Anti-DDoS Pro

Product Introduction

Product Documentation

Contents

Product Introduction
Overview

Last updated：2020-04-02 10:00:55

Product Introduction

Anti-DDoS Pro is a paid anti-DDoS service for business deployed in Tencent Cloud. It works directly on Tencent Cloud services and users don't need to change their IPs. It is easy to use and requires no additional changes on your end. Anti-DDoS Pro supports both IPv6 and IPv4 addresses, and provides Single-IP instances and Multi-IP instances for your choice.
Anti-DDoS Pro offers two types of instances, single IP instances and multi-IP instances. You can choose either one as required:

- Single IP instance: provides dedicated protection for a single IP.
- Multi-IP instance: provides protection for multiple IPs.

Key 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.
DDoS protection at the application layer	Filters out CC attacks and HTTP slow attacks, and supports HTTP custom filtering such as host filtering, user-agent filtering and referer filtering.

Flexible Defense Options

Anti-DDoS Pro offers protection for a single IP or multiple IPs to meet your diverse business needs. You can flexibly change what you want to protect among CVM, CLB, WAF, and NAT Gateway, etc.

Advanced Security Policies

Anti-DDoS Pro comes with basic security policies, which can cope with common DDoS attacks by leveraging IP portrait, behavioral analysis, AI-based identification, and other protection algorithms. It also offers advanced protection policies, which can be tailored to your special needs to deal with ever-changing attack tricks.

Protection Statistics and Analysis

Anti-DDoS Pro provides real-time and detailed traffic reports and attack defense details so that you can evaluate its performance timely and accurately. Meanwhile, it can capture and download attack packets for fast troubleshooting.

Strengths

Last updated：2020-04-02 10:00:56

Anti-DDoS Pro is a paid service which can enhance DDoS protection capabilities of Tencent Cloud services such as CVM, CLB, and NAT gateway. 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.

Massive Protection Resources

Utilizing BGP protection bandwidth, Anti-DDoS Pro can provide BGP protection capability of up to 300 Gbps, meeting the high requirements for security and stability of critical business such as promotion 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 attack traffic. With the aid of a smart AI engine that continuously optimizes the algorithms, Anti-DDoS Pro is also flexible in coping with attack tricks.

Fast Speed and Reliability

With a 30-line BGP network encompassing ISPs across Mainland China, Anti-DDoS Pro features an average protection delay of less than 30 ms.

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.

Cost Optimization

Anti-DDoS Pro 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 basic protection bandwidth, it provides elastic protection to ensure the continuance 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 Pro can generate accurate and detailed defense reports. It can also capture attack packets automatically for troubleshooting.

Use Cases

Last updated：2020-04-02 10:00:56

Games

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

Finance

Anti-DDoS Pro helps the finance industry meet the compliance requirements and provide fast, secure, and reliable 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 government credibility.

Enterprises

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

Concepts

Last updated：2021-01-26 18:28:13

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

There are two types of protection bandwidth: base protection bandwidth and elastic protection bandwidth.

- Base protection bandwidth: base protection bandwidth of the Anti-DDoS Pro instance, which is on the frozen fees payment.
- Elastic protection bandwidth: the largest possible protection bandwidth of the Anti-DDoS Pro 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 bandwidth of an Anti-DDoS Pro instance will be the base protection bandwidth. If elastic protection is enabled, the maximum bandwidth will be the elastic protection bandwidth. Once the attack traffic exceeds the maximum protection bandwidth, IP blocking will be triggered.

Note：

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

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 Pro will continue to protect your IPs to ensure the continuity of your business.

Elastic protection billing

With elastic protection 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 as 50 Gbps. If the actual peak attack bandwidth of the day is 35 Gbps, you will need to pay for the elastic protection according to the price of the 30-40 Gbps tier.
For more information, please see Billing Overview.

Cleansing

If the public network traffic of the target IP exceeds the pre-set protection threshold, Tencent Cloud Anti-DDoS service will automatically cleanse the inbound public network traffic of the target IP. With the Anti-DDoS 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.

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 bandwidth you have purchased, Tencent Cloud will block the IP from all public network access. If your IP address is blocked, you can log in to the console to unblock it.

Blocking threshold

The blocking threshold of a protected IP equals the maximum protection bandwidth you have purchased. Anti-DDoS Pro offers various options. For more information, 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 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 using clouds by sharing the 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 target servers. To protect other users and ensure network stability, we have to block the target server IP.

Why isn't anti-DDoS service always free

DDoS attacks not only threaten the targets but also the entire cloud network, affecting non-attacked Tencent Cloud users as well. Also, DDoS protection incurs high costs, including cleansing costs and bandwidth costs, in which bandwidth costs the most. Bandwidth costs are calculated based on the total amount of traffic; there is no difference between costs incurred by normal traffic and attack traffic.
Therefore, Tencent Cloud provides Anti-DDoS Basic service free of charge for all users. But once the attack traffic exceeds the free quota, we will have to block the attacked IP from all public network access.
For more information on IP blocking, see About Blocking.

Relevant Products

Last updated：2020-05-06 16:25:00

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