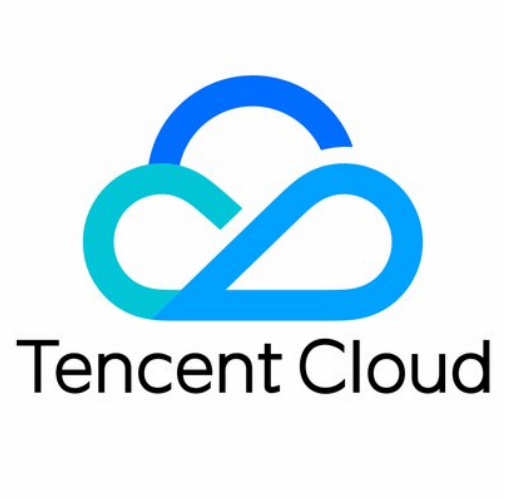
Tencent Cloud EdgeOne

Release Notes and Announcements

Product Documentation



Contents

Release Notes and Announcements

Release Notes

Last updated：2024-01-02 10:06:34

November 2023

Update	Description	Time	Documentation
Prepaid plans support self-service refunds	For eligible prepaid plans, user self-service refunds are supported and the user refund process is simplified.	2023-11	Refund Policy
The personal edition supports richer security protection capabilities	Open vulnerability protection rule set, web protection > rate limiting, Web attack log, Web security analysis and other security protection-related capabilities to the personal edition plan.	2023-11	Comparison of EdgeOne Plans

October 2023

Update	Description	Time	Documentation
Security protection actions support dimension upgrade	Rate limiting and Bot related rules, supporting redirection and returning of custom pages.	2023-10	Action
Custom error page	Addition of entrance to custom error page.	2023-10	-
Support for collecting source IP list	Support for collecting EdgeOne origin-pull IP list through a link.	2023-10	Collect EdgeOne origin-pull node IP

September 2023

Update	Description	Time	Documentation

Display optimization of the same name sites	In the site management list page, the display mode for sites with same name has been optimized. Multiple sites under the same name are consolidated under the same domain name, making it convenient for user searches. It also supports filtering by the type of access mode, service area, and effective status.	2023-09	-
Integration of SSL certificates management into domain name services	Within domain name services, HTTPS certificates can be selected directly for domains, and batch deployment of certificates is also supported.	2023-09	Configuring Own Certificate for A Domain Name
Prepaid plan supports unbinding sites	For prepaid plans, unbinding from the site by deletion is supported. Once deleted, other sites can be reselected for access within the same plan.	2023-09	-
Personal edition enables real-time logs capabilities	The personal edition plan supports real-time logs, satisfying personal edition plan users' demand for access log analysis.	2023-09	Comparison of EdgeOne Plans

August 2023

Update	Description	Time	Documentation
Edge functions provide default access domain	Support for providing a default access domain for edge functions, which can be triggered by the default access domain even without site access.	2023-08	-
Web Security Analysis supports more analysis dimensions	Web Security Analysis supports Request path, JA3 fingerprint, Request method, and Request ID as statistical dimensions.	2023-08	Web Security Analysis
L4 proxy supports port translation mapping	L4 proxy ports are no longer limited to keeping the forwarding port and origin port consistent, and can be configured as long as the port segment length is consistent.	2023-08	Create L4 proxy instances
Usage capping policy released	Support for configuring usage capping policies, which will trigger service suspension when the limit is reached, avoiding abnormal usage and high bill risks.	2023-08	-
Automatic preheating	Combining Tencent Cloud COS+SCF+EdgeOne can automatically preheat resources to EdgeOne edge nodes	2023-08	-

capability released	after uploading to COS.		
Dynamic packaging capability released	Combining Tencent Cloud COS+SCF+EdgeOne can automatically trigger cloud functions to process APK base package with different information insertion after uploading to COS.	2023-08	-

July 2023

Update	Description	Time	Documentation
Rule engine supports variables	New ability to obtain variables, allowing users to dynamically extract and process data information within request in the rule engine.	2023-07	Variables
Self-service debugging capability released	Provide self-service debugging capability to help users quickly obtain node cache TTL, whether resources are cacheable, Cache Key, etc., for easy business configuration debugging.	2023-07	Self-service debugging
Cache Purge supports selecting deletion method	In Cache Purge, you can support using "marked expired" and "directly delete" two methods according to different cache purge types.	2023-07	Cache Purge

June 2023

Update	Description	Time	Documentation
Enterprise plan upgrade	Plan mode upgrade, supporting more flexible value-added service purchase capabilities.	2023-06	Billing Overview (New)
New standalone DDoS protection capability	For Enterprise plan users, if they have higher requirements for DDoS protection, they can choose to purchase, and provide a standalone DDoS protection platform.	2023-06	Exclusive DDoS protection related fees (Pay-as-you-go)
Web Protection custom rule supports	Support request content matching method, adapting to more flexible security scenarios.	2023-06	-

content matching			
Origin-pull supports any private object storage bucket compatible with S3	Object storage origin now supports any third-party private read object storage bucket that uses AWS Signature v4 & v2 compatible authentication protocol.	2023-06	-
Support for deploying SM2 encryption certificates	By uploading the SM2 encryption certificate to the SSL console, the certificate can be deployed to the specified domain in EdgeOne, with up to one SM2 encryption certificate supported per domain.	2023-06	-

May 2023

Update	Description	Time	Documentation
Rewrite access URL supports regex matching	Support separate configuration of request protocol, hostname, and path after redirect, with path supporting exact match and regex match.	2023-05	Access URL Redirection
IP grouping supports batch import	Support batch configuration of security protection IPs and IP segments by importing.	2023-05	-
Web Protection Managed rules support auto-renewal	When there are updates to 0-day vulnerability rules, automatically update rule configurations according to user configuration and protection level.	2023-05	-

April 2023

Update	Description	Time	Documentation
Bot management supports active detection	Through Cookie verification and Client behavior verification, detect and identify potential malicious bot access, meeting customer requirements for accurate interception of malicious traffic in complex network environments.	2023-04	-

Web Protection Exception rules support skipping CC protection	Solves the problem of misjudgment of valid high-concurrent traffic in specific scenarios, ensuring business continuity and reliability.	2023-04	-
API supports IP group configuration	Support for configuring IP groups through API, closely linked with security policy, quickly adjusting IP groups according to security policy in real-time, reducing operation and maintenance costs.	2023-04	Modify security IP grouping
QUIC SDK released	QUIC SDK officially released to the public, providing developers with simple and easy-to-use API interfaces for quick integration of QUIC protocol into developer Apps.	2023-04	QUIC SDK
L4 proxy acceleration capability optimization	Support configuration of port segments, removal of port quantity limit, and support for SPP protocol.	2023-04	-

March 2023

Update	Description	Time	Documentation
Transmitting analysis results of Bot management to the origin server	Supports transmitting the analysis results of Bot management to the origin server through the request header, providing the origin server with multi-dimensional security analysis results.	2023-03	-
Post verification for site ownership	After connecting the site to EdgeOne, you can verify the site ownership through the third-level domain.	2023-03	-
Metrics for origin-pull	Metrics related to origin-pull are added, which help users analyze the origin-pull performance.	2023-03	-
SSL/TLS security level selection	You can configure the protocol version and Cipher suite that are allowed to use when a client shakes hands with an edge server TLS as needed, and also disable insecure encryption suites.	2023-03	Configuring SSL/TLS Security Level

February 2023

Update	Description	Time	Documentation
Optimized domain name service experience	Completed the reconstruction of domain name service module. Fixed the problem of configuration splitting for service connection. All types of origins can be configured and recommended configurations specific to a scenario are added.	2023-02	-
WAF protection upgrade	WAF custom protection rules supports extracting the client IP in X-Forwarded-For header for conditional matching, and frequency data can be collected based on the actual client IP.	2023-02	-
Custom rules of Bot management	The matching conditions and execution actions of the rules can be customized, and obfuscated confrontation and combined disposal are added.	2023-02	-

January 2023

Update	Description	Time	Documentation
`X-Forward-For` request header	The origin-pull request carries the `X-Forward-For` header by default to indicate the IP addresses of the client and proxies.	2023-01	-
`Vary` header	The response from the origin carries the `Vary` header to indicate the data to be cached. This header makes caching more flexible in multiple scenarios.	2023-01	-
gRPC protocols	EdgeOne supports gRPC protocols, including the Simple RPC and Server-side streaming RPC protocols.	2023-01	gRPC
Plan switchover	You can easily switch between the Enterprise plan and Standard plan in pay-as-you-go billing mode.	2023-01	-

December 2022

Update	Description	Time	Documentation
Enhancement of custom fields in real-time logs	You can add custom HTTP request headers, HTTP response headers, and cookie headers in real-time logs to be pushed.	2022-12	-
Release of the image resize feature	The origin stores only the original images. The size and format of an image can be changed as needed on EdgeOne nodes.	2022-12	Resizing and Converting Images
Enhancement of Web protection rules	More rule matching methods, such as regular matching, are supported.	2022-12	-

November 2022

Update	Description	Time	Documentation
IP information query	Query whether an IP is used by an EdgeOne node and view its geolocation and ISP information.	2022-11	-
Certificate Management 2.0	New **SSL Certificate** page. Support configuring certificates for multiple domain names at a time. Provide free certificates for sites connected via CNAME.	2022-11	-
Optimized navigation	The navigation structure is optimized so that the statistics and settings of each site are displayed on the details page of the site.	2022-11	-
Webhooks for security alarm pushing	Push Web monitoring alerts to Webhook addresses. The event push formats of WeCom, Lark, and DingTalk are supported.	2022-11	-

Security log filters	The policy optimization process is streamlined. You can quickly configure hit rules to filter logs, and can create protection exception rules with a few clicks.	2022-11	-

October 2022

Update	Description	Time	Documentation
Traffic scheduling management	Set up custom traffic scheduling policies to control traffic between the origin and service providers to implement smooth canary migration of traffic and flexible allocation of services	2022-10	Traffic Scheduling Management
Release of Rule Engine 2.0	Support more types of nested conditional expressions and improve cache and origin-pull configuration capabilities. In addition, rich rule management features, such as quick rule copy and automatic generation of dynamic rule navigation, are provided.	2022-10	Rule Engine
Support for Terraform	EdgeOne supports the Terraform resource orchestration tool to make infrastructures codified and versioned, simplify configuration change and management, and effectively improve the Ops efficiency.	2022-10	Terraform
Support for security policy templates	Multiple sites and domain names can be quickly reused, and security policy configurations are adjusted accordingly, greatly simplifying the configuration process.	2022-10	For more information, contact Us
Support for cache purge based on `Cache-Tag`	Caches can be purged based on the tag value of the `Cache-Tag` response header in the HTTP response packet. This feature is only applicable to the Enterprise plan.	2022-10	Cache Purge

September 2022

Update	Description	Time	Documentation

Alias domain name	For business scenarios with many domain names and the same configuration, such as SaaS site construction, only one target domain name needs to be connected, and all other bound domain aliases can enjoy the EdgeOne acceleration and security services.	2022-09	For more information, contact Us
Release of Edge Functions	Edge Functions is a serverless code execution environment provided by Tencent Cloud for enterprises and developers. Custom requirements can be met simply by writing business function code and setting trigger rules for deployment to edge nodes.	2022-09	For more information, contact Us
File-based site ownership verification	A file verification method is provided, which allows for adding specified files on the origin server of the domain name to verify their ownership. Currently, EdgeOne supports DNS txt verification and file verification.	2022-09	Verifying Site Ownership

August 2022

Update	Description	Time	Documentation
Security whitelist policies	Managed web protection rules and bot management exception rules are supported, so you can configure business allowlists to avoid false positives.	2022-08	Web Protection
Support for Chinese Mainland regions	EdgeOne is available in Chinese mainland regions.	2022-08	Overview

July 2022

Update	Description	Time	Documentation
Release of the Standard and	The Standard and Enterprise plans are launched for you to purchase based on your business needs.	2022-07	Billing Overview

Enterprise plans			
Support for IPv6 access and protection	IPv6 is supported comprehensively for IPv6 access and layer-4/7 security protection.	2022-07	CNAME Access
Release of RUM	Real User Monitoring (RUM) is a one-stop frontend monitoring solution that supports page performance analysis, access analysis, and resource speed test for real users.	2022-07	Real User Monitoring
More match conditions supported by the rule engine	Match conditions **URL Full** and **Filename** are added to the rule engine to support more custom configuration scenarios.	2022-07	Rule Engine

June 2022

Update	Description	Time	Documentation
Support for tag management	Tags are supported for you to use different standards to easily manage cloud resources with the same attributes by category.	2022-06	Tags
Origin health check	You can customize the origin health check mechanism to monitor the origin health status.	2022-06	Origin Health Check
Support for smart bot analysis and client filtering for security protection	IP profiling-based bot management rules (client reputation) are added. Requests can be matched with categories that are configured with different processing methods. Smart client filtering is supported to accurately block high-risk clients	2022-06	Bot Management
Integration of data statistics with Tencent Cloud Observability Platform	Data statistics are connected to Cloud Monitor, so you can configure custom monitoring alarms.	2022-06	Creating Alarm Policy

May 2022

Update	Description	Time	Documentation
Enhancement of site acceleration and rule engine capabilities	The async cache purge feature and capabilities such as Transport Layer Security (TLS) versioning, Online Certificate Status Protocol (OCSP) stapling, maximum upload size, Brotli compression, and custom cache key are supported to flexibly meet diversified business needs.	2022-05	Rule Engine
Security enhancement	JavaScript challenge, dynamic verification code, AI engine-based SQL injection and XSS attack identification, and dynamic DDoS protection policies based on business baseline analysis are added to make protection more fine-grained and accurate and make deployment easier.	2022-05	DDoS Mitigation
Data analysis enhancement	Traffic analysis: Bandwidth data can be queried and filtered by country/region to meet the requirements in more query scenarios. Cache analysis: Cache analysis is supported to analyze data such as cache traffic, origin-pull traffic, and top URLs in real time.	2022-05	Traffic Analysis
L4 proxy support for log download and real-time log push	The L4 proxy provides log download capabilities and supports real-time log push.	2022-05	Real-time Logs

April 2022

Update	Description	Time	Documentation
Support for more acceleration	Capabilities such as video dragging, Range GETs, custom origin domain, Cloud Object Storage (COS) origin, and token authentication are supported.	2022-04	Origin Group List Rule Engine

and origin-pull capabilities			
L4 proxy support for Anycast IP addresses	The L4 proxy can be connected through an anycast IP address, making the connection easier and more secure.	2022-04	L4 Proxy
DDoS protection with dedicated resources	You can enable protection enhancement to use dedicated resources to improve protection capabilities. You can also subscribe to DDoS attack alarms.	2022-04	DDoS Mitigation
Support for more web protection methods	Various web protection methods are added, including IP blocking, redirection, returning to the specified page, and returning the specified error code.	2022-04	Web Protection
Basic bot protection capabilities	Bot management rules and custom rules are provided to implement basic bot management features.	2022-04	Bot Management

March 2022

Update	Description	Time	Documentation
Release of EdgeOne	Tencent Cloud EdgeOne provides acceleration and security solutions in regions outside the Chinese mainland based on Tencent edge computing nodes to safeguard diverse industries such as e-commerce, retail, finance service, content and news, and gaming and improve their user experience.	2022-03	Overview

Security Announcement
Protection against DDoS attacks targeting HTTP/2 protocol vulnerabilities

Last updated：2023-10-13 12:40:16

Overview

Starting from September 2023, EdgeOne has noticed a new type of HTTP DDoS attack that exploits a new vulnerability in the HTTP/2 protocol. This vulnerability (CVE-2023-44487) poses a security threat to Web services and applications that use the HTTP/2 protocol to provide shared services. EdgeOne's reverse proxy architecture and security policy can effectively isolate and mitigate the risks posed by such DDoS attacks.

The DDoS attack exploiting this vulnerability is also known as the "HTTP/2 Rapid Reset Attack" and targets flawed HTTP/2 applications through the HTTP/2 protocol mechanism. EdgeOne's reverse proxy architecture and implementation of HTTP/2 have provided corresponding isolation and mitigation mechanisms for this feature of the HTTP/2 protocol.

Based on known information and vulnerability behavior, the attack form exploiting this vulnerability is a DDoS attack, affecting the availability of HTTP/2 application services; a single attack exploiting this vulnerability will not cause business data leakage. There is currently no evidence to suggest that any customer information has been leaked due to this vulnerability.

Attack Details

Attackers can exploit this HTTP/2 protocol vulnerability to launch DDoS attacks on HTTP/2 application services. By first sending a large number of HEADERS frames and then a large number of RST_STREAM frames, attackers can generate a large amount of traffic to HTTP/2 application services in a short period of time. By exploiting the connection mechanism of HTTP/2 (for details, please refer to RFC9113: HTTP/2 Stream Lifecycle and State Transition Mechanism), attackers can send a large number of HEADERS and RST_STREAM frames within the same TCP connection, causing high CPU load and exhausting service resources for flawed HTTP/2 application services.

Protection against CVE-2023-44487

This attack is a DDoS attack targeting the application layer protocol (L7 protocol). EdgeOne has optimized and strengthened its proxy architecture and security policy for application layer protocols, protecting Web application services using EdgeOne. EdgeOne's reverse proxy architecture and HTTP/2 implementation can effectively isolate the business availability risks caused by attacks exploiting this vulnerability. At the same time, EdgeOne will continue to monitor new security threats and evaluate security policies, continuously optimizing protection efficiency.

We recommend that you:
Check your origin and HTTP/2 service architecture, update security vulnerability patches in a timely manner, and mitigate the risk of DDoS attacks exploiting this vulnerability.
Configure security protection policies, enable and configure Rate Limiting rule. EdgeOne's rate limiting can provide effective protection against application layer security threats, including HTTP DDoS attacks.
If you cannot update security vulnerability patches for your origin, we recommend enabling Origin protection and allowing only origin-pull requests from EdgeOne to avoid attackers launching attacks by directly accessing the origin server.

Using EdgeOne's HTTP Security Protection

To protect your Web services, EdgeOne offers a variety of HTTP security features (Refer to Web Protection) depending on your subscribed service specs. You can refer to the following methods to reduce the risk of application layer DDoS attacks.

Mitigate high-frequency DDoS attacks that cause a decline in origin availability. You can enable CC attack defense rules to dynamically identify and mitigate high-risk HTTP DDoS attacks.
Block IPs or CIDR subnets with a history of malicious access. You can configure Custom rule to block specified IP list or subnet list.
Limit the allowed access service area. You can configure Custom rule to block access from outside the specified business area.
Control resource consumption. You can configure rate limiting rules to mitigate the resource consumption caused by high-frequency access. We suggest limiting the request rate for global or non-specified business areas to control resource consumption.
Note:
Enterprise users can contact us to evaluate customized protection strategies, including advanced rate limiting rules based on headers and JA3 fingerprint[1], to specifically mitigate application layer DDoS attacks and service abuse risks.
Note 1: The rate limiting option based on JA3 fingerprint requires subscribing to Bot management service.
Block high-risk bot access behavior. You can enable and configure Bot Intelligent analysis, which dynamically identifies bot behavior and tags requests, helping you identify and block malicious bot access.

Block access from high-risk clients. You can enable and configure Client reputation, which helps you identify and block high-risk clients through continuously updated IP threat intelligence.

Announcements

【Tencent Cloud EdgeOne】Cloud API Change Notification

Last updated：2024-04-15 10:48:39

Due to CAM Authentication requirements, Tencent Cloud EdgeOne will change all cloud API parameters involving site ID (ZoneId/ZoneIds) from optional to mandatory after May 30, 2024. It is suggested that you adjust the API input parameters before this date to avoid API call errors. If you have already input the parameter or have not called the above API, this adjustment will not affect you.

The specific impact is as follows:
Taking the DescribePurgeTasks API as an example, the current ZoneId parameter of this API is optional, and you need to input the site to be queried when calling the API.

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params. The value used for this API: DescribePurgeTa
Version	Yes	String	Common Params. The value used for this API: 2022-09-01.
Region	No	String	Common Params. This parameter is not required.
ZoneId	No	String	ZoneId. The parameter is required.

The list of specific APIs involved is as follows:
DescribePrefetchTasks
DescribePurgeTasks
DescribeDefaultCertificates
DescribeApplicationProxies
DescribeOriginProtection
DescribeOriginGroup
DescribeTimingL4Data
DownloadL7Logs
DownloadL4Logs

DescribeTimingL7AnalysisData
DescribeTopL7CacheData
DescribeTopL7AnalysisData
DescribeOverviewL7Data
DescribeTimingL7CacheData
DescribeDDoSAttackEvent
DescribeDDoSAttackTopData
DescribeDDoSAttackData