Anti-DDoS Pro

FAQs

Product Documentation

Contents

FAQs
Blocking-related FAQs

Last updated：2019-09-26 18:33:57

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

If the elastic protection bandwidth of the Anti-DDoS Pro instance in use is not adjusted to the highest, you can change the bandwidth in **Anti-DDoS Console** to improve the elastic protection capability against larger attack traffic.

Why is my IP blocked when under attack?

Tencent Cloud reduces the cost by sharing the infrastructure, with one public IP being shared among all users. When a large traffic attack occurs, the entire Tencent Cloud network may be affected, in addition to the attacked servers. To protect other servers and to ensure the network stability, we need to block the attacked server IP.

Why do you charge for Anti-DDoS Advanced traffic?

DDoS attacks have negative effects on not only the targets but also the entire cloud network, affecting other non-attacked users in the cloud as well. Moreover, building the anti-DDoS system costs high, including the cleansing cost and the bandwidth cost. Specifically, the largest expense is bandwidth and it is calculated based on the total traffic. No difference exists between normal traffic and attack traffic in terms of the bandwidth cost.
Therefore, although Tencent Cloud can afford limited free DDoS Basic service for all users, we have to block inbound public network traffic of the attacked servers when the attack traffic exceeds the free quota.

Why can't my IP be unblocked immediately after the attack ends?

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

Because the IP blocking takes effect in the carrier's network, Tencent Cloud is unable to monitor whether the attack traffic flow has been stopped. If the IP is recovered but the attack is still going on, the IP will be blocked again. A gap exists between the recovery and the re-blocking that the attack traffic can take the advantage of directly entering the Tencent Cloud's basic network, resulting in negative effects on other cloud users. In addition, the IP blocking is a service Tencent Cloud purchases from carriers with limited numbers of the unblocking and blocking frequency.

How can I unblock the IP earlier in case of an emergency?

Starting or upgrading the elastic protection capability and adjusting the elastic protection to the maximum value will allow for earlier automatic unblocking.

Why is there a limit on the number of self-unblocking? What are the limitations?

Tencent Cloud pays carriers for blocking attacked IPs, and carriers impose limits on the time and frequency of unblocking.
Only **three** chances of self-unblocking are provided for users with Anti-DDoS Pro every day. The system resets the self-unblocking chances daily at midnight. Unused chances cannot be accumulated to the following day.

How do I connect to a blocked server?

If data migration or other operations are required, you may use either of the following methods to connect to the blocked server:

- Connect to the blocked server using the private IP through another CVM in the same region.
- In CVM Console, click **Login** in the line of the blocked server to connect through browser VNC.

How can I prevent the IP from being blocked?

When you purchase Anti-DDoS Pro, you can choose an appropriate base protection bandwidth or enable elastic protection at the same time based on the historical attack traffic data to ensure that the maximum protection bandwidth exceeds the attack bandwidth.

How can I prevent my anti-DDoS IP from being blocked again?

You are advised to upgrade the elastic protection bandwidth to improve the defense capability. Enabling the elastic protection can protect you from large traffic attacks. In addition, the elastic protection is charged flexibly by day on demand, reducing your security cost effectively.

Feature-related FAQs

Last updated：2019-09-26 18:34:05

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

No. Anti-DDoS Pro only provides DDoS protection for public network IPs of Tencent Cloud. For protection of IPs other than Tencent Cloud, please purchase Anti-DDoS Advanced.

What if the bound resource expires but the Anti-DDoS Pro instance does not expire?

An Anti-DDoS Pro instance is purchased by month, and provides protection based on IPs. If the resource of the bound protected object expires and you do not replace the IP bound to the Anti-DDoS Pro instance, the instance may continue protection for the bound IP, but the corresponding resource may not be yours. You are advised to renew the cloud service in time or replace a new protected object IP.

Does Anti-DDoS Pro protect domain names?

No. For domain name protection and application-layer protection, please purchase Anti-DDoS Advanced.

The protection bandwidth of Anti-DDoS Basic is 2 Gbps. If I also purchase an Anti-DDoS Pro instance, will the final protection bandwidth be the sum of the two?

The final protection bandwidth a user enjoys is the protection bandwidth of the Anti-DDoS Pro instance. The default protection bandwidth of Anti-DDoS Basic will not add to it.
Assume the IP of a certain cloud virtual machine enjoys a 2 Gbps free protection bandwidth. Due to frequent attacks, the user purchases a 20 Gbps Anti-DDoS Pro instance for this IP, and then the maximum protection capability is 20 Gbps.

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

- Protected objects:
  - Anti-DDoS Pro only provides anti-DDoS protection for services within Tencent Cloud.
  - Anti-DDoS Advanced is available for non-Tencent Cloud resources, providing non-Tencent Cloud service IPs/domain names with protection.
- Access:
  - The access configuration of Anti-DDoS Pro is more convenient without the need of changing public network IP addresses.
  - Anti-DDoS Advanced requires you to modify DNS or business IP before accessing the protection.

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

Differences	Anti-DDoS Pro	Non-BGP Protection
Cost of Access	It does not require changing of the server IP, and directly improves the defense capability of cloud products with immediate effect and low cost of access.	It requires you to replace the server IP with non-BGP IP and enter the domain name and port information. The configuration is quite complex.
Access Quality	It uses BGP bandwidths, minimizing access latency across networks. The access speed increases by over 30%.	It has no BGP bandwidths, the network latency is higher, and the quality is poor.
Pricing Policy	The pricing policy is flexible. It allows for base + elastic pricing, and allows sharing.	The pricing policy is complex, and requires you to pay traffic fees.

Billing-related FAQs

Last updated：2019-09-26 18:34:13

Does the same billing mode apply to the Anti-DDoS Pro elastic protection services? How is it calculated?

Yes, it does. The elastic protection services are also charged based on the elastic protection bandwidth range corresponding to the daily maximum protected attack traffic bandwidth. For more information, please see Billing Overview.
For example, assume that you have purchased an Anti-DDoS Pro instance with 20 Gbps base protection bandwidth + 50 Gbps elastic protection bandwidth. An DDoS attack occurs that day and the highest attack traffic is 45 Gbps. Because 45 Gbps exceeds the base protection bandwidth and triggers the elastic protection, and it falls in the 40 Gbps < elastic bandwidth ≤ 50 Gbps billing range, the elastic cost of that day is charged according to the 40 Gbps < elastic bandwidth ≤ 50 Gbps billing range.

Need I pay for the attack traffic even after my Anti-DDoS Advanced IP is blocked due to high traffic attack?

The elastic protection billing rules of Anti-DDoS Pro apply to billing of attack traffic that exceeds the base protection bandwidth and is lower than or equal to the elastic protection bandwidth. If the IP is blocked, the attack traffic already exceeds the set elastic protection bandwidth. Therefore, the attack traffic that exceeds the elastic protection bandwidth does not fall in the billing range.

I purchased the elastic protection service a month ago and no attacks occur. Do I still have to pay?

No elastic protection cost incurs in this case.

If I have purchased 100 Gbps of base protection bandwidth, can I reduce it to 50 Gbps?

No. The base protection does not support upgrade or degradation.

Can I raise the elastic protection bandwidth when my business is being attacked?

Yes. On the basic information page of Anti-DDoS Pro, you can upgrade or degrade the elastic protection bandwidth. The elastic protection bandwidth varies depending on the region. For more information, please see Billing Overview.

> If fees of the attack traffic are already incurred on the day you modify the bandwidth, you will be charged according to the modified elastic protection bandwidth the next day.

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

The Anti-DDoS Pro service is billed based on the highest attack traffic bandwidth during the day and is only billed for once in a day.

If I purchase two Anti-DDoS Pro instances, and the attack traffic bandwidths for both of them exceed the base protection bandwidth, how do I pay for the elastic protection?

The elastic protection is billed by instance. If both attack traffic bandwidths of the Anti-DDoS Pro instances exceed the base protection and are within the elastic protection range, you need to pay for the elastic protection of these two instances separately.