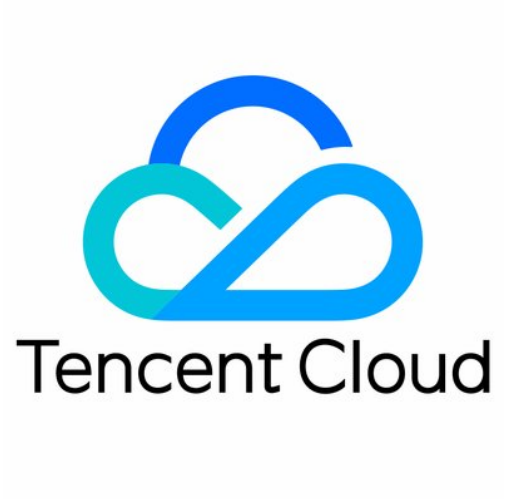
Tencent Cloud EdgeOne

Data Analysis&Log Service

Product Documentation



Contents

Data Analysis&Log Service
Log Service
Real-time Logs
Overview

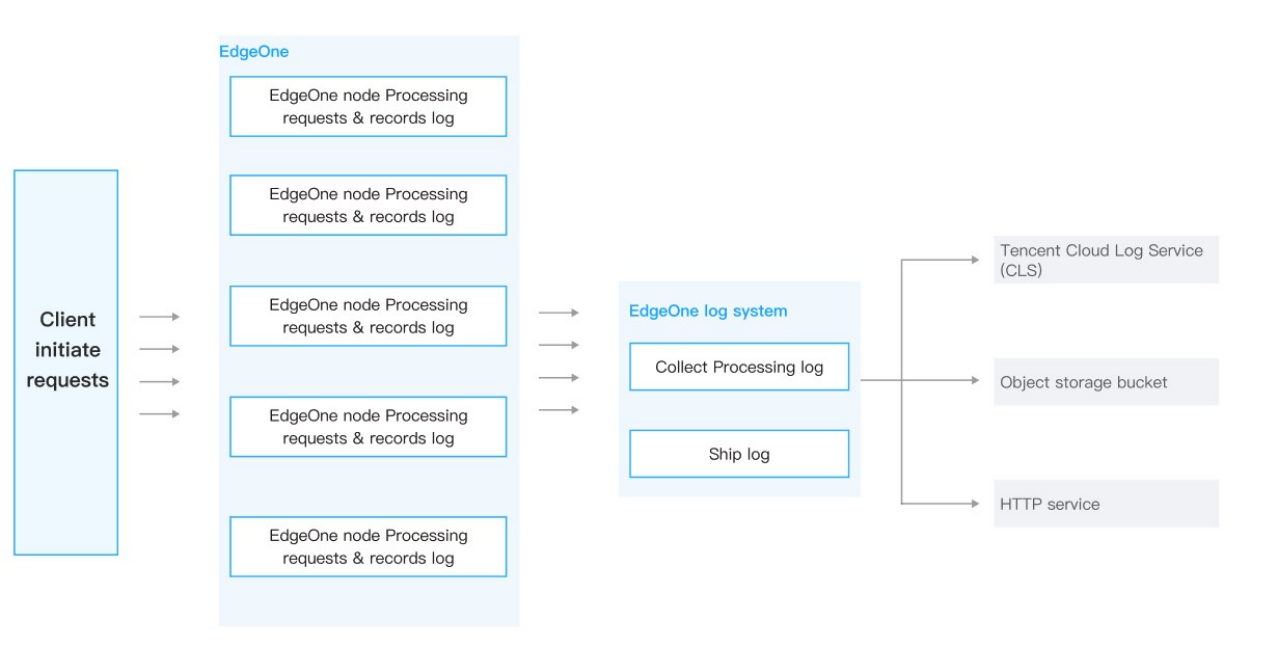
Last updated：2023-08-16 16:08:04

Function Overview

After adding your site to EdgeOne Service, EdgeOne provides you with a wealth of pre-built reports to help you monitor and analyze the operation of your business, including traffic analysis, cache analysis, L4 proxy, security analysis, etc. However, in data analysis, you may have more personalized data analysis demands, such as the following data analysis scenarios:

Scenario	Scenario Demands
Deep Data Analysis	Need to specify one or more conditions to find logs that meet the conditions. For example: By specifying the client IP, query the access statistics (access URL, number of accesses, etc.) within a specified time range. Refine the analysis of status code distribution by filtering status codes, time, and URLs. By filtering logs with the action set to "observe", summarize the request header content and other request features carried, and adjust the security policy.
Monitoring Service Metrics	Analyze the quality of EdgeOne Service and the access efficiency of users to detect exceptions in a timely manner. Access efficiency includes overall response time, download speed, origin-pull response time, etc.
Identifying Unauthorized Access	Identify client IPs with behaviors such as unauthorized access by analyzing traffic anomalies, access patterns, and access frequency.
Unified Monitoring of Data from Multiple Cloud Vendors	Build your own data dashboard to monitor application data from multiple cloud vendors.
Storing Logs	User-related access logs need to be retained for 30 days or longer.

For the above scenario demands, EdgeOne real-time logging provides the ability to collect and ship logs in real-time, allowing you to ship your logs to Tencent Cloud Log Service (CLS) or your self-built data center, helping you to implement flexible log data retrieval and analysis on your own. Currently, EdgeOne supports shipping site logs, L4 proxy logs, and security service logs to the following destinations:
Tencent Cloud Log Service (CLS): Ship logs to the one-stop log processing service (CLS) provided by Tencent Cloud for further log analysis on CLS.
Object Storage: Storage buckets compatible with AWS Signature V4 authentication method.
HTTP Service (POST): Ship logs to the specified backend server via HTTP POST requests.



Note：
1. In general, the log delivery delay is within 2-5 minutes. To ensure the real-time performance of log delivery, EdgeOne ships logs in fixed log quantities or fixed time periods as a batch to the corresponding destinations.
2. When shipping real-time logs to CLS service, traffic, storage, and other fees may be generated in CLS, and the related fees are charged by CLS product. For details, please view the Log Service Billing Overview.

Billing and Quota Description

Billing Description: Real-time log shipping is a value-added service, and the billing method is based on the number of logs shipped. For details, please view the VAU Fee（Pay-as-You-Go）.
Quota Description: The number of real-time log shipping tasks varies depending on the plan, and the specific quota can be viewed in the Comparison of EdgeOne Plans.

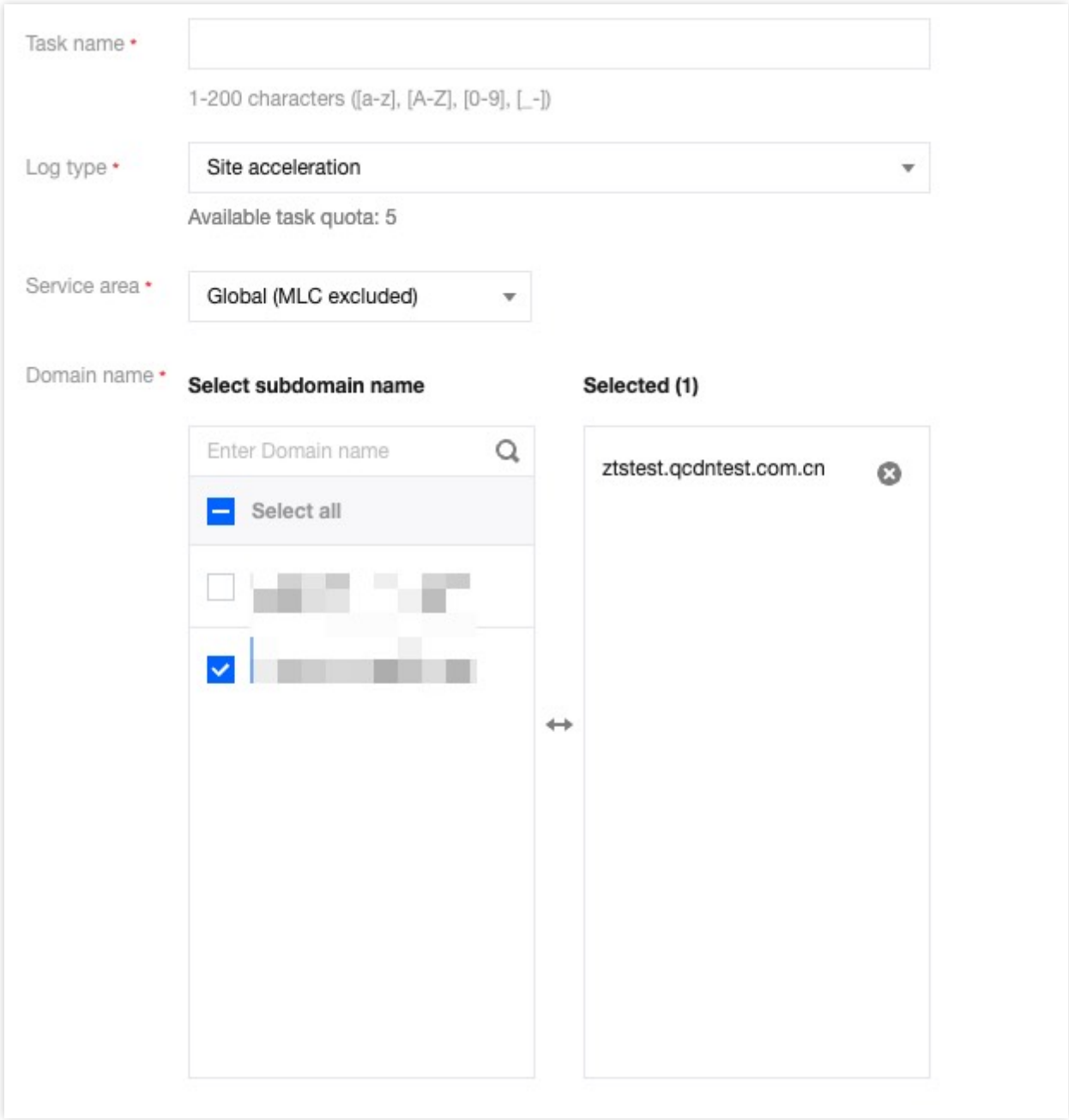
Ship Real-time logs

Last updated：2024-01-02 10:25:33

This document will guide you on how to push logs to a specified service.

Step 1: Select the log source

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the site list, click the target site to enter the site details page.
2. On the site details page, click **Log Service** > **Real-time logs**.
3. On the real-time log page, click **Create shipping Task**.
4. On the Select Log Source page, choose the log source information you want to push, configure the related parameters, and click **Next**.



Log Type: You can choose from site acceleration log, L4 proxy log, rate limiting log, CC attack defense log, Web attack defense log, custom rule log, and Bot management log;

Service Area: Select the log area you want to push. EdgeOne real-time log push tasks can push logs from the "Chinese mainland" or the "Global(MLC excluded)", but cannot directly push logs from the "Global". If you need to push logs from the "Global", please create two push tasks, one for the "Chinese mainland" and another for the "Global(MLC excluded)".

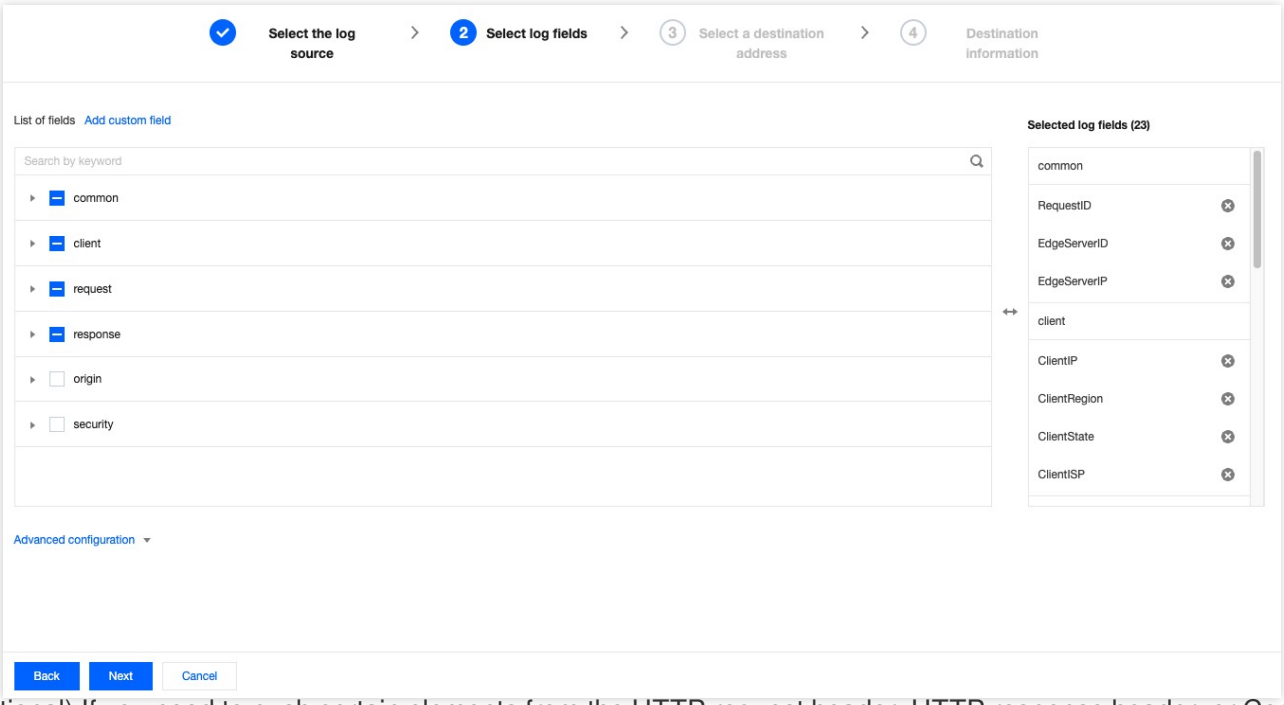
Domain: Select the subdomain or L4 instance for which you want to push logs. The same log does not support multiple push tasks, i.e., logs from subdomains/L4 proxy instances in the same region can only support one push task. For example, if the "Chinese mainland" site acceleration log of `www.example.com` has been configured with push task A, push task B cannot select `www.example.com` .

Step 2: Select log fields

1. In the Select Log Fields section, configure the fields you want to push. You can select them by checking the boxes in the field list; for a description of the related fields, please refer to the real-time log field description.

Note：

Currently, only **site acceleration logs** and **L4 proxy logs** support custom selection of logs to be pushed.

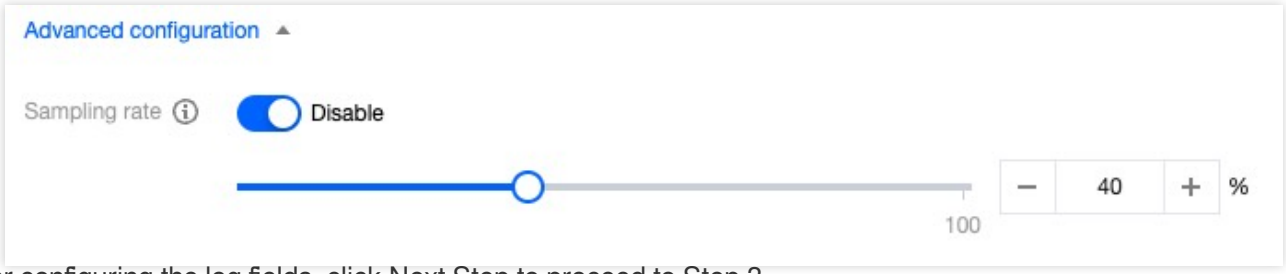


2. (Optional) If you need to push certain elements from the HTTP request header, HTTP response header, or Cookie for analysis, you can click Add Custom Field to configure the HTTP request header, HTTP response header, or Cookie name you want to push. You can record this information accurately in the log in key-value pair format. For example, the information corresponding to the `Accept-Language` header can be directly obtained from the `Accept-Language` field in the log.

Note：

1. Fields are case-sensitive by default, so they need to match the original fields exactly;
2. Currently, only **site acceleration logs** support adding custom fields.

3. (Optional) If you have a large volume of logs and only need to monitor and analyze the real-time log push data without requiring all log data, you can click Advanced Configuration to configure the sampling ratio to reduce the number of logs pushed. After configuration, EdgeOne will randomly extract logs according to the set percentage and push them to your specified destination.



4. After configuring the log fields, click Next Step to proceed to Step 3.

Step 3: Select the push destination

You can choose to push real-time logs to Tencent Cloud CLS, S3 compatible bucket, or a specified HTTP server according to your needs. Follow the steps below for configuration:

Ship to Tencent Cloud CLS

Ship to S3 compatible

Ship to specified HTTP server

If you have not yet built your own data analysis system, Tencent Cloud provides Log Service (CLS) to help you complete the collection, shipping, and search analysis of real-time logs in a one-stop manner, reducing your development and maintenance costs. You can follow the steps below to ship real-time logs to Tencent Cloud CLS service:

Prerequisites

You have already activated Cloud Log Service (CLS) and granted permission to Tencent Cloud EdgeOne to create a logset.

Note：

1. Log Service (CLS) is a paid service, for related fees, please refer to: Log Service Billing Overview.

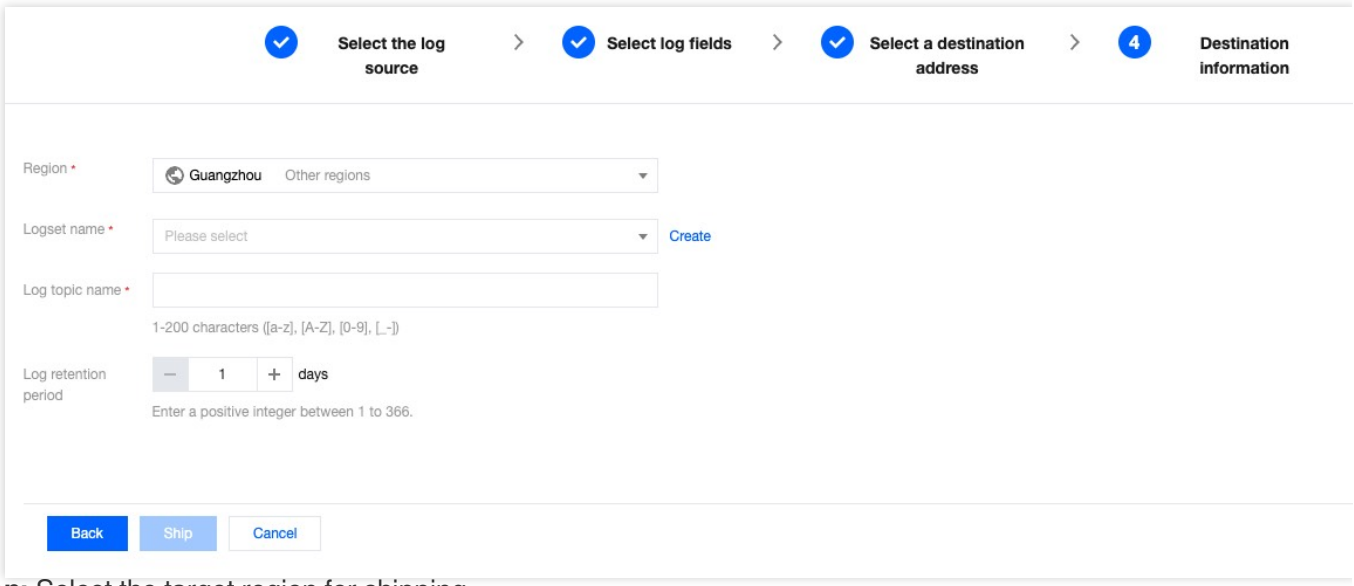
2. It is suggested to enable the service with the root admin account. If it is a sub-account or collaborator, you need to grant them the relevant permissions.

Directions

Create a shipping task

1. In Step ③, select the destination as **Tencent Cloud Log Service (CLS)** and click **Next**.

2. Fill in the relevant parameter information, the parameter explanation is as follows:



Region: Select the target region for shipping.

Target set name: Select the logset in the target region.

Note:

If this is empty or you need to create a new logset, click **Create** to create a logset in the selected region.

Log topic name: You can enter 1-200 characters, allowed characters are `a-z, A-Z, 0-9, _, -`.

Log retention time: Please enter a positive integer between 1 and 366.

Related references

Log search

Log search supports various types of search analysis methods and chart analysis forms. For detailed explanations, please refer to Log Search.

EdgeOne performs log search based on shipping tasks. On the Real-time logs page, select the shipping task you want to search, and click Search to enter the log search page.

You can later manage logsets and other modules through Tencent Cloud Log Service (CLS), such as modifying the logset name.

Logset

A logset (Logset) is a project management unit of Tencent Cloud Log Service (CLS), used to distinguish logs of different projects, and a logset corresponds to a collection. Tencent Cloud EdgeOne logset has the following basic attribute information:

Region: The region where the logset belongs.

Logset name: Logset naming.

Log retention time: The retention period of data in the current logset.

Creation time: Logset creation time.

Log topic

A log topic (Topic) is a basic management unit of Tencent Cloud Log Service (CLS). A logset can contain multiple log topics. A log topic corresponds to a type of application or service, and it is recommended to collect the same type of logs from different machines into the same log topic. For example, a business project has three types of logs: operation logs, application logs, and access logs, and each type can create a corresponding log topic.

The log service system manages different log data of users based on log topics, and each log topic can be configured with different data sources, different index rules, and delivery rules. Therefore, the log topic is the basic unit for configuring and managing log data in the log service. After creating a log topic, you need to configure the relevant rules to effectively collect logs and use search analysis and delivery functions as scheduled.

From a functional perspective, log topics mainly provide:
Collect logs to log topics.
Store and manage logs in units of log topics.
Search and analyze logs in units of log topics.
Deliver logs from log topics to other platforms.
Download and consume logs from log topics.
Note
The above information is excerpted from the Cloud Log Service (CLS) product documentation. Please refer to the explanations on the Log Service (CLS) side.
Each real-time log shipping task shipped to Tencent Cloud Log Service (CLS) will ship the logs of the selected subdomains to a corresponding log topic.

If you currently have your own built-in data source and need to ship real-time logs to a compatible Amazon Simple Storage Service bucket, you can refer to the following steps to continue the operation:
Note：
Currently, only support shipping site acceleration logs and L4 proxy logs to compatible Amazon S3 Storage Service buckets.
The format for log shipping is JSON Lines.

Directions

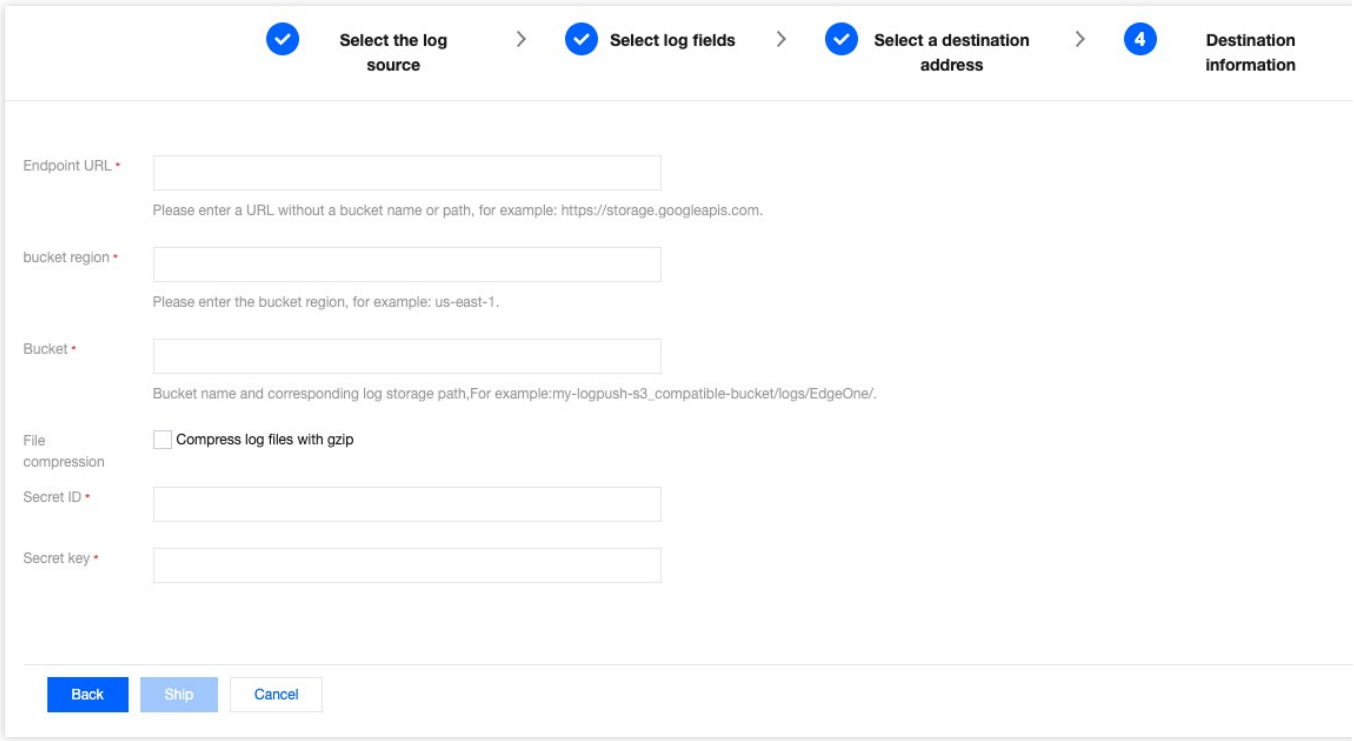
1. In Step ③, Select the destination as **S3 compatible** and click **next**.
2. Fill in the corresponding destination parameters:

Endpoint URL: URL that does not contain the bucket name or path, such as: `https://storage.googleapis.com` , `https://s3.ap-northeast-2.amazonaws.com` .
Bucket Region: The region where the bucket is located, such as: `ap-northeast-2` .
Bucket: The bucket name and the corresponding log storage path: for example, `your_bucket_name/EO-logs/` .

File Compression: Whether to use gzip compression for log files. If checked, the shipped log files will be compressed with gzip, and the file name will be changed to `filename.log.gz` .

SecretId: Access Key ID used to access the bucket.

SecretKey: Secret key used to access the bucket.



Note：

1. The bucket needs to be compatible with AWS Signature Version 4 Authentication Algorithm. For specific compatibility, please refer to the instructions provided by your bucket provider.

2. File name description: Logs will be stored in the specified bucket path in the format of `UploadTime_Random.log` , and logs will be archived in a folder by date (UTC +00:00), such as: `logs/20230331/20230331T185917Z_2aadf5ce.log` .

UploadTime: Log file upload time, using ISO-8601 format, UTC+00:00 timezone.

Random: Random characters. In cases where there are large log volumes, there may be multiple log files with the same upload time, and this random character string is used to identify different files.

3. Click **Push**. After issuing the real-time log shipping task, EdgeOne will ship a test file to the target bucket path to verify connectivity. For instance, a file named `1699874755_edgeone_push_test.txt` will be shipped with the fixed string `test` .

If you currently have a self-built data source, EdgeOne can call the backend interface address you provided by an HTTP POST request, transmitting the logs to your designated server within the HTTP body.

Note：

1. HTTP is plaintext transmission, so it is suggested that you use an encrypted HTTPS address for the API.

2. To further enhance the security verification of request sources, we provide a request authentication scheme. You can fill in the relevant authentication information in the push destination configuration, and the authentication algorithm can be found at:Request Authentication Algorithm.

3. The log shipping format comprises an array of multiple JSON objects, and each JSON object is a log.

Operation Guide

Create a shipping task

1. In Step ③, select the destination as **HTTP service (POST)** and click **Next**.

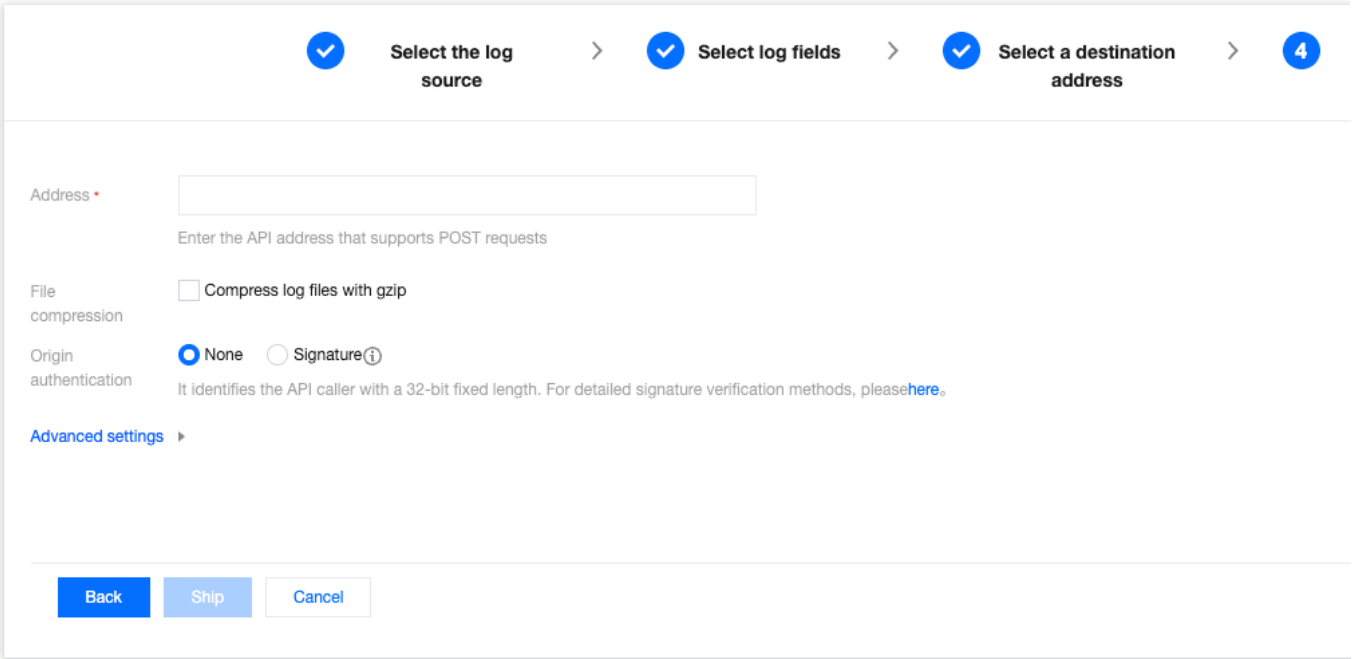
2. Fill in the relevant destination and parameter information, with the following parameter descriptions:

API address: Enter your data source API address, e.g., `https://www.example.com/log`

File compression: To reduce the size of log files and save traffic costs, you can enable file compression by checking "**Compress log files with gzip**". EdgeOne will use gzip format to compress logs before transmission and will add an HTTP request header `content-encoding = gzip` to indicate the compression format.

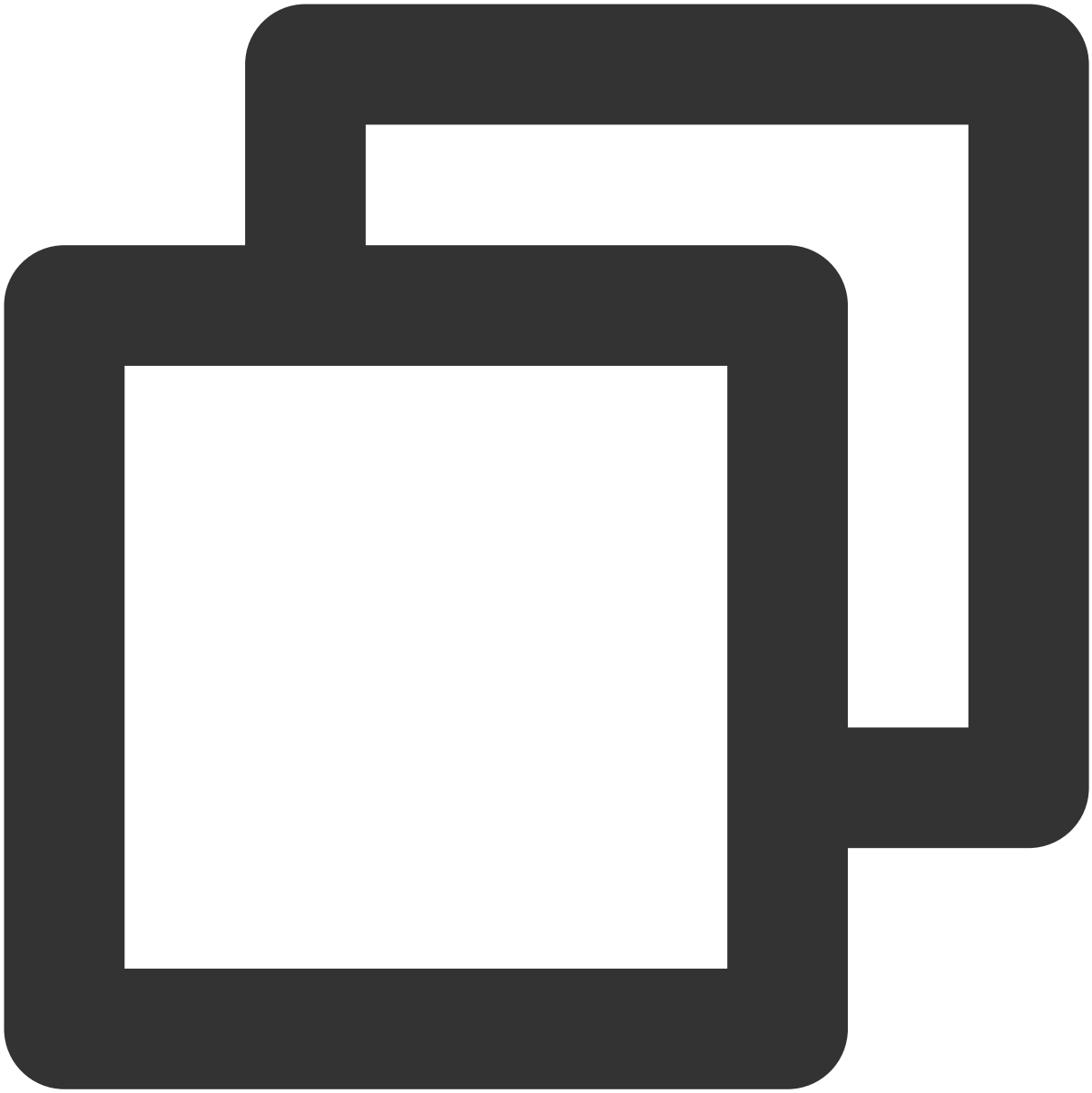
Origin authentication: When selecting encryption authentication, the shipping logs will carry authentication information for the origin to verify, ensuring the security of the data source identity.

Custom HTTP request headers: Add the HTTP headers that need to be carried when EdgeOne initiates a request. For example, if you need to identify the log source vendor as EdgeOne, you can add a header `log-source = EdgeOne` to identify the log source.



3. Click **"ship"** to issue a real-time log shipping task.

4. During the configuration phase of the real-time log shipping task, in order to verify the interface connectivity, an empty data will be sent to the interface address for verification. The data format is as follows:




```
[{
        "BotClassAccountTakeOver": "-",
        "BotClassAttacker": "-",
        "BotClassMaliciousBot": "-",
        "BotClassProxy": "-",
        "BotClassScanner": "-",
        "ClientDeviceType": "-",
        "ClientIP": "-",
        "ClientISP": "-",
        "ClientRegion": "-",
        "ClientState": "-",
```

```
        "EdgeCacheStatus": "-",
        "EdgeEndTime": "-",
        "EdgeInternalTime": "-",
        "EdgeResponseBodyBytes": "-",
        "EdgeResponseBytes": "-",
        "EdgeResponseStatusCode": "-",
        "EdgeResponseTime": "-",
        "EdgeServerID": "-",
        "EdgeServerIP": "-",
        "EdgeSeverRegion": "-",
        "LogTime": "-",
        "OriginDNSResponseDuration": "-",
        "OriginIP": "-",
        "OriginRequestHeaderSendDuration": "-",
        "OriginResponseHeaderDuration": "-",
        "OriginResponseStatusCode": "-",
        "OriginSSLProtocol": "-",
        "OriginTCPHandshakeDuration": "-",
        "OriginTLSHandshakeDuration": "-",
        "ParentRequestID": "-",
        "RemotePort": "-",
        "RequestBytes": "-",
        "RequestHost": "-",
        "RequestID": "-",
        "RequestMethod": "-",
        "RequestProtocol": "-",
        "RequestRange": "-",
        "RequestReferer": "-",
        "RequestSSLProtocol": "-",
        "RequestTime": "-",
        "RequestUA": "-",
        "RequestUrl": "-",
        "RequestUrlQueryString": "-"
}]
```

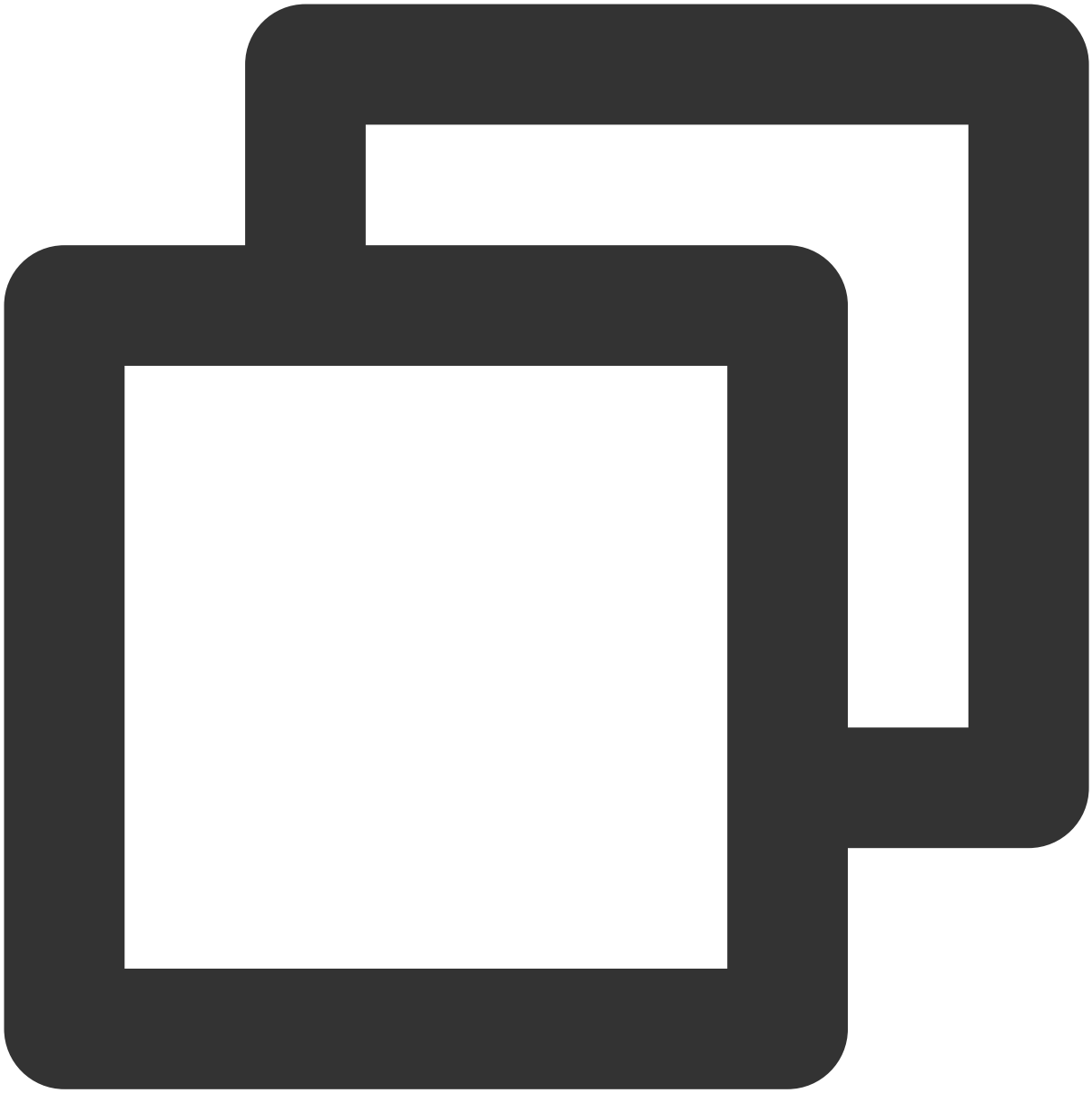

Related References

Request Authentication Algorithm

If you have selected encryption signature in the origin authentication of the push destination information, you can custom input your custom Configuration SecretId and SecretKey. EdgeOne will add the signature `auth_key` and `access_key` in the Request URL. The details of the signature algorithm are as follows:

1. **Request URL composition**

As shown below, the Request URL will carry `auth_key` and `access_key` after the "?".



```
http://DomainName[:port]/[uri]?auth_key=timestamp-rand-md5hash&access_key=SecretID
```

Parameter description:

timestamp: The current time of the request, using a Unix 10-digit second-level timestamp.

rand: random number

access_key: used to identify the identity of the API requester, that is, your custom Configuration SecretID.

SecretKey: fixed Length 32, that is, your custom Configuration SecretKey.

uri: resource identifier, for example: `/access_log/post` .

md5hash: md5hash = `md5sum(string_to_sign)` , where string_to_sign = `"uri-timestamp-rand-SecretKey"` . The verification string calculated by the md5 algorithm, a mixture of numbers 0-9 and lowercase English letters a-z, fixed Length 32.

2. **Calculation example**

Assuming the filled in parameters are:

API address: `https://www.example.com/access_log/post`

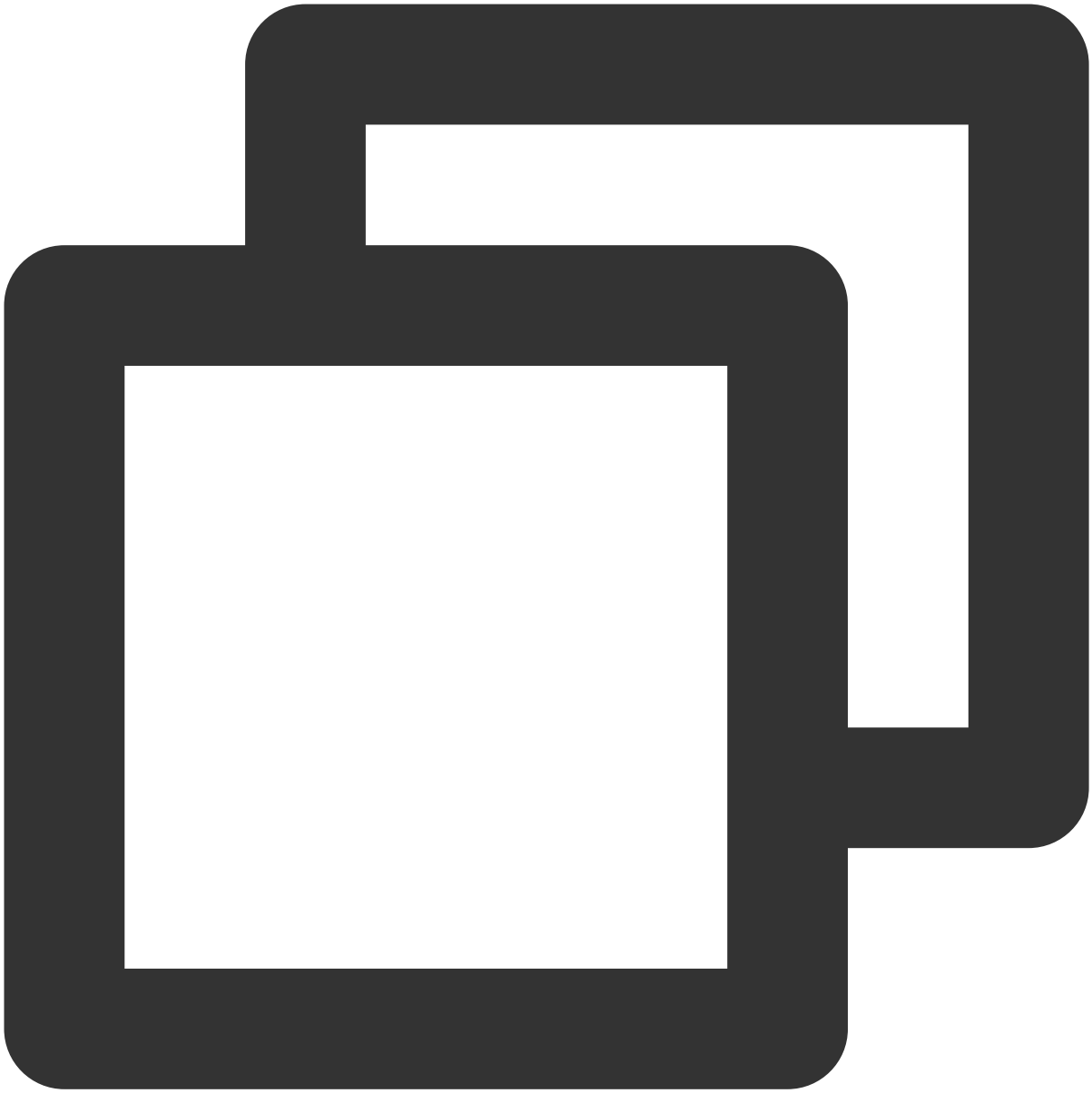
SecretID = `YourID`

SecretKey = `YourKey`

uri = `/access_log/post`

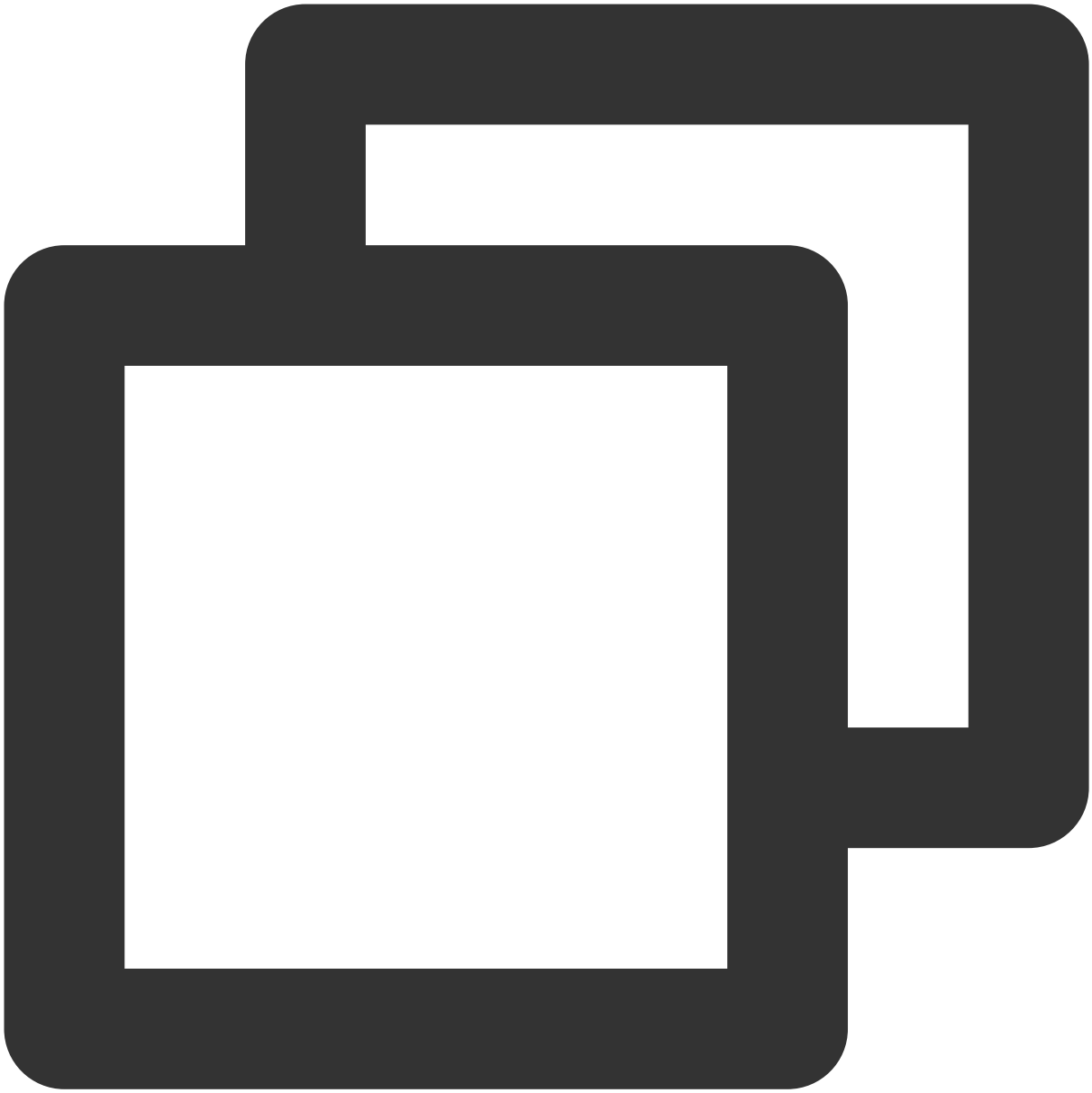
timestamp = `1571587200`

rand = `0`



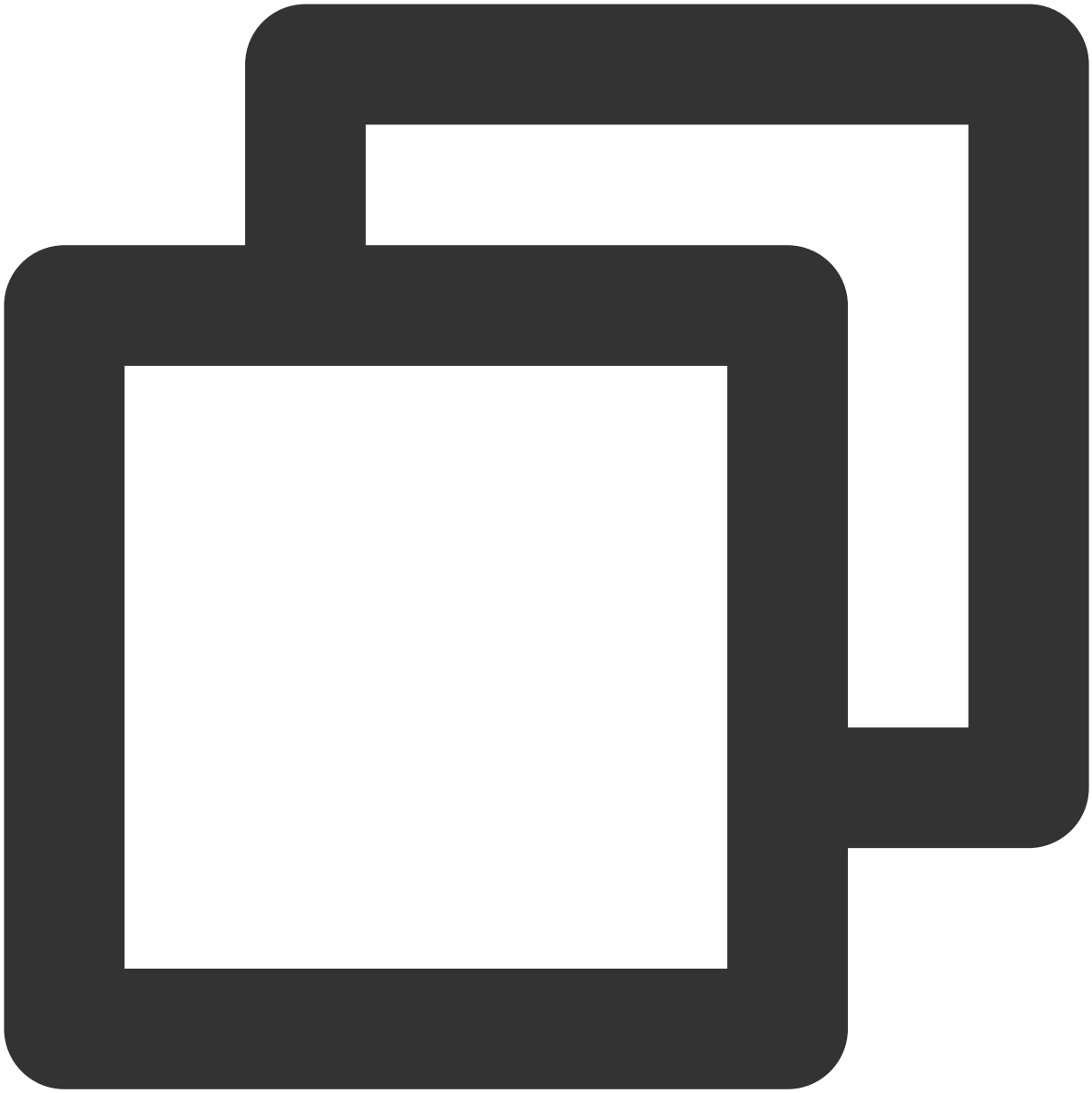
```
string_to_sign = "/access_log/post-1571587200-0-YourKey"
```

Based on this string, calculate



```
md5hash=md5sum("/access_log/post-1571587200-0-YourKey")=1f7ffa7bff8f06bbfbe2ace0f14
```

The final push request URL is:



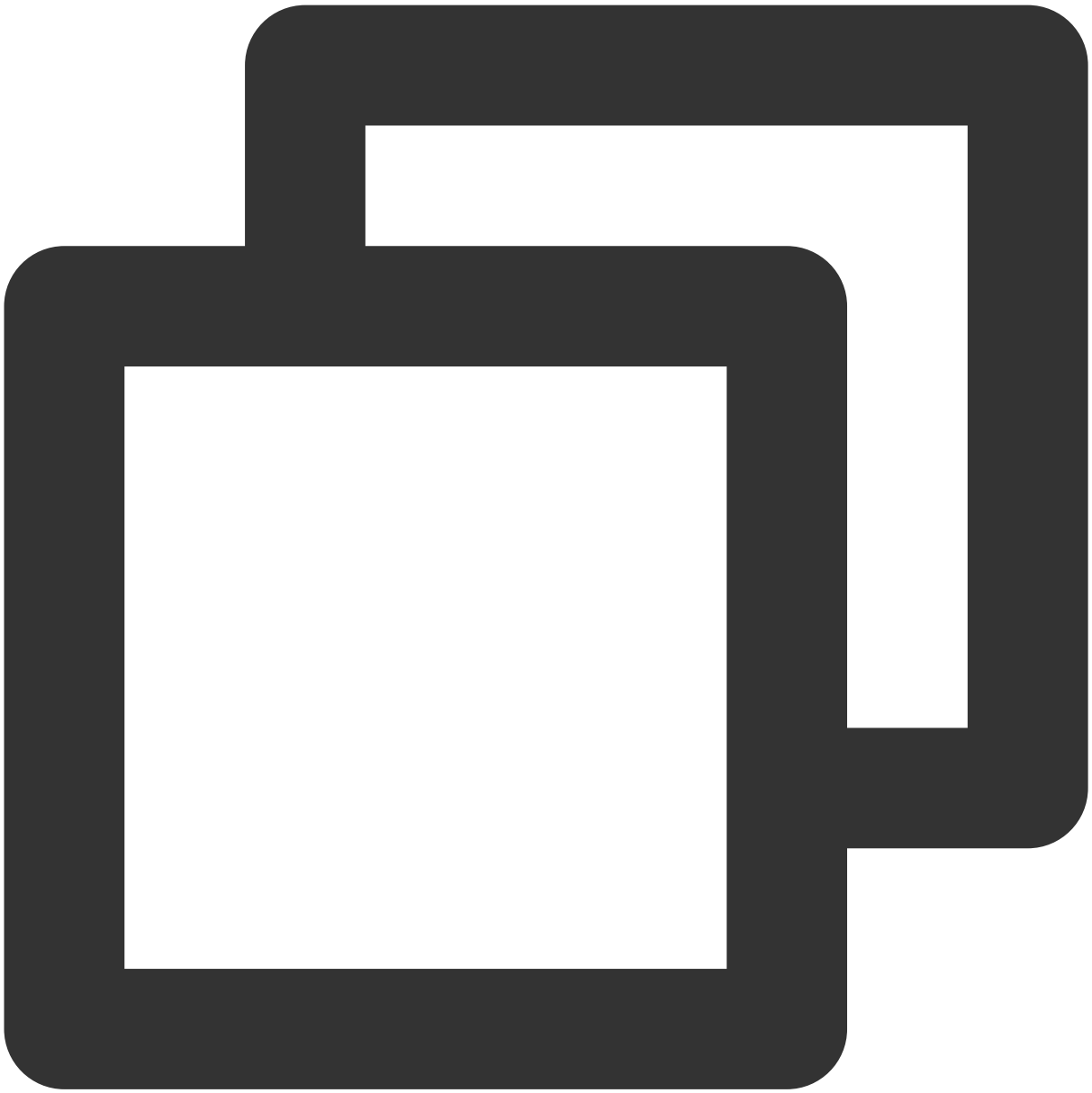
```
https://www.example.com/cdnlog/post?auth_key=1571587200-0-1f7ffa7bff8f06bbfbe2ace0f
```

After the service receives the push request, it extracts the value of `auth_key` . Split the value of `auth_key` to obtain `timestamp` , `rand` , and `md5hash` . You can first check whether the timestamp is expired, the suggested expiration time is `300s` , and assemble the encryption string based on the above rules. Use `SecretKey` to assemble the string to be encrypted, and compare the encrypted result with the `md5hash` value in `auth_key` . If they are the same, it means the authentication has passed.

3. **Server-side authentication request resolution code example**

Python

Goland



```
import hashlib

from flask import Flask, request

app = Flask(__name__)


def get_rsp(msg, result={}, code=0):
```

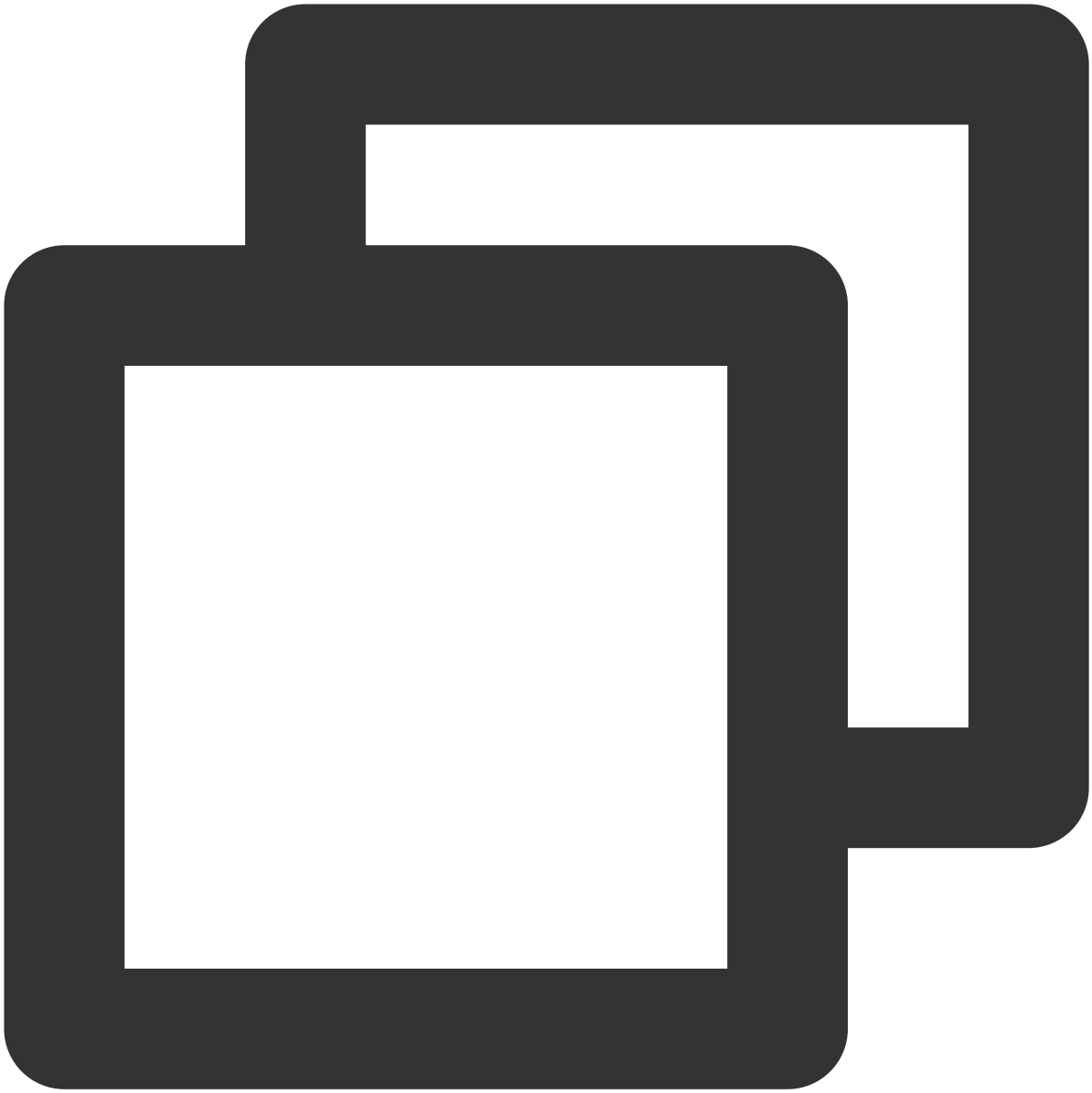
```
    return {
        "respCode": code,
        "respMsg": msg,
        "result": result
    }


def get_secret_key(access_key):
    return "secret_key"


@app.route("/access_log/post", methods=['POST'])
def access_log():
    if request.method == 'POST':
        if request.content_type.startswith('application/json'):
            current_time_ts, rand_num, md5hash = request.args.get("auth_key").split
             # Judge whether the requests Time is within the Validity period
            if time.time() - int(current_time_ts) > 300:
                return get_rsp(msg="The request is out of time", code=-1)

            access_key = request.args.get("access_key")
            # collected secret_key through access_key(SecretID)
            secret_key = get_secret_key(access_key)
            raw_str = "%s-%s-%s-%s" % (request.path, current_time_ts, rand_num, sec
            auth_md5hash = hashlib.md5(raw_str.encode("utf-8")).hexdigest()
            if auth_md5hash == md5hash:
                # Authentication Pass
                if request.headers['content-encoding'] == 'gzip':
                    # Decompression Data
                    pass
                # Data Processing
            return get_rsp("ok")
        return get_rsp(msg="Please use content_type by application/json", code=-1)
    return get_rsp(msg="The request method not find, method == %s" % request.method

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=8888, debug=True)python
```



```
package main

import (
    "context"
    "crypto/md5"
    "fmt"
    "log"
    "net/http"
    "os"
    "os/signal"
    "strings"
```

```
    "syscall"
)

func main() {
    mux := http.NewServeMux()
    mux.Handle("/access_log/post", &logHandler{})

    server := &http.Server{
        Addr:    ":5000",
        Handler: mux,
    }

    // Create system Signal receiver
    done := make(chan os.Signal)
    signal.Notify(done, os.Interrupt, syscall.SIGINT, syscall.SIGTERM)
    go func() {
        <-done

        if err := server.Shutdown(context.Background()); err != nil {
            log.Fatal("Shutdown server:", err)
        }
    }()

    err := server.ListenAndServe()
    if err != nil {
        if err == http.ErrServerClosed {
            log.Print("Server closed under request")
        } else {
            log.Fatal("Server closed unexpected")
        }
    }
}

type logHandler struct{}

func (*logHandler) ServeHTTP(w http.ResponseWriter, r *http.Request) {
    if r.Method == "POST" {
        query := r.URL.Query()
        authKey := query.Get("auth_key")
        accessKey := query.Get("access_key")//access_key is the SecretID you Provid
        authKeys := strings.Split(authKey, "-")
        if len(authKeys) == 3 {
            currentTimeTs := authKeys[0]

            //Carry out Timestamp Validity period judgment
            RandNum := authKeys[1]
            md5Hash := authKeys[2]
```

```
            secretKey := getSecretKey(accessKey)
            authStr := fmt.Sprintf("%s-%s-%s-%s", "/access_log/post", currentTimeTs
            data := []byte(authStr)
            has := md5.Sum(data)
            authMd5 := fmt.Sprintf("%x", has) //Conversion to String for Comparison
            if authMd5 == md5Hash {
                // todo Authentication successful
                if r.Header.Get("Content-Encoding") == "gzip" {
                    //Decompression Data
                }
                //Data Processing
            }
        } else {
            //exception handling
        }
    }
}

// collected SecretKey
func getSecretKey(accessKey string) string {
    if accessKey != "" {
        // collected Secret_Key through Access_key(SecretID)
        return "secret_key"
    }
    return ""
}
```

Real-time log field Description

Last updated：2023-12-05 15:40:41

This article introduces the field explanation of site acceleration logs and L4 proxy logs in real-time logs.

Note:

When a field has no value:

If the data type of the field is String and the field has no data, the field value is: "-".

If the data type of the field is Integer and the field has no data, the field value is: -1.

Site Acceleration Log

Name	Data Type	Description
LogTime	Timestamp ISO8601	Time when the log is generated
RequestID	String	Unique ID of the client request
ClientIP	String	Client IP
ClientRegion	String	Country/region parsed from the client IP. Format standard: ISO-3166 alpha-2
ClientState	String	The client IP parses out the country's lower-level administrative divisions. Currently only data within mainland China is supported. Format standard: ISO-3166 alpha-2
ClientISP	String	ISP information resolved from client IP. Data within mainland China is recorded under the ISP's Chinese name. Global Availability Zones (excluding mainland China) data is recorded as Autonomous System Number (ASN)
RequestTime	Timestamp ISO8601	Client request time, time zone: UTC +00:00
RequestStatus	Integer	Status of the client request, if using Websocket protocol, EdgeOne will periodically print logs, this field can be used to determine the connection status. Value options: 0:Not ended 1:Request ended normally

		2:Ended abnormally
RequestHost	String	Host of the client request
RequestBytes	Integer	Size of the client request, unit: Byte
RequestMethod	String	HTTP Method of the client request, value options: GET POST HHEAD PUT DELETE CONNECT OPTIONS TRACE PATCH
RequestSSLProtocol	String	SSL (TLS) protocol used by the client, if the value is "-", there is no SSL handshake in the request; value options: TLS 1.0 TLS 1.1 TLS 1.2 TLS 1.3
ClientDeviceType	String	Device type of the client request, value options: TV Tablet Mobile Desktop Other
RequestUrl	String	URL of the client request
RequestUrlQueryString	String	Query parameter carried by the client request URL
RequestUA	String	User-Agent information of the client request
RequestRange	String	Range parameter information of the client request
RequestReferer	String	Referer information of the client request
RequestProtocol	String	Application layer protocol of the client request, value options: HTTP/1.0 HTTP/1.1 HTTP/2.0 HTTP/3

		WebSocket
RemotePort	Integer	Port for establishing a connection between the client and the node under the TCP protocol
EdgeCacheStatus	String	Whether the client request hits the node cache, value options: hit: Resource provided by the node cache miss: Resource can be cached, but provided by the origin dynamic: Resource cannot be cached
EdgeResponseStatusCode	Integer	Status code returned by the node response to the client
EdgeResponseBytes	Integer	Size of the node response returned to the client, unit: Byte
EdgeResponseBodyBytes	Integer	Body size of the node response returned to the client, unit: Byte
EdgeResponseTime	Integer	Time consumed from the start of receiving the client request by EdgeOne to the end of the client receiving the server response; unit: ms
EdgeInternalTime	Integer	Time consumed from the start of receiving the client request by EdgeOne to the first byte of the response to the client; unit: ms
EdgeServerIP	String	EdgeOne server IP address obtained by DNS resolution of Host
EdgeServerID	String	Unique identifier of the EdgeOne server accessed by the client
EdgeSeverRegion	String	Country of the responding EdgeOne node IP, format standard reference: ISO-3166 alpha-2
EdgeEndTime	Timestamp ISO8601	Time to complete the response to the client request
OriginDNSResponseDuration	Float	The duration taken to receive the DNS resolution response from the origin server. If there is no return to the origin, it is recorded as -1, unit: ms
OriginIP	String	Origin IP accessed by the origin-pull, if not origin-pull, record as "-"
OriginRequestHeaderSendDuration	Float	The duration taken to send the request header to the

		origin server is usually 0. If there is no return to the origin, it is recorded as -1, unit: ms
OriginSSLProtocol	String	SSL protocol version used for requesting the origin, if not origin-pull, record as "-"; value options: TLS 1.0 TLS 1.1 TLS 1.2 TLS 1.3
OriginTCPHandshakeDuration	Float	Time consumed to complete the TCP handshake when requesting the origin, if not origin-pull, record as "-1", unit: ms; Note: 0 when the connection is reused
OriginTLSHandshakeDuration	Float	Time consumed to complete the TLS handshake when requesting the origin, if not origin-pull, record as "-1", unit: ms; Note: 0 when the connection is reused
OriginResponseHeaderDuration	Float	Time consumed from sending the request header to the origin to receiving the response header from the origin, if not origin-pull, record as "-1", unit: ms
OriginResponseStatusCode	Integer	Origin response status code, if not origin-pull, record as "-1"
BotClassAttacker	String	Risk level of the client IP with attack behavior (such as DDoS, high-frequency malicious requests, site attacks, etc.) based on recent intelligence data, "-" corresponds to no historical data, other value options: high: corresponding to high risk medium: corresponding to medium risk low: corresponding to low risk
BotClassProxy	String	Risk level of the client IP with suspicious proxy ports open and used as network proxies (including Proxy) based on recent intelligence data, "-" corresponds to no historical data, other value options: high: corresponding to high risk medium: corresponding to medium risk low: corresponding to low risk
BotClassScanner	String	Based on recent intelligence data, the risk level of the client IP requesting scans for known vulnerabilities is as follows: "-" corresponds to no historical data, and other values are: high: corresponding to high risk medium: corresponding to medium risk

		low: corresponding to low risk
BotClassAccountTakeOver	String	Based on recent intelligence data, the risk level of the client IP requesting malicious account cracking and initiating account takeover attacks is as follows: "-" corresponds to no historical data, and other values are: high: corresponding to high risk medium: corresponding to medium risk low: corresponding to low risk
BotClassMaliciousBot	String	Based on recent intelligence data, the risk level of the client IP requesting malicious bots, hotlinking, and brute force cracking behaviors is as follows: "-" corresponds to no historical data, and other values are: high: corresponding to high risk medium: corresponding to medium risk low: corresponding to low risk

Note：

In the site acceleration log, using the WebSocket protocol for long connections, EdgeOne will periodically record logs and record a log at the end of the final request. You can identify requests by the `RequestID` field, and logs with the same `RequestID` represent the same connection; you can also determine the connection status at the time of log recording through the `RequestStatus` .

L4 Proxy Log

Name	Data Type	Description
ServiceID	String	Unique identifier ID for L4 proxy service
SessionID	String	Unique identifier ID for TCP connection or UDP session
ConnectTimeStamp	Timestamp ISO8601	Connection establishment time; default UTC +0 timezone
DisconnetTimeStamp	Timestamp ISO8601	Disconnection time; default UTC +0 timezone
DisconnetReason	String	Disconnection reason; Format is "direction: reason" Direction values: up: origin direction down: Client direction

		Reason values: net_exception_peer_error: read/write peer returns error net_exception_peer_close: peer has closed connection create_peer_channel_exception: failed to create channel to next hop channel_eof_exception: channel has ended (at the end of the request, the node that ends the request sends channel_eof to the adjacent node to inform that the request has ended) net_exception_closed: connection is closed net_exception_timeout: read/write timeout
ClientRealIP	String	Client real IP
ClientRegion	String	2-letter country/region code of the client, in accordance with ISO-3166 alpha-2 standard
EdgeIP	String	IP address of the accessed EdgeOne server
ForwardProtocol	String	TCP/UDP forwarding protocol configured by the customer
ForwardPort	Integer	Forwarding port configured by the customer
SentBytes	Integer	Inbound traffic generated from the last log record time to this log record time, unit: Byte
ReceivedBytes	Integer	Outbound traffic generated from the last log record time to this log record time, unit: Byte
LogTimeStamp	Timestamp ISO8601	Log generation time; default UTC +0 timezone

Note：

In the case of TCP long connections, EdgeOne will periodically record logs and record the last log when the connection ends. You can determine whether the connection is disconnected by whether the `DisconnetReason` field is empty; you can also use the `SessionID` to identify the connection, and logs with the same `SessionID` record the behavior of the same connection.

Offline Logs

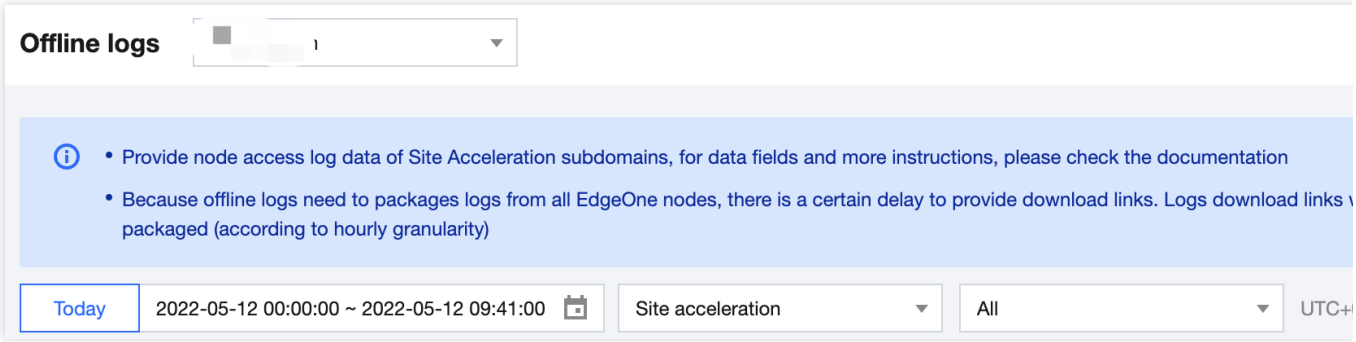
Last updated：2024-04-15 15:00:09

Edge Access Logs

Access logs are collected on an hourly basis and stored for 30 days. You can download the logs as need during the retention period.

Directions

1. Log in to the EdgeOne console. Click **Log Service** > **Offline Logs** on the left sidebar.
2. On the page that displays, select a site or the log file of a subdomain name. You can also filter logs by time.

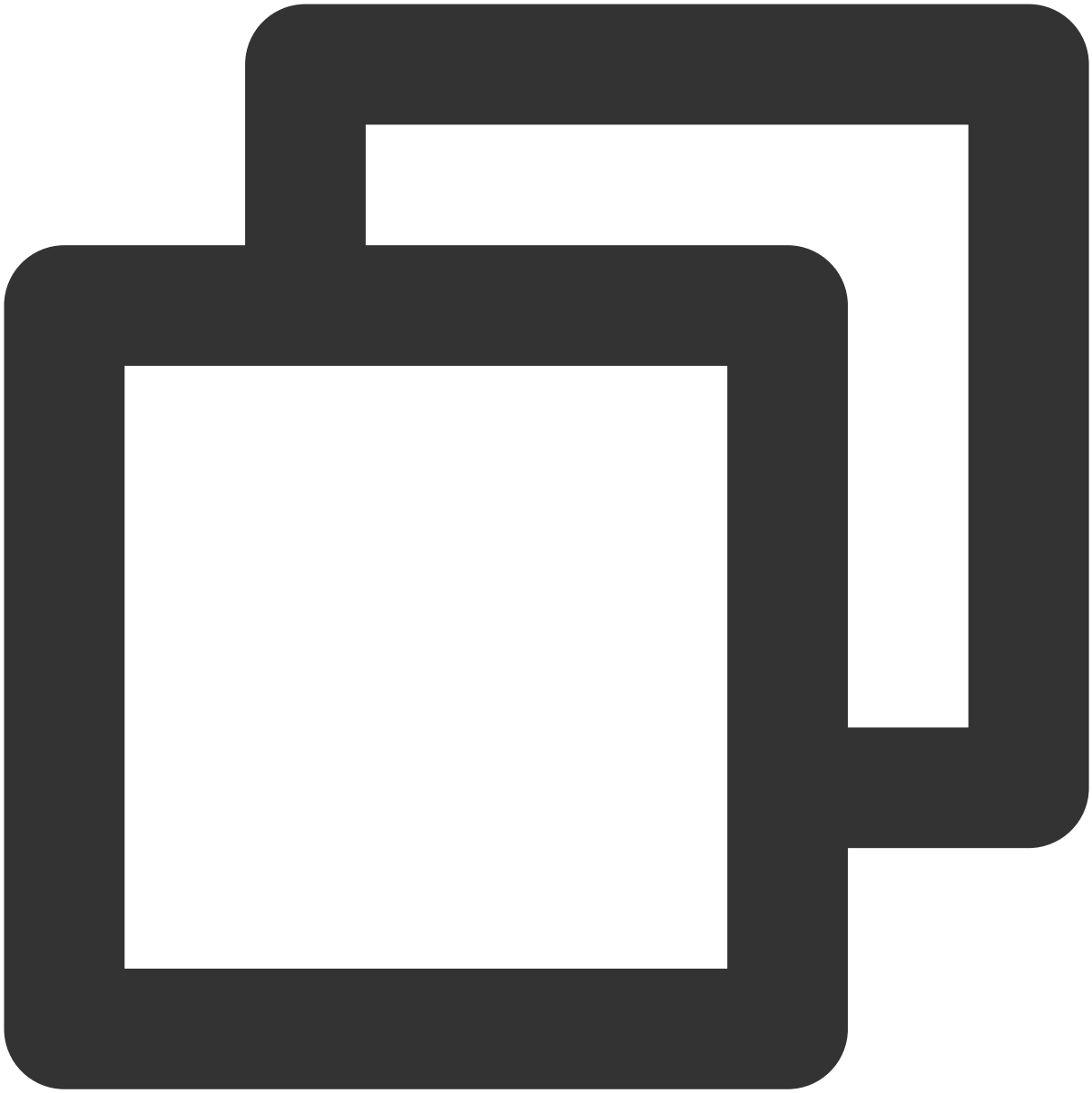


3. Click **Download** in the **Operation** column.

Important

The access logs are collected on an hourly basis. If the selected domain name is not requested during the period, no logs are generated.

The access logs are compressed to a .gz file. Due to defects of the MacOS directory system, the .gz file may failed to be decompressed on MacOS by double-clicking it. In this case, you can run the following Terminal commands:



```
gunzip {your_file_name}.log.gz
```

EdgeOne nodes are distributed over the globe. To synchronize the time across time zones, logs are stored and queried in UTC+00:00 by default.
Generally, it takes around 30 hours to generate log data as it is collected from all EdgeOne nodes. The log data will be complete within 24 hours after being generated.

Field Description

Logs are stored in JSON format by default. The log fields are described as follows:

When a field is not specified:

For a string field, the field value is set to `-` if the field has no data.

For an integer field, the field value is set to `-1` if the field has no data.

Site acceleration logs

Name	Data type	Description
RequestID	String	Unique ID of the client request
ClientIP	String	Client IP
ClientRegion	Sting	Country/Region of the client IP. Format: ISO-3166 alpha-2
ClientState	String	The client IP parses out the country's lower-level administrative divisions. Currently only data within mainland China is supported. Format: ISO 3166-2.
ClientISP	String	ISP information resolved from client IP. Data within mainland China is recorded under the ISP's Chinese name. Global Availability Zones (excluding mainland China) data is recorded as Autonomous System Numbers (ASN).
RequestTime	String	The time that the client initiates a request, which is record in UTC +00:00 and defined in the ISO-8601 standard.
RequestStatus	int	Status of the client request. Values: `0` (not completed), `1` (completed successfully), `2` (completed abnormally)
RequestHost	String	Host of the client request
RequestBytes	int	Size of the client request, in bytes
RequestMethod	String	The HTTP method used by the client
RequestUrl	String	The URL for the client request
RequestUrlQueryString	String	The query string contained in the request URL
RequestUA	String	The User-Agent sent by the client
RequestRange	String	The Range parameter sent by the client
RequestReferer	String	The Referer parameter sent by the client

RequestProtocol	String	The application layer protocol used by the client. Values: `HTTP/1.0`, `HTTP/1.1`, `HTTP/2.0`, `HTTP/3`, `WebSocket`
RemotePort	int	The port that connects the client and node over the TCP protocol.
EdgeCacheStatus	String	Whether the client request results in a cache hit. Hit: Resources are served by node cache. Madam: Resources are served by the origin server and can be cached. Dynamic: Resources cannot be cached. other: Unidentifiable Cache Status.
EdgeResponseStatusCode	int	The status code that the node returns to the client
EdgeResponseBytes	int	Size of the response that the node returns to the client, in bytes
EdgeResponseTime	int	The amount of time elapsed between EdgeOne receiving a request from the client and waiting till the client receives the response from the server side. Unit: ms
EdgeInternalTime	int	The amount of time elapsed between EdgeOne receiving a request from the client and waiting till the client receives the response from the server side. Unit: ms
EdgeServerIP	String	IP address of the EdgeOne server, which can be resolved from the host using DNS.
EdgeServerID	String	The unique ID that identifies the EdgeOne server accessed by the client
SecurityAction	String	The rule action. Values: `Monitor` (observe), `JSChallenge` (JavaScript challenge), `Deny` (block), `Allow` (allow), `BlockIP` (block the IP), `Redirect` (redirect), `ReturnCustomPage` (return the custom page), `ManagedChallenge` (implement the managed challenge)
SecurityRuleID	String	ID of the security rule used
SecurityUserNote	String	The tag defined by the user
SecurityModule	String	Security feature of the hit security rule. Values: `CustomRule` (custom rules), `BotManagement` (bot management), `RateLimiting` (preset rate limiting rules), `RateLimitingCustomRule` (custom rate limiting rules), `ManagedRule` (managed rules), `BotClientReputation`

		(client reputation), `BotBehaviorAnalysis` (bot intelligence), `RateLimitingClientFiltering` (client filtering)

L4 proxy logs

Name	Data type	Description
ServiceID	String	Unique ID of the L4 proxy service
ConnectTimeStamp	String	The time that the connection is established, which is recorded in UTC +0 and defined in the ISO-8601 standard.
DisconnetTimeStamp	String	The time that the connection is disconnected, which is recorded in UTC +0 and defined in the ISO-8601 standard.
DisconnetReason	String	Cause of disconnection Format: [Direction: Reason]. Direction: `up` (origin)/ `down` (client) Reason: `Net_exception_peer_error` : Read/write peer error `Net_exception_peer_close` : Connection closed by the peer `Create_peer_channel_exception` : Failed to create the channel to the next hop `Channel_eof_exception` : Channel ended. When the quest ends, the related node sends `channel_eof` to neighbor nodes. `Net_exception_closed` : Connection closed `Net_exception_timeout` : Read/write timed out
ClientRealIP	String	Real client IP
ClientRegion	String	The 2-digit country/region code of the client in the ISO-3166 alpha-2 standard.
EdgeIP	String	IP address of the EdgeOne server accessed
ForwardProtocol	String	The TCP/UDP forwarding protocol configured by the client
ForwardPort	Int	The forwarding port configured by the client
SentBytes	Int	Outbound traffic produced when the log is generated, in bytes
ReceivedBytes	Int	Outbound traffic produced when the log is generated, in bytes
LogTimeStamp	String	The time that the log is generated, which is recorded in UTC +0 and

		defined in the ISO-8601 standard.

Notes

The traffic/bandwidth data (in bytes) recorded in the access log field "EdgeResponseBytes" may be different from the actual billing data for the following reasons:
Only application-layer data can be recorded in access logs. During actual data transfer, the traffic generated over the network is around 5-15% more than the application-layer traffic, including the following two parts:
Consumption by TCP/IP headers: in TCP/IP-based HTTP requests, each packet has a maximum size of 1,500 bytes and includes TCP and IP headers of 40 bytes, which generate traffic during transfer but cannot be counted by the application layer. The overhead of this part is around -4%.
TCP retransmission: During normal data transfer over the network, around 3% to 10% packets are lost on the internet, and the server will retransmit the lost ones. This type of traffic cannot be counted by the application layer, which accounts for 3% to 7% of the total traffic.
When smart acceleration is enabled, the traffic/bandwidth generated when the client sends a request to the EdgeOne node incurs charges. For more details, see Billing Overview.

Data Analysis Overview

Last updated：2023-09-21 15:07:50

Tencent Cloud EdgeOne security acceleration platform analyzes access log data and provides various data metrics in the data analysis page for you to understand your business data from multiple dimensions.

Applicable Scenarios

Scenario	Specific Demand
Daily monitoring and inspection	By observing the trends and distribution of various data metrics of acceleration domain names/L4 proxy instances, continuously monitor whether EdgeOne has high latency or failures.
Troubleshooting analysis	By analyzing access logs, understand the path and content of the user's access to locate and troubleshoot issues.
Business data insight	By analyzing and mining client data, understand user profiles.

Function Details

Data analysis function	Function introduction
Traffic analysis	By analyzing L7 (application layer) access logs, understand the source, traffic/bandwidth, and latency of user access to websites or services, helping you better understand user needs and optimize network performance.
Cache analysis	By analyzing cache hit rate and cache content data, understand the effectiveness of cache strategies, helping you better optimize cache configuration.
Security analysis	By analyzing access logs, network data, etc., understand the attack surface data related to your business, including attack sources, attack methods, etc., helping you better understand the attack situation and formulate more effective security policies.
DNS resolution	By analyzing DNS resolution data in NS access mode, understand access volume, return codes, etc., helping you better understand the operation of the resolution system.

L4 proxy	By analyzing L4 (transport layer) access logs, understand the source, traffic, and connection duration of user access to L4 proxy instances, helping you better monitor the operation of L4 proxy instances.

Traffic Analysis

Last updated：2023-09-21 11:45:23

Overview

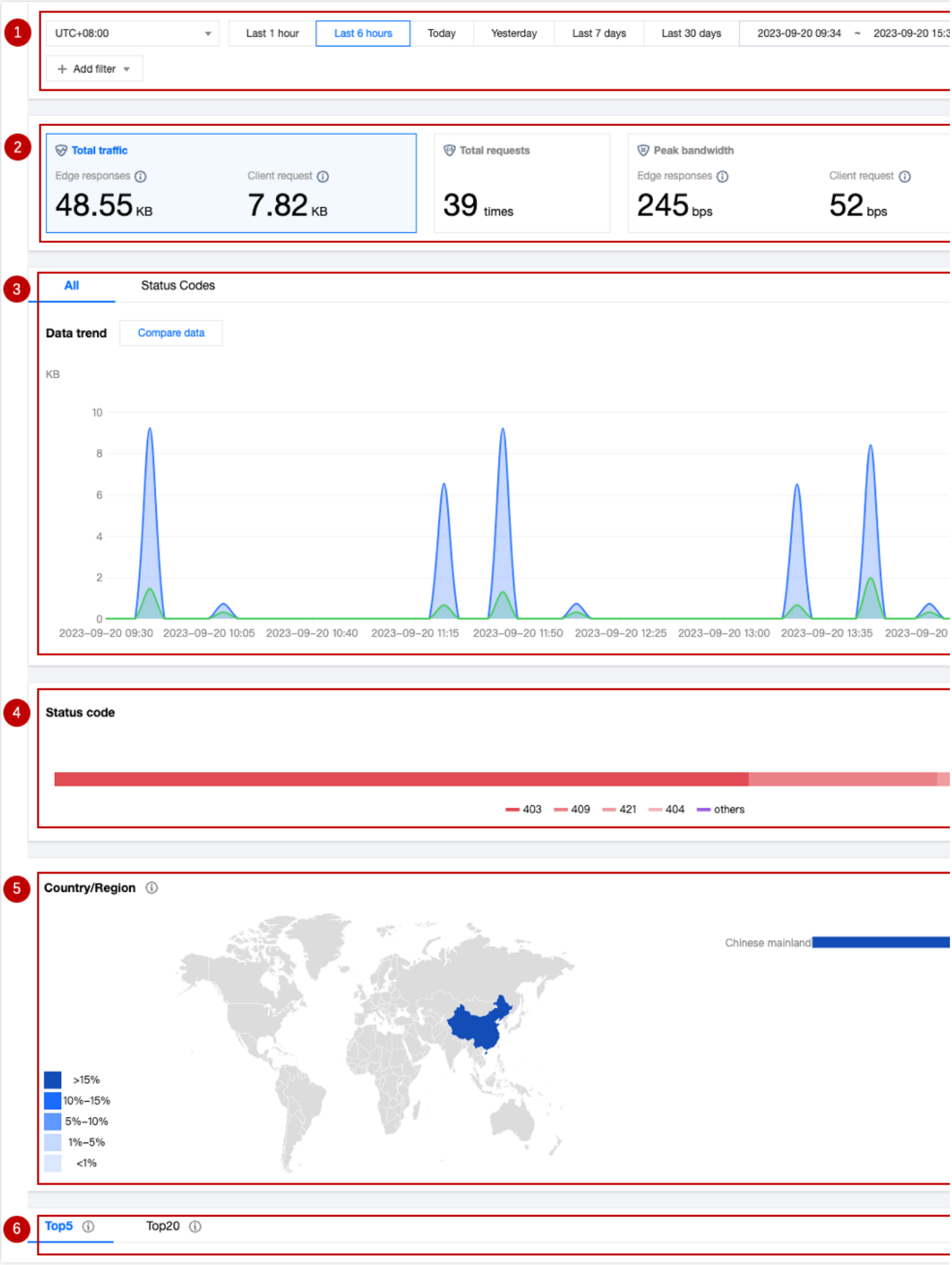
EdgeOne Service analyzes L7 (application layer) access log data to provide you with multi-dimensional, visualized traffic analysis, including time trend curves of traffic, requests, and other indicators, as well as country/region distribution and TOP rankings.

Supported Capabilities

Traffic analysis supports data statistics for traffic, requests, and bandwidth. You can switch between different core indicator data areas by clicking on them.

Note:

Temporarily not supported to switch to the "Unique IP count" indicator.



1. Data Filtering and Selection

Supports selecting the time range for data query, for details, please refer to How to Modify the Query Time Range.
Supports filtering by site, Hosts, country/region, status code, URL, and other dimensions, for details, please refer to How to Use Filter Conditions.

2. Core Indicators

Total Traffic:
EdgeOne responded: The sum of all traffic transmitted from EdgeOne to the client, i.e., downstream traffic.
Client request: The sum of traffic received by EdgeOne from client requests, i.e., upstream traffic.
Total Requests: The number of requests EdgeOne receives from clients.
Peak Bandwidth:
EdgeOne response: The peak of all bandwidth transmitted from EdgeOne to the client, i.e., downstream bandwidth peak.
Client request: The peak of bandwidth received by EdgeOne from client requests, i.e., upstream bandwidth peak.
Number of independent IPs: The number of requests obtained by deduplicating client IP addresses, which can reflect the number of IP addresses accessing the business.
Note:
The calculation method of the bandwidth peak indicator will vary depending on the time granularity.
1-minute granularity: Total traffic within 1 minute * 8 / 60 seconds.
5-minute granularity: Total traffic within 5 minutes * 8 / 300 seconds.
Hourly basis: The maximum value among all 5-minute granularity bandwidth peak points.
Daily basis: The maximum value among all 5-minute granularity bandwidth peak points.

3. Time Trend Chart

Under the "All" tab, the time trend curve of the currently selected core indicator is displayed.
Under the "Status Code" tab, the time trend bar chart of the currently selected core indicator, divided by status code, is displayed.
Note:
When the core indicator is selected as the bandwidth peak, the status code tab data is not supported.

4. Status Code Distribution

Displays the distribution of the currently selected core indicator in the status code dimension. By default, only the Top 4 are displayed, and other status codes are classified as "Others".
Note:
1. The status code used here is the one responded by EdgeOne nodes to the client.
2. When the core indicator is selected as the bandwidth peak, the status code distribution is not supported.

5. Country/Region Distribution

Displays the distribution of the currently selected core indicator in the country/region.

Note:

1. The data here is based on the country/region of the client, which may differ from the billing data. The regional distribution of billing data is based on the actual service user's EdgeOne node location.
2. Due to the delay and algorithm influence, the country/region distribution is for reference only, and it is suggested to refer to the actual log analytics results.

6. TOP Rankings

The TOP ranking dimensions supported by traffic analysis are as follows:

Hosts: Subdomains requested by the client.

URLs: Specific resource paths requested by the client.

Resource Type: Resource types requested by the client, such as ".png", ".json", etc.

Client IP Address: The specific source IP address of the client request.

Referers: The Referer information of the client request.

Client Device Type:

Device Type: The hardware device type used by the client request, with values:

TV: Television.

Tablet: Tablet computer.

Mobile: Mobile phone.

Desktop: Computer.

Other: Others.

Browser: The browser type used by the client request.

Operating System: The operating system type used by the client request.

Note:

1. TOP Client IP Address ranking only supports the following filter options: Host, Country/Region, HTTP version, TLS version, HTTP/HTTPS.
2. Due to the delay and algorithm influence, the TOP ranking data is for reference only, and it is suggested to refer to the actual log analytics results.
3. When the core indicator is selected as "Bandwidth Peak", the TOP ranking is not supported.

Analysis Examples

Scenario 1: Troubleshooting URLs with access errors

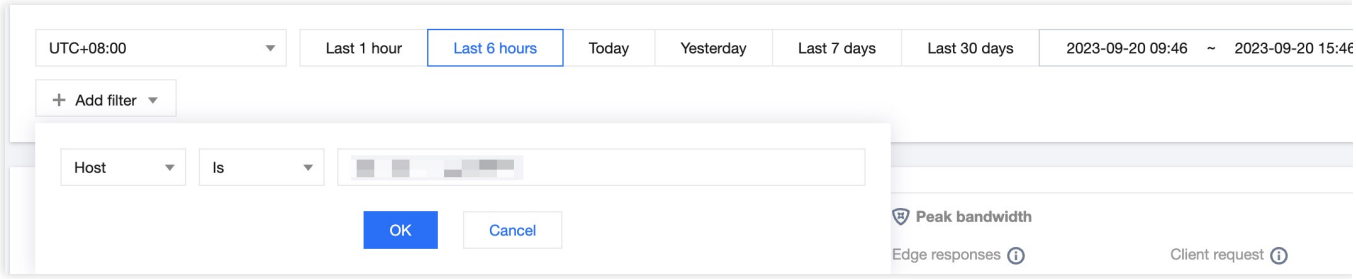
Scenario Example

After adding `www.example.com` to the EdgeOne Service through Add acceleration domain name, many end-users report that they cannot open the webpage. To analyze the cause of the problem and its impact, you can perform

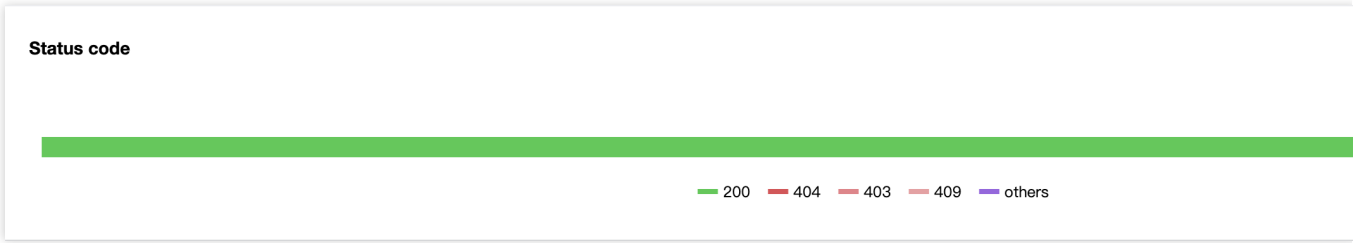
the following operations in the **Data Analysis > Traffic Analysis** page.

Directions

1. Log in to the EdgeOne console, click on the Site List in the left menu bar, and click on the site you are concerned about in the Site List to enter the Site Details page.
2. In the Site Details page, click on **Data Analysis > Traffic Analysis** to enter the Traffic Analysis page.
3. In the Traffic Analysis page, click **Add Filter**, add the filter condition `Host=www.example.com` , and click **OK**.



4. View the status code distribution, observe the proportion of abnormal status codes, and find that there are abnormal status codes "404".



5. View the time-based trend of status codes, such as a higher proportion of "404" during certain periods, which can be traced back to a higher number of business access failures during that time, requiring special attention.

6. Add filter conditions status `code=404,` and by viewing the TOP URL, you can get the specific URLs with access exceptions. In the next step, you can go to the origin to troubleshoot whether there is a problem with this URL.

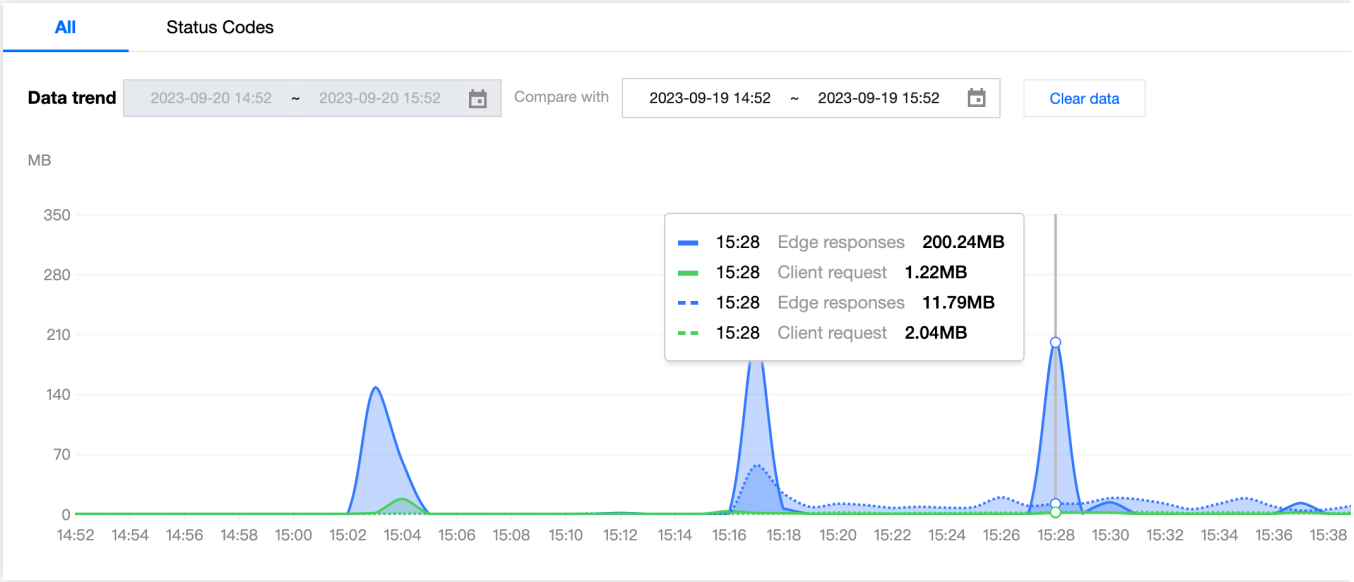
Scenario 2: Monitoring the traffic trend of all sites under the account

Scenario Example

After adding multiple sites and running them stably on EdgeOne for a period of time, you want to regularly inspect the traffic trends of all sites in the console. You can follow the steps below.

Directions

1. Log in to the EdgeOne console, and in the left menu bar, click on **Data Analysis** > **Traffic Analysis** to enter the multi-site aggregated traffic analysis page.
2. View the time trend chart, observe whether the traffic and requests have a sudden increase or decrease, and judge whether the overall business is running smoothly.
3. Click on **Compare Data** to compare the traffic curves of the same time period in the last two days, and observe whether the business has a sudden increase or decrease in day-to-day comparison.



Cache Analysis

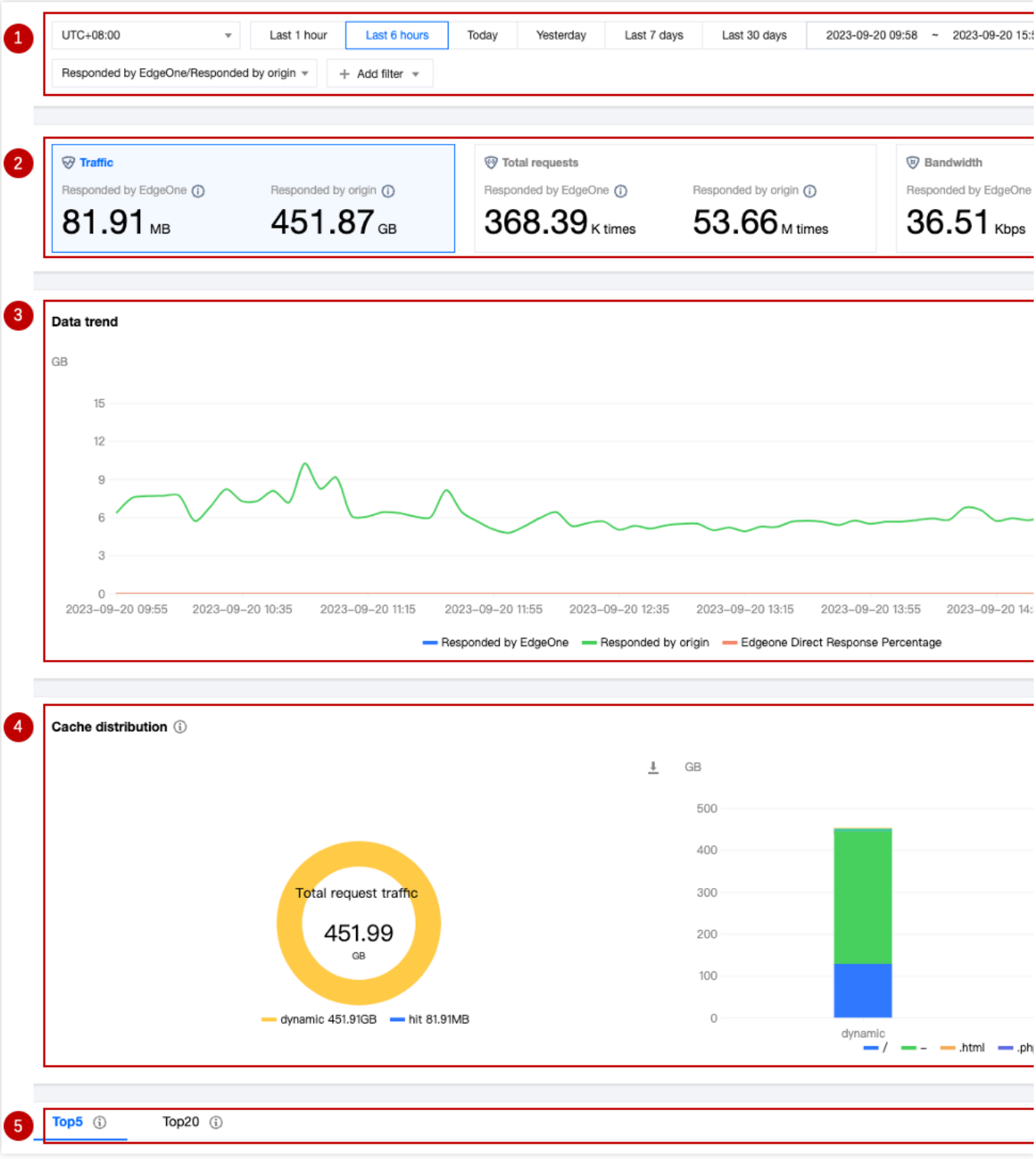
Last updated：2023-11-24 14:55:36

Overview

EdgeOne provides multi-dimensional, visualized cache analysis by analyzing L7 (application layer) access log data, including time trend curves of traffic, requests, and other metrics, cache status distribution, and TOP rankings.

Supported Capabilities

Cache analysis supports data statistics for traffic, requests, and bandwidth. You can switch between different core metrics by clicking on the data area at the top.



1. Data Filtering and Selection

Select the time range for data query. For details, please refer to Modify Query Time.

Supports filtering by site, Host, cache status, status code, and other dimensions. For details, please refer to How to Use Filters.

Supports switching the core metrics displayed on the page.

Responded by EdgeOne: Displays the traffic/requests/bandwidth peak directly responded by EdgeOne node cache.
Responded by origin: Displays the traffic/requests/bandwidth peak responded by the origin.

2. Core Metrics

Traffic: All traffic transmitted from EdgeOne to the client, i.e., downstream traffic.
Responded by EdgeOne**:** Traffic directly responded by EdgeOne node cache.
Responded by origin**:** Traffic responded by the origin.
Total requests: Requests received by EdgeOne from the client.
Responded by EdgeOne**:** Requests directly responded by EdgeOne node cache.
Responded by origin**:** Requests responded by the origin.
Bandwidth: The peak of all bandwidth transmitted from EdgeOne to the client, i.e., downstream bandwidth peak.
Responded by EdgeOne**:** Bandwidth peak directly responded by EdgeOne node cache.
Responded by origin**:** Bandwidth peak responded by the origin.
Note:
The calculation method of the bandwidth peak metric varies depending on the time granularity.
1-minute granularity: Total traffic within 1 minute * 8 / 60 seconds.
5-minute granularity: Total traffic within 5 minutes * 8 / 300 seconds.
Hourly basis: The maximum value among all 5-minute granularity bandwidth peak points.
Daily basis: The maximum value among all 5-minute granularity bandwidth peak points.

3. Data trend

Displays the time trend of the absolute values of the core metrics directly responded by EdgeOne and Origin response, as well as the time trend of the EdgeOne direct response proportion (i.e., cache hit rate) under the current core metric.

4. Cache Distribution

Cache status distribution, values include:
hit:The request hits EdgeOne's cache, and the resource is directly responded by EdgeOne.
miss:The resource can be cached, but it does not hit EdgeOne's cache, and the resource is responded by the origin.
dynamic:The resource is not eligible for caching, and the resource is responded by the origin.
other:Unable to Identify Cache state.
Cross-analysis of cache status and resource type: Displays the resource type distribution in each cache status category through bar charts.
Note:
When the core metric is "bandwidth," cache distribution is not supported.

5. TOP Ranking

The dimensions supported by cache analysis TOP ranking are as follows:

Resource Type: The resource type requested by the client, such as ".png" and ".json."
Hosts: The subdomains requested by the client.
URLs: The specific resource paths requested by the client.
Status Code: The status code responded by EdgeOne node to the client.
Note:
1. Due to the delay and algorithm's influence, TOP ranking data is for reference only. It is suggested to rely on actual log analytics results.
2. When the core metric is "bandwidth," TOP ranking is not supported.

Analysis Example

Scenario 1: Monitor the cache hit rate of the domain

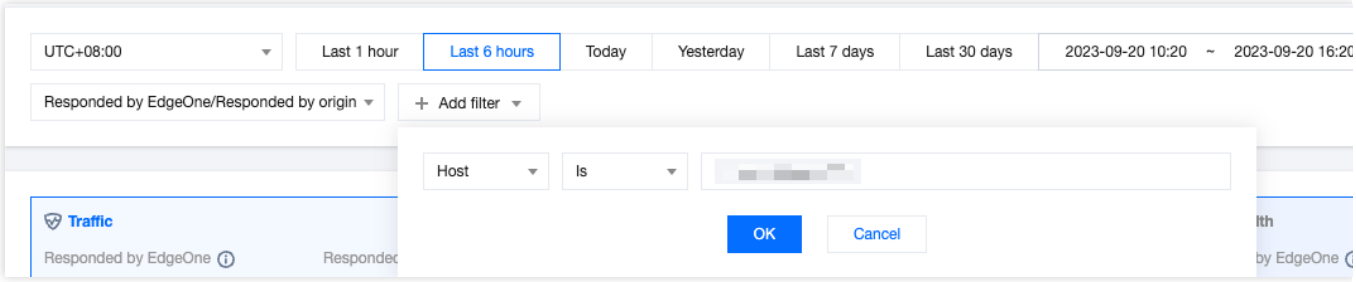
Continuously monitor the cache hit rate of the specified domain through the trend chart in cache analysis, combined with different filter items.

Scenario Example

After you Add Acceleration Domain Name and Configure Cache Policy, you want to monitor the cache hit rate of the domain `www.example.com` to evaluate and optimize the cache configuration. You can perform the following operations in the **Data Analysis > Cache Analysis** page.

Directions

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site you are interested in within the site list, and enter the site details page.
2. In the site details page, click on **Data Analysis > Cache Analysis** to enter the cache analysis page.
3. In the Cache analysis page, click on **Add Filter**, add the filter condition `Host=www.example.com` , and click **OK**.



4. In the Time Trend Chart, view the **Responded by EdgeOne** curve trend, which represents the cache hit rate trend of `www.example.com` .

5. If you think the cache hit rate is low, you can add the filter condition `Cache Status=miss`, and then view the TOP Ranking to troubleshoot the reasons for the cache hit rate not meeting expectations.
For example, observe the TOP Ranking of resource types and find that a large number of ".mp4" file extensions have not hit the cache. You can refer to Node Cache TTL Configuration to optimize the corresponding configuration.

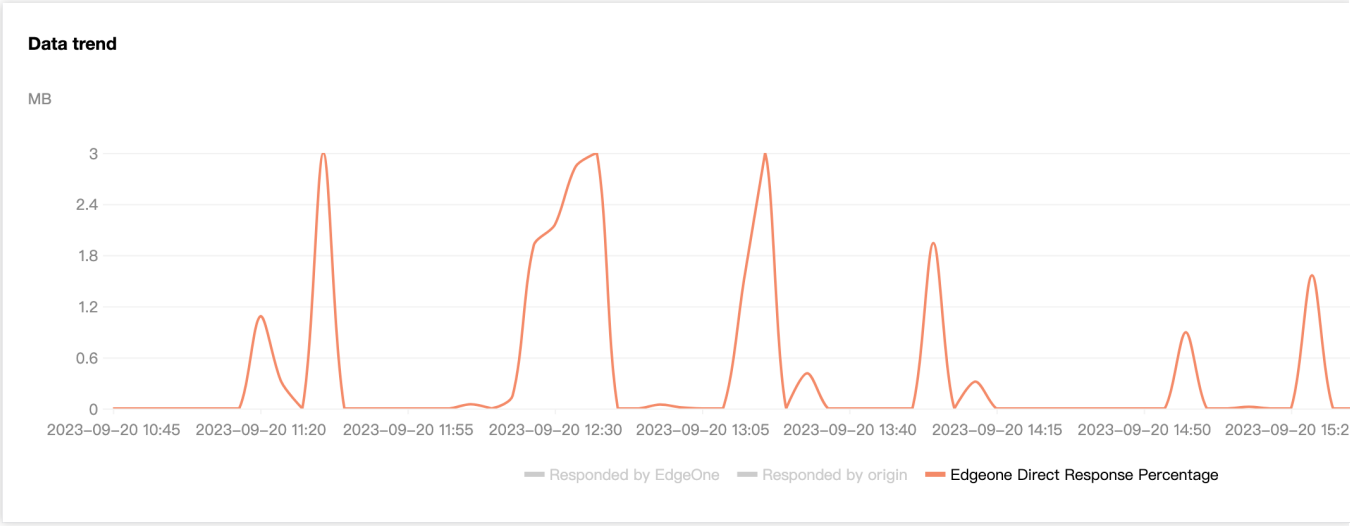
Scenario 2: Monitor the cache hit rate of all sites

Scenario Example

When all your sites are static websites and have been running stably on EdgeOne for a while, you need to monitor the cache hit rate of static resources for all sites. You can follow the steps below.

Directions

1. Log in to the EdgeOne console, click on Data Analysis > Cache Analysis in the left menu bar, and enter the cache analysis page for multiple site aggregation.
2. View the trend curve to see the aggregated data of all sites directly responded by EdgeOne.



3. In the filter, you can further select the corresponding site to view the proportion of resources directly responded by EdgeOne for the specified site.

Security Analysis
Site Security Overview

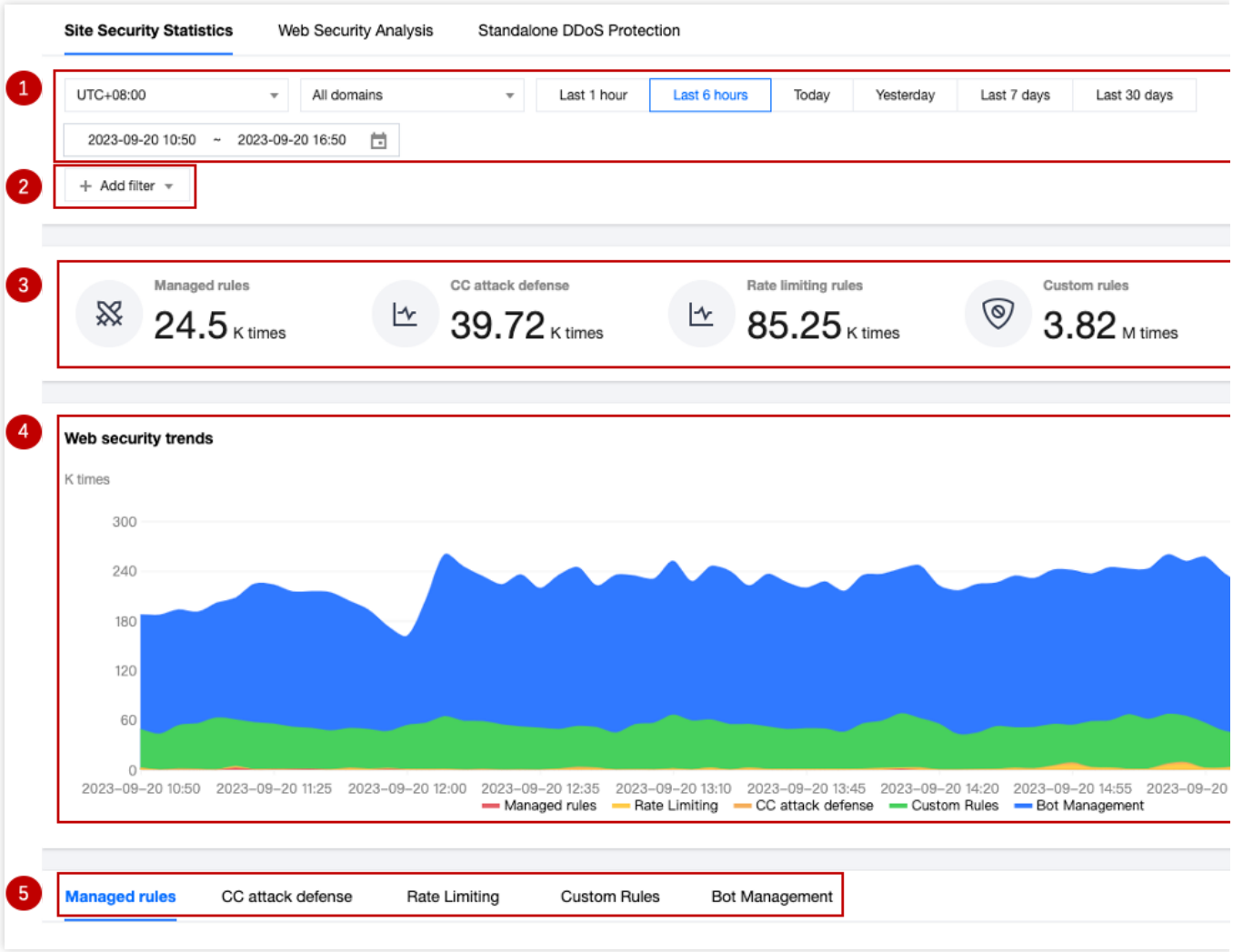
Last updated：2023-09-21 15:07:19

Overview

The Site Security Overview focuses on displaying the main security risks faced by the site. By showing the request statistics of the EdgeOne security module over a period of time, including trend charts and TOP N charts, the Site Security Overview can provide you with multiple dimensions of security risk reference: risk severity and urgency level (security event scale and trend), main objects of security risks (main target domain names, paths, etc. of attacks), and risk classification (main attack methods, such as HTTP DDoS attack, vulnerability attack, and crawler access). Through this information, you can quickly understand the current security threats faced by the site and adjust or strengthen the security policy accordingly.

Supported Capabilities

The Site Security Overview provides various statistical analysis functions, displaying the overall situation of requests hitting security rules to help you quickly assess threats.



1. Data Range

Adjust the data time range to display the security event data in different time periods.

2. Filtering and Screening

Note:

The screening conditions will take effect on all data on the page, including custom rules, rate limiting, CC attack defense, managed rules, and bot management pagination statistics.

When the amount of data queried is large, it may take a longer time to query.

The filter options supported by the Site Security Overview can be referred to as How to Use Filter Conditions.

3. Key Protection Indicator Data

Managed rules: View requests carrying vulnerability attack features that hit managed rules.

CC Attack Defense: View requests that hit CC attack defense, which may pose a risk to site availability.

Rate Limiting Rule: View requests that trigger rate limiting rules, which may abuse resources or application interfaces.

Custom rule: View requests that trigger custom rules. You can further analyze the request trend and evaluate your customized security policy.
Bot Management: View requests from automated programs (bots), including various crawler requests from search engines and automation tools.

4. Security Event Trend Chart

The trend chart helps you understand the external security risk trend over a period of time and displays the overall risk scale and the scale trend of each risk classification through a stacked chart method, helping you quickly assess the severity and priority of risks and take appropriate measures.
Note:
The trend chart is a stacked area chart, in which:
The vertical axis shows the number of requests hitting various security modules, including custom rules, rate limiting, CC attack defense, managed rules, and bot management module.
The horizontal axis shows the timestamp, corresponding to the start time of the counting window. For example, when the data is displayed at a granularity of 1 minute, the data point at 16:05:00 corresponds to the total number of requests from 16:05:00 to 16:05:59.

5. Security Event Classification Statistics Display

Indicator	Indicator Description
Hit Rule Statistics	Top 10 security protection rule hit statistics, including the host, rule ID, action, hit time, and hit request count information of the hit rules
Request Path Statistics	Top 10 data of request paths hitting security protection rules
Client IP Statistics	Top 10 statistics of client IPs hitting security protection rules
Client Distribution Statistics	Top 10 statistics of client distribution areas hitting Web Protection rules
Intercepted Malicious Client Statistics	Statistics of the number of malicious client IPs intercepted in CC attack defense
Bot Label Trend	Statistics of intercepted bot label trends

In security events, you can also click on the corresponding domain name, request path, rule ID, and client IP to quickly add them as filter conditions and view more detailed dimension statistical analysis data;
If you find that a rule ID in the security overview has intercepted normal requests, you can click on the rule ID, click on the new protection exception rule, and quickly create a new protection exception rule.

Analysis Example

Scenario 1: Viewing ongoing CC attack activities

Use the trend chart in the Site Security Overview, where the peak of the trend chart corresponds to the total number of various attacks, and the scale of CC attacks usually corresponds to the number of requests hitting rate limiting and CC attack defense.

The number of clients used for CC attacks often corresponds to the intensity of the attack and the cost input of the attackers. You can view the number of malicious clients intercepted in the CC attack defense pagination to judge the resources invested by the attackers as a reference for defense.

Note:

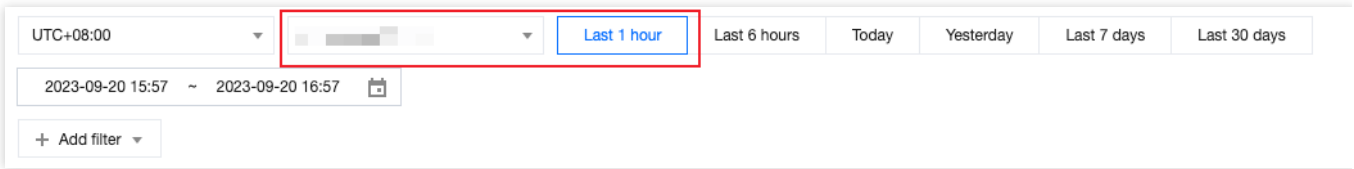
When the number of intercepted malicious clients exceeds 2000, it usually means that the attacker has invested more resources and called one or more botnet networks. Please consider upgrading to the Enterprise version and purchasing independent DDoS protection to ensure that there are sufficient protection resources to fight against the attack and avoid business losses.

Scenario Example

When your site example.com's domain name www.example.com has been subjected to a large-scale CC attack in the past hour, you need to know the information about the threat in real-time to develop targeted defense strategies or evaluate existing strategies. In addition to viewing the status code ratio on the traffic analysis page to check whether it has an impact on the business, you can also view the security module statistics in the Security Analysis > Site Security Overview page.

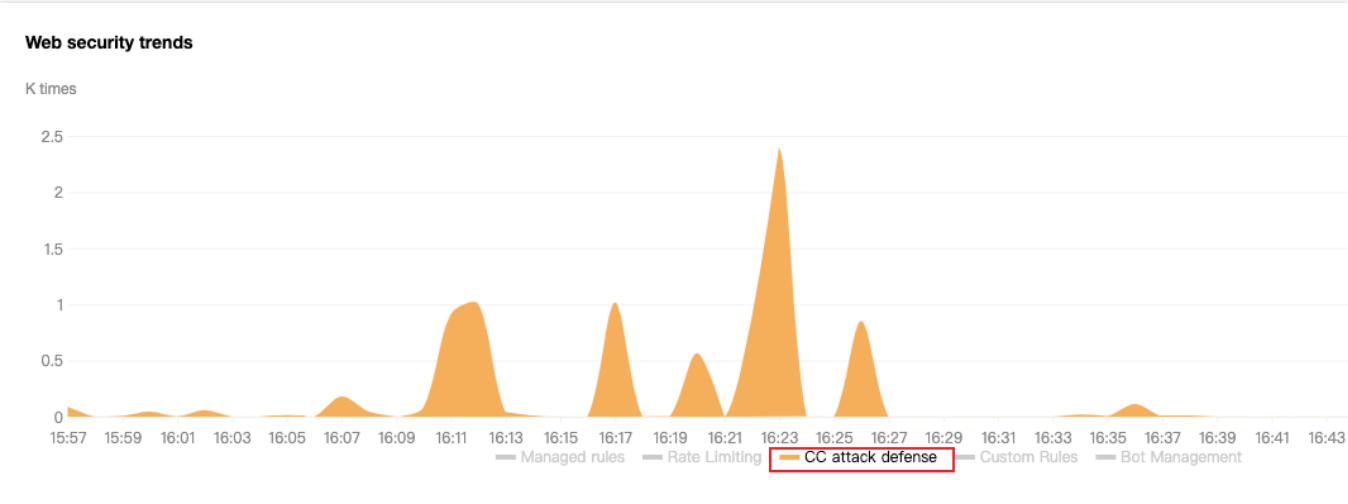
Directions

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site to be configured in the site list, and enter the site details page.
2. In the site details page, click on **Data Analysis > Security Protection**, and enter the Site Security Overview analysis page by default.
3. Modify the domain name and time range of the site to be analyzed. In this scenario, for example, select the security protection data of the domain name `www.example.com` in the past hour.

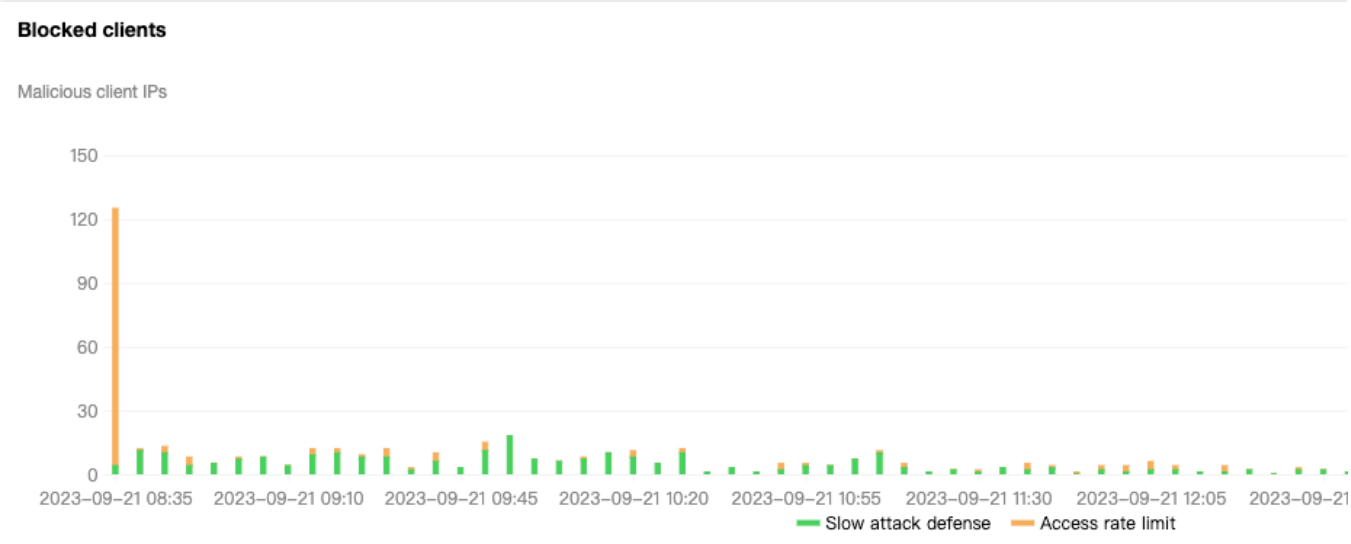


4. After filtering, the security analysis data will be automatically queried according to the filtering results. View the Web Protection trend, and you can click on the indicator value below the legend to close the display of other indicators and

only display the attack scale and trend of CC attack defense.



5. In the security classification event statistics below, click on CC Attack Defense to view the intercepted malicious client statistics, which can show the current number and trend distribution of triggered intercepted client IPs, and confirm the number of client IPs initiating the attack.



6. Switch to the CC Attack Defense and Rate Limiting pages separately to view the TOP rule list with the most hits for the domain name, thus clarifying the main target and corresponding method of the attack. Based on the analysis results, you can go to CC Attack Defense and Rate Limiting to configure and adjust the corresponding protection strategies.

Scenario 2: Assessing Vulnerability Attack Defense Strategy

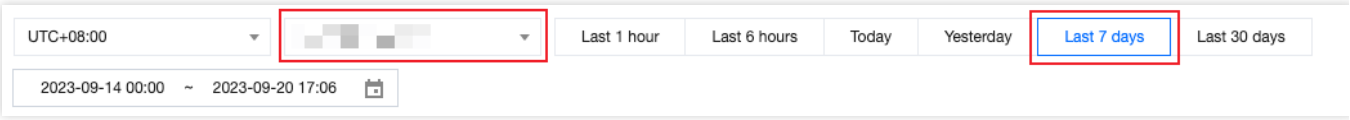
When using Managed rules to protect against vulnerability attacks, it is necessary to test and fine-tune to avoid false-positive rate. At this time, the Site Security Overview can help you evaluate the overall recognition of the rules and quickly identify rules that may have false alarms.
In general, vulnerability attacks have sporadic characteristics, and only a few scenarios (such as scanning site vulnerabilities) may have continuous hits on Managed rules. Therefore, when observing continuous hits on fixed rules, it is necessary to rule out false alarm situations.

Example Scenario

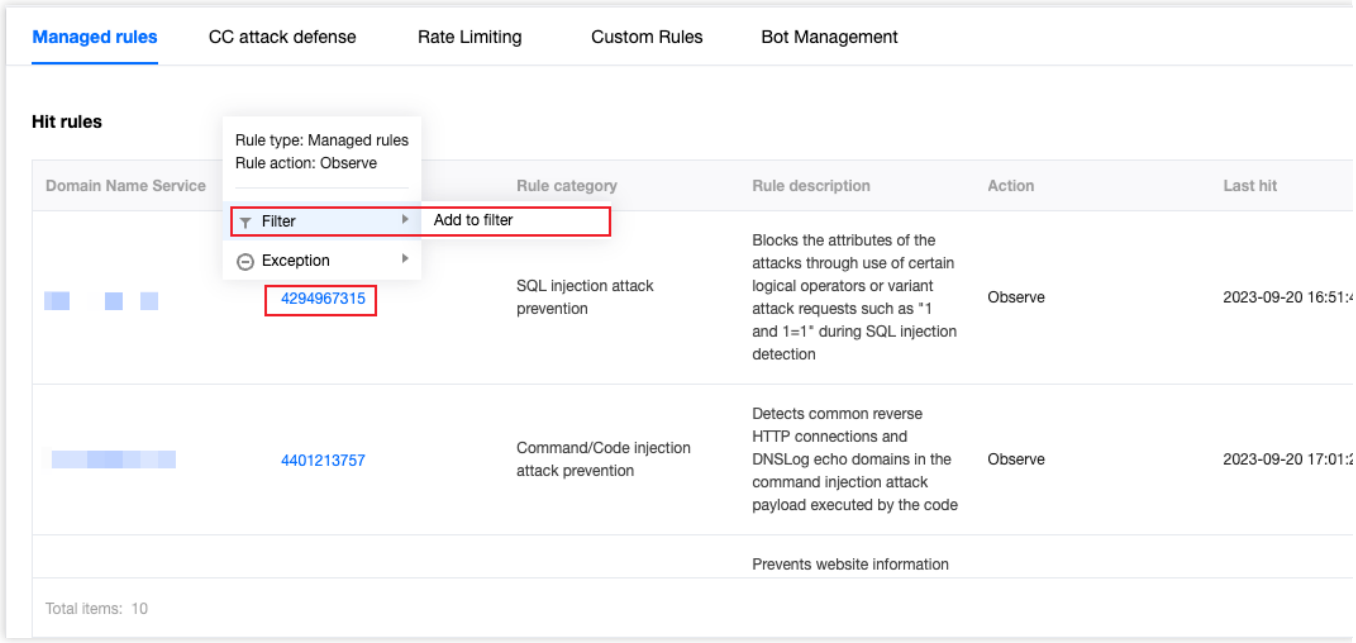
When you continuously receive feedback from different users that their current requests are blocked and they cannot access the content of the domain www.example.com within the site example.com, you need to check whether the user's request is blocked due to hitting the security protection rule and needs to be fine-tuned. In this case, the client IP is 1.1.1.1, and the user is a trusted internal test user who is also intercepted.

Directions

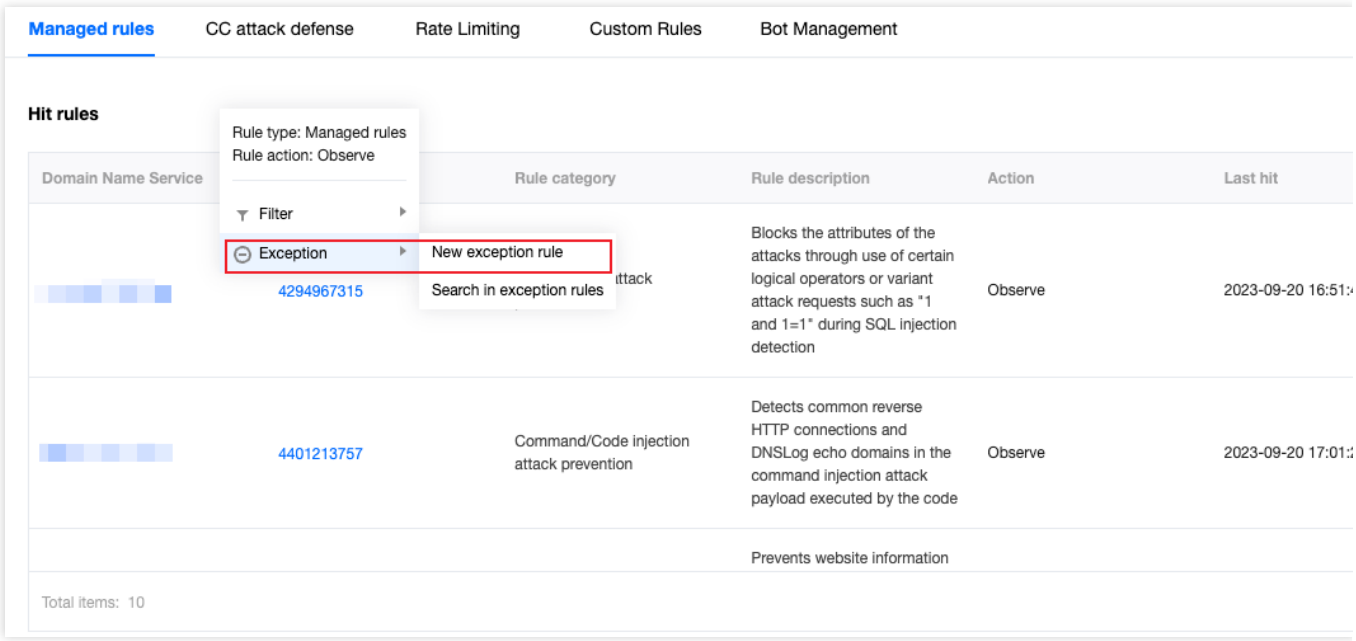
1. Log in to the EdgeOne console, click on the Site List in the left menu bar, click on the site to be configured in the Site List, and enter the Site Details Page.
2. In the Site Details Page, click Data Analysis > Security Protection, and enter the Site Security Overview analysis page by default.
3. Filter and view the domain name and time range to be analyzed. In this scenario, select the security protection data of the domain www.example.com within the last 7 days.



4. In the Managed Rules tab, view all hit rule statistics. When a large amount of requests hit a rule ID, click on the **rule ID**, select **Filter > Add to Filter**, and add the rule ID to the filter conditions to view all requests that hit the rule ID, the detailed request path, client IP, and hit trend information.



5. After analysis, if you find that the rule indeed intercepts normal path requests or client IPs, but also intercepts some abnormal business requests, you can click on the **rule ID**, select **Rule Exception > Create Protection Exception Rule**, and quickly create a new Web Protection Exception Rule. In this scenario, create a new rule and add the trusted client IP `1.1.1.1` to the protection exception rule to skip the scanning of the rule ID.



6. If you need to view more detailed rule hit logs, you can record the rule ID and use Web Security Analysis to further view the request samples that hit the rule ID to determine whether they are normal requests.

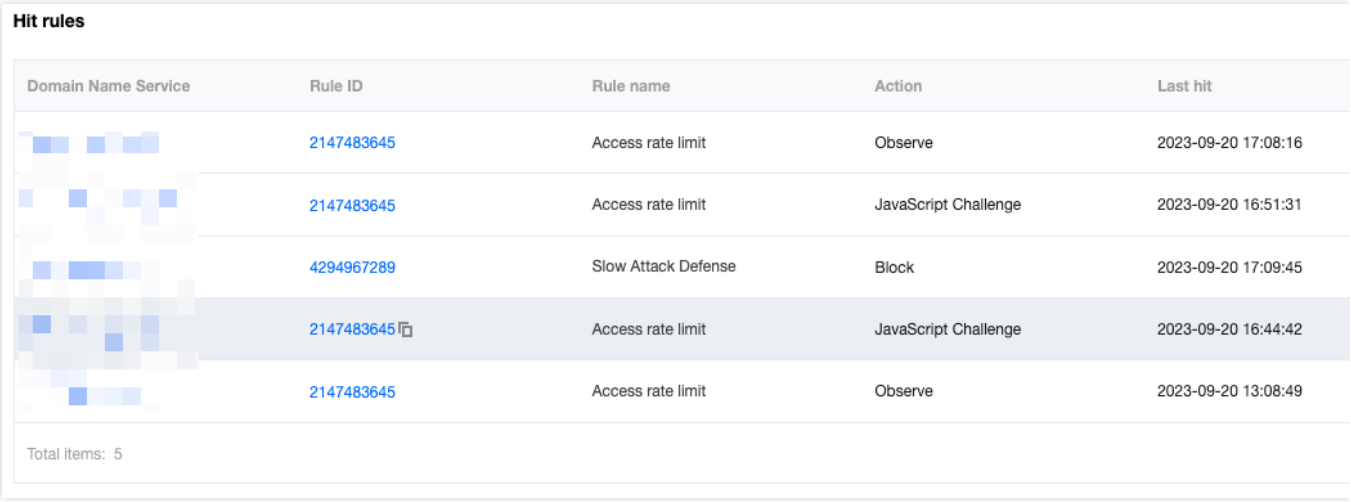
Scenario 3: Viewing the Overall Security Trend of All Sites

Example Scenario

After adding multiple sites and running EdgeOne stably for a period of time, to view the security protection trend of all sites and find out the sites and domain names that frequently encounter CC attacks for further strengthening the protection of the site domain name, you can follow the steps below.

Directions

1. Log in to the EdgeOne console, click on **Data Analysis > Security Analysis** in the left menu bar, and enter the multi-site aggregation cache analysis page, which is the Site Security Overview page by default.
2. In this page, you can view the security protection statistics of all sites. In the Security Event Classification Statistics Display below, click on CC Attack Defense to view the hit rule statistics, and you can see the domain names with the most CC rule hits, rule names, actions, and the number of requests.



3. You can further click on the corresponding domain name, add the domain name as a filter, and further analyze the trend and client distribution of the CC defense rules triggered by the domain name. Then refer to the CC Attack Defense Configuration Document to further optimize the defense strategy.

Web Security Analysis

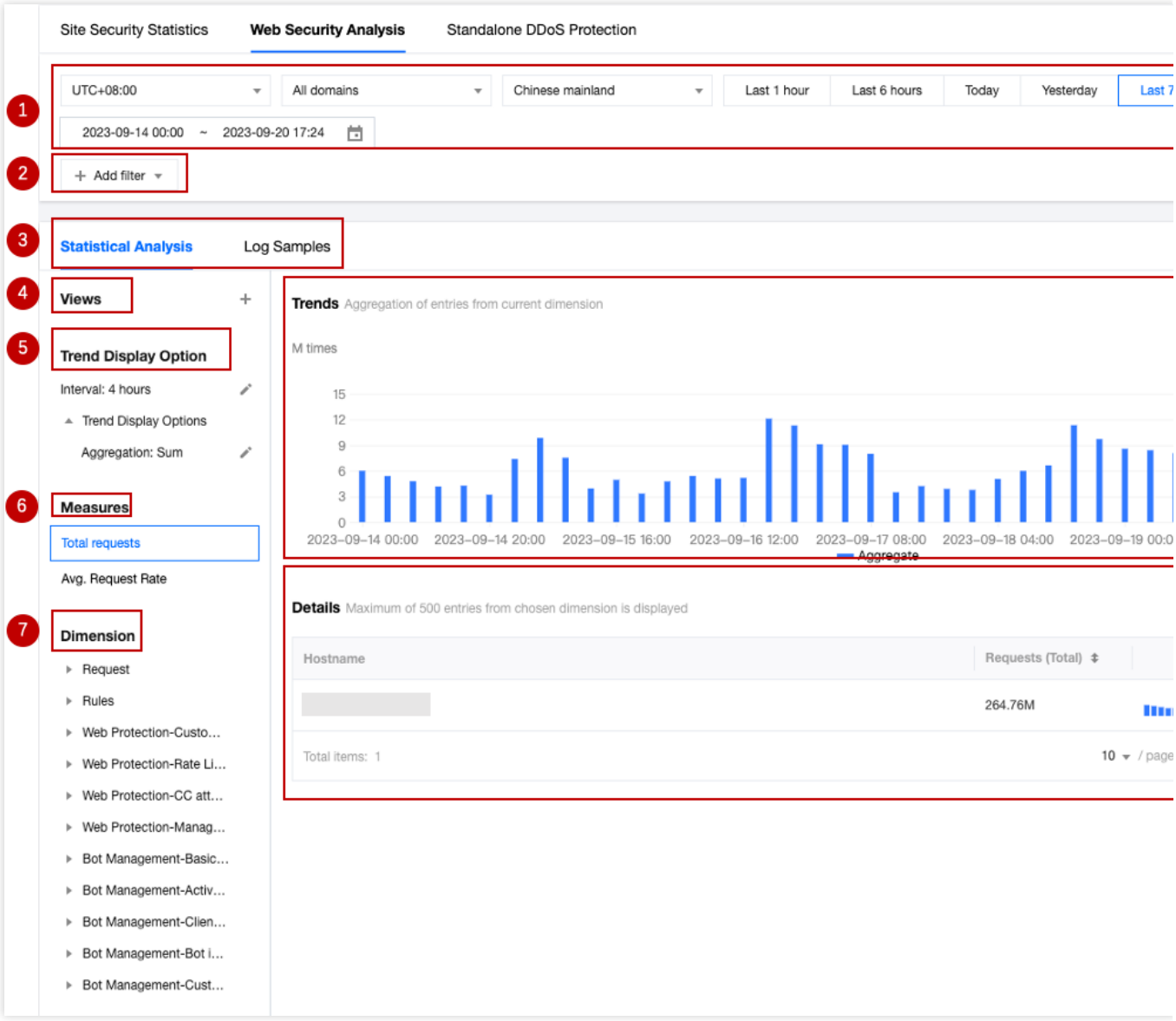
Last updated：2023-09-21 15:03:49

Overview

Web security analysis provides fine-grained analysis tools for security events, offering reference for you to formulate or adjust security policies. You can not only view the statistical analysis and distribution trends of recent security events in dozens of dimensions, but also further understand the specific content and detailed information of an event by viewing sample logs. Web security analysis provides multiple analysis dimensions for EdgeOne's web security features, helping you develop efficient security strategies.

Supported capabilities

Note:
In a security event, a single request may hit multiple security rules. When filtering or selecting statistical dimensions, please distinguish between the rule's disposal method and the request's disposal result.
For example: A request hits multiple rules with the disposal method set to observe, and also hits a rule with the disposal method set to intercept, resulting in the final disposal result of the request being intercepted.



1. Data time range

By adjusting the query time range, you can query the security events of a specific time period.

Note:

For the query time range supported by different version plans, please refer to the Comparison of EdgeOne Plans.

2. Add filter

Supports filtering Web security data by request features, rule ID, and other dimensions. For the filter items supported by Web security analysis, please refer to How to use filter conditions.

Note:

1. A single request may hit multiple rules, so when using rule ID filtering, the statistical details and trend distribution of other rules hit simultaneously will be displayed.

2. You can click on the feature value you want to filter in the statistical details to quickly add it to the filter.

3. Analysis dimensions

Statistical analysis: Helps you display the ranking of indicators by the selected dimension, discover abnormal access volume and abnormal access trends. For example: When you choose to display by User-Agent header dimension, you can view the distribution of accessed devices and access indicator trends, thus identifying devices with abnormal access volume and suspicious access behavior with uniform speed cycle.
Sample logs: Help you further view the details of security events and determine whether the security policy hit by the request meets expectations. For example: You can view the managed rules hit by the request and the field content matched by the managed rules through sample logs, which will help you determine whether it is a false intercept and adjust the security policy accordingly.

4. Common views

You can save the current view options as a common view for quick access later according to your needs. You can name the view, which will save the current trend display options, statistical indicators, and statistical dimension information.

5. Trend display statistical method

Note:
When adjusting the data filter time range, the data granularity will be adjusted accordingly to ensure an appropriate trend chart display.
You can adjust the trend chart display options as needed:
Data granularity: The data statistics duration corresponding to each column in the trend chart.
Aggregation method: The calculation method of the data corresponding to each column in the trend chart.
Sum: Displays the sum of all indicators of the statistical items in the selected dimension filtered data within that time period. For example: In the statistical period corresponding to a column in the trend chart, there are 6000 requests, and the column displays data as 6000.
Average value: Displays the average value of all indicators of the statistical items in the selected dimension filtered data within that time period. For example: When displaying statistical data by Host dimension, the data contains 5 Host data, and in the statistical period corresponding to a column in the trend chart, there are 6000 requests, then the column displays data as 6000 / 5 = 1200.
Maximum value: Displays the maximum data item in the selected dimension split data within that time period.
99th percentile value: Displays the minimum value of the data items greater than 99% in the selected dimension split data within that time period, i.e., this value is greater than 99% of the other statistical item indicator values.
99.9th percentile value: Displays the minimum value of the data items greater than 99.9% in the selected dimension split data within that time period, i.e., this value is greater than 99.9% of the other statistical item indicator values.

6. Statistical indicators

You can choose to display the number of requests or the average request rate indicator to display the required statistical features (such as rate features or request number features).

Number of requests: Displays the total number of requests by the current statistical dimension, used to distinguish the characteristics of visitors with a large number of requests. For example: Analyzing by request Host dimension can distinguish the concentrated business domain names.
Average request rate: Calculates the average request rate by the current statistical dimension, used to distinguish the characteristics of visitors with high access frequency. For example: Analyzing by User-Agent header dimension can distinguish the device types with abnormal access frequency.

7. Statistical dimensions

Web security analysis provides the following analysis dimension categories, and you can adjust the statistical objects and grouping methods according to the selected dimensions:
Statistical dimensions classified by request attributes include:
Client IP: Counts the number of requests from different client IPs.
Client IP (XFF header priority): Counts the number of requests from different client IPs. If the client accesses through a Web proxy, the IP of the most recent hop in the XFF header will be counted.
User-Agent: Counts requests from different device types (distinguished by HTTP User-Agent header).
Request URL: Counts requests accessing different URLs (including access paths and query parameters).
Hostname: Counts requests accessing different domains (distinguished by HTTP header Hostname).
Request Referer: Counts requests accessing resources using different referencing methods (distinguished by HTTP Referer header).
Statistical dimensions classified by rule attributes include:
Category: Counts requests hitting different security modules (such as custom rules, managed rules, etc.).
Rule ID: Counts requests hitting different rules.
Note:
1. You can use the rule ID option in the rule classification to merge and display requests hitting all security protection rules.
2. You can also use the rule ID option in the specific security feature classification to view only the situation of hitting rules in that module. For example: Count requests by the rule ID of the Web Protection custom rules hit.
3. Different version plans support different statistical dimensions, please refer to the Comparison of EdgeOne Plans for details.
You can also choose other analysis options provided by the protection features, such as the hit field of managed rules, the bot label of bot intelligent analysis, etc., to perform statistical analysis.

8. Statistical trend chart

The statistical trend chart will display the corresponding aggregated data bar chart according to your trend display options and filter conditions.

9. Statistical details

Displays the request feature values of different dimensions and their corresponding indicators according to your statistical dimension and statistical indicator options. For example: When the number of `requests indicator` and `User-Agent` analysis dimension are selected, the statistical details section will display the number of requests for different client device types (User-Agent header values), displayed in descending order of the number of requests, and the request trends of each device type.

Analysis example

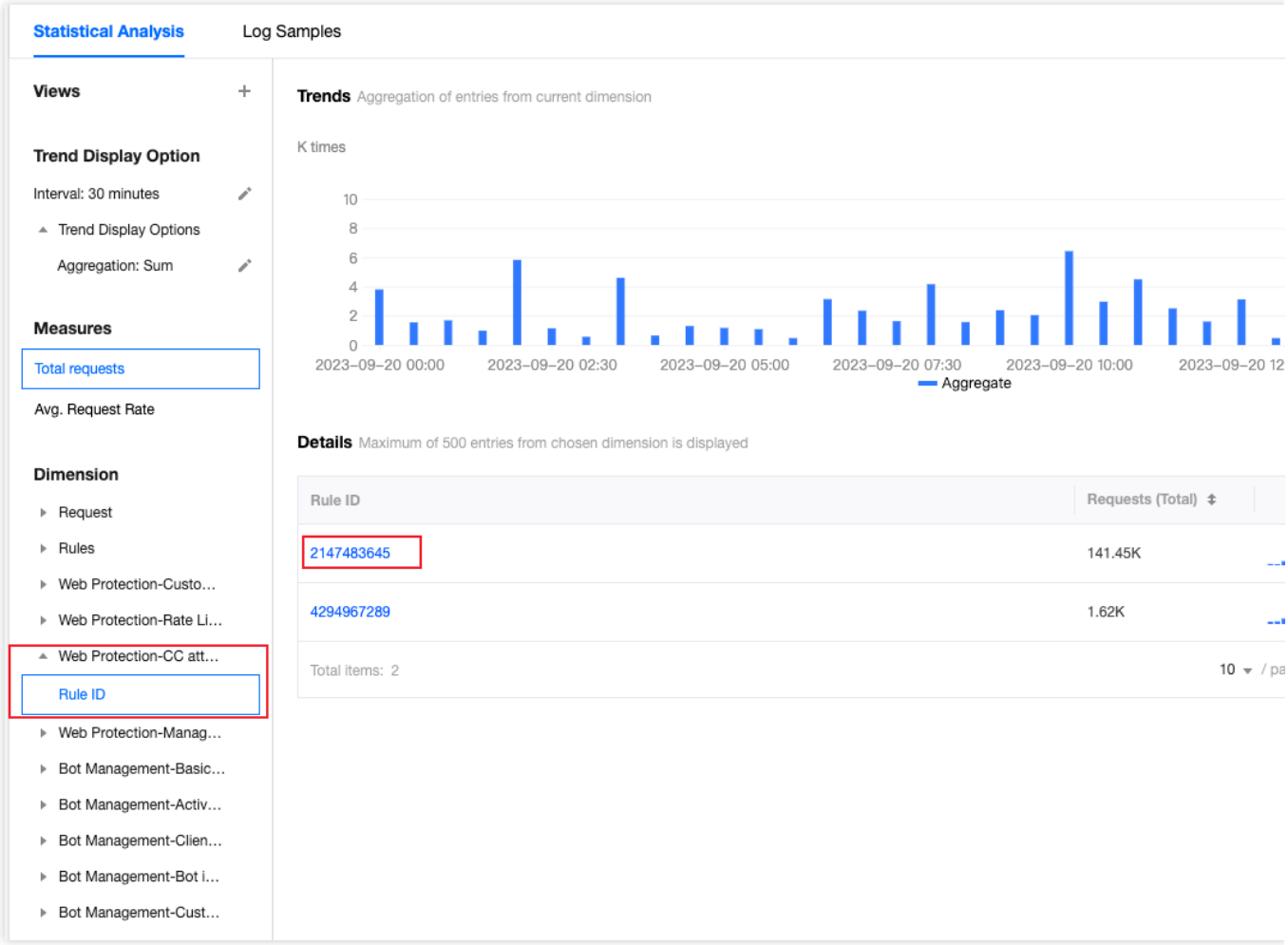
Scenario 1: Analyze the request trend of CC attack defense in the past 1 day

Scenario example

Suppose your site `example.com` finds a suspicious surge in access volume, hitting the CC attack defense rule. To analyze whether all requests hitting CC attack defense in the past 1 day are normal requests, you can follow the steps below for analysis.

Directions

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site to be configured in the site list, and enter the site details page.
2. In the site details page, click on **Data Analysis > Security Protection**, and enter the site security overview analysis page by default. Click on **Web Security Analysis** at the top.
3. Filter and view the domain name, time range, and aggregation conditions of the site to be analyzed. In this scenario, you can select the time range within the past 1 day.
4. In the statistical analysis, click on **Web Protection-CC Attack Defense > Rule ID**.



5. View the data results. As shown in the figure above, the number of requests triggered by intelligent client filtering is very high (Rule ID: 4294967293). You can click on the rule ID to add it to the filter. Then click on Request > User Agent in the left statistical dimensions to view the summary information of all User Agent headers hitting the rule. You can judge whether the User Agent value meets your normal client expectations. You can also continue to add other statistical dimensions in the statistical dimensions, such as Client IP and Request URL, to further narrow down the filter range.

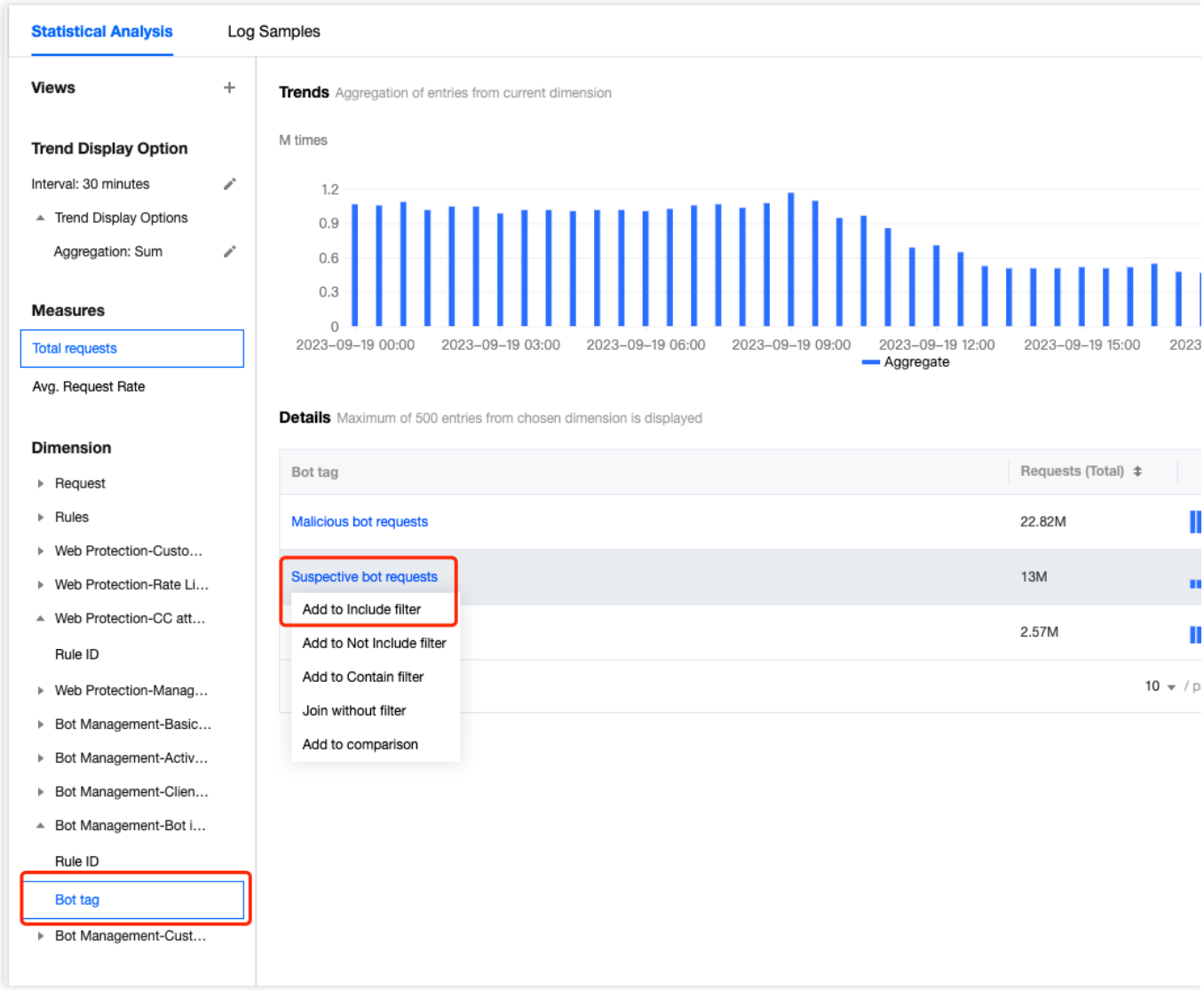
Scenario 2: Analyze whether there are abnormal requests in suspicious bot requests within the last 1 day

Scenario Example

Suppose your site `example.com` has recently been frequently visited by suspicious bots, and you need to analyze whether all suspicious bot request accesses in the past 1 day are normal requests. You can refer to the following steps for analysis.

Directions

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site to be configured in the site list, and enter the site details page.
2. On the site details page, click **Data Analysis > Security Protection**, and enter the site security overview analysis page by default. Click Web Security Analysis at the top.
3. Filter and view the domain name, time range, and aggregation conditions of the site to be analyzed. In this scenario, you can select the time range within the past 1 day.
4. In the statistical analysis, click **Bot Management-Bot Intelligent Analysis > Bot Tag**.
5. Query the data results, and in the statistical details, you can see the request times of the corresponding bot tags. In this scenario, you can click **Suspective Bot Requests > Add Equal Filte**r for further analysis. After adding the filter condition, you can also continue to add other statistical dimensions in the statistical dimension, such as User-Agent to further narrow the filter range.



6. Click Sample Log to switch to detailed sample log analysis. Click the arrow on the left side of each log to expand and view the detailed request header and hit rules situation to determine whether the request is a normal request.

L4 Proxy

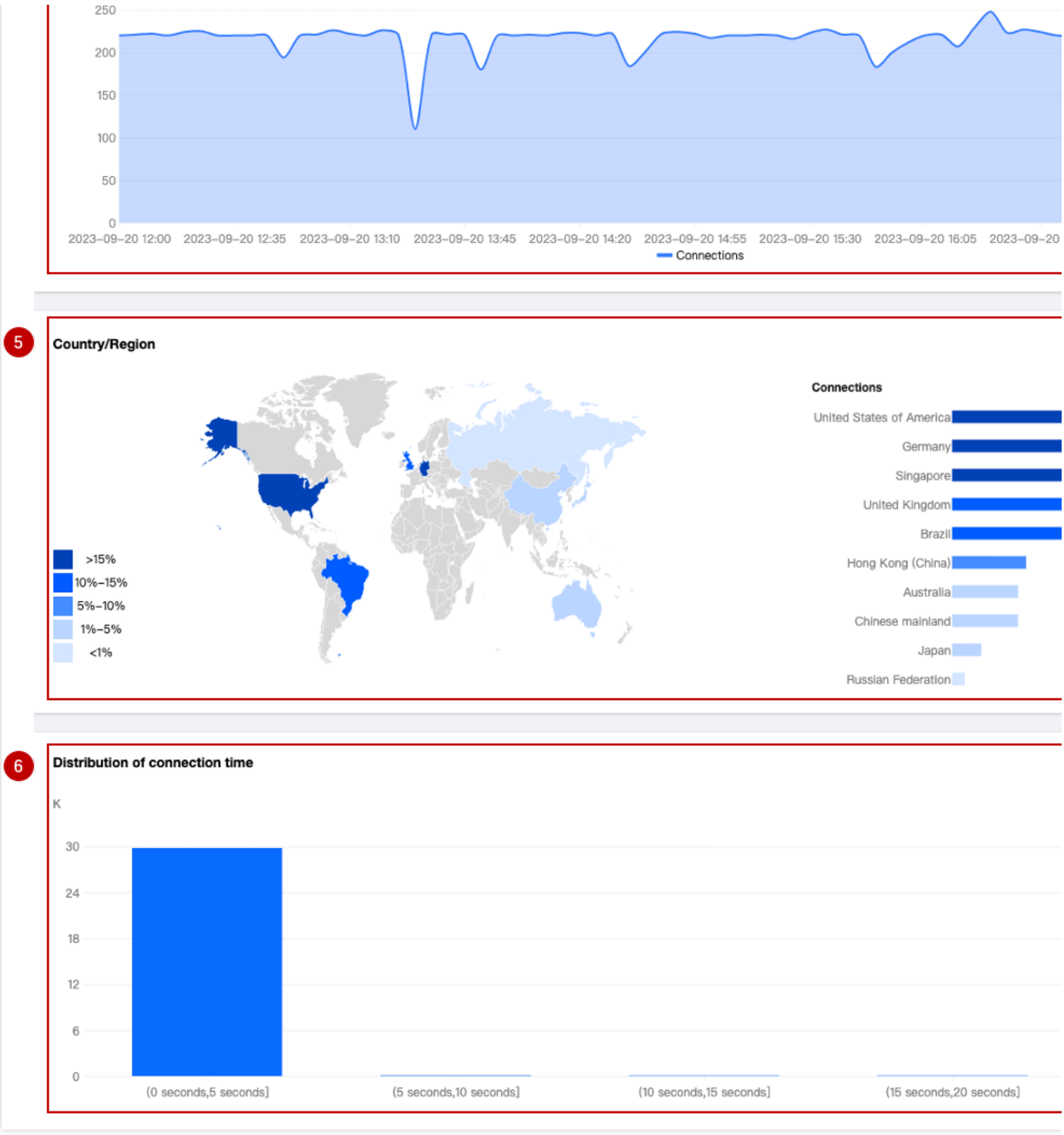
Last updated：2023-09-21 11:36:39

Overview

EdgeOne provides data analysis and display of user access to L4 (transport layer) proxy instances by analyzing L4 access logs, including traffic, connection count, connection duration, and other data, helping you better monitor the operation of L4 proxy instances.

Supported capabilities

The L4 proxy analysis page supports the statistical display of traffic, connection count, connection duration, and other data for L4 proxy instances, and supports adding filtering conditions.



1. Data filtering and filtering

Supports selecting the time range for data query, for details, please refer to How to modify the query time range.
Supports filtering by site, service name, forwarding rules, country/region, and other dimensions, for details, please refer to How to use filtering conditions.

2. Core indicators

Outbound traffic: Traffic transmitted from EdgeOne nodes to clients.
Inbound traffic: Traffic received by EdgeOne nodes from client requests.

Connections: The number of connections that exist within the selected time range.
Connection time (95th percentile): For connections that exist within the selected time range, the 95th percentile of connection duration is calculated, i.e., this value is greater than 95% of other connection durations.

3. Time trend chart - Traffic

Displays the time-sharing trend curve of outbound and inbound traffic.

4. Time trend chart - Connection count

Displays the time-sharing trend curve of connection count.

5. Country/Region distribution

Displays the distribution of connection count in countries/regions.
Note:
1. The data here is based on the country/region of the client, and may differ from billing data. The regional distribution of billing data is based on the actual region where the EdgeOne node serving the client is located.
2. Due to the delay and algorithm, the country/region distribution is for reference only, and it is suggested to refer to the actual log analytics results.

6. Connection duration distribution

Displays the histogram distribution of connection duration.

Analysis examples

Scenario 1: Monitor the traffic and connection count indicators of L4 proxy instances in a certain country

Under certain filtering conditions, the time trend chart on the L4 proxy analysis page can be used to monitor the operation of L4 proxy instances.

Scenario example

After you create a new L4 proxy instance, if you want to monitor the traffic and connection count indicators of the L4 proxy instance named example in Singapore, you can perform the following operations in the **Data Analysis > L4 Proxy page**.

Directions

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site you are interested in within the site list, and enter the site details page.
2. In the site details page, click on **Data Analysis > L4 Proxy** to enter the L4 Proxy page.

3. In the L4 Proxy page, click **Add Filter**, add filtering conditions `Service Name=example` `Country/Region=Singapore` , and click Confirm.
4. View the time trend chart of traffic and connection count, observe whether there is a sharp increase or decrease, and determine whether the business you are concerned about is running normally.

Scenario 2: View the overall operation trend of L4 proxy instances for all sites

Scenario example

After you have added multiple L4 proxy instances to multiple sites and they have been running stably on EdgeOne for a period of time, you may want to regularly inspect the traffic trend of L4 proxy services usage for all sites in the console. You can follow the steps below.

Directions

1. Log in to the EdgeOne console, click on **Data Analysis > L4 Proxy** in the left menu bar, and enter the aggregated data analysis page for multiple sites.
2. View the time trend chart, observe whether the traffic and connection count have a sharp increase or decrease, and determine whether the overall business is running normally.
3. In the connection count card, click Compare Data to compare the traffic curve for the same time period in the last two days, and observe whether the business has a sudden increase or decrease in day-to-day comparison.

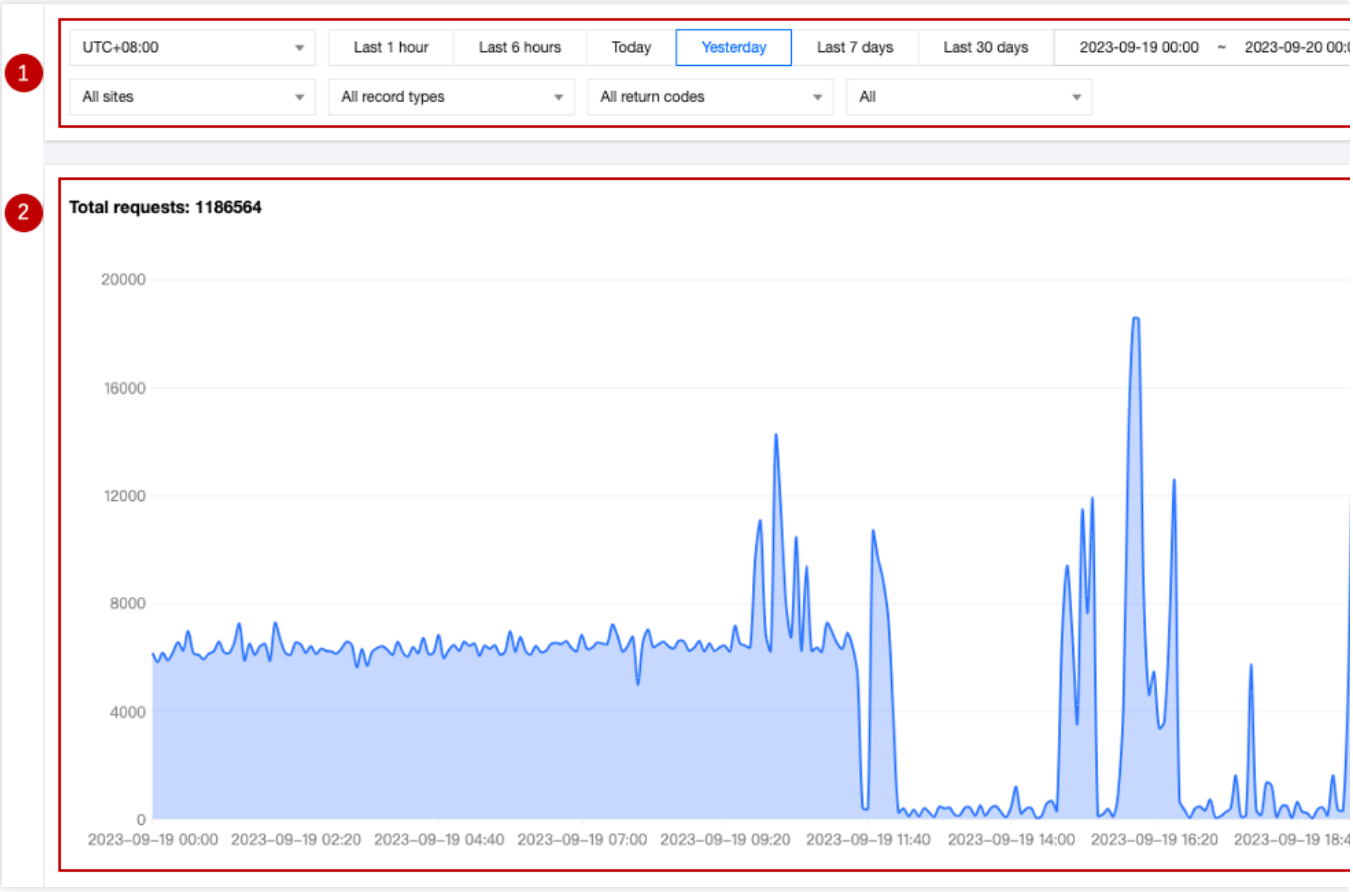
DNS Resolution

Last updated：2023-09-21 11:37:43

Overview

This page mainly displays the number of resolution requests received by EdgeOne DNS. Only data from sites that support NS mode access is available.

Supported Capabilities



1. Data Screening and Filtration

Select the time range for data query, for details, please refer to How to Modify the Query Time Range.
Filter by site, subdomain, record type, return code, client request region, and other dimensions, for details, please refer to How to Use Filter Conditions.

2. Time Trend Chart

Display the time-sharing trend curve of the number of EdgeOne DNS requests.

Analysis Instances

Scenario 1: View the DNS resolution performance of a specified site

Example Scenario

After the site `example.com` is accessed through NS mode to EdgeOne, you need to view the related DNS resolution request times, you can follow the steps below.

Directions

1. Log in to the EdgeOne console, click on the site list in the left menu bar, click on the site you are interested in within the site list, and enter the site details page.
2. In the site details page, click on **Data Analysis > DNS Resolution** to enter the DNS resolution subpage.
3. On the DNS resolution subpage, you can view the trend of all resolution request times under the site. You can also further filter statistical data based on subdomains, record types, return codes, and regional dimensions.

Scenario 2: View the DNS resolution performance of all sites

Example Scenario

When all your sites are accessed through NS mode to EdgeOne, if you need to query the DNS resolution request times and changing trends of all sites, you can follow the steps below.

Directions

1. Log in to the EdgeOne console, and in the left menu bar, click Data Analysis > DNS resolution to enter the multi-site aggregation data analysis page.
2. On this page, you can view all the resolution requests and trends under all sites. You can also further filter statistical data based on site, record type, return code, and region dimensions by using filter conditions.

Related References

How to use filter condition

Last updated：2023-09-21 11:32:08

Currently, EdgeOne data analysis supports two types of filtering conditions:
1. Time filtering condition (required): View the data within the selected time range, for details, please refer to How to modify the query time range.
2. Other filtering conditions: Customize the data filtering according to the filtering options supported by each page. The following is a detailed explanation of this part.

Supported Operators

Operator	Description
Equal	Query data with the filter item equal to any specified value
Does not equal	Query data with the filter item not equal to any specified value
Contain	Query data with URL, Referer, and resource type containing the specified string (e.g., query URL contains /example data)
Does not contain	Query data with URL, Referer, and resource type not containing the specified string (e.g., query URL does not contain /example data)
Starts with	Query data with URL, Referer, and resource type prefix matching the specified string
Does not start with	Query data with URL, Referer, and resource type prefix not matching the specified string
Ends with	Query data with URL, Referer, and resource type suffix matching the specified string
Does not end with	Query data with URL, Referer, and resource type suffix not matching the specified string

Relationship between multiple filtering conditions

The relationship between multiple filtering conditions is "And", and the relationship between multiple values within the same filtering condition is "Or".

For example, adding filtering conditions `Country/Region=Singapore` ; Thailand and `Status Code=404` means querying data that meets the access from Singapore or Thailand clients and the edge response status code is 404.

Filtering options supported by different data analysis pages

Traffic Analysis

Site: Filter data belonging to different sites, support multiple selection, only available in multi-site aggregated data analysis.
Host: The host requested by the client, supports multiple selection, only available in single-site data analysis.
Country/Region: The country or region where the client request comes from, supports multiple selection.
Status Code: The status code of EdgeOne responding to the client, supports multiple selection, only available in single-site data analysis.
HTTP: The HTTP version used by the client request, supports multiple selection, values are:
HTTP/1.0
HTTP/1.1
HTTP/2.0
HTTP/3.0 (QUIC Protocol)
Websocket Over HTTP/1.1 (Websocket protocol initiated by HTTP/1.1)
TLS Version: The TLS protocol version used by the client request, supports multiple selection, only available in single-site data analysis. Values are:
TLS 1.0
TLS 1.1
TLS 1.2
TLS 1.3
URL: The URL path (path) requested by the client, only available in single-site data analysis. Supports entering multiple values, separated by semicolons. For example: /example1;/example2
Referer: The referer of the client request, only available in single-site data analysis. Supports entering multiple values, separated by semicolons.
Resource Types: The resource type requested by the client, only available in single-site data analysis. Supports entering multiple values, separated by semicolons. For example: .txt;.jpg
Device Type: The device type of the client request, derived from the User-Agent in the HTTP request header, supports multiple selection, only available in single-site data analysis. Values are:
TV
Tablet
Mobile
Desktop

Other
Empty
Browser: The browser type used by the client request, only available in single-site data analysis. Supports multiple selection.
System Type: The operating system type used by the client request, only available in single-site data analysis. Supports multiple selection.
IP Version: The IP address version used by the client request, only available in single-site data analysis. Values are:
IPv4
IPv6
HTTP/HTTPS: The HTTP protocol type used by the client request, values are:
HTTP
HTTPS
Province: The province where the client request comes from, only available in single-site data analysis. Only available for sites in the Chinese mainland.
Carrier: The carrier where the client request comes from, only available in single-site data analysis. Only available for sites in the Chinese mainland.
Note:
1. When the core indicator is selected as "Bandwidth Peak", only the "Country/Region", "Host", "HTTP/HTTPS", and "HTTP Version" filtering options are supported.
2. Different plans may support different filtering conditions, for details, please refer to Plan Comparison.

Cache Analysis

Site: Filter data belonging to different sites, support multiple selection, only available in multi-site aggregated data analysis.
Host: The host requested by the client, supports multiple selection, only available in single-site data analysis.
Cache Status: The cache status of the client request, only available in single-site data analysis. Values are:
Hit: The request hits the EdgeOne node cache, and the resource is provided by the node cache.
Miss: The request does not hit the EdgeOne node cache, and the resource is provided by the origin.
Dynamic: The requested resource cannot be cached/is not configured to be cached by the node, and the resource is provided by the origin.
Status Code: The status code of EdgeOne responding to the client, supports multiple selection.
URL: The URL path (path) requested by the client, only available in single-site data analysis. Supports entering multiple values, separated by semicolons. For example: /example1;/example2
Resource Type: The resource type requested by the client, only available in single-site data analysis. Supports entering multiple values, separated by semicolons. For example: .txt;.jpg

Security Analysis

Site Security Overview

Request Disposal Result: Only view requests that hit security rules and apply the corresponding action (excluding release or exception rules).
Request Path: Only view request data for specific request paths.
Rule ID: Only view request data that hits specific rules.
Client IP: Only view request data from a specific client IP.
Host: Only view request data for a specific domain service.

Web Security Analysis

Supports filtering based on request features, rule features, and detailed Web Protection rules and Bot management policies features. The description of the related filtering options for request features is as follows:
Client IP: Only view request data from a specific client IP, supports entering multiple values, separated by Enter.
Client IP (XFF Header Priority): Only view request data from a specific client IP, if the client accesses through a Web proxy, the first IP in the XFF header will be used for filtering. Supports entering multiple values, separated by Enter.
User Agent: The User Agent information carried in the client request, supports entering multiple values, separated by Enter.
URL: Only view request data for a specific URL (excluding Host, only including request path and query parameters), supports entering multiple values, separated by Enter.
Hostname: The host requested by the client, supports entering multiple values, separated by Enter.
Request Referer: The referer carried in the client request, supports entering multiple values, separated by Enter.
Applied action: Only view requests that hit specific security rules and apply the corresponding action, supports multiple selection. For detailed request disposal result descriptions, please refer to Web Protection action and Bot Management action.
Request Path: Only view request data for a specific path (HTTP request path, excluding Host and query parameters). Supports entering multiple values, separated by Enter.
Request JA3 Fingerprint: View request data matching a specific JA3 fingerprint.
Request Method: Only view request data using a specific HTTP Method to access the site, supports multiple selection.
Request ID: Only view specific requests (the request ID is the same as the request ID in the interception page and log, corresponding to a unique request).

DNS Resolution

Site: Filter data belonging to different sites, support multiple selection, only available in multi-site aggregated data analysis.
Subdomain: The host requested by the client, supports multiple selection, only available in single-site data analysis.
Record Type: DNS record type, for values please refer to Record Type.
Return Code: DNS resolution response status code. Values are:
NOError: No error, successful response

NXDomain: Non-existent record

NotImp: Not implemented, DNS server does not support the requested query type; implemented request query types refer to Record Type.

Refused: Refused, DNS server refuses to execute the specified operation due to policy.

Area: The continent where the client request comes from, currently supports the following options:

Asia

Europe

Africa

Oceania

America

How to Modify Query Time Range

Last updated：2023-09-21 11:31:39

The EdgeOne data analysis page supports users to custom filter the time range. The following mainly introduces two ways to filter the time range.

Note:

In order to improve the query efficiency, the granularity of data in different time ranges is as follows:

Time Range ≤ 2 hours: 1 minute.

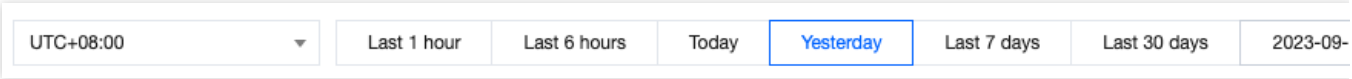
2 hours < Time Range ≤ 48 hours: 5 minutes.

48 hours < Time Range ≤ 7 days: 1 hour.

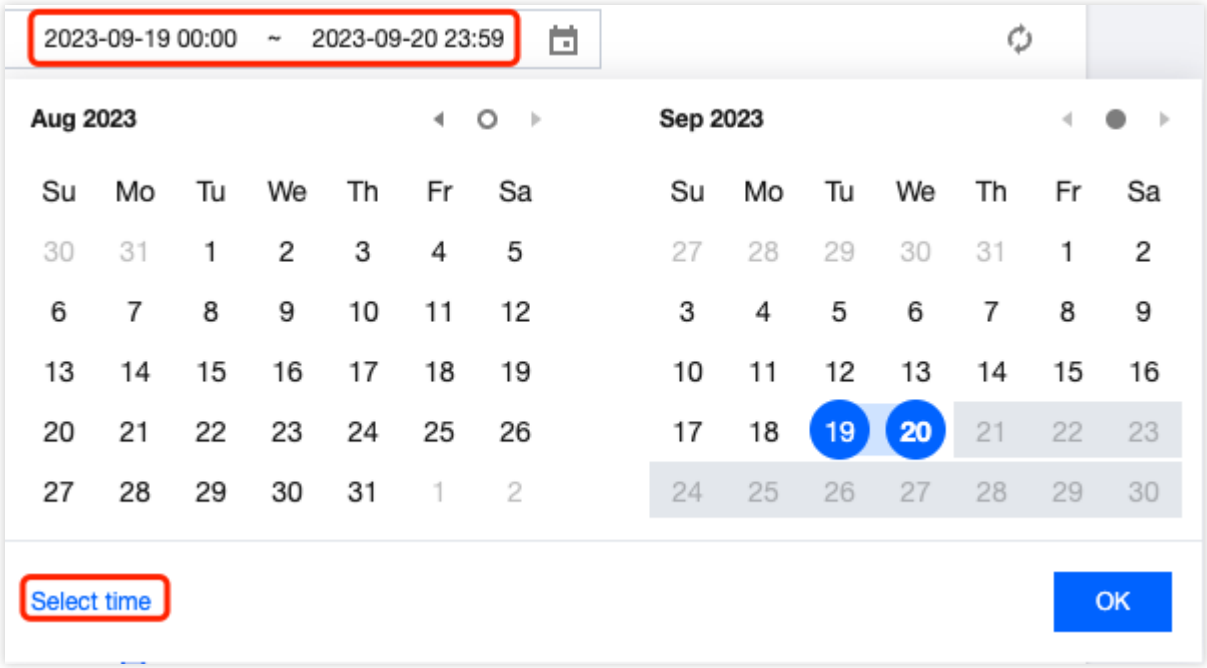
Time Range > 7 days: 1 day.

Method 1: Set the query time range through the filter bar

Quick Query: Quickly query the corresponding time range data by clicking on the buttons such as "Last 1 hours", "Last 6 hours", "Today", "Yesterday".



Custom Query: You can query the data within the custom time range by selecting a specific date and time range.

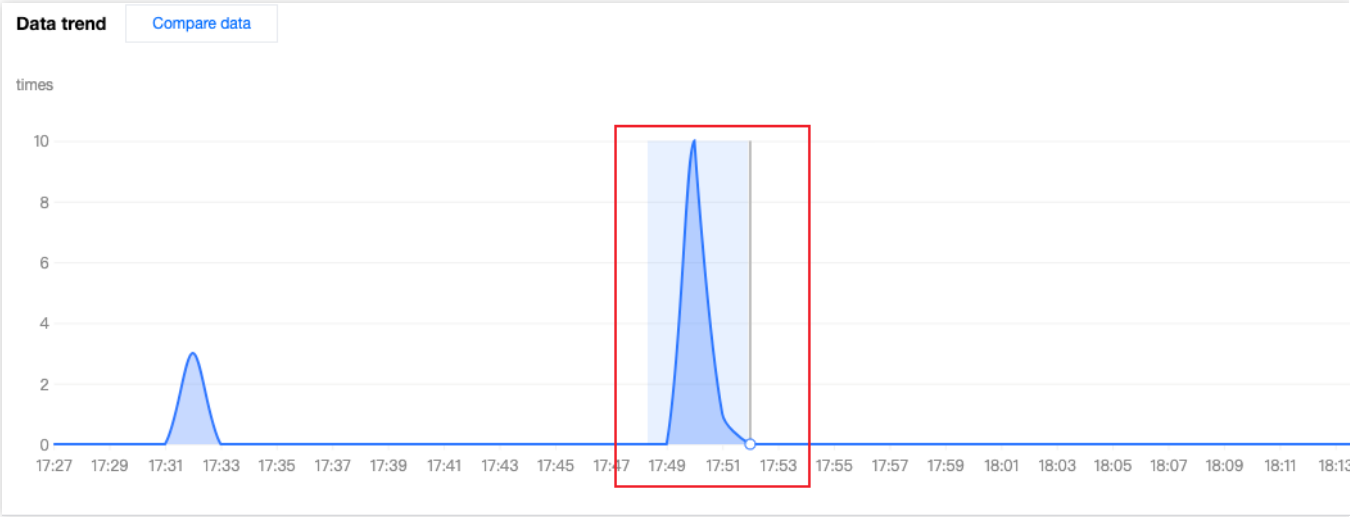


Note:

1. When you select "Last 1 hours", "Last 6 hours", "today", the page will Show the data of the last 1 hour, 6 hours, and the current day (starting from 00:00) and refresh every 5 minutes.
2. The maximum query time range for a single time is 31 days.
3. Due to different Plan versions, different sites may support different data query ranges. For details, please refer to the Plan selection comparison.
4. To be compatible with data queries of different Plans, directly clicking on the data analysis in the left navigation bar only supports querying data for the last 61 days.

Method 2: Select the query time range on the time trend chart

If you want to View the specific time period on the curve, as shown in the figure below, you can select the specific region of the curve by clicking and sliding the mouse on the curve. The time range corresponding to this region will be backfilled to the top filter bar and affect the statistics of other data on the page.



How to Export Statistical Data and Reports

Last updated：2024-01-02 10:31:34

This document describes how to export statistical data and reports from the EdgeOne data analysis page. The specific steps are as follows.

Exporting Statistical Data

1. Log in to the EdgeOne Console and enter any **Data Analysis** page.
2. Click  to download the corresponding statistical data table. The file format is .csv and the filter conditions on the current page will be applied to the exported data.

Export Report

1. Log in to the EdgeOne Console and enter any **Data Analysis** page.
2. Click on the  located on the top-right corner of the filter bar. EdgeOne will then initiate the browser's print window where you may choose to print or save your report as a PDF. The filter conditions on the current page will be printed in your report at the same time.