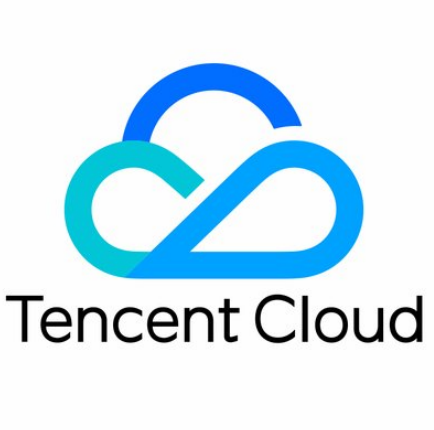
Anti-DDoS Advanced

Product Introduction

Product Documentation



Contents

Product Introduction
Overview

Last updated : 2020-07-07 17:19:06

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. You can configure a protected IP and then point the business IP to it or resolve the business DNS record to the assigned CNAME address for redirection. All internet traffic will first pass through the Anti-DDoS cluster. Attack traffic will be cleansed and filtered out in the Anti-DDoS cleansing center, and normal access traffic will be forwarded to the business real servers, 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, gaming, and other business scenarios.

Key Features

Multi-Dimensional 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.

Security protection policy

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. It also offers flexible protection policies, which can be tailored to your actual business needs for targeted protection.

Custom cleansing mode

Anti-DDoS Advanced supports 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.

Self-Service IP unblocking

If a protected IP is blocked when the attack traffic bursts or the protection bandwidth of your Anti-DDoS Advanced instance is too low, you can unblock the IP in a self-service manner on the security protection overview page in the console.

Protection statistics and analysis

You can access multi-dimensional 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.

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.

Comparison of Anti-DDoS Protection Schemes

Last updated : 2020-07-07 17:19:07

Based on Tencent's many years of practical experience in security and attack protection in various fields such as social networking, gaming, news, and finance, Anti-DDoS provides a rich set of comprehensive security solutions, satisfying your needs in security protection against different DDoS attacks in different business scenarios.

This document describes the basic information and use cases of different Anti-DDoS solutions.

If you want to customize a dedicated security solution, please submit a ticket for assistance.

Product Name	Applicable User	Projected Object	Connection Method	Billing Mode	Protection Capability	Configuration Description

Product Name	Applicable User	Projected Object	Connection Method	Billing Mode	Protection Capability	Configuration Description
Anti-DDoS Basic	Tencent Cloud resources only	It is applicable to Tencent Cloud services such as CVM and CLB. General users can enjoy security protection of 2 Gbps, while VIP users 10 Gbps.	No configuration is required.	Free of charge.	• It mainly protects the businesses of Tencent Cloud users that are unlikely to be attacked and where attack traffic does not exceed the free basic protection capability. If you need a higher protection capability, you are recommended to use Anti-DDoS Pro. • By default, general users can enjoy protection of 2 Gbps, while VIP users 10 Gbps. If your business is frequently attacked, Tencent Cloud will adjust the basic DDoS protection capability based on historical attacks to ensure the overall stability of the Tencent Cloud platform.	Tencent Cloud service IPs are automatically protected with no configuration required.

Product Name	Applicable User	Projected Object	Connection Method	Billing Mode	Protection Capability	Configuration Description
Anti-DDoS Pro	Tencent Cloud resources in Beijing, Shanghai, and Guangzhou regions only	It is applicable to Tencent Cloud services such as CVM, CLB, WAF, NAT IP, EIP, and GAAP IP and users who have a lot of Tencent Cloud service IPs that need to be protected.	It takes effect after a protected IP is bounded in the Anti-DDoS Console. For more information, please see Getting Started.	It is billed by protected times and number of protected resources.	• Tencent Cloud provides at least 30 Gbps DDoS protection capability within the purchased protected times. The maximum protection capability is adjusted dynamically based on the actual network conditions of the region. • HTTP CC protection is supported.	You can enjoy a higher DDoS protection capability simply by purchasing an Anti-DDoS Pro instance and binding the Tencent Cloud service IP to be protected with no need to adjust your business.
Anti-DDoS Advanced (in Mainland China)	All internet users whose businesses are deployed in Mainland China	TCP, UDP, HTTP, and HTTPS businesses are supported (WebSocket is supported by default).	The traffic is sent to the proxy through the Anti-DDoS Advanced instance and then forwarded to the backend real server IP. For more information, please see Website Business Connection and Non-website Business Connection.	It is billed by base protection bandwidth, elastic protection bandwidth, forwarding bandwidth, and number of forwarding rules.	HTTP/HTTPS CC protection is supported. Protective lines include BGP line and non-BGP line: • BGP line provides an up to 300 Gbps protection capability. • Non-BGP line provides an up to 1 Tbps protection capability.	By configuring connection based on a forwarding rule, you can use an Anti-DDoS Advanced instance as the address to provide your business and hide your real server.

Product Name	Applicable User	Projected Object	Connection Method	Billing Mode	Protection Capability	Configuration Description
Anti-DDoS Advanced (outside Mainland China)	All internet users whose businesses are deployed outside Mainland China	TCP, UDP, HTTP, and HTTPS businesses are supported (WebSocket is supported by default).	The traffic is sent to the proxy through the Anti-DDoS Advanced instance and then forwarded to the backend real server IP. For more information, please see Website Business Connection and Non-website Business Connection.	It is billed by base protection bandwidth, elastic protection bandwidth, forwarding bandwidth, and number of forwarding rules.	• Currently, an up to 400 Gbps protection capability is provided. • HTTP/HTTPS CC protection is supported. • The cleansing centers are deployed in regions such as Hong Kong (China), Taiwan (China), Singapore, Seoul, Tokyo, and Virginia.	By configuring connection based on a forwarding rule, you can use an Anti-DDoS Advanced instance as the address to provide your business and hide your real server.

Relevant Concepts

Last updated : 2020-07-07 17:19:08

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 exhaust 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

This is divided into base protection bandwidth and elastic protection bandwidth.

- Base protection bandwidth: protection capability of an Anti-DDoS Advanced instance, which is prepaid on a monthly basis.
- Elastic protection bandwidth: maximum elastic protection capability of an Anti-DDoS Advanced instance, which is pay-as-you-go on a daily basis.

If elastic protection is not enabled, the maximum protection bandwidth of the Anti-DDoS Advanced instance will be the base protection bandwidth; otherwise, it will be the elastic protection bandwidth. If the attack traffic bandwidth exceeds the maximum protection bandwidth, blocking will be triggered.

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

Elastic protection bandwidth usage

With elastic protection enabled, when the attack traffic bandwidth 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 business.

Elastic protection billing

After elastic protection is enabled, it will be triggered and incur fees once the attack traffic bandwidth exceeds the base protection bandwidth. Fees will be charged based on the billing tier corresponding to the actual attack traffic peak on the day and a bill will be generated the next day.
For example, if you have purchased 20 Gbps base protection bandwidth and set the elastic protection bandwidth as 50 Gbps, when the actual attack bandwidth peak of the day is 35 Gbps, you need to pay for elastic protection at the price of the 30–40 Gbps tier.

Cleansing

When the public network traffic of the target IP exceeds the threshold, Anti-DDoS will automatically cleanse the inbound traffic to the IP. The DDoS 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 target IP.
In general, cleansing does not affect access except on special occasions or when the cleansing policy is configured improperly.

Blocking

When the attack traffic suffered by the target IP exceeds the blocking threshold, Tencent Cloud will block all public network access requests to this IP through applicable ISP services to prevent other Tencent Cloud users from being affected. In short, when the bandwidth of the attack traffic suffered by your IP exceeds the maximum protection capability of your purchased Anti-DDoS Advanced instance, Tencent Cloud will block all public network access requests to it. When your IP is blocked, you can unblock it in the console in a self-service manner.

Blocking threshold

The blocking threshold of an Anti-DDoS Advanced instance is the actual maximum protection bandwidth configured for the instance. Anti-DDoS Advanced provides different protection specifications. For more information, please see Billing Overview.

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 duration 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 duration will extend automatically.
- Traffic volume of the attack: the blocking duration will extend automatically in case of ultra-large volume of attack traffic.

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

Why is blocking necessary?

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.