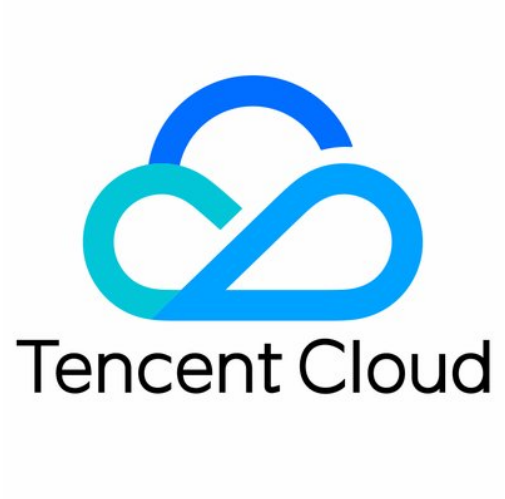
Anti-DDoS

Product Introduction

Product Documentation



Contents

Product Introduction
Overview

Last updated：2024-07-01 11:20:28

Overview

Tencent Cloud Anti-DDoS provides comprehensive, efficient, and professional DDoS protection capabilities in forms of multiple Anti-DDoS solutions such as Anti-DDoS Basic, Anti-DDoS Pro, and Anti-DDoS Advanced for enterprises and organizations to combat DDoS attacks. Leveraging its abundant, quality DDoS protection resources and the ever-evolving "proprietary + AI recognition" cleansing algorithm, Tencent Cloud Anti-DDoS guarantees the stable and secure operations of businesses in the gaming, internet, video, finance, and government sectors.

Service packages

Anti-DDoS Basic

With Tencent Cloud Anti-DDoS Basic, you can enjoy free 2 Gbps basic DDoS protection capability for resources such as Cloud Virtual Machine (CVM) and Cloud Load Balancer (CLB) to meet your daily security protection needs. Tencent Cloud will dynamically adjust the blocking threshold based on your security reputation score that is subject to historical attacks and cloud resource details. If your score is too low, you may not use the free protection capability until your security reputation is restored. Anti-DDoS Basic is enabled by default to monitor network traffic in real time and cleanse attack traffic as soon as it is detected, with protection for Tencent Cloud public IPs started within seconds.

Anti-DDoS Pro

Anti-DDoS Pro (Standard)

Anti-DDoS Pro (Standard) is designed for Tencent Cloud users whose business is deployed in the Chinese mainland. Tencent Cloud provides all-out protection. The maximum protection capability can be adjusted dynamically based on the actual network conditions of the region. To use Anti-DDoS Pro (Standard), you only need to purchase an instance and bind it to the IP address you want to protect.

Anti-DDoS Pro (Enterprise)

Anti-DDoS Pro (Enterprise) is aimed at Tencent Cloud users whose business is deployed in or outside the Chinese mainland.

Anti-DDoS Pro (Enterprise) delivers Tbps-level protection capability across the globe, which requires you to create an Anti-DDoS EIP. It is applicable to enterprises that have higher requirements for business security. Diverse protection capabilities are available for you to choose and configure according to your needs, making it easier to save costs in business protection.
Chinese mainland: The protection capability adopts the "base protection + elastic protection" mode.
Outside the Chinese mainland: Tencent Cloud Anti-DDoS cleansing center provides all-out protection.
Note:
Chinese mainland: Beijing, Shanghai, and Guangzhou.
Outside the Chinese mainland: Hong Kong (China), Singapore, Tokyo, Jakarta, Silicon Valley, Frankfurt, Virginia, and Sao Paulo.
All-out protection: Integrating the local cleansing capability, all-out protection aims to spare no effort to successfully defend against each DDoS attack. Tbps-level protection capability is provided both in and outside the Chinese mainland.

Anti-DDoS Advanced

Anti-DDoS Advanced (Chinese Mainland) and Anti-DDoS Advanced (Global Standard)

Anti-DDoS Advanced is a paid protection service defending businesses such as gaming, internet, and finance against DDoS attacks that may disable user access. By configuring Anti-DDoS Advanced to point your business IP to Anti-DDoS Advanced or resolve your domain name to a CNAME address, all public network traffic will first pass through an Anti-DDoS Advanced cluster, where the attack traffic is cleansed in its cleansing center while the normal access traffic is forwarded to the real 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, ecommerce, gaming, and other business scenarios.

Anti-DDoS Advanced (Global Enterprise)

Anti-DDoS Advanced (Global Enterprise) is a paid service that enhances DDoS protection capabilities outside the Chinese mainland for businesses deployed on Tencent Cloud.
Anti-DDoS Advanced (Global Enterprise) provides ten Tencent Cloud entries around the world to relieve bandwidth pressure with all-out protection, making access to each node as smooth as possible.
Anycast supports near-real-server cleansing and reinjection, with Tpbs-level protection capability. This ensures smooth traffic and low latency by cleansing attack traffic in a cleansing node and then forwarding normal traffic back to the nearest real server. Anti-DDoS Advanced (Global Enterprise) directly protects target IPs on Tencent Cloud.

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 floods, SYN floods, TCP floods, ICMP floods, ACK floods, FIN floods, RST floods, 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.

Note:
DDoS protection at the application layer is only available for Anti-DDoS Advanced.

Binding and switching protected objects

Anti-DDoS supports switching the IPs of protected objects to protect public IPs of different Tencent Cloud resources. Supported objects include CVM, CLB, WAF, and NAT Gateway.

Security protection policies

Anti-DDoS provides a basic security policy by default on the basis of protection algorithms such as attack profiling, behavior pattern analysis, and AI-based smart recognition to effectively combat common DDoS attacks. It also offers diverse and flexible DDoS protection policies, which can be tailored to your special needs to deal with ever-changing attack techniques.

IP unblocking

If your protected business IP is blocked because the attack traffic surges or the protection bandwidth of your Anti-DDoS instance is too low, you can unblock the IP in the console.

Protection statistical reports

Anti-DDoS Pro provides multi-dimensional traffic reports and attack protection details to help you stay on top of the protection effects of your Anti-DDoS Pro instances in a timely and accurate manner.
Anti-DDoS Advanced provides statistical data on DDoS attacks, CC attacks, and forwarded traffic, keeping you updated on your business security. It also supports automatic packet capture for quick troubleshooting.
Anti-DDoS Advanced (Global Enterprise) provides multi-dimensional traffic reports and attack protection details to help you stay on top of the protection effects of your Anycast Anti-DDoS Advanced (Global Enterprise) instances in a timely and accurate manner.

Customizable cleansing threshold

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

Strengths

Last updated：2024-07-01 11:20:28

Anti-DDoS Basic

Anti-DDoS Basic provides basic DDoS protection capability for Tencent Cloud users to meet their daily security protection needs.

Anti-DDoS Pro

Anti-DDoS Pro is a paid service that can enhance the DDoS protection capabilities of Tencent Cloud services such as CVM, CLB, WAF, NAT Gateway, and Lighthouse. It has the following strengths:

Quick connection

Anti-DDoS Pro is easy to connect and requires no business changes on your end. After you purchase an instance, it only takes a couple of minutes to get started. You only need to bind the instance to the IP address of the Tencent Cloud service you want to protect.

Dual-protocol protection

Anti-DDoS Pro now supports both IPv6 and IPv4 addresses. By simply binding the IP addresses of your Tencent Cloud services to an Anti-DDoS Pro instance, you can obtain DDoS protection, with no need to purchase an extra Anti-DDoS Pro instance or upgrade it.

Massive protection resources

With ultra-large BGP protection bandwidth, Anti-DDoS Pro covers a wide range of ISPs including China Telecom, China Unicom, and China Mobile, easily defending against DDoS attacks to ensure security and stability for essential businesses such as promotional campaigns and launch events.

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 Pro can accurately and promptly detect business traffic. With the aid of a smart AI engine that continuously optimizes the algorithms, it is also flexible in coping with various attacks.

Fast speed and reliability

With a 30-line BGP linkage encompassing ISPs across China, Anti-DDoS Pro can effectively reduce latency and increase access speed for various user groups.

Detailed protection reports

Anti-DDoS Pro provides multi-dimensional statistical reports to display clear, accurate protection traffic and attack details, helping you stay on top of attacks in time.

Lower security protection costs

Anti-DDoS Pro offers a simplified billing mode where you are only charged by "the number of protected IPs" you set for your business bandwidth and protection needs. When high-traffic attacks occur, the maximum DDoS protection capability of Tencent Cloud in the region of the Anti-DDoS Pro instance is reachable without extra payments.

Anti-DDoS Advanced

Anti-DDoS Advanced (Chinese Mainland) and Anti-DDoS Advanced (Global Standard)

Anti-DDoS Advanced (Chinese Mainland) and Anti-DDoS Advanced (Global Standard) are paid services that can protect a business that is not deployed on Tencent Cloud against high-volume DDoS attacks. They have the following strengths:

Massive protection resources

Connected with 30 ISPs across China and with dozens of protection nodes deployed overseas, Tencent Cloud's BGP linkage can provide a protection bandwidth of up to 1 Tbps for a single customer (point) in the Chinese mainland, protection bandwidth of up to 400 Gbps outside the Chinese mainland, and CC protection capability of 700,000 QPS, helping you handle 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 (Chinese Mainland) and Anti-DDoS Advanced (Global Standard) can accurately and promptly detect business traffic. With the aid of a smart AI engine that continuously optimizes the algorithms, they are also flexible in coping with various attacks.

Fast speed and reliability

With a 30-line BGP linkage encompassing ISPs across China, Anti-DDoS Advanced (Chinese Mainland) and Anti-DDoS Advanced (Global Standard) can effectively reduce latency and increase access speed for various user groups.

Hiding real servers

Anti-DDoS Advanced (Chinese Mainland) and Anti-DDoS Advanced (Global Standard) can replace and hide users' real servers. An Anti-DDoS Advanced instance is used as the internet-facing address of the real server. All business access traffic will pass through the Anti-DDoS Advanced instance, which will forward normal access traffic to the real server. In addition, the Anti-DDoS Advanced instance will cleanse attack traffic and then forward clean traffic to the real server.

Wide applicability

Anti-DDoS Advanced (Chinese Mainland) and Anti-DDoS Advanced (Global Standard) support website and non-website businesses for sectors such as finance, ecommerce, gaming, and government, meeting the security needs of different businesses.

Cost optimization

Anti-DDoS Advanced (Chinese Mainland) and Anti-DDoS Advanced (Global Standard) offer 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, Tencent Cloud provides elastic protection to ensure the continuance of your business. Such a seamless transition requires no additional devices and configuration on your side, reducing your daily protection costs.

Detailed protection reports

Anti-DDoS Advanced (Chinese Mainland) and Anti-DDoS Advanced (Global Standard) provide accurate protection traffic reports and detailed attack information, enabling you to stay on top of attacks in time. In addition, automatic capture of attack packets is supported for quick troubleshooting.

Anti-DDoS Advanced (Global Enterprise)

Cloud-native solution for quick deployment

Anti-DDoS Advanced (Global Enterprise) provides a solution more toward a cloud-native protection architecture to facilitate quick deployment. After purchasing an Anti-DDoS Advanced (Global Enterprise) instance, you only need to bind it to the target object, with no adjustment required.

Massive protection resources

Anti-DDoS Advanced (Global Enterprise), with ten cleansing nodes outside the Chinese mainland, supports Tbps-level protection capability globally, providing security and stability for essential businesses such as promotional campaigns and launch events.

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 (Global Enterprise) can accurately

and promptly detect business traffic. With the aid of a smart AI engine that continuously optimizes the algorithms, it is also flexible in coping with various attacks.

Stable access experience

Tencent Cloud's BGP linkage covers multiple ISPs, which can effectively reduce access latency and ensure network quality. It also supports smart routing and automatic network scheduling, delivering a stable, smooth access experience for various user groups.

Detailed protection reports

Anti-DDoS Advanced (Global Enterprise) provides multi-dimensional statistical reports to display clear, accurate protection traffic and attack details, helping you stay on top of attacks in time.

Lower security protection costs

1. The simplified billing mode enables you to flexibly choose "the number of protected IPs + unlimited number of times of all-out protection" according to your business bandwidth and protection needs. The following solutions are available to cope with high-volume traffic attacks:
Leverages the collective protection capability of multiple nodes across the world to defend against DDoS attack traffic for all-out protection.
Maximizes the availability of your business by scheduling and blocking, particularly when under attacks.
2. The billing mode of "pay-as-you-go business bandwidth + quarterly subscription" helps reduce your security cost.

Use Cases

Last updated：2024-07-01 11:20:28

Gaming

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

Website

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

Finance

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

Government

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

Enterprise

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

Ecommerce

The overseas ecommerce industry has been worldwide with increasing global visits and orders during festivals and promotional campaigns. Anti-DDoS safeguards continuity and security for global businesses, especially during major ecommerce promotions.

Concepts

Last updated：2024-07-01 11:20:28

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.

Protection capability

Protection capability refers to the ability to defend against DDoS attacks. The Anti-DDoS service promises to provide all-out protection subject to the maximum DDoS protection capability of Tencent Cloud in the current region.

Cleansing

If the public network traffic of the target IP exceeds the preset protection threshold, Tencent Cloud Anti-DDoS service will automatically cleanse the inbound public network traffic of the target IP. With the BGP routing protocol, the traffic will be redirected to the DDoS cleansing devices which will analyze the traffic, discard the attack traffic, and forward the clean traffic back to the target IP.
In general, cleansing does not affect access except on special occasions or when the cleansing policy is configured improperly. If no exception is found (which is dynamically determined based on the attack) in the traffic for a period of time, the cleansing system will determine that the attack has stopped and then stop cleansing.

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 capacity of Tencent Cloud in the current region, 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 threshold

The blocking threshold of a protected IP of an Anti-DDoS instance is equal to the maximum protection capability in the current region.

Blocking duration

An attacked IP is blocked for two 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 mainly affected by the following factors:
Continuity of the attack: The blocking duration will extend if an attack continues. Once the duration extends, a new blocking cycle will start.
Frequency of the attack: Users who are frequently attacked are more likely to be attacked continuously. In such a case, the blocking duration extends automatically.
Traffic volume of the attack: The blocking duration extends automatically in case of an 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 is blocking necessary?

Tencent Cloud reduces the 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.

Protection bandwidth

There are two types of protection bandwidth: base protection bandwidth and elastic protection bandwidth.
Base protection bandwidth: refers to the base protection capability of an Anti-DDoS Advanced instance. Base protection bandwidth is a prepaid monthly subscription feature.
Elastic protection bandwidth: refers to the largest possible protection capability of an 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 protection capability of an Anti-DDoS Advanced instance will be the base protection bandwidth. If elastic protection is enabled, the maximum protection capability will be the elastic protection bandwidth. Once the attack traffic exceeds the maximum protection capability, IP blocking will be triggered.

Note:

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

Protection bandwidth is only available for Anti-DDoS Advanced and Anti-DDoS Advanced Global Enterprise.

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 business.

Elastic protection billing

When 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 to 50 Gbps. If the actual peak attack bandwidth of the current day is 35 Gbps, you will need to pay for the elastic protection according to the price of the 10-20 Gbps tier.

Blocking Policies

Last updated：2024-07-01 11:20:28

What is blocking?

Once the attack traffic exceeds the blocking threshold, Tencent Cloud will notify the related ISP to block the attacked IP from the Internet.

Note:

The blocking threshold of a protected IP of an Anti-DDoS instance is equal to the maximum protection capability in the related region.

Integrating the local cleansing capability, all-out protection aims to spare no effort to successfully defend against every DDoS attack.

In short, once the traffic attacking your IP exceeds the maximum protection capability Tencent Cloud supports in the current region, Tencent Cloud will block the IP from all public network access.

How do I unblock my IP?

IP blocking is a service Tencent Cloud purchases from ISPs with limitations on the number of times and the frequency of unblocking.

Note:

Only **three** chances of self-service unblocking are available for each Anti-DDoS Pro and Anti-DDoS Advanced user every day. The system resets the chance counter daily at midnight. Unused chances will not be carried forward to the next day.

If you want to unblock your IP immediately, see Business IPs Blocked Due to High-traffic Attacks.

Why is my IP blocked?

Tencent Cloud reduces cloud costs by sharing infrastructure, with one public IP shared among all users. When a high-traffic attack occurs, the entire Tencent Cloud network may be affected, not only the attack targets.

To protect other users and ensure network stability, we have to block the target IP.

Blocking duration

An attacked IP is blocked for two 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 mainly affected by the following factors:
Continuity of the attack: The blocking duration will extend if an attack continues. Once the duration extends, a new blocking cycle will start.
Frequency of the attack: Users who are frequently attacked are more likely to be attacked continuously. In such a case, the blocking duration extends automatically.
Traffic volume of the attack: The blocking duration extends automatically in case of an ultra-large volume of attack traffic.
Note:
For IPs that are blocked frequently, Tencent Cloud reserves the right to extend the blocking duration and lower the blocking threshold.
To view the unblocking time, see View Blocking Time.

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 ISPs' networks, Tencent Cloud is 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 Tencent Cloud users. In addition, IP blocking is a service Tencent Cloud purchases from ISPs with limitations on the number of times and the frequency of unblocking.

Relevant Products

Last updated：2024-07-01 11:20:28

Anti-DDoS can be used in conjunction with the following Tencent Cloud products.

Cloud Virtual Machine (CVM): A scalable cloud computing service that frees you from estimation of resource usage and upfront investment. With Tencent Cloud CVM, you can launch any number of CVM instances and deploy applications quickly.

Cloud Load Balancer (CLB): Distributes traffic to multiple CVM instances securely and quickly so as to eliminate single points of failure for higher availability.

Web Application Firewall (WAF): An AI-based, one-stop web service protection solution.

NAT Gateway: An IP address translation service, featuring SNAT and DNAT. It provides secure and high-performance Internet access for resources in virtual private clouds (VPCs).

VPN connection: This is a transfer service based on network tunneling technology that brings about connectivity between local IDCs and resources on Tencent Cloud. It can help you quickly build a secure and reliable encrypted tunnel over the Internet.

Cloud Bare Metal (CBM): This is an on-demand pay-as-you-go physical server rental service that provides high-performance, securely isolated physical server clusters for cloud users.

Bare Metal Cloud Load Balancer: It virtualizes multiple physical servers in the same availability zone into a high-performance and high-availability application service pool by setting a virtual IP (VIP) address.

Bare Metal Elastic IP (Bare Metal EIP): A Bare Metal EIP address is an IP address dedicated to dynamic cloud computing, and it is a public IP address that can be separately applied for.

Global Application Acceleration Platform (GAAP): This is a PAAS product that allows optimum access latency for businesses across the globe. Via high-speed connections, cluster forwarding, and intelligent routing among global nodes, it enables users in different regions to access the closest nodes and forwards traffic to the origin server, reducing access lag and latency.

Elastic Network Interface (ENI): An ENI is used to bind a CVM instance within a VPC, and it can be freely migrated among CVM instances. ENIs can help configure and manage networks, as well as develop highly reliable network solutions.

Tencent Cloud Lighthouse: This is a new-gen, out-of-the-box cloud server service for small- and medium-sized enterprises (SMEs) and developers. It is designed for cloud-based lightweight use cases, such as websites, web applications, mini programs, mini games, apps, ecommerce, cloud storage, image hosting, and various development and testing environments. It is easier to use than traditional cloud server services and integrates common basic cloud services into different high-bandwidth/traffic packages. Such packages contain popular open-source software programs, enabling you to build applications swiftly and enjoy a minimalist cloud experience.