Anti-DDoS Pro

Product Introduction

Product Documentation

Contents

Product Introduction

Overview

Last updated：2023-06-25 14:35:01

Anti-DDoS Pro is a paid service to improve DDoS protection capabilities for users whose applications are deployed on Tencent Cloud. It provides protection for IPs on Tencent Cloud. You can use it by binding it to the target IPs (An EIP is required if you want to use the Enterprise Edition). With comparison to Anti-DDoS Advanced, it features convenient access and zero changes.

Packages

Standard

Anti-DDoS Pro (Standard) is dedicated for Tencent Cloud users whose applications are deployed in some regions within the Chinese mainland.

Tencent Cloud provides an all-out protection. The maximum protection capability can be adjusted dynamically based on the actual network conditions of the region. To get started, you only need to bind it with the IP addresses you want to protect.

Enterprise

Anti-DDoS Pro (Enterprise) is dedicated for Tencent Cloud users whose applications are deployed in and outside the Chinese mainland.

Anti-DDoS Pro (Enterprise) provides Tbps-level protection capability. It takes effect only after binding with an Anti DDoS EIP. It is applicable to enterprises with high demand on application security. With rich protection capabilities, it offers different configurations, helping enterprises reduce protection costs.

- Chinese mainland: Base protection + elastic protection
- Outside the Chinese mainland: Tencent Cloud Anti-DDoS cleansing center provides an all-out protection

> Note：
>
> - Chinese mainland regions: Beijing, Shanghai, Guangzhou
> - Outside the Chinese mainland: Hong Kong (China), Singapore, Tokyo, Jakarta, Silicon Valley, Frankfurt, Virginia, São Paulo
> - All-out protection: Integrating the local cleansing capability, the all-out protection aims to spare no effort to successfully defend against each DDoS attack. Tbps-level protection capability is provided in and outside

the Chinese mainland.

General

Anti-DDoS Pro (General) is dedicated for Tencent Cloud users whose applications are deployed in the Chinese mainland.

It provides an all-out protection for up to 60 Gbps of bandwidth in the Chinese mainland. To get started, you only need to bind it with the IPs you want to protect. Anti-DDoS Pro (General) is dedicated for small and medium-sized enterprises whose assets are attacked/blocked on the cloud.

Product Features

Multidimensional protection

Protection Type	Description
Malformed packet filtering	Filters out Frag Flood, Smurf, Stream Flood, and Land Flood attacks, as well as IP, TCP and UDP malformed 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.

Bind and switch the protected targets

Anti-DDoS Pro supports switching protected public IPs of your Tencent Cloud resources such as CVM, CLB, WAF and NAT Gateway.

Security protection policy

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

IP unblocking

If a protected IP is blocked when the attack traffic bursts or the protection bandwidth of your Anti-DDoS Pro instance is too low, you can unblock the IP in a self-service manner in the console. For details, see Blocking Policy.

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 in a timely and accurate manner.

Strengths

Last updated：2022-08-16 11:33:03

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

One-Click Access

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

Dual-protocol Protection

Anti-DDoS Pro now supports both IPv6 and IPv4 address. By simply binding the IPs of your cloud products with 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 can cover a wide range of ISPs including China Telecom, China Unicom, and China Mobile, 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, DDoS Edge Defender 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 Speed and Reliability

With a 30-line BGP network encompassing ISPs across the Chinese mainland, 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 and accurate protection traffic and attack details, helping you stay on top of attacks in real time.

Lower Security Protection Costs

Anti-DDoS Pro offers a simplified billing mode where you are only charged by "number of protected IPs" you set for your business size 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.

Use Cases

Last updated：2020-07-07 15:56:26

Gaming

DDoS attacks are particularly common in the gaming industry. Anti-DDoS Pro 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 Pro ensures smooth and uninterrupted access to websites, especially during major ecommerce promotions.

Finance

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

Government Affairs

Anti-DDoS Pro 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 Pro 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：2023-04-20 16:05:35

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.

Protection Capability

Protection capability refers to the ability to defend against DDoS attacks. The Anti-DDoS Pro service promises an all-out protection with Tencent Cloud's maximum DDoS protection capability in the current region.

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 Tencent Cloud in the current region, 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 a protected IP of an Anti-DDoS Pro instance is equal to the maximum protection capability in the current region.

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 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.

Blocking Policy

Last updated：2022-08-16 11:41:47

What is blocking?

Once the attack traffic exceeds the blocking threshold of a target IP, Tencent Cloud will block the target IP from all public network accessing through ISP service to protect other Tencent Cloud users.

Note：

- The blocking threshold of a protected IP of an Anti-DDoS Pro instance is equal to the maximum protection capability in the current region.
- Integrating the local cleansing capability, the all-out protection aims to spare no effort to successfully defend against each DDoS attack.

In short, once the traffic attacking your IP goes over the maximum protection bandwidth Tencent Cloud provided, Tencent Cloud will block the IP from all public networks' access.

Why is my IP blocked?

Tencent Cloud reduces cloud costs by sharing infrastructure, with one public IP shared among all users. When a large 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 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.

Relevant Products

Last updated：2023-06-25 14:35:48

Anti-DDoS Pro can be activated for the following products:

- Tencent Cloud Virtual Machine (CVM) is a scalable cloud computing service that frees you from estimation of resource usage and upfront investment. With Tencent Cloud CVM, you can start CVM instances and deploy applications immediately.
- Cloud Load Balancer (CLB) is a service that distributes traffic to multiple CVM instances securely and quickly so as to eliminate single points of failure for a higher availability.
- Web Application Firewall (WAF) is an AI-based, one-stop web service protection solution.
- NAT Gateway is a service that supports IP address translation and provides the SNAT and DNAT capabilities. It provides secure and high-performance Internet access for resources in VPCs.
  VPN connection is a transfer service based on network tunneling technology that brings connectivity between local IDCs and resources on Tencent Cloud. It helps you to quickly build a secure and reliable encrypted tunnel on the Internet.
- CBM is a type of on-demand pay-as-you-go physical server rental service that provides high-performance and securely isolated physical server clusters for cloud users.
- BM CLB 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.
- BM EIP is an IP address dedicated for dynamic cloud computing, and is a public IP address that can be applied for independently.
- Global Application Acceleration Platform (GAAP) is a PAAS product that allows optimum access delay for applications across the globe. Via high-speed connections, cluster forwarding and intelligent routing among global nodes, it allows users in different regions to access the closest nodes and forwards traffic to the real server, reducing access lag and latency.
- An Elastic Network Interface (ENI) is used to bind CVM within a VPC instance, and can be freely migrated among CVMs. ENIs can help configure and manage networks, as well as develop highly reliable network solutions.