Anti-DDoS Advanced

FAQ

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

FAQ

FAQ about Block

Last updated : 2020-05-09 18:03:50

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 isn't anti-DDoS service always free?

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

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

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 basic 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.

How can I unblock my IP earlier in case of emergency?

- You can upgrade the base protection capacity, so that the blocked IP can be unblocked automatically.
- You have three chances each day to unblock the IP by yourself in case of emergency.

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 Advanced every day. The system resets the chance counter daily at midnight. Unused chances cannot be accumulated for the next day.

How can I prevent my IP from being blocked?

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

How can I prevent my IP from being blocked again?

You are recommended to increase the base protection bandwidth or elastic protection bandwidth to improve the protection capability. Enabling elastic protection can help you defend against high-traffic attacks. In addition, elastic protection is pay-as-you-go, which can reduce your security costs.

FAQ about Billing

Last updated : 2019-05-07 10:27:12

Does the same billing model apply to the Anti-DDoS Advanced elastic defense services? How is it calculated?

Yes. You will be billed according to your daily elastic protection bandwidth range. See Billing Overview for more billing details.
For example, suppose you bought an Anti-DDoS Advanced instance with 20 Gbps base protection bandwidth and 50 Gbps elastic protection bandwidth. Suppose your instance experienced a DDoS attack on one day with 45-Gbps peak traffic flow, which exceeded the base protection bandwidth limit and therefore activated elastic protection. 45 Gbps falls within the 40 Gbps to 50 Gbps range and your elastic charge for that day will be based on the range.

Should I pay for the attack traffic even after my Anti-DDoS Advanced IP is blocked?

No. According to the billing model mentioned above, and because your IP is automatically blocked when the attack traffic exceeded the elastic protection bandwidth, you only need to pay for the difference between the base protection bandwidth limit and the elastic protection bandwidth limit. The amount of traffic that exceeds the elastic protection bandwidth limit will not be calculated.

I purchased the elastic defense service a month ago and has not experienced any attacks. Do I still have to pay?

No. In such cases, no additional elastic defense service fees will apply.

If I have purchased base protection bandwidth with a speed of 100 Gbps, can I reduce the bandwidth speed to 50 Gbps?

No. You can increase, but not decrease your base protection bandwidth.

Can I increase the elastic protection bandwidth when my application is being attacked?

Yes. You can increase and decrease elastic protection bandwidth on the Anti-DDoS Advanced Basic Info page. The available options vary by region. For details, please see Product Overview.

> If you have already been billed for attack traffic when you made the adjustment, you will be billed based on the new plan starting the next day.

If a protected IP suffers more than one attack during a day, will I be billed repeatedly for those attacks?

The Anti-DDoS Advanced service is billed based on the peak attacking traffic during the day and for once only.

If I have purchased two Anti-DDoS Advanced instances, and the base protection bandwidth limits of both Anti-DDoS Advanced instances are exceeded, how do I pay for the elastic protection?

You need to pay for the instances separately if both of them have exceeded their base protection bandwidth limits.

FAQ about Feature

Last updated : 2020-05-09 18:03:50

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

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.

> 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 intermediate IPs to the security group?

No. You need to manually add the intermediate 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 intermediate IP range to the whitelist 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?

Anti-DDoS Advanced supports downloading packet capture files. For detailed directions, please see Viewing Statistics Report .

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

- Load balancing based on source IP hash is used for website applications.
- 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. The quantity can be increased.
- Domain names: 60 forwarding rules for HTTP/HTTPS protocol are provided free of charge by default. The quantity can be increased.

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.

> 100 Mbps forwarding bandwidth is available free of charge for each Anti-DDoS Advanced instance.

Does Anti-DDoS Advanced support session persistence?

Anti-DDoS Advanced support 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.