Anti-DDoS Advanced

Product Introduction

Product Documentation

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

Product Introduction

Overview

Last updated：2022-08-16 15:28:12

Overview

Anti-DDoS Advanced is a paid protection service defending businesses such as games, internet services, and finance operations against DDoS attacks that may disable user access. It directs public network traffic in two ways: via pointing your business IP to Anti-DDoS Advanced or resolving your domain name to CNAME address, where attack traffic is redirected to its cleansing center for cleansing and access traffic is forwarded to the origin server. In this way, your business stability and availability can be ensured.

Anti-DDoS Advanced can be accessed via public network proxy and supports TCP, UDP, HTTP, HTTPS, and HTTP2 protocols, making it well suited for finance, e-commerce, games and other business use cases.

Key Features

Multidimensional protection

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

Security protection policy

Anti-DDoS Advanced provides basic security protection based on IP reputation and behavior pattern analysis and AI recognition algorithms. Meanwhile, policies can be customized to suit your needs.

Customizable cleansing threshold

Anti-DDoS Advanced allows you to specify the protection level and cleansing threshold to meet your needs.

IP unblocking

When a large number of IP addresses are blocked due to attack traffic surges or low protection bandwidth, you can unblock them in the console.

Protection statistics and analysis

Anti-DDoS Advanced provides visibility into statistical data of DDoS and CC attacks and forwarding traffic, keeping you updated on your business security. It also supports automatic packet capture to locate exceptions.

Strengths

Last updated：2020-07-07 17:19:06

Anti-DDoS Advanced is a paid product to protect your business off Tencent Cloud 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

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 Defense Report

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

Use Cases

Last updated：2020-07-07 17:19:07

Gaming

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

Website

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 stable 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 the government credibility.

Enterprises

Anti-DDoS Advanced ensures the availability of company websites to avoid financial losses and damage to brand image caused by DDoS attacks. In addition, it helps reduce investments in infrastructure, hardware, and maintenance.

Relevant Concepts

Last updated：2022-07-07 09:34:18

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 overwhelming its system with a flood of Internet traffic.

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 Advanced instance, which is on the monthly-subscribed frozen fees payment.
- Elastic protection bandwidth: the largest possible protection bandwidth of the Anti-DDoS Advanced instance. The part that exceeds the base protection bandwidth is billed on a daily pay-as-you-go basis.

If elastic protection is not enabled, the maximum bandwidth of an Anti-DDoS Advanced 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.

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

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 the continuity of your application.

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 according to the price of the 10-20 Gbps tier.

Blocking Strategies

Last updated：2022-08-16 11:34:40

What is blocking?

Once the attack traffic exceeds the blocking threshold of the target IP, Tencent Cloud will block the IP from all public network access through ISP service to protect other Tencent Cloud users. In short, once the traffic attacking your IP goes over the maximum protection bandwidth you have purchased, Tencent Cloud will block the IP from all public network access. If your protected IP address is blocked, you can log in to the console to unblock it.

Blocking Duration

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.

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

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 the IP blocking takes effect in the ISP's network, Tencent Cloud is unable to monitor whether or not the attack traffic flow has been stopped. If the IP is recovered while the attack is still going on, the IP will be blocked again, where there’s a gap between the recovery and the re-blocking that the attack traffic can take advantage of to directly enter the Tencent Cloud's classic network, resulting in negative effects on other cloud users. In addition, the IP blocking is a service Tencent cloud purchased from ISPs with limited numbers of blocking and blocking frequency.