Anti-DDoS Pro

Product Introduction

Product Documentation

Contents

Product Introduction
- Overview
- Benefits
- Scenarios
- Related Concepts

Product Introduction
Overview

Last updated：2019-09-26 18:29:26

Overview

Anti-DDoS Pro is a paid anti-DDoS service for businesses deployed on Tencent Cloud. It works directly on Tencent Cloud services and users don't need to change their IPs. After purchasing, you only need to bind the IP addresses you wish to protect to start using the service. It is easy to use and require no additional changes on your end.
Anti-DDoS Pro provides two types of Anti-DDoS Pro instances, Single IP instance and the Multi-IP instance. You can choose either one as required:

- Single IP instance: Provides the dedicated protection capability for one IP.
- Multi-IP instance: Provides the shared protection capability for multiple IPs.

Key Features

Multidimensional Protection

Protection Types	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 Network Layer	Filters 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 Application Layer	Filters CC attacks and HTTP slow attacks, and supports HTTP custom filtering such as `host` filtering, `user-agent` filtering and `referer` filtering.

Switchable Protected Objects

Anti-DDoS Pro supports single IP and also supports multiple IPs to share the protection resources, catering for various scenarios. You can switch the protected objects according to business needs. The objects include CVM, CLB, WAF, and NAT Gateway.

Flexible Advanced Security Policies

By default, Anti-DDoS Pro provides basic security policies, which are based on IP portrait, behavioral analysis, AI-based identification, and other protection algorithms, to respond to common DDoS attacks effectively. Meanwhile, it provides Anti-DDoS Advanced Protection policies. You can flexibly tailor the policies to special business to deal with the ever-changing attack methods.

Protection Statistics and Analysis

Anti-DDoS Pro provides real-time detailed traffic reports and detailed information about attack defense to help you understand the protection effect of Anti-DDoS Pro timely and accurately. Meanwhile, it supports attack forensics, which executes capture download of the attack, making analysis of exceptional issues and tracing easy and fast.

Benefits

Last updated：2019-09-26 18:29:40

Anti-DDoS Pro is a paid service to improve the DDoS protection capability of cloud products such as CVM, CLB, and NAT gateway in Tencent Cloud. It has the following strengths:

One-Click Access

With the simple configuration feature, users do not need to change IP addresses. Once purchased, it takes only a few minutes to bind it to the cloud product’s IP address for protection.

Massive Protection Resources

Exclusive support of 30-line BGP access to the protection node and up to 300Gbps protection bandwidth helps easily defend against DDoS attacks, meeting the high security and stability demands of large-scale events such as major sales promotion and launch activities.

Leading Cleaning Capability

Utilizing Tencent Cloud's powerful proprietary protective clusters and with the aid of a smart AI engine, Anti-DDoS Advanced continuously optimizes multi-dimensional algorithms such as protection policies, IP profiling, behavior pattern analysis and cookie challenges to accurately clean attacking traffic and protect customer business in real time.

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.

Cost Optimization

Anti-DDoS Pro offers a “base protection + elastic protection” combo package. This package offers elastic protection only when needed and charges by the actual attacking traffic, helping reduce your daily

protection costs.

Rich Attack Defense Report

The report provides accurate, detailed real-time statistics and automatic packet capturing that allows you to trace and analyze the attacks.

Scenarios

Last updated：2019-09-26 18:29:49

Games

DDoS attacks are particularly common in the gaming industry. Anti-DDoS Pro effectively ensures usability and continuity to guarantee a smooth experience for players. At the same time, it ensures that normal gaming continues throughout peak periods, such as the release of new games or during festivals and holidays.

Website

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

Finance

Anti-DDoS Pro helps you meet financial compliance and provide fast, secure, and reliable online transaction services to your customers.

Government Affairs

To meet the high-security standards required for government cloud deployment, Anti-DDoS Pro provides high-level security for major government conferences and activities, especially during sensitive periods. It ensures the availability of public services and thus helps increase government credibility.

Enterprises

Anti-DDoS Pro ensures that company websites are always available and helps to prevent the financial losses and negative affect on brand image resulting from DDoS attacks. In addition, you can save on investments in infrastructure, hardware, and maintenance.

Related Concepts

Last updated：2019-09-26 18:29:58

DDoS Attacks

A Distributed Denial of Service (DDoS) attack is a malicious attempt to make service unavailable by blocking the network bandwidth or overwhelming the system of the target server with a flood of Internet traffic.

Network Layer DDoS Attacks

A network layer DDoS attack attempts to make service unavailable by blocking the network bandwidth to exhaust system layer resources of the target server using a flood of Internet traffic.
Common attacks include SYN Flood, ACK Flood, UDP Flood, ICMP Flood, and DNS/NTP/SSDP/memcached attacks.

CC Attacks

A CC attack is a malicious attempt to make service unavailable by occupying application layer resources and exhausting the processing performance of the target server.
Common attacks include GET/POST Flood, Layer-4 CC, and Connection Flood based on HTTP/HTTPS.

Protection Bandwidth

The protection bandwidth consists of the base protection bandwidth and elastic protection bandwidth.

- Base protection bandwidth: Monthly prepaid Anti-DDoS service plan that provides base bandwidth protection of an Anti-DDoS Pro instance.
- Elastic protection bandwidth: The max possible protection bandwidth of the instance. The elastic protection bandwidth is billed on a postpaid daily basis.

If the elastic protection is disabled, the base protection bandwidth is the maximum bandwidth of the Anti-DDoS Pro instance. If elastic protection is enabled, the elastic protection bandwidth is the maximum bandwidth of the Anti-DDoS Pro instance. IP blocking is triggered when traffic exceeds the maximum protection bandwidth of the Anti-DDoS Pro instance.

> Elastic protection is disabled by default. Enable elastic protection after checking the related costs of this service. You can adjust the elastic protection bandwidth as required.

Function of the Elastic Protection Bandwidth

After elastic protection is enabled, if the traffic peak exceeds the purchased base protection bandwidth and remains within the elastic protection bandwidth, Tencent Cloud Anti-DDoS Pro continues protection to ensure business continuity.

Elastic Protection Fees

After elastic protection is enabled, the elastic protection will be triggered if the traffic exceeds the base protection bandwidth, and will incur cost according to the billing tier of the peak attack bandwidth. The related bill is generated on the following 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, then you need to pay elastic protection fees according to the tier of 30-40 Gbps.
For more information, please see Billing Overview.

Cleansing

If the public network traffic of the target IP exceeds the set protection threshold, Tencent Cloud Anti-DDoS service will automatically cleanse the inbound public network traffic of the target IP. The BGP routing protocol redirects the traffic of the original network path to the DDoS cleansing devices of the Anti-DDoS service. The cleansing devices identify the traffic of the IP, discard the attack traffic, then forward the clean traffic to the target IP.
In general, cleansing does not influence regular access, except for special occasions or when the cleansing policy is incorrectly configured.

Blocking

When the attack traffic exceeds the blocking threshold of the target IP, Tencent Cloud will shield access from external networks through services of the carrier to protect other users on the cloud platform. In short, when one of your IPs is attacked by Internet traffic which exceeds the maximum protection bandwidth you have purchased, Tencent Cloud will shield access from external networks to the attacked IP.

Threshold

The blocking threshold of the protection IP of the Anti-DDoS Pro instance is the maximum protection bandwidth that you have purchased. The Anti-DDoS Pro provides multiple packs. For more information,

please see Billing Overview.

Duration

The blocking period is 2 hours by default. The actual duration can be up to 24 hours, depending on the triggering times and peak attack bandwidth.
The duration of the blocking period is influenced by the following elements:

- Continuity. The blocking period extends when an attack continues. The duration of this period is calculated when the extension takes place.
- Frequency. Users that are frequently attacked are more likely to be attacked continuously. In these cases, the blocking period extends automatically.
- Traffic volume. The blocking period extends automatically to offer protection against ultra-large attack traffic volumes.

> For users with frequent blocks, Tencent Cloud reserves the right to extend the duration and reduce the threshold.

Reasons for Blocking

Tencent Cloud reduces the cost by sharing the infrastructure, with one public IP being shared among all users. When a large traffic attack occurs, the entire Tencent Cloud network may be affected, in addition to the target servers. To protect other servers and to ensure the network stability, we need to block the target server IP.

Reasons for Charging for Anti-DDoS Service

DDoS attacks have negative effects on not only the targets but also the entire cloud network, affecting other non-attacked users in Tencent Cloud as well. Moreover, building the anti-DDoS system costs high, including the cleansing cost and the bandwidth cost. Specifically, the largest expense is bandwidth and it is calculated based on the total traffic. No difference exists between normal traffic and attack traffic in terms of the bandwidth cost.
Therefore, although Tencent Cloud can afford limited free DDoS Basic service for all users, we have to block inbound public network traffic of the attacked servers when the attack traffic exceeds the free quota.
For more information, please see Block FAQs.