pro instance has not?

An Anti-DDoS Pro instance is purchased by month, and provides protection based on IPs. If the resource protected by your Anti-DDoS Pro instance expires and you do not change the IP bound to the instance, the instance will continue to provide protection for the bound IP, but the resource corresponding to the IP may not be yours. It is recommended to renew your Tencent Cloud resources or change the IP you want to protect in time.

The protection bandwidth of Anti-DDoS Basic is no greater than 2 Gbps. If I purchase an Anti-DDoS Pro instance, will the final protection bandwidth be the sum of the two?

No. In such a case, the final protection bandwidth you enjoy will be the protection bandwidth of the Anti-DDoS Pro instance. The default protection bandwidth of Anti-DDoS Basic will not be added to it.

For example, if a CVM IP has a free protection bandwidth of no greater than 2 Gbps and you purchase an Anti-DDoS Pro instance for it, the maximum protection capability the CVM IP enjoys will be the maximum protection capability of the Anti-DDoS Pro instance in the current region.

What are the differences between Anti-DDoS Pro and Anti-DDoS Advanced?

Protection coverage:

Anti-DDoS Pro provides DDoS protection only for services within Tencent Cloud.

Anti-DDoS Advanced is for users both in and off Tencent Cloud and supports protection for website domain names and service ports.

Connection:

Anti-DDoS Pro is easy to connect and you do not need to change your public IPs.

To connect to Anti-DDoS Advanced, you need to modify DNS or your business IPs.

What are the differences between Anti-DDoS Pro and non-BGP protection?

Difference	Anti-DDoS Pro	Non-BGP protection
Low-cost connection	Enhanced protection capability for your cloud resources and low-cost connection without the need to change your server IPs.	Complicated configuration where you need to replace your server IPs with non-BGP IPs and enter the domain name and port information.
Access quality	It uses BGP bandwidth and offers a lower access latency across networks and 30% higher access speed.	It has no BGP bandwidth with a high network latency and poor quality.
Pricing policy	Billed according to the "number of protected IPs + protection times" with all-out protection available at no additional elastic costs.	Billed in a complicated manner with traffic fees incurred.

What is a managed IP?

A managed IP refers to a customized network routing solution, which is not provided by but can be protected by Anti-DDoS Pro.

If you need managed IPs, submit a ticket.

What will happen if the protection threshold of Anti-DDoS Pro is exceeded?

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

Does Anti-DDoS Pro Light allow three chances per month to manually unblock IPs?

Yes.

Does Anti-DDoS Pro Light allow chances to manually unblock IPs for Lighthouse resources?

No.

Which edition of Anti-DDoS Pro should I purchase if I use Lighthouse?

Both editions of Anti-DDoS Pro can be purchased to protect Lighthouse instances. The difference lies in the protection capabilities and discounts. For more information, see Billing Overview.

Anti-DDoS Advanced

### Is Anti-DDoS Advanced available for non-Tencent Cloud users?

Yes. Anti-DDoS Advanced is available for any servers with access to internet, including but not limited to those in Tencent Cloud, other clouds, and customer IDCs.

Note:

ICP filing issued by the Chinese MIIT is required for all domain names connected to Anti-DDoS Advanced in the Chinese mainland.

Does Anti-DDoS Advanced support wildcard domain names?

Yes. You can use it to protect wildcard domain names by configuring website traffic forwarding rules.
Wildcard domain name resolution involves using wildcards (\\*) as secondary domain names to allow all secondary domain names to point to the same IP. For example, you can configure \\*.tencent.com.

What exactly does behavior pattern analysis refer to in Anti-DDoS Advanced security protection policy?

Behavior pattern analysis mainly includes the identification of packets with attack characteristics, packets that do not comply with the protocol specifications, abnormal connections, and so on. You can configure behavior pattern analysis based on your business needs to cope with the ever-changing attack techniques. For more information, see Protection Configurations.

Does Anti-DDoS Advanced automatically add forwarding IPs to a security group?

No. You need to manually add the forwarding IP range to a CVM security group. If you have deployed a firewall or other host security protection software on the real server, you also need to add the forwarding IP range to the allowlist to prevent business traffic from being affected by IP blocking or speed restriction.

Can I set a private IP as the real server IP in Anti-DDoS Advanced?

No. Anti-DDoS Advanced forwards traffic to the real server over the public network. Therefore, you cannot use a private IP.

What is a forwarding IP in Anti-DDoS Advanced?

After you connect your business to Anti-DDoS, the system automatically assigns multiple forwarding IPs to you. The forwarding IPs are used as the egress IPs of your Anti-DDoS instance to forward cleansed access traffic to your real server. For the real server, the egress IPs are the source IPs of business traffic.

How long does it take for a real server IP update to take effect?

Changes to the real server IP protected by Anti-DDoS Advanced take effect in seconds.

How long does it take for configuration changes in the Anti-DDoS Advanced console to take effect?

Changes to Anti-DDoS Advanced service configurations take effect in seconds.

Does Anti-DDoS Advanced support IPv6 protocol for traffic forwarding?

No.

Does Anti-DDoS Advanced support HTTPS mutual authentication?

For websites, HTTPS mutual authentication is not supported.

For non-websites using TCP, HTTPS mutual authentication is supported.

Does Anti-DDoS Advanced have packet capture files?

Currently, the new Anti-DDoS Advanced does not provide attack packet files for download.

How does Anti-DDoS Advanced deal with load balancing if multiple real server IPs are configured?

For website businesses, default round-robin load balancing is used.

For non-website businesses, weighted round-robin load balancing is used to forward traffic to real server IPs in turn.

What are the differences between L4 and L7 forwarding?

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

Layer-4 forwarding: uses the "IP + port" method, that is, "connection via port".

Layer-7 forwarding: uses the "connection via domain" method.

What is protection bandwidth in Anti-DDoS Advanced?

There are two types of protection bandwidth: base protection bandwidth and elastic protection bandwidth.

Base protection bandwidth: refers to the base protection capability of an Anti-DDoS Advanced instance. Base protection bandwidth is a prepaid monthly subscription feature.

Elastic protection bandwidth: refers to the maximum protection capability of an Anti-DDoS Advanced instance. The part that exceeds the base protection bandwidth is billed on a daily pay-as-you-go basis.

If elastic protection is not enabled for an instance, its maximum protection capability will be the base protection bandwidth.

If elastic protection is enabled for an instance, its maximum protection capability will be the elastic protection bandwidth.

When the attack traffic exceeds the maximum protection capability of an instance, IP blocking will be triggered.

How many forwarding ports and domain names are supported by a single Anti-DDoS Advanced instance?

Forwarding ports: 60 forwarding rules for TCP/UDP protocol are provided free of charge by default. Up to 500 ports can be supported.
Domain names: 60 forwarding rules for HTTP/HTTPS protocol are provided free of charge by default. Up to 500 domain names can be supported.

How many IPs can be added to the blocklist and allowlist of CC protection respectively? Do they support expansion?

You can add up to 50 IPs to the blocklist and allowlist of CC protection respectively. If you need to add more, submit a ticket.

What is business bandwidth? What will happen if its value is exceeded?

The business bandwidth purchased is for the entire Anti-DDoS Advanced instance. It refers to the incoming and outgoing normal business traffic to and from the instance.
If your business traffic exceeds the free tier, it will trigger traffic speed limit, which may result in random packet loss. If this problem persists, please upgrade the business bandwidth in time.
Note:
Tencent Cloud users who purchase Anti-DDoS Advanced and whose business is deployed in the Chinese mainland will be given 100 Mbps forwarding service bandwidth for free by default. This offer is not available for businesses deployed outside the Chinese mainland.

Does Anti-DDoS Advanced support session persistence?

Anti-DDoS Advanced supports session persistence, which is not enabled by default. For non-website businesses, you can configure this feature in the console as instructed in Configuring Session Persistence.

Does Anti-DDoS Advanced support health check?

Health check is enabled by default for non-website businesses, which is recommended. You can modify this feature as instructed in Configuring Health Check.

WS is not enabled on my real server. After I bind my business to Anti-DDoS Advanced, why is access to the real server slow?

Anti-DDoS servers have Window Scaling (WS) enabled by default. If WS is not enabled on the real server, a delay will occur when the sliding window is filled up while receiving slightly larger files. You are recommended to enable WS for your real server. For more information about WS, contact us.

Billing

Last updated：2024-07-01 11:41:51

Anti-DDoS Pro

Does an Anti-DDoS Pro instance take effect immediately after purchase?

It will take effect immediately after successful purchase and connection.

How is the monthly 95th percentile bandwidth calculated?

In each calendar month, the inbound/outbound bandwidth is sampled every five minutes. At the end of the month, all the sampled values are sorted from highest to lowest and the top 5% are removed. The highest value left is the 95th percentile, which will be the billable bandwidth of the month.

For example, one traffic point is taken every five minutes in a month, so there are 12 points in an hour, 12 x 24 points in a day, 12 x 24 x 30 = 8640 points in the month (30 days); the highest 5% of the values are removed, and the remaining highest bandwidth is the billable 95th percentile bandwidth.

What are the billing differences between the all-out protection of Anti-DDoS Pro and the elastic protection of 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 all-out protection, which is included in the instance and will not incur additional fees.
The elastic protection of Anti-DDoS Advanced is billed by the elastic protection bandwidth range corresponding to the maximum attack traffic generated on the day.

Anti-DDoS Advanced

How do I bind an IP to the purchased Anti-DDoS Advanced instance?

Please see Website Business Connection or Non-Website Business Connection.

How do I select a proper line?

If your server is in the Chinese mainland, select the non-BGP line for your Anti-DDoS Advanced instance during purchase. Otherwise, select the BGP line.

Can one Tencent Cloud account purchase multiple Anti-DDoS Advanced instances at once?

Currently, we haven't set a limit on the number of instances. If you have special needs for a huge number of instances but failed to purchase them, please submit a ticket to us for assistance.

Are the billing modes the same for elastic protection of different Anti-DDoS services? How are the fees for elastic protection calculated?

Yes, they are. Elastic protection is billed based on the tiered price of the elastic bandwidth of the day (peak attack bandwidth minus base protection bandwidth). For more information, see Billing Overview.

For example, you have purchased an Anti-DDoS Advanced instance with 30 Gbps base protection bandwidth and 60 Gbps elastic protection bandwidth. A DDoS attack occurs one day with a peak attack traffic bandwidth of 45 Gbps. Since 45Gbps exceeds the base protection bandwidth and triggers elastic protection, and the billable elastic bandwidth (45 Gbps - 30 Gbps = 15 Gbps) falls within the range between 10 Gbps and 20 Gbps, the fees for elastic protection of the day will be billed according to the tiered price of the billing tier between 10 Gbps and 20 Gbps.

If the IP protected by my Anti-DDoS Advanced instance is blocked due to large-traffic attacks, will I be billed for the attack traffic over the maximum protection bandwidth?

No. You will be billed for elastic protection when the attack traffic exceeds the base protection bandwidth but is lower than or equal to the elastic protection bandwidth. If your IP is blocked, it means that the attack traffic already exceeds the elastic protection bandwidth. Therefore, you will not be billed for the excessive attack traffic.

I enabled elastic protection a month ago but no attack has occurred so far. Do I still have to pay for this feature?

In this case, you only need to pay the monthly subscription fees for base protection. No additional fees will be incurred.

Can I increase the elastic protection bandwidth when my business is under attack?

Yes. You can increase or decrease the elastic protection bandwidth of an Anti-DDoS Advanced instance. The protection capability varies by region. For more information on the range of elastic protection bandwidth, please visit the purchase page.

Note:

If protection fees have already been incurred on the day you make the modification, you will be billed according to the latest elastic protection bandwidth on the following day.

If a protected IP is attacked several times in a day, will I be charged repeatedly?

The Anti-DDoS Advanced service is billed based on the peak attack traffic bandwidth during a day. Therefore, you will not be charged repeatedly for multiple attacks in a day.

I have purchased two Anti-DDoS instances, and both of them are under attack traffic that exceeds the base protection bandwidth. How will I be charged for elastic protection?

Elastic protection is billed by instance. If both of your Anti-DDoS instances are under attack traffic that exceeds the base protection bandwidth, you will need to pay for elastic protection for the two instances separately.

How do I get a refund for my Anti-DDoS Advanced instance?

Tencent Cloud Anti-DDoS Advanced does not support return or five-day unconditional refund if you already have used the instance.