Anti-DDoS
Product Introduction

Copyright Notice

Trademark Notice

Tencent Cloud

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Product Introduction
- Overview
- Advantages
- Use Cases
- Relevant Concepts
- Block Policy
- Related Products

Product Introduction
Overview

Last updated: 2025-03-19 21:09:12

Overview

Anti-DDoS offers comprehensive, efficient, and professional DDoS protection capabilities, providing businesses with various DDoS solutions such as Anti-DDoS Basic, Anti-DDoS Pro, and Anti-DDoS Advanced to combat DDoS attacks. Through ample and high-quality DDoS protection resources, combined with continuously evolving "self-research + AI Intelligent Identification" cleaning algorithms, it ensures the stable and secure operation of user businesses. Protection scenarios cover industries such as gaming, internet, video, finance, and government.

Product Package

Anti-DDoS Pro Package

Anti-DDoS Pro (Standard)

Anti-DDoS Pro (standard version) is designed for Tencent Cloud users whose businesses are deployed domestically.
Tencent Cloud provides full protection, with the highest protection capability dynamically adjusted according to the actual network situation in each region. There is no need to change the ip address; after purchasing, you only need to bind the ip that needs protection to use it.

Anti-DDoS Pro (Enterprise Edition)

Anti-DDoS Pro (corporate version) is designed for Tencent Cloud users whose businesses are deployed both domestically and internationally.
It has T-level protection capabilities both domestically and internationally, and it can only take effect after creating and binding a high-protection EIP. Suitable for businesses with high requirements for business security. Rich protection capabilities can be flexibly selected and configured according to needs, and purchased in combination to control business protection costs.

- Chinese mainland region: The protection capability adopts a combination of baseline protection and elastic protection.
- Region outside Chinese mainland: Utilize the capabilities of Tencent Cloud's high-protection scrubbing center for full protection.

Note:

- Chinese mainland regions: Beijing, Shanghai, Guangzhou.
- Regions outside Chinese mainland: Hong Kong (China), Singapore, Tokyo, Jakarta, Silicon Valley, Frankfurt, Virginia, São Paulo.
- Full protection: Aiming to successfully defend against every DDoS attack, it integrates the current local cleaning center capabilities to fully resist attacks. Both at home and abroad have T-level protection capabilities.

Anti-DDoS Pro (Inclusive Edition)

Anti-DDoS Pro (inclusive edition) is designed for Tencent Cloud users whose businesses are deployed domestically.
It has the full protection capability of up to 60Gbps domestically. There is no need to change the ip address; after purchasing, you only need to bind the ip that needs protection to use it. It is a protection product specially designed for SMEs in the scenario of cloud asset attack blocking.

- Users of Anti-DDoS Pro (inclusive edition) 10Gbps version will have three self-service unlocking opportunities per month. If exceeded three times in a month, unlocking operations will not be available.
- Users of Anti - DDoS Pro (inclusive edition) with 30Gbps and 60Gbps specifications are provided with three self - service unlocking chances per day. After exceeding three times on the same day, unlocking operations cannot be carried out.

Anti-DDoS Pro (Lite Edition)

Anti-DDoS Pro (lightweight version) is an exclusive high-protection product for Tencent Cloud Lighthouse users.
It has the full protection capability of up to 10Gbps domestically. There is no need to change the ip address; after purchasing, you only need to bind the ip that needs protection to use it. It is a lightweight protection product specially customized for Tencent Cloud Lighthouse.

DDoS High Defense IP

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

Anti-DDoS Advanced is a paid protection service launched for businesses such as gaming, Internet and finance that suffer from large-volume DDoS attacks resulting in unavailable user services. By configuring Anti-DDoS Advanced, direct the business ip to Anti-DDoS Advanced or resolve the DNS domain name of the business to the CNAME address for traffic attraction. All public network traffic will first pass through the high-protection cluster. Attack traffic will be cleaned and filtered in the high-protection cleaning center, and normal access traffic will

be forwarded to the business origin server, thereby ensuring the stable availability of the origin server business.
Anti-DDoS Advanced uses the public network proxy access method and supports protocols such as TCP, UDP, HTTP, HTTPS and HTTP2, covering various businesses such as finance, ecommerce and gaming.

Anti-DDoS Advanced (Global Enterprise Edition)

Anti-DDoS Advanced (Global Enterprise Edition) is a paid product that enhances DDoS protection capabilities for businesses deployed on Tencent Cloud.

- Anti-DDoS Advanced (global enterprise) provides 10 Tencent Cloud entries around the world, sharing the bandwidth pressure of each individual entry and providing full protection services. Maximize the smooth access of nodes in various places.
- Anycast achieves near-origin filtering and near-origin reinjection, providing global T-level protection capabilities. The normal business traffic after passing through each cleaning node will be reinjected to the server near the origin, ensuring the smoothness and low latency of the business traffic. Anti-DDoS Advanced (global enterprise) directly takes effect on IPs on Tencent Cloud.

Product Features

Multiple Types Of Protection

Protection Category	Description
Malformed packet filtering	Filter Frag Flood, Smurf, Stream Flood, Land Flood attacks, filter malformed IP packets, malformed TCP packets, malformed UDP packets.
Network layer DDoS attack protection	Filter UDP Flood, SYN Flood, TCP Flood, ICMP Flood, ACK Flood, FIN Flood, RST Flood, DNS/NTP/SSDP and other reflection attacks, null connections.
Application layer DDoS attack protection	Filter CC attacks, support HTTP custom feature filtering such as host filtering, user-agent filtering, referer filtering.

Note:
Application-layer DDoS protection is only supported by Anti-DDoS Advanced IP.

Bind and Switch Protection Objects

Anti-DDoS supports protection object IP switching to meet your needs for protecting different cloud resource public IP addresses. The supported switching objects include CVM, CLB, WAF, NAT Gateway, etc.

Security Protection Policy

Anti-DDoS provides basic security policies by default. The policies are based on attack profile, behavior pattern analysis, AI intelligent identification and other protection algorithms to effectively deal with common DDoS attack behaviors. At the same time, it provides diverse and flexible DDoS protection policies. You can set them flexibly according to the special business characteristics to cope with the constantly changing attack methods.

Block Self-Service Removal

When the attack traffic suddenly increases or the protection bandwidth of Anti-DDoS is small, causing the business IP connected to the high defense to be blocked, you can unblock it through the console by yourself.

Protection Statistics Report

- Anti-DDoS Pro provides multi-dimensional traffic reports and detailed attack protection information, helping you understand the protection effectiveness of Anti-DDoS Pro in a timely and accurate manner.
- 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.
- Anti-DDoS Advanced (global enterprise) provides multi-dimensional traffic reports and detailed attack protection information, helping you understand the protection effectiveness of overseas Anycast Anti-DDoS Advanced in a timely and accurate manner.

Customization Of Cleaning Mode

DDoS Anti-DDoS IP supports multiple protection levels and provides a custom cleansing threshold, allowing users to flexibly adjust based on attack conditions, swiftly respond to various types of DDoS attacks, and fully meet the diverse business needs of different users.

Advantages

Last updated: 2025-03-19 21:09:34

Anti-DDoS Pro Package

It is only applicable to Tencent Cloud products, including CVM, CLB, WAF, NAT Gateway, Lighthouse and other cloud services. It is a paid security service to enhance their DDoS protection capabilities and has the following strengths:

Connect With One Click, Zero Change

No business change is required. The connection configuration is convenient. After purchasing Anti-DDoS Pro, you only need to bind the IP address of the cloud product that needs protection to use it, which can take effect in a few minutes.

Support Dual - Protocol Protection

Anti-DDoS Pro supports simultaneous protection for both IPV6 and IPV4 types of IP addresses, meeting customers' protection needs for IPV6 type servers. There is no need for additional purchase or upgrade of Anti-DDoS Pro. After binding the IP address of the cloud product that needs protection, DDoS protection can be achieved.

Ultra - Large Protection Resources

Anti-DDoS Pro has a super-large BGP protection bandwidth, covering different ISPs such as China Telecom, China Unicom and China Mobile, easily resisting DDoS attacks and meeting the security and stability guarantee needs of important businesses such as promotional activities and launch of activities.

Leading Scrubbing Capability

Relying on Tencent's self-developed protection cluster, it adopts multi-dimensional algorithms such as IP profiling, behavior analytics and Cookie challenge, and continuously updates the protection algorithm through AI intelligent engine to accurately and quickly detect business traffic and flexibly respond to various attack behaviors.

Ultra - Fast Access Experience

Tencent Cloud's BGP link connects with 30 ISPs across the country, offering wide coverage, effectively solving access delay issues, ensuring access speed for various user groups, and providing an extremely fast access experience.

Rich Protection Reports

Anti-DDoS Pro provides multi-dimensional statistical reports to display clear and accurate protection traffic and attack details, helping users stay informed about real-time attack situations.

Optimize Security Cost

Simplify the billing method. You can flexibly choose the "number of protected IPs" according to your business scale and protection needs. When suffering from large-scale traffic attacks, call the maximum Anti-DDoS capability of Tencent Cloud in the current region to provide full protection without paying additional elastic fees, reducing your daily security expenditure.

DDoS Protective IP

Anti-DDoS IP (Chinese Mainland), Anti-DDoS IP (Outside Chinese Mainland, Standard Version)

Anti-DDoS Advanced (Chinese mainland) and Anti-DDoS Advanced (global standard) are paid products launched by Tencent Cloud for cloud external user businesses when their services become unavailable after suffering from large-scale DDoS attacks. The product advantages are as follows:

Ultra-Large Protection Resources

Tencent Cloud's BGP link connects with 30 ISPs across the country. A single customer at a single point can provide up to 1T of Anti-DDoS protection capability. It provides 700,000 QPS of CC protection capability. Dozens of protection nodes overseas, with up to 400Gbps of protection capability, easily cope with various DDoS attacks.

Leading Scrubbing Capability

Relying on Tencent's self-developed protection cluster, it adopts multi-dimensional algorithms such as IP profiling, behavior analytics and Cookie challenge, and continuously updates the protection algorithm through AI intelligent engine to accurately and quickly detect business traffic and flexibly respond to various attack behaviors.

Ultra-Fast Access Experience

Tencent Cloud's BGP link connects with 30 ISPs across the country, covering a wide area and effectively solving access delay problems, ensuring the access speed of various user groups and bringing an extremely fast access experience.

Hide User Origin Server

The Anti-DDoS Advanced (Chinese mainland) and Anti-DDoS Advanced (global standard) services can replace and hide the user's origin server. Use the Anti-DDoS IP as the external

service address of the origin server. All business access traffic passes through the Anti-DDoS IP, which forwards the normal access traffic to the origin server. The attack traffic is cleaned on the Anti-DDoS IP, and after cleaning, the Anti-DDoS IP returns the clean traffic to the origin server.

Full Business Support

The Anti-DDoS Advanced (Chinese mainland) and Anti-DDoS Advanced (global standard) services support both website and non-website businesses, covering finance, ecommerce, gaming, government and other types of businesses, fully meeting users' different business security protection needs.

Flexible Pricing To Optimize Cost

Provide a billing method that combines "baseline protection + elastic protection" to reduce users' daily security costs. Adjust the elastic protection as needed when necessary without adding any new equipment or adjusting the configuration. When the attack traffic exceeds the peak value of baseline protection, Tencent Cloud still continues to protect users to ensure uninterrupted business and pay according to the actual attack volume on that day.

Rich Attack Protection Reports

Provide accurate protection traffic reports and attack detail information to enable users to understand the actual situation of attacks in time. Support automatic packet capture for attacks, which is convenient for subsequent analysis and tracing the source.

Anti-DDoS Advanced (Global Enterprise Edition)

Cloud - Native - Fitting Protection Architecture For One - Click Integration

The product solution is more in line with the cloud native protection architecture, and the connection configuration is convenient. After purchasing Anti-DDoS Advanced (global enterprise), you only need to associate the anti-DDoS instance with the required protection object to achieve one-click access and rapid deployment.

Ultra-Large Protection Resources

Anti-DDoS Advanced (global enterprise) integrates the capabilities of Tencent Cloud's high-protection scrubbing centers outside the Chinese mainland, covering 10 scrubbing nodes overseas, providing global T-level protection capabilities, and meeting the security and stability guarantee needs of important businesses such as promotional activities and launch of activities.

Leading Scrubbing Capability

Relying on Tencent's self-developed protection cluster, it adopts multi-dimensional algorithms such as IP profiling, behavior analytics and Cookie challenge, and continuously updates the protection algorithm through AI intelligent engine to accurately and quickly detect business traffic and flexibly respond to various attack behaviors.

Stable Access Experience

Tencent Cloud's BGP linkage connects with multiple ISPs, has a wide coverage, can effectively solve the problem of access latency and ensure network quality. It intelligently selects routes and automatically completes network scheduling to ensure the access stability of various user groups, bringing stable and smooth access experience.

Rich Protection Reports

Anti-DDoS Advanced (global enterprise) provides multi-dimensional statistical reports, displaying clear and accurate attack protection traffic and attack detail information, enabling users to understand the actual situation of attacks in time.

Optimize Security Cost

1. Simplify the billing method. You can flexibly choose "number of protection IPs + unlimited full protection" according to your business scale and protection needs. When encountering large-scale traffic attacks:
   - Utilize the protection capabilities of multiple nodes worldwide to share and resist DDoS attack traffic simultaneously, achieving full protection.
   - Adopt a combination of scheduling & blocking to maximize business availability for customers and increase availability during attacks.
2. Business bandwidth is paid as needed on a postpaid basis, and the flexible billing mode of quarterly sales reduces your daily security expenditure.

Use Cases

Last updated: 2025-03-19 21:16:49

Games

The game industry is a prime target for DDoS attacks. Anti-DDoS can effectively ensure the availability and sustainability of games, guarantee a smooth experience for players, and provide security protection during events, new game releases, or peak holiday revenue periods, ensuring the normal operation of the game business.

Internet

Ensure smooth access to internet web pages and uninterrupted normal business operations, providing security protection during major events such as ecommerce promotions.

Finance

Meet the compliance requirements of the financial industry and ensure the real-timeness and security stability of online transactions.

Government

Meet the security needs of national government cloud construction standards, provide security assurance for important meetings, events, and sensitive times, ensure the normal availability of people's livelihood services, and maintain government credibility.

Enterprise

Ensure the continuous availability of enterprise website services, avoid economic losses and damage to the corporate brand image caused by DDoS attacks, with zero hardware and zero maintenance, saving on security costs.

E-Commerce

Ecommerce business outside Chinese mainland is spread across the world. Accompanied by holidays and various promotions in different regions, accesses and orders keep increasing. Anti - DDoS can effectively ensure the normal and uninterrupted global business operations and provide security protection during major events such as ecommerce promotional activities.

Relevant Concepts

Last updated: 2025-03-19 21:17:04

DDoS Attack

A Distributed Denial of Service (DDoS) attack refers to an attacker remotely controlling a large number of zombie hosts over the network to send a large number of attack requests to one or more targets, blocking the network bandwidth of the target server or exhausting its system resources, making it unresponsive to normal Service requests.

Network Layer DDoS Attack

A network layer DDoS attack mainly refers to an attack method where attackers use high-traffic attacks to congest the network bandwidth of the target server, consume server system layer resources, and cause the target server to be unable to normally respond to customer access.
Common attack types include SYN Flood, ACK Flood, UDP Flood, ICMP Flood, and DNS/NTP/SSDP/memcached reflection attacks.

CC Attack

A CC attack mainly refers to an attack method that maliciously occupies application layer resources of the target server, consumes processing performance, and causes it unable to provide services properly.
Common attack types include HTTP/HTTPS-based GET/POST Flood, Layer-4 CC, and Connection Flood.

Protection Capability

Protection capability refers to the ability to resist DDoS attacks. The Anti-DDoS service commitment provides full protection according to the maximum Anti-DDoS protection capability of Tencent Cloud in the current region.

Scrubbing

When the public network traffic of the target IP exceeds the set protection threshold, the Tencent Cloud Anti-DDoS protection system will automatically scrub the inbound public network traffic of this IP. Through the BGP routing protocol, the traffic is redirected from the original network path to the Tencent Cloud Anti-DDoS cleaning equipment. The cleaning equipment identifies the traffic of this IP, discards the attack traffic, and forwards the normal traffic to the target IP.

Normally, cleaning will not affect normal access. It may impact normal access only in special scenarios or when the cleaning strategy configuration is incorrect. When the traffic continues for a specified period (determined dynamically according to the attack situation) without exceptions, the cleaning system will deem the attack ended and stop cleaning.

Block

When the attack traffic received by the target IP exceeds its blocking threshold, Tencent Cloud will block all public network access of this IP through the operator's service blocking to protect other users on the cloud platform from being affected. In short, when the attack traffic received by your certain IP exceeds the maximum protection capability of Tencent Cloud in the current region, Tencent Cloud will block all public network access of this IP. When your protected IP is blocked, you can log in to the management console to perform self-service unblocking.

Blocking Threshold

The blocking threshold of the protected IP of the DDoS High Protection Instance is equal to the maximum protection capability of the current region.

Blocking Duration

The blocking duration defaults to 2 hours. The actual blocking duration is related to the trigger count and peak value of blockings on that day, and can be up to 24 hours at most. The blocking duration is mainly affected by the following factors:

- Whether the attack continues: If the attack continues, the blocking time will be extended, and the blocking time will be recalculated starting from the moment of extension.
- Whether the attack is frequent: The probability of continuous attacks for users who are frequently attacked is large, and the blocking time will be automatically extended.
- Traffic size of the attack: The blocking time will be automatically extended for users who are under ultra-large traffic attacks.

> **Note:**
> For individual users who are blocked too frequently, Tencent Cloud reserves the right to extend the blocking duration and reduce the blocking threshold.

Why Perform Blocking

Tencent Cloud reduces cloud cost by sharing infrastructure. All users share Tencent Cloud's public egress IP address. When a high-traffic attack occurs, in addition to affecting the attacked object, the entire Tencent Cloud network may be affected. To prevent attacks from

affecting other users who are not attacked and guarantee the stability of the entire cloud platform network, blocking needs to be performed.

Protection Bandwidth

Protection bandwidth is divided into baseline protection bandwidth and elastic protection bandwidth.

- Baseline protection bandwidth: Refers to the base protection capability of a high-defense IP instance. The guaranteed part is prepaid by year/month.
- Elastic protection bandwidth: Refers to the maximum elastic protection capability of a high-defense IP instance. The elastic part is paid after daily usage.

If Elastic Protection is not enabled, the baseline protection bandwidth is the highest protection capability of the high-defense IP instance. If Elastic Protection is enabled, the elastic protection bandwidth serves as the highest protection capability of the high-defense IP instance. Blocking is triggered when the attack traffic exceeds the highest protection capability of the high-defense IP instance.

Note:

- Elastic Protection is off by default. If you need to enable Elastic Protection, please enable it after acknowledging the related charges. Based on their specific business needs, users can adjust the elastic protection bandwidth at any time.
- Protection bandwidth is only supported for high-defense IPs and global enterprise.

Role of Elastic Protection Bandwidth

After you enable Elastic Protection, when the attack traffic exceeds the purchased base protection capability and is within the scope of the elastic protection capability, Tencent Cloud Anti-DDoS Advanced can continue to provide protection for users, guaranteeing the continuity of business access.

How Is Elastic Protection Charged

After enabling Elastic Protection, when the attack traffic exceeds the base protection capability, Elastic Protection will be triggered and fees will be charged. Billing will be based on the interval corresponding to the highest peak value of actual attack generated on the day, and the bill will be generated on the next day.
For example, if the guaranteed protection you have purchased is 20 Gbps and the elastic protection you have set is 50 Gbps. If the actual peak attack bandwidth on the day is 35 Gbps, you need to pay for the elastic protection fee in the 10 Gbps – 20 Gbps interval.

Protection Times of Full Protection and High Defense Insurance

When the attack traffic exceeds **basic protection capability (see in the table below)**, the attack duration will start to accumulate and count as one protection. When the cumulative duration of a single protection exceeds 30 minutes, the next protection will be enabled.

- If an attack event causes IP blocking, the **protection times will not be consumed**.
- When the protection times of **full protection and High Defense Insurance protection** are 0, the assets bound to the High Defense Package or High Defense Insurance will be protected according to **basic protection capability (see in the table below)**.

Protection Type	Basic Protection Capability
Anti-DDoS Pro (standard version 2.0) 2 times of protection	10 Gbps
Anti-DDoS High Defense Insurance	2 Gbps (Anti-DDoS Basic)

Block Policy

Last updated: 2026-03-11 17:19:21

What Is Blocking?

When the attack traffic received by the destination ip exceeds its blocking threshold, Tencent Cloud will block all public network access of the ip through the ISP's service to protect other users on the Cloud Platform from being affected.

Note:
- Blocking threshold: The blocking threshold of the protected IP of the Anti-DDoS instance is equal to the maximum protection capability in the current region.
- Full protection aims to successfully defend against every DDoS attack by integrating the capabilities of the current local cleansing center.

In short, when the attack traffic received by one of your ips exceeds the maximum protection capability of Tencent Cloud in the current region, Tencent Cloud will block all public network access of the ip.

How To Unblock?

Blocking is a service purchased by Tencent Cloud from ISPs, and there are limitations on the count and frequency of unblocking.

Note:
- Users of Anti-DDoS Pro (excluding the lightweight and inclusive versions) and Anti-DDoS IP will have three chances of self-service unlocking every day. The system resets the chance counter daily at midnight. Unused chances cannot be accumulated for the next day.
- Users of the lightweight edition of Anti-DDoS Pro are provided with three self-service unlocking capabilities per month, which can only be used to unlock lightweight server resources.
- Users of the 10Gbps specification of Anti-DDoS Pro (inclusive edition) are provided with three self-service unlocking capabilities per month. If the number exceeds three in a month, unlocking operations will not be available.

If you can't wait for the automatic unblocking, you can refer to Business is blocked due to large-scale traffic attacks for handling.

Why Block?

Tencent Cloud reduces cloud costs by sharing infrastructure. All users share Tencent Cloud's public egress IP address. When a large-scale traffic attack occurs, besides affecting the targeted object, the entire Tencent Cloud network may be affected.
To prevent attacks from affecting other unaffected users and ensure the stability of the entire Cloud Platform network, blocking is necessary.

Blocking Duration

The default blocking duration is 2 hours, but the actual blocking duration is related to the daily blocking trigger count and attack peak value, and can last up to 24 hours. The blocking duration is mainly affected by the following factors:

- Whether the attack is continuous: If the attack continues, the blocking time will be extended, and the blocking time will be recalculated from the moment of extension.
- Whether the attack is frequent: Users who are frequently attacked are more likely to suffer continuous attacks, and the blocking time will be automatically extended.
- The size of attack traffic: Users who are attacked by extremely large traffic will have their blocking time automatically extended.

> **Note:**
> For individual users who are blocked too frequently, Tencent Cloud reserves the right to extend the block duration and lower the block threshold.

For viewing the unblocking time, please refer to View Blocking Time.

Why Can'T It Be Unblocked Immediately?

Typically, DDoS attacks will last for a period of time and will not stop immediately after blocking. The specific duration is uncertain. Tencent Cloud's security team will set the default blocking duration based on the results of big data analysis.
Since blocking takes effect in the ISP network, once the attacked public IP enters blocking, Tencent Cloud cannot monitor whether the attack traffic has stopped. If the block is lifted while the attack has not ceased, the attacked public IP will enter blocking again. Moreover, during the time from unblocking to the re-blocking taking effect, the attack traffic will directly enter Tencent Cloud's basic network, potentially affecting other customers within the cloud. Additionally, blocking is a service purchased by Tencent Cloud from ISPs, and there are limitations on the count and frequency of unblocking.

Related Products

Last updated: 2026-03-26 15:39:36

Using Anti-DDoS can enhance the Anti-DDoS capability for the following products:

- Cloud Virtual Machine: It is a scalable computing service provided by Tencent Cloud. Using CVMs eliminates the need to estimate resource usage and make upfront investments required with traditional servers, helping you quickly launch any number of VMs in a short time frame and instantly deploy applications.
- Cloud Load Balancer: Provides secure and fast traffic distribution services. Access traffic can be automatically distributed to multiple CVMs in the cloud through CLB. This expands the system's service capabilities and eliminates single points of failure.
- Web Application Firewall: It is an AI-based one-stop solution for web business operation risk protection.
- NAT Gateway: It is a kind of IP address conversion service that provides SNAT and DNAT capabilities and can provide secure and high-performance internet access services for resources in Virtual Private Cloud (VPC).
- VPN Connections: It is a transmission service based on network tunneling technology, which realizes the connection between local data centers and resources on Tencent Cloud. It can help you quickly build a secure and reliable encrypted tunnel on the Internet.
- Bare Metal CVM: It is a physical server rental service that can be purchased on demand and pay-as-you-go, providing you with a dedicated, high-performance, and security-isolated physical server cluster in the cloud.
- Global Application Acceleration: Global Application Acceleration Platform (GAAP) relies on high-speed channels, forwarding clusters, and smart routing technology between global nodes to achieve proximity access for users worldwide. By connecting directly to the origin server area through high-speed channels, it helps businesses solve the problem of global users experiencing lag or high latency.
- Elastic Network Interface: It is an elastic network interface bound to CVMs within a Virtual Private Cloud (VPC), which can be freely migrated among multiple CVMs. Elastic Network Interfaces are very helpful in configuring and managing networks and building highly reliable network solutions.
- Tencent Cloud Lighthouse: It is a new generation of out-of-the-box, lightweight cloud server products aimed at lightweight application scenarios. It helps small and medium-sized enterprises and developers to build websites, web applications, mini programs/games, apps, e-commerce applications, cloud storage/image hosting, and various development and testing environments on the cloud conveniently and efficiently. Compared to regular cloud servers, it is simpler and more application-oriented. It is sold as

a package of basic cloud resources with high-bandwidth traffic packages, integrating popular open-source software for one-click application deployment, providing an extremely simple cloud experience.