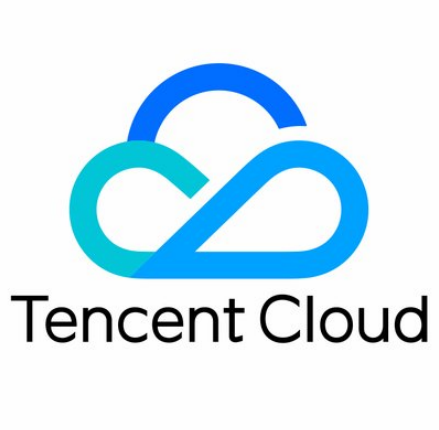
Anti-DDoS Pro

Product Introduction

Product Documentation



Contents

Product Introduction
Overview

Last updated : 2020-07-07 15:56:25

Anti-DDoS Pro Overview

Anti-DDoS Pro is a paid product that enhances DDoS protection capabilities for businesses deployed in Tencent Cloud and upgrades smoothly on the basis of Anti-DDoS Basic. It takes effect directly on the IPs in Tencent Cloud with no need to change the IP addresses. After purchasing, you only need to bind the IP to be protected for use. Compared with Anti-DDoS Advanced, it features easier connection and requires no changes to businesses.

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.

Flexible defense options

Anti-DDoS Pro supports switching IPs of the protected object to meet your different protection needs for public IPs of Tencent Cloud resources. The objects that support switching include CVM, CLB, WAF, NAT Gateway, etc.

Security protection policy

Anti-DDoS Pro 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 diverse and flexible protection policies, which can be tailored to your special needs to deal with ever-changing attack tricks.

Self-Service IP unblocking

If a protected business 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.

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 Anti-DDoS Pro instances in a timely and accurate manner.

Strengths

Last updated : 2020-07-07 15:56:26

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

Quick Configuration with Zero Adjustment Required

Anti-DDoS Pro is easy to access and requires no changes of your business. After you purchase an instance, it only takes 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 addresses. By simply binding the IPv6 addresses of your Tencent Cloud services with an Anti-DDoS Pro instance, you can enjoy DDoS protection with no need to purchase an extra instance or upgrade it.

Massive Protection Resources

Anti-DDoS Pro has an ultra-high BGP protection bandwidth and covers different ISPs such as China Telecom, China Unicom, and China Mobile. It can easily defend against DDoS attacks and meet your security and stability guarantee requirements for important businesses such as major promotion campaigns and event launches.

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 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 Pro features an extremely low latency in protection and fast access.

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.

Reduced Security Protection Costs

The simplified billing mode enables you to flexibly choose the "number of protected IPs + protected times" according to your business size and protection needs. When high-traffic attacks occur, the maximum DDoS protection capability of Tencent Cloud in the current region can be called to provide max protection with no additional elastic fees incurred, which helps reduce your daily security protection costs.

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.

Comparison of Anti-DDoS Protection Schemes

Last updated : 2020-07-07 15:56:27

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. Protected 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 15:56:28

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 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 Capability

Protection capability refers to the ability to defend against DDoS attacks. The Anti-DDoS Pro service promises to provide max protection of no less than 30 Gbps subject to the maximum DDoS protection capability of Tencent Cloud 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.

> 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.

Relevant Products

Last updated : 2020-07-07 15:56:28

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

- Cloud Virtual Machine
- Cloud Load Balancer
- Web Application Firewall
- NAT Gateway
- VPN Connection
- Global Application Acceleration Platform
- Elastic Network Interface