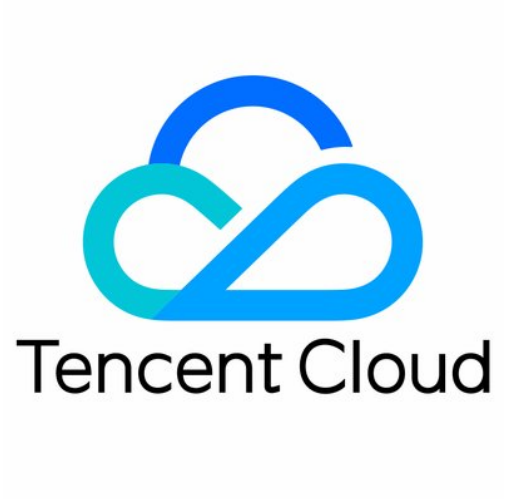
Anti-DDoS Pro

FAQs

Product Documentation



Contents

FAQs
Blocking

Last updated：2020-07-07 16:10:34

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

You have three chances each day to unblock the IP by yourself on the protection overview page in the console if you need to resume your business urgently.

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.
Only **three** chances of self-service unblocking are provided for Anti-DDoS Pro every day. The system resets the chance counter daily at midnight. Unused chances cannot be accumulated for the next day.

How do I connect to a blocked server?

If you need to perform operations such as data migration, you may use either of the following methods to connect to the blocked server:

- Connect to the blocked server by using the private IP through another CVM instance in the same region.
- In the CVM Console, click **Log In** in the row of the blocked server and connect by using the VNC method.

Attack-related Issues

Last updated：2023-06-25 14:44:48

Will I receive alerts for DDoS attacks?

Yes. You will receive an alarm message once DDoS attacks are detected. You can also customize an inbound traffic alarm threshold for notification. For details, see Configuring Security Event Notification.

Why my application suffers DDoS attacks when it is not running on the server?

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

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

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

What are the targets when the server is attacked?

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

What are the common types of attacks?

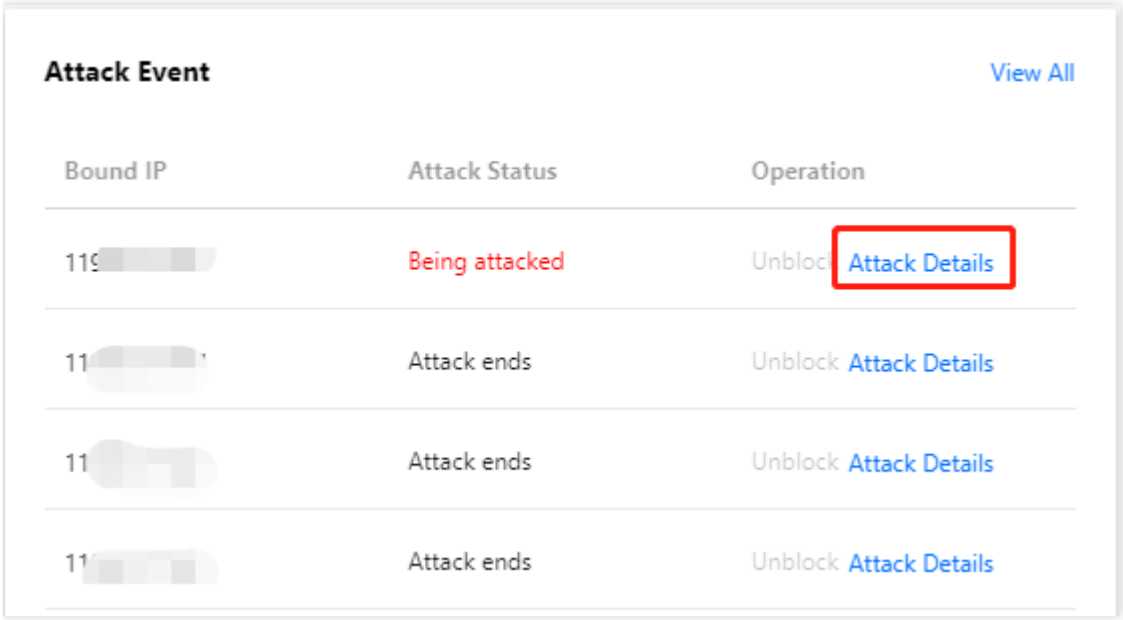
- Network layer attacks: It includes UDP reflection attacks, SYN floods, and connection attacks. This type of attacks causes a denial of service by consuming server bandwidth and connection resources.
- Application layer attacks: It includes DNS floods, HTTP floods, and CC attacks. This type of attacks cause a denial of service by exhausting server performance.

Where can I view attack logs for the attacked server?

On the Overview page, you can view attack logs for the attacked server over the selected time period.

Where can I view details of the attack source IP?

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



What should I do when the lightweight server is under DDoS attacks?

We recommend that you purchase an Anti-DDoS Pro instance to defeat DDoS attacks and guarantee the availability of your server and applications.

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

Users can enjoy free basic protection bandwidth of up to 2 Gbps. Once the threshold is reached, blocking will be triggered, causing potential application 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.

I have added the source IP to a blocklist configured for the Anti-DDoS Pro instance when my application is attacked, but the IP still has access to my application. 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 application.

Features

Last updated：2023-06-25 14:43:54

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 service for VPN gateways?

Yes.

Does Anti-DDoS Pro provide protection service for Anycast EIP?

Anycast EIP does not support access to Anti-DDoS Pro. If you need DDoS protection, please purchase Anti-DDoS Advanced (Global Enterprise) and then bind the Anycast EIP to the Anti-DDoS Advanced instance.

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 not exceeding 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 not exceeding 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 on Tencent Cloud.
- Anti-DDoS Advanced is for users both on and off Tencent Cloud and supports protection for website domain names and service ports.
- Access:
  - Anti-DDoS Pro is easy to access and you do not need to change your public IPs.
  - To access Anti-DDoS Advanced, you need to modify DNS or your application IPs.

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

Differences	Anti-DDoS Pro	Non-BGP Protection
Access costs	Low access costs without the need of changing 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 an all-out protection available at no additional elastic costs.	Billed in a complex manner with traffic fees incurred.

What is hosted IP?

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

If you need hosted IP, please 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 Lightweight Edition allow three chances per month to manually unblock IPs?

Yes.

Does Anti-DDoS Pro Lightweight Edition allow chances to manually unblock IPs for non-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.

Billing

Last updated：2023-02-03 14:28:39

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

It will take effect immediately after successful purchase and access.

How is the 95th percentile bandwidth calculated?

In each calendar month, the inbound/outbound bandwidth is sampled every 5 minutes and the maximum is taken as the peak bandwidth on each day. At the end of the month, the sampled values are sorted from highest to lowest, and the top 5% are removed. The 95th largest value is the billable bandwidth of the month.

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

What are the billing differences between the full protection of Anti-DDoS Pro and resilient 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 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.