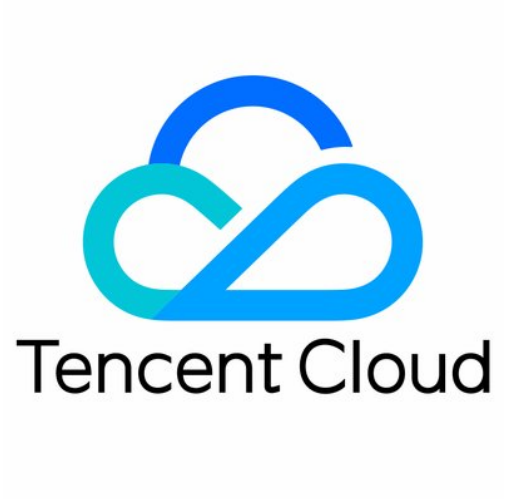
TencentCloud EdgeOne

Product Introduction

Product Documentation



Contents

Product Introduction

Overview

Last updated：2022-08-26 11:45:48

EdgeOne Overview

Tencent Cloud EdgeOne provides an acceleration and security solution based on Tencent edge nodes to safeguard diverse industries such as ecommerce, retail, finance service, content and news, and gaming and improve their user experience.

- Acceleration: Edge nodes are closer to users, which greatly reduce the data access latency, avoid data transfer jitters, and guarantee the stability and effectiveness during the transfer of massive amounts of data. In addition, EdgeOne has many acceleration features, including dynamic/static data acceleration, cross-border acceleration, and smart route optimization, to efficiently support latency-sensitive businesses.
- Security: Security protection services such as WAF and Anti-DDoS are provided. Nodes identify and block various layer-3/4/7 attack requests, cleanse DDoS attack traffic, and use the smart AI engine and bot policy engine to analyze the behaviors of web, bot, and CC attacks and update attack blocking policies. This helps prevent malicious requests from reaching your origin servers and guarantee a smooth and stable access to your business.

Features

DNS

Domain management

It supports DNS resolution and unified management for domains of any type and can add DNS records.

Automatic DNS record import

After a domain name is added, all host records are automatically imported under the domain name.

Real-time synchronization

DNS record modifications can be synchronized to the DNS server within seconds.

Exception alarms

Alarming is provided to detect exceptional operations during DNS record modification, which helps ensure domain security.

Record type

The following record types are supported: A, AAAA, MX, CNAME, TXT, NS, SRV, URL, and Framed URL.

Cloud resource binding

Association with Tencent Cloud resources allows resolution to CVM and CLB.

Others

Features such as DNS statistics, domain lock, and CNAME acceleration are also offered.

DDoS mitigation

Tencent Cloud Anti-DDoS is a comprehensive, efficient, and professional service for DDoS attack prevention, providing enterprises and organizations with various solutions. Leveraging abundant, quality DDoS protection resources and with the aid of ever-improving cleansing algorithms, Tencent Cloud Anti-DDoS brings security and safety to user business.

Web protection

Based on Tencent's massive web attack samples, EdgeOne supports identifying good access requests from bad ones and protecting your origin server against web attacks including SQL injection, XSS attacks and local file inclusion in real time. With the self-developed AI engine incorporating Tencent's billion-level threat intelligence, a more accurate and effective identification and blocking mechanism can be implemented.

Bot protection

It integrates the Tencent Cloud bot program management feature and has a bot behavior library covering many crawler types such as ads, screencapturing tools, search engines, site monitoring, and link query. Its unique AI technology analyzes and builds models for all user request behaviors to intelligently identify abnormal traffic. In addition, it supports custom session protection policies.

Acceleration

EdgeOne uses a combination of edge nodes and regional centers to enhance acceleration via intelligent cross-node routing and targeted path optimization. This service effectively resolves cross-border latency issues and delivers an improved global user experience.

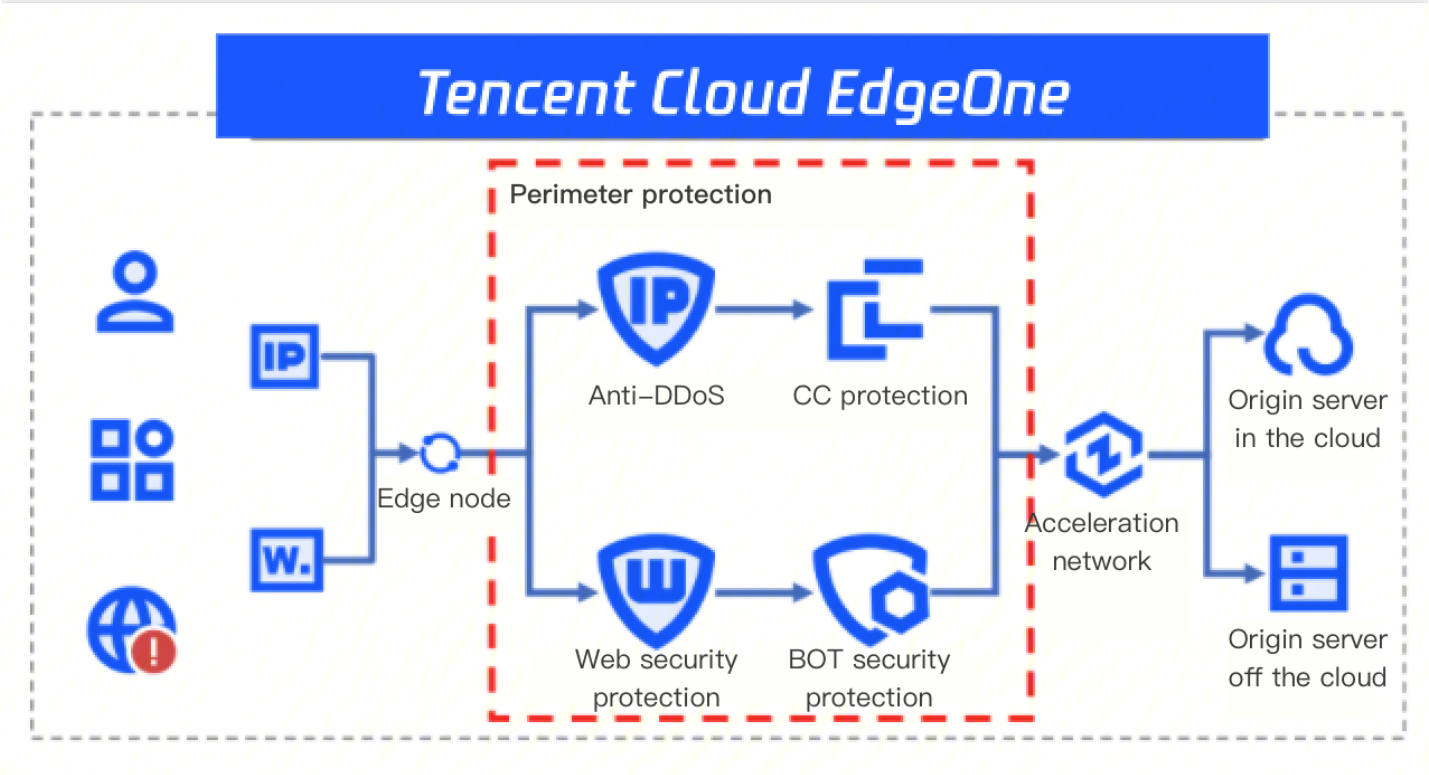
Strengths

Last updated：2022-08-26 11:45:48

Integrated Platform

EdgeOne is an integrated edge security and acceleration platform offering 3D protection from layers 3 to 7.

- Anti-DDoS: It detects and cleanses DDoS attack traffic and guarantees the business availability based on diverse measures, for example, IP blocklist/allowlist and port blocking policies.
- Rate limit: It uses mechanisms such as HTTP field match and access frequency monitoring to effectively cleanse CC attack traffic.
- Web security protection: It effectively prevents top 10 OWASP web ricks like SQL injection and cross-site scripting (XSS) and quickly identifies and blocks bot behaviors.
- API security protection: It guarantees API access security based on a secure and reliable access authentication mechanism.



Web or Bot Attack Protection

Bot recognition and protection

Based on the characteristics of protocols, IP intelligence, and custom sessions, it can accurately recognize and block various bots. In addition, it leverages data and threat intelligence to comprehensively analyze and learn crawler behaviors to build a crawler recognition model, which effectively solves problems of malicious crawler passthrough and benign crawler kill.

Web attack protection

It has an extensive attack characteristic library covering common OWASP security threats to effectively block web business security problems, including web attacks, intrusion vulnerability exploits, trojans, and backdoors. It also prevents zero-day vulnerabilities and adopts syntax analysis and AI smart detection engine to further improve the detection accuracy and reduce false positives.

Around-the-clock active monitoring and response

Tencent Security team monitors your business security 24/7 to discover and respond to problems actively, greatly improving the responsiveness.

Smart Protection

A smarter automatic protection service is developed based on multiple years of experience in attack backtracking.

Smart captcha

Based on many years of experience in CC attack prevention and research on cutting-edge trends in CC attack defense, the CC attack prevention system forms an effective client marking and identification solution. It continuously tracks clients to effectively solve problems of attack passthrough and normal user traffic kill in intense attack defense scenarios.

Automatic API recognition

An accurate automatic API recognition model is set up based on characteristic comparison in multiple dimensions such as UA, root directory, and CGI through in-depth analysis of big data. It can automatically recognize APIs to avoid mistakenly killing APIs, greatly improving the API protection capabilities.

Attack backtracking

As an important component in response during and after security events, attack backtracking analyzes and collects evidence from the attack traffic to reveal the attack means used by attackers and get important information like attack source IPs and attack methods. This helps with subsequent protection policy adjustment and attack source tracing to avoid secondary attacks.

The system captures and analyzes the exception/attack event packets to extract the attack sources and packets as key evidence for attack backtracking. In addition, EdgeOne offers an all-around monitoring page to display a wide variety of information, including attack types, sources, ports, and traffic, which serves as the basis for you to adjust protection policies.

Accurate Attack Source Positioning

The fingerprint recognition solution pinpoints attack sources to prevent your business from being affected.

Protocol flood attack protection

Attackers randomly forge large amounts of traffic over seldom used protocols. The system uses basic protection policies such as protocol blocking, regional traffic blocking, blocklist/allowlist, and network ACL, as well as the proprietary fingerprint recognition solution to perform in-depth recognition and match for diverse protocol characteristic fields, cleanse the flood attack traffic over all types of protocol, and thus prevent your business from being affected.

Accurate attack source positioning through fingerprint algorithm

Based on passive analysis of massive amounts of traffic and characteristics of multiple parameters such as TCP option, timestamp, and TTL, EdgeOne automatically determines the client operating system, application type, and device UID to accurately recognize attack sources. This helps effectively tackle different industry challenges like CC attack protection passthrough.

Use Cases

Last updated：2022-06-30 16:07:06

Gaming

Use Case	Challenge/Need	Solution/Applicable Feature
Login server	• Low-latency access • High reliability • Layer-4/7 origin-pull	• Anti-DDoS • Web protection • Network acceleration
Battle server	• Low-latency access • Protection of high numbers of IP addresses	• Anti-DDoS • Network acceleration • BGP and IP broadcasting
Game update	• DNS scheduling • Cache acceleration	• Smart DNS scheduling • Static hosting • Global cache

Video

Use Case	Challenge/Need	Solution/Applicable Feature
Video on demand	• High-reliability access • Smart prefetch • Smooth playback and low-latency access	• Anti-DDoS • Web protection • Network acceleration • Nearby access • URL prefetch
Video live streaming	• Smooth playback • Real-time interaction • High-speed origin-pull and low-latency access	• Anti-DDoS • Web protection • Network acceleration • Nearby access
Video upload	• Efficient upload • Linkage origin-pull	• Network acceleration • Nearby access
Video download	• High-reliability access • Smart prefetch • High-speed download	• Network acceleration • Nearby access • URL prefetch

Ecommerce and Retail

Use Case	Challenge/Need	Solution/Applicable Feature
Ecommerce website	• Smooth access • High reliability • Attack prevention • Tampering prevention • Anti-cheating	• Nearby access • Network acceleration • Static acceleration • Dynamic acceleration • URL prefetch • Anti-DDoS • Web protection

Finance

Use Case	Challenge/Need	Solution/Applicable Feature
Bank website/securities trading	• Smooth access • High reliability and attack prevention • Tampering prevention • Leakage prevention	• Nearby access • Network acceleration • Static acceleration • Dynamic acceleration • URL prefetch • Anti-DDoS • Web protection
Interbank clearing system	• Fast data transfer • High reliability • Data origin-pull	• Network acceleration • Anti-DDoS • Web protection

Logistics and Traditional Business

Use Case	Challenge/Need	Solution/Applicable Feature
Logistics/Traditional businesses	• Smooth access • High reliability • Attack prevention • Tampering prevention • Leakage prevention	• Nearby access • Network acceleration • Static acceleration • Dynamic acceleration • Anti-DDoS • Web protection