Anti-DDoS Advanced

FAQs

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

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：2022-08-16 11:36:42

Why is my IP blocked?

Tencent Cloud reduces 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.

Why can't my IP be unblocked 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 ISP network, Tencent Cloud cannot monitor whether the attack traffic has stopped after the attacked public IP is blocked. If the IP is unblocked but the attack is still going on, the IP will be blocked again. During the gap between the IP being unblocked and blocked again, 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 purchased from ISPs with restrictions on the total number of times and the frequency of unblocking.

Why is there a limit on the number of chances for self-service 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.

How can I prevent my IP from being blocked?

When purchasing an Anti-DDoS Advanced instance, you can select the appropriate protection bandwidth based on the historical attack traffic data to ensure that the maximum protection bandwidth is higher than the peak historical attack traffic bandwidth.

How can I prevent my IP from being blocked again?

You are recommended to enable elastic protection and set a high elastic protection bandwidth to defend against large-traffic attacks. In addition, elastic protection is pay-as-you-go on a daily basis, which can help reduce your security costs.

Attack-related FAQ

Last updated：2023-04-25 15:25:37

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 Alerts.

Why my business suffers DDoS attacks without my business running on the server?

- A DDoS attack is an attack involving multiple machines attempts 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 my business is attacked again after I have Anti-DDoS Advanced products deployed?

- Your business may be at risk of DDoS attacks if it communicates over the public network.
- Your business protected by Anti-DDoS Advanced products may still be targeted, but it is 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: includes UDP reflection attacks, SYN floods, and connection attacks. This type of attacks causes a denial of service by consuming server bandwidth and connection resources.
- Application layer attacks: includes DNS floods, HTTP floods, and CC attacks. This type of attacks cause a denial of service by exhausting server performance.

What types of attack statistics are provided by Anti-DDoS Advanced?

Anti-DDoS Advanced provides the following types of attack statistics:

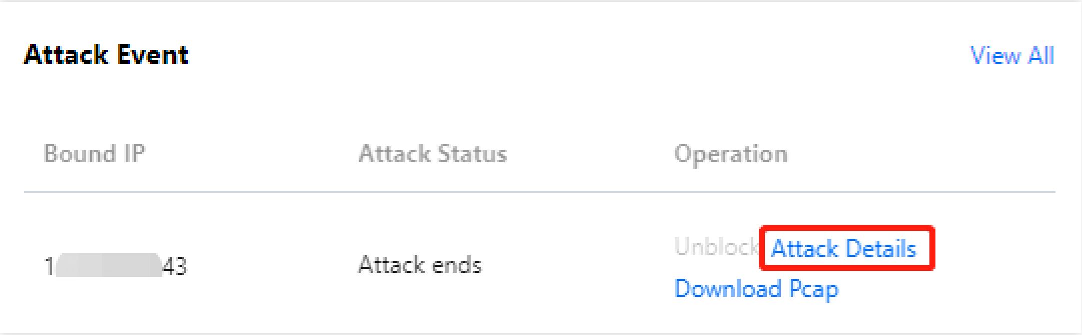
- **Total attack traffic**: presents how the attack traffic on the protected IP distributes over different protocols within the selected time period.
- **Attack packets**: presents how the attack packets to the protected IP distribute over different protocols within the selected time period.
- **Total attacks**: presents how the attacks on the protected IP distribute over different attack types within the selected time period.

Where to view attack logs for the attacked server?

In the "Recent Events" section of the Overview page, you can view the recent attack events and logs.

Where to view details of the attack source IP?

In the "Recent Events" section of the Overview page, select an attack event you want to view, and then click **View details** to check the attack source information, source region, attack traffic and attack packet size.



Attack Event

View All

Bound IP	Attack Status	Operation
1[redacted]43	Attack ends	Unblock Attack Details Download Pcap

What to do when the lightweight server is under DDoS attacks?

We recommend getting an Anti-DDoS Advanced instance to defeat DDoS attacks and guarantee the availability of your server and business.

What is the protection bandwidth threshold for the server? What will happen if the threshold reaches?

Each public IP of all Tencent Cloud users in the Chinese mainland can enjoy free basic protection, with a maximum bandwidth of 2 Gbps for general users and 10 Gbps for VIP users. Users outside the Chinese mainland can enjoy up to 2 Gbps bandwidth. Blocking will be triggered after the threshold reaches, causing potential business interruptions.

How to 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.

A source IP is added to the Anti-DDoS Pro instance’s blocklist, but it still has access to my business. Is the instance not working?

The access restriction for the IP will not be taken 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：2022-01-17 17:00:24

Is Anti-DDoS Advanced available for non-Tencent Cloud resources?

Yes. Anti-DDoS Advanced can protect all types of servers on the internet, including but not limited to those in Tencent Cloud, other clouds, and customer IDCs.

> Note：
> ICP filing issued by MIIT is required for all domain names connected to Anti-DDoS Advanced in Mainland China.

Does Anti-DDoS Advanced support wildcard domain names?

Yes. You can 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.

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

No. You need to manually add the forwarding IP range to the CVM security group. If you have deployed firewall or other server 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 due to blocking or speed limiting.

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

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

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 modifications in the Anti-DDoS Advanced Console to take effect?

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

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

Currently, the IPv6 protocol is not supported.

Does Anti-DDoS Advanced support HTTPS mutual authentication?

- For website applications, HTTPS mutual authentication is not supported.
- For non-website applications over TCP, HTTPS mutual authentication is supported.

Does Anti-DDoS Advanced have packet capture files?

Currently, 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 applications, default load balancing based on round robin is used.
- For non-website applications, load balancing based on weighted round robin is used to forward traffic to real server IPs in turn.

How many forwarding ports and domain names are supported by one 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.

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

The business bandwidth purchased is for the entire Anti-DDoS Advanced instance. It refers to the inbound and outbound traffic of all normal businesses in 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.

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 consoles as instructed in Configuring Session Persistence.

Does Anti-DDoS Advanced support health check?

Health check is enabled 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 the access to the real server slow?

Anti-DDoS servers have Window Scaling (WS) enabled by default. If this 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.

Billing

Last updated：2022-01-28 10:54:50

What should I do if I want to end the Anti-DDoS Advanced service?

Anti-DDoS Advanced adopts a pay-as-you-go model. If you want to end the service, you need to submit a ticket to terminate your instances. Otherwise, charges are still be incurred.

- After you apply for a termination in the current month, the monthly-subscribed items will be settled as usual, while the daily billable items are settled based on the actual usage. After you terminate your instances, the service will be stopped immediately and the instances will no longer be billed for the next month.
- The entire termination takes 1-3 working days to complete and is subject to the actual operation (protection fees may be incurred during the period).

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 peak attack traffic bandwidth of the day. For more information, please see Billing Overview.
For example, you have purchased an Anti-DDoS Advanced instance with 20 Gbps base protection bandwidth and 50 Gbps elastic protection bandwidth. A DDoS attack occurs one day with the peak attack traffic bandwidth of 45 Gbps. Since 45 Gbps exceeds the base protection bandwidth and triggers elastic protection, and it falls between 40 Gbps and 50 Gbps, the fees for elastic protection of the day will be billed according to the tiered price of the billing tier between 40 Gbps and 50 Gbps.

If the IP protected by my Anti-DDoS Advanced instance is blocked due to high 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 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 the 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 reduce the elastic protection bandwidth of Anti-DDoS Advanced. 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 during a day.

I purchased two Anti-DDoS instances, and both of them are under attack traffic that exceeds the basic 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 basic protection bandwidth, you will need to pay for elastic protection for the two instances separately.