Anti-DDoS Advanced

Product Introduction

Product Documentation

©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

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

©2013-2022 Tencent Cloud. All rights reserved.

Product Introduction

Product Overview

Last updated：2020-07-30 11:33:07

Overview

Anti-DDoS Advanced is a paid protection service defending businesses such as games, internet services, and finance operations against high-volume distributed denial of service (DDoS) attacks that may disable user access. It can direct attack traffic to Anti-DDoS Advanced IPs for cleansing, thus ensuring business stability and availability of the real servers.

Anti-DDoS Advanced can be connected to through internet proxy and supports TCP, UDP, HTTP, HTTPS, and HTTP/2 protocols, making it ideal for finance, ecommerce, games, and other business scenarios.

Key Features

Multidimensional protection

Protection Type	Description
Malformed packet filtering	Filters out frag flood, smurf, stream flood, and land flood attacks as well as malformed IP, TCP, and UDP packets
DDoS protection at the network layer	Filters out UDP flood, SYN flood, TCP flood, ICMP flood, ACK flood, FIN flood, RST flood, and DNS/NTP/SSDP reflection attacks and null sessions.
DDoS protection at the application layer	Filters out CC attacks and slow HTTP attacks, and supports HTTP custom filtering such as host filtering, user-agent filtering, and referer filtering.

Flexible advanced protection policies

Anti-DDoS Advanced provides basic security policies by default on the basis of protection algorithms such as IP profiling, behavior pattern analysis, and AI-based smart recognition, effectively coping with common DDoS attacks. Meanwhile, it provides advanced DDoS protection policies such as IP blocklist/allowlist, protocol/port closing, packet characteristic filtering, and null session prevention to enable more targeted protection, and you can customize them as needed.

Custom cleansing mode

©2013-2022 Tencent Cloud. All rights reserved.

Anti-DDoS Advanced opens up its multiple protection levels and provides a custom cleansing threshold to allow flexible adjustment based on the attack characteristics, helping you swiftly respond to various types of DDoS attacks and meet your diversified business requirements.

Protection statistics and analysis

You can access multidimensional statistics of DDoS attacks, CC attacks, forwarded traffic, and other metrics, which helps you stay up to date with your business and attack conditions. In addition, Anti-DDoS Advanced supports automatic capture of attack packets, helping you quickly troubleshoot exceptions and problems.

Supported Regions

Anti-DDoS Advanced can protect all types of servers on the internet, including but not limited to those in customer IDCs, Tencent Cloud, and other clouds. It is currently available in following regions:

- Mainland China: South China (Guangzhou), East China (Shanghai), and North China (Beijing).
- Outside Mainland China: Hong Kong (China), Taiwan (China), Asia Pacific (Singapore, Seoul, Bangkok, India, and Japan), West US (Silicon Valley), East US (Virginia), North America (Toronto), and Europe (Frankfurt and Moscow).

The table below describes the protection bandwidth of Anti-DDoS Advanced for different regions.

Region	Base Protection	Elastic Protection	Maximum Protection Bandwidth
Guangzhou	20–50 Gbps	30–100 Gbps	100 Gbps
Beijing	20–50 Gbps	30–100 Gbps	100 Gbps
Shanghai	20–100 Gbps	30–300 Gbps	300 Gbps
Outside Mainland China	10–100 Gbps	30–400 Gbps	400 Gbps

> You are recommended to choose a region closest to your real server so as to reduce access latency and accelerate access.

©2013-2022 Tencent Cloud. All rights reserved.

Product Strengths

Last updated：2020-05-09 18:03:48

Anti-DDoS Advanced is a paid product to protect your business from being affected by high-volume distributed denial-of-service (DDoS) attacks. It has the following advantages.

Massive Protection Resources

Connected with 30 ISPs across Mainland China and dozens of protection nodes overseas, Tencent Cloud's BGP linkage can provide protection bandwidth up to 900 Gbps for a single customer (point) in Mainland China and up to 400 Gbps outside Mainland China, enabling you to defend against all types of DDoS attacks with ease.

Leading Cleansing Capability

Leveraging the powerful protective clusters developed by Tencent and multi-dimensional algorithms, such as IP profiling, behavior pattern analysis, and cookie challenges, Anti-DDoS Advanced can accurately and promptly detect attack traffic. With the aid of a smart AI engine that continuously optimizes the algorithms, it is also flexible in coping with attack tricks.

Fast Access

With a 30-line BGP network encompassing various ISPs across Mainland China, Anti-DDoS Advanced features an extremely low delay in protection and fast access.

Hiding Real Server

Anti-DDoS Advanced replaces and hides your real server. It can be seen as a firewall before the real server for external access. All business access traffic passes through Anti-DDoS Advanced, which directly forwards normal traffic to the real server while cleansing attack traffic before it reaches the real server, helping boost the real server security.

Wide Applicability

©2013-2022 Tencent Cloud. All rights reserved.

Anti-DDoS Advanced fully supports website and non-website businesses and covers various businesses like finance, ecommerce, gaming, and government affairs, comprehensively satisfying the security protection needs in different application scenarios.

Cost Optimization

Anti-DDoS Advanced offers a "base protection + elastic protection" combo package where you are only charged by the amount of actual attack traffic. When the attack traffic exceeds the base protection bandwidth, it provides elastic protection to ensure the continuity of your business. Such seamless transition requires no additional devices and configuration on your side, reducing your daily protection costs.

Detailed Protection Report

Anti-DDoS Advanced can generate accurate and detailed protection reports. It can also capture attack packets automatically for troubleshooting.

©2013-2022 Tencent Cloud. All rights reserved.

Application Scenarios

Last updated：2020-04-03 14:35:43

Gaming

DDoS attacks are particularly common in the gaming industry. Anti-DDoS Advanced ensures the availability and continuity of the games to deliver a smooth experience for players. Meanwhile, it helps ensure that normal gaming continues throughout events, new game releases, and peak periods such as holidays.

Internet

Anti-DDoS Advanced ensures smooth and uninterrupted access to websites, especially during major ecommerce promotions.

Finance

Anti-DDoS Advanced helps the finance industry meet the compliance requirements and provide fast, secure, and reliable online transaction services to customers.

Government Affairs

Anti-DDoS Advanced satisfies the high security requirements of government clouds and provides high-level security for major government conferences and events especially during sensitive periods. It ensures the availability of public services and thus helps enhance government credibility.

Enterprises

Anti-DDoS Advanced ensures the availability of company websites to avoid potential financial losses and damage to brand reputation caused by DDoS attacks. In addition, you can save on investments in infrastructure, hardware, and maintenance.

Relevant Concepts

Last updated：2020-05-13 19:36:20

DDoS Attack

A Distributed Denial of Service (DDoS) attack is a malicious attempt to make a targeted server unavailable by blocking its network bandwidth or exhausting its system resources with a flood of attacking requests sent from large numbers of botnets.

Network-Layer DDoS Attack

A network-layer DDoS attack attempts to make a targeted server unavailable to its intended users by blocking its network bandwidth and exhausting its system-layer resources with a flood of internet traffic.
Common attacks include SYN flood, ACK flood, UDP flood, ICMP flood, and DNS/NTP/SSDP/Memcached reflection attacks.

CC Attack

A CC attack is a malicious attempt to make a targeted server unavailable by occupying its application-layer resources and exhausting its processing capacity.
Common attacks include HTTP/HTTPS-based GET/POST flood, layer-4 CC, and connection flood attacks, etc.

Protection Bandwidth

There are two types of protection bandwidth: base protection bandwidth and elastic protection bandwidth.

- Base protection bandwidth: base protection bandwidth of the Anti-DDoS service instance.
- Elastic protection bandwidth: the largest possible protection bandwidth of the Anti-DDoS service instance. The part in excess of the base protection bandwidth is billed daily in a pay-as-you-go manner.

If elastic protection is not enabled, the maximum bandwidth of an Anti-DDoS service instance will be the base protection bandwidth. If elastic protection is enabled, the maximum bandwidth will be the elastic protection bandwidth. Once the attack traffic exceeds the maximum protection bandwidth, IP blocking will be triggered.

> Elastic protection is disabled by default. If you need the feature, please check the pricing and billing information and enable it on your own. You can adjust the elastic protection bandwidth as required.

©2013-2022 Tencent Cloud. All rights reserved.

Benefits of Elastic Protection Bandwidth

With elastic protection enabled, when the attack traffic is higher than the base protection bandwidth but lower than the elastic protection bandwidth, Tencent Cloud Anti-DDoS Advanced will continue to protect your IPs to ensure your business continuity.

Elastic Protection Billing

With elastic protection enabled, elastic protection will be triggered and incur fees once the attack traffic goes over the base protection bandwidth. You will be billed on the following day based on the peak attack bandwidth of the current day.
For example, assume that you have purchased 20 Gbps of base protection bandwidth and set the elastic protection bandwidth as 50 Gbps. If the actual peak attack bandwidth of the day is 35 Gbps, you will need to pay for the elastic protection at the price of the 30–40 Gbps tier.
For more information, please see Billing Overview.

Cleansing

When the public network traffic of a target IP exceeds the threshold, Anti-DDoS will automatically cleanse the inbound traffic to the IP. The BGP routing protocol will be used to redirect the traffic from the original network route to the DDoS cleansing devices of Anti-DDoS, which will identify the traffic, discard attack traffic, and forward normal traffic to the IP. In general, cleansing does not affect normal access except on special occasions or when the cleansing policy is configured improperly.

Blocking

When the attack traffic suffered by a target IP exceeds the blocking threshold, Tencent Cloud will block all public network access requests to this IP through applicable ISP services to protect other Tencent Cloud users from being affected. This means that when the bandwidth of the attack traffic suffered by your IP exceeds the maximum protection bandwidth of your purchased Anti-DDoS package, Tencent Cloud will block all public network access requests to it. If your protected IP is blocked, you can log in to the console to unblock it.
Block

Blocking threshold

The blocking threshold of a protected IP equals the maximum protection bandwidth you have purchased. Anti-DDoS Advanced offers various specifications. For more information, please see Billing Overview.

Blocking period

An attacked IP is blocked for 2 hours by default. The actual duration can be up to 24 hours depending on how many times the IP is blocked and how high the peak attack bandwidth is.
The blocking duration is subject to the following factors:

- Continuity of the attack. The blocking period will extend if an attack continues. Once the period extends, a new blocking cycle will start.
- Frequency of the attack. Users that are frequently attacked are more likely to be attacked continuously. In such a case, the blocking period extends automatically.
- Traffic volume of the attack. The blocking period extends automatically in case of ultra-large volume of attack traffic.

> For IPs that are blocked too frequently, Tencent Cloud reserves the right to extend the duration and lower the threshold.

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.
For more information on blocking, please see Blocking.

©2013-2022 Tencent Cloud. All rights reserved.