Anti-DDoS Pro

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

About Blocking

Last updated：2020-04-02 10:00:59

What should 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 increase the bandwidth in Anti-DDoS Pro Console to improve the elastic protection capability against attacks of larger traffic.

In addition, you have three times each day to unblock the IP by yourself.

Why is my IP blocked?

Tencent Cloud reduces costs of using clouds by sharing the infrastructure, with one public IP shared among all users. When a large traffic attack occurs, the entire Tencent Cloud network may be affected, not only the target servers. To protect other users and ensure network stability, we have to block the target server IP.

Why isn’t anti-DDoS service always free?

DDoS attacks not only threaten the targets but also the entire cloud network, affecting non-attacked Tencent Cloud users as well. Also, DDoS protection incurs high costs, including cleansing costs and bandwidth costs, in which bandwidth costs the most. Bandwidth costs are calculated based on the total amount of traffic; there is no difference between costs incurred by normal traffic and attack traffic.

Therefore, Tencent Cloud provides Anti-DDoS Basic service free of charge for all users. But once the attack traffic exceeds the free quota, we will have to block the attacked IP from all public network access.

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 ISPs’ network, Tencent Cloud will be unable to monitor whether the attack traffic has stopped after the attacked public IP is blocked. If the IP is recovered but the attack is still going on, the IP will be blocked again. During the gap between the IP being recovered and blocked again, Tencent Cloud's basic network will be exposed to the attack traffic, which may affect other users in Tencent Cloud. In addition, IP blocking is a service offered by ISPs with limitations on the total number of times and the frequency of unblocking.

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

1. You can upgrade the base protection bandwidth, in this case, the blocked IP is recovered automatically.
2. You have three times each day to unblock the IP by yourself.

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

How can I prevent my IP from being blocked?

When you purchase Anti-DDoS Pro, you can set an appropriate protection bandwidth based on the historical attack traffic data to ensure that the bandwidth of most attacks is lower than the maximum protection bandwidth.

How can I prevent my IP from being blocked again?

We recommend you upgrade the base protection bandwidth or elastic protection bandwidth. Elastic protection can help defense against high-traffic attacks, and you only pay for what you use per day, which reduces your cost.

About Features

Last updated：2020-04-02 10:01:00

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

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

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.

Does Anti-DDoS Pro provide protection sevice for 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 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, a CVM IP has a free protection bandwidth of 2 Gbps. If you purchase a 20 Gbps Anti-DDoS Pro instance for it, the maximum protection capability the CVM IP enjoys is 20 Gbps.

What’re the differeces 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 can protect non-Tencent Cloud resources, including non-Tencent Cloud service IPs and domain names.
- 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 business 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	Uses BGP bandwidth and offers a lower access latency across networks and 30% higher access speed	No BGP bandwidth with a high network latency and poor quality
Pricing	Flexible pricing that supports sharing and a combination of base and elastic protection	Complicated pricing where you need to pay for traffic

Billing-related FAQs

Last updated：2020-02-11 16:13:53

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 bandwidth of the day. For more information, please see Billing Overview.

For example, you have purchased an Anti-DDoS Pro instance with 20 Gbps base protection bandwidth and 50 Gbps elastic protection bandwidth. An DDoS attack occurs one day with the peak attack bandwidth of 45 Gbps. Since 45 Gbps goes over the base protection bandwidth and triggers elastic protection, and it falls between 40 Gbps and 50 Gbps, the fees for elastic protection of that 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 Pro instance is blocked due to large traffic attacks, will I be billed for the attack traffic over the maximum protection bandwidth?

You will be billed for elastic protection when the attack traffic is over 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 attack traffic that exceeds the elastic protection bandwidth.

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

You will not be billed for elastic protection in this case.

I purchased 100 Gbps of base protection bandwidth. Can I downgrade it to 50 Gbps?

No. You can upgrade but not downgrade your base protection bandwidth.

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

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

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

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 peak attack bandwidth during a day. Therefore, you will not be charged repeatedly for multiple attacks during a day.

I purchased two Anti-DDoS Pro 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 is over the basic protection bandwidth but within the elastic protection bandwidth, you will need to pay for the elastic protection of the two instances separately.