Tencent Cloud EdgeOne

Data Analysis&Log Service

Product Documentation

Contents

Data Analysis&Log Service
- Log Service
  - Overview
  - Real-time Logs
    - Real-time Logs Overview
    - Push to Tencent Cloud CLS
    - Push to AWS S3-Compatible COS
    - Push to HTTP Server
  - Offline Logs
  - Related References
    - Field description
      - L7 Access Logs
      - L4 Proxy Logs
    - Real-Time Log Push Filter Conditions
    - Custom Log Push Fields
- Data Analysis
  - Overview
  - Traffic Analysis
  - Cache Analysis
  - Security Analysis
    - Site Security Overview
    - Web Security Analysis
  - L4 Proxy
  - DNS Resolution
  - Related References
    - How to use filter condition
    - How to Modify Query Time Range
    - How to Export Statistical Data and Reports
- Analytics

Data Analysis&Log Service
Log Service
Overview

Last updated：2024-07-15 09:31:09

The site acceleration, L7 security protection, and other feature modules of EdgeOne global availability zone nodes support recording detailed logs when processing requests for your services. The CLS module collects and aggregates logs from various feature modules, and then provides the logs to users. You can use the log details for troubleshooting, checking the impact of configuration updates, generating monitoring metrics, etc.

Supported Features

Real-time Log Push: Ships the access request logs to your specified destination with low latency, and supports configuration through the console or API. The latency from initiating a request to receiving the logs by the destination is within 5 minutes. It is suitable for scenarios requiring high timeliness such as real-time troubleshooting and monitoring. The recording scopes for various types of request logs are described as follows.
Site Acceleration Logs: Records the domain access logs. By default, only the logs of requests after protection are recorded. Logs of the requests blocked by Anti-DDoS are not recorded.
Note:
The feature of Real-time Logs - Site Acceleration Logs to record full L7 request logs (including L7 protection block logs) is in beta testing. If needed, please contact us.
L4 Proxy Logs: Records the access logs of L4 proxy instances. Only the logs of accesses after protection are recorded. Logs of the accesses blocked by Anti-DDoS are not recorded.
Rate Limiting and CC Attack Protection Logs: Only records the request logs that match the security rules of the L7 Protection - Rate Limiting and CC Attack Protection module, no matter whether the requests are blocked or not.
Managed Rule Logs: Only records the request logs that match the security rules of the L7 Protection - Managed Rules module, no matter whether the requests are blocked or not.
Custom Rule Logs: Only records the request logs that match the security rules of the L7 Protection - Custom Rules module, no matter whether the requests are blocked or not.
Bot Management Logs: Only records the request logs that match the security rules of the L7 Protection - Bot Management module, no matter whether the requests are blocked or not.
Offline Logs: By default, the access logs are retained for 30 days. You can obtain the download URL for the log package via the console or API. Usually, the download URL for the log package is available 3 hours after a request is initiated, and the integrity of the logs within the log package will be guaranteed after 24 hours. It is suitable for scenarios not requiring high timeliness, such as long-term log retention and periodic reconciliation.

Site Acceleration Logs: Records the domain access logs. Only the logs of requests after protection are recorded. Logs of the requests blocked by Anti-DDoS are not recorded.
L4 Proxy Logs: Records the access logs of L4 proxy instances. Only the logs of accesses after protection are recorded. Logs of the accesses blocked by Anti-DDoS are not recorded.

Package Support Differences

Sub-feature	Individual Edition	Basic Edition	Standard Edition	Enterprise Edition
Real-time Log Push	2 Task/Log Types	2 Task/Log Types	3 Task/Log Types	5 Task/Log Types
Offline Logs	Supported. The log retention duration is 30 days.			

Billing Description

Real-time Log Push

EdgeOne Real-time Log Push is a value-added service, charged based on the number of logs pushed. Typically, when log push filter conditions or log sampling is not enabled, the greater the volume of requests for accessing your business, the more the logs generated correspondingly. For billing standards, see VAU Fee (Pay-as-You-Go).
It's important to note that after you configure real-time log push tasks, the destination of log shipping may also incur charges. For example, after configuring log push to Tencent Cloud CLS, traffic and storage charges may be generated for the Tencent Cloud CLS product. For details, refer to CLS Billing Overview.

Offline Logs

After accessing EdgeOne, you will obtain the offline logs feature by default, without any additional charges.

Real-time Logs
Real-time Logs Overview

Last updated：2024-07-15 09:31:09

Feature Overview

After your site accesses EdgeOne, you will obtain abundant pre-built reports that can 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:

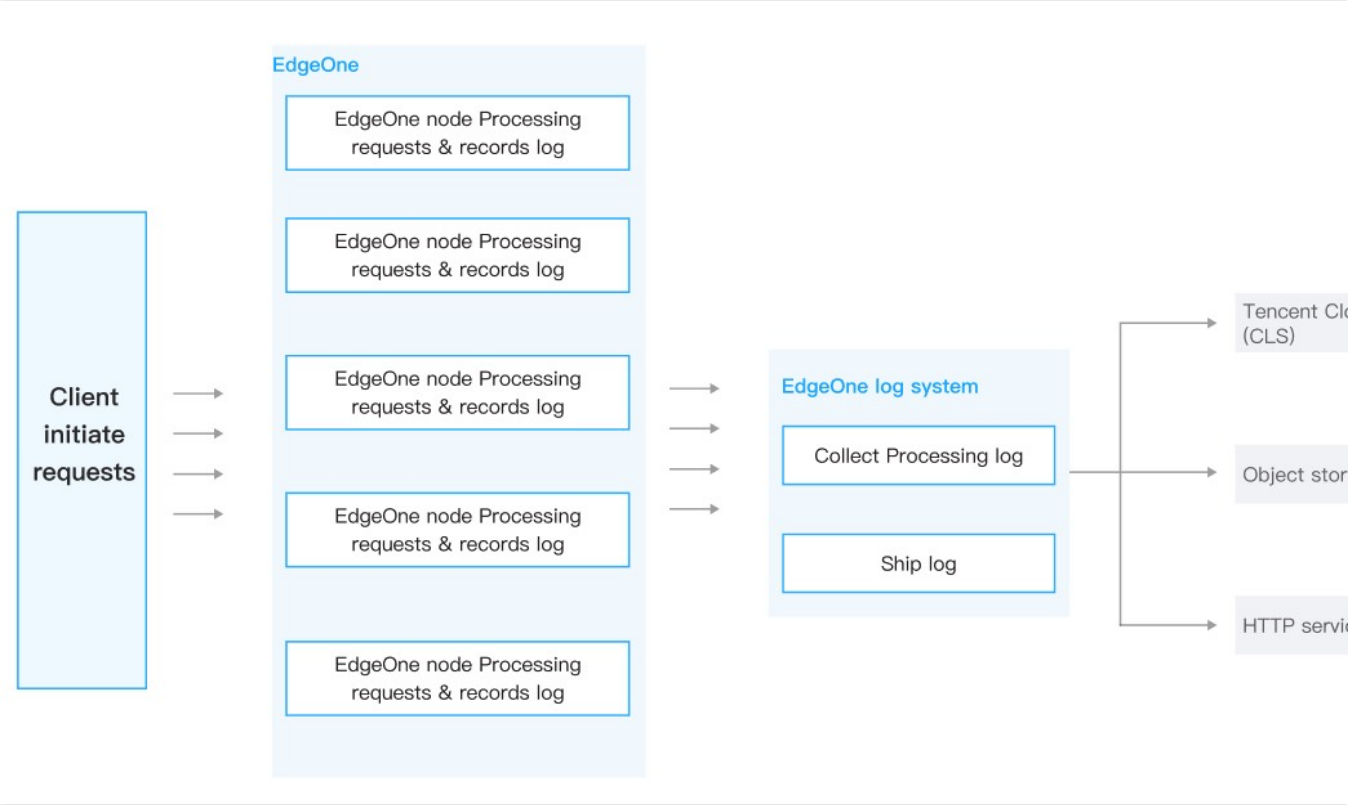
Scenario	Scenario Demands
Deep Data Analysis	Specify 1 or more conditions, to search logs that meet the conditions. For example: Specify the client IP, to query the access statistics (access URL, number of accesses, etc.) within a specified time range. Filter by status code, time, and URL, to analyze the detailed distribution of status codes. Filter out the logs processed by observation, and summarize the request header content and other request characteristics carried, to 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. The access efficiency includes the overall response time of EdgeOne, download speed, origin-pull response time, etc.
Identifying Hotlinking	Analyze the traffic exceptions, access modes, and access frequencies, to identify client IPs with behaviors such as hotlinking.
Unified Monitoring of Data from Multiple Cloud Vendors	Monitor the application data from multiple cloud vendors through a self-built data dashboard.
Log Storage	Retain user-related access logs for 30 days or longer.

For the above scenario demands, the EdgeOne real-time log service provides the ability to collect and push logs in real-time. It supports pushing your logs to Tencent Cloud Log Service (CLS) or your self-built data center, and helps you independently perform flexible search and analysis of log data. Currently, EdgeOne supports pushing logs to the following destinations:

Push to Tencent Cloud CLS: Pushes logs to the one-stop Tencent Cloud Log Service (CLS) for further log search and analysis.

Push to AWS S3-Compatible COS: Pushes logs to storage buckets compatible with the authentication method of AWS Signature V4.

Push to HTTP Server: Pushes logs to a specified backend server via HTTP POST requests.



Note:

Under normal circumstances, the latency of log shipping is within 5 minutes. To ensure real-time log shipping, EdgeOne pushes logs to a corresponding destination in batches based on a fixed number of logs or a fixed time period. The default policy is pushing 1,000 log entries per batch preferentially. When the log entries are less than 1,000, but the time interval from the last push is 5 seconds, it will also trigger a second push.

Billing and Quota Description

Refer to Package Support Differences and Billing Overview.

Push to Tencent Cloud CLS

Last updated：2024-07-15 09:31:09

EdgeOne Real-Time Log Push supports pushing logs to Tencent Cloud Log Service (CLS). You can configure it through the console or API. For more information about CLS, refer to CLS Product Documentation.

Prerequisites

1. Log in to the Tencent Cloud CLS console and activate CLS.
2. If you wish to use a sub-account for CLS-related operations, refer to CLS Permission Management Guide, to complete sub-account authorization and ensure that the sub-account has related read and write permissions for CLS log sets and log topics.

Note:
You must authorize EdgeOne to access your log sets and log topics through the service role `TEO_QCSLinkedRoleInRealTimeLogCLS` . EdgeOne will use the service role to query log sets and log topics, modify index configurations, and push logs.

Directions

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. Then click on the **site** to be configured in the site list, to enter the site details page.
2. On the site details page, click **Log Service** > **Real-time Logs**.
3. On the real-time logs page, click **Create Push Task**.
4. On the log source selection page, enter a task name, select a log type, service area, and domain name/L4 proxy instance requiring log push, and click **Next**.
5. On the push content definition page:

(Required) Check the log fields to be pushed from the predefined field list.
(Optional) Add a custom log field, which supports extracting specified field names from the request headers, response headers, and Cookie headers.
(Optional) Configure the log push filter conditions. Full logs are pushed by default.
(Optional) In advanced configuration, set the sampling ratio. By default, sampling is not enabled and 100% of logs are pushed to the destination.
(Optional) In advanced configuration, set the log output format. The default format is JSON Lines.

Note:
For pushing logs to CLS, only the JSON format can be selected. Prefixes, suffixes, and separators are not effective.

6. On the destination selection page, select **CLS** and click **Next**.
7. On the destination information page, select the region, log set, and log topic for the destination log set.
8. Click **Push**, confirm the related cost tips in the pop-up window, and click **Confirm Creation**.
9. In the pop-up window, select the index configuration method. It is recommended to click **Quick Index Configuration**. EdgeOne will create a key-value index for the previously selected log topic. You can also configure the index yourself in the CLS Console. Note that if Key-Value Index is not enabled, you will fail to search logs.

Note:

When the log volume is too large, and the log topic auto-split feature of CLS is disabled or the partition value has reached its limit, CLS will restrict the log push request frequency, which may result in log data loss. To avoid such issues, refer to CLS Log Topic for configuration.

Push to AWS S3-Compatible COS

Last updated：2024-07-15 09:31:09

EdgeOne Real-time Log Push supports configuration through the console or API, to push logs to AWS S3 Signature Version 4 Authentication Algorithm compatible COS, such as:
Tencent Cloud COS
AWS S3
Google Cloud Storage
IBM Cloud Object Storage
Linode Object Storage
Oracle Cloud Object Storage, etc

Directions

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. Then click on the **site** to be configured in the site list, to enter the site details page.
2. On the site details page, click **Log Service** > **Real-time Logs.**
3. On the real-time logs page, click **Create Push Task.**
4. On the log source selection page, enter a task name, select a log type, service area, and domain name/L4 proxy instance requiring log push, and click **Next**.

Note:
Currently, it only supports pushing site acceleration logs and L4 proxy logs to S3-compatible COS.

5. On the pushing content definition page:
(Required) Check the log fields to be pushed from the predefined field list.
(Optional) Add a custom log field, which supports extracting specified field names from the request headers, response headers, and Cookie headers.
(Optional) Configure the log push filter conditions. Full logs are pushed by default.
(Optional) In advanced configuration, set the sampling ratio. By default, sampling is not enabled and 100% of logs are pushed to the destination.
(Optional) In advanced configuration, set the log output format. The default format is JSON Lines.
6. On the destination selection page, select **S3-compatible** and click **Next**.
7. On the destination information page, enter the related destination and parameter information.

Parameter Name	Description
Endpoint URL	URL not containing a bucket name or path, for example: `https://cos.ap-nanjing.myqcloud.com` .

Bucket Region	Region where the bucket is located, for example: `ap-nanjing` .
Bucket	Bucket name and log storage directory, for example: `your_bucket_name/EO-logs/` . No matter whether the directory ends with `/` or not, it will be correctly parsed and processed.
File Compression	After checking, log files will be compressed with gzip.
SecretId	Access key ID used to access the bucket.
SecretKey	Secret key used to access the bucket.

8. Click **Push**, confirm the related cost tips in the pop-up window, and click **Confirm Creation**.
9. After issuing the real-time log push task, EdgeOne will push a test file to the destination bucket directory to verify the connectivity, for example, `1699874755_edgeone_push_test.txt` . The file contains a fixed string "test".

File Name Description

Logs are stored in the specified bucket directory in the format `{{UploadTime}}_{{Random}}.log` , and archived by date (UTC+00:00) into folders, for example: `20230331/20230331T185917Z_2aadf5ce.log` . When gzip compression is enabled, the file name is `20230331/20230331T185917Z_2aadf5ce.log.gz` .
UploadTime: Upload time of the log file, in ISO-8601 format with UTC+00:00 time zone.
Random: Random characters used to identify different files when there are multiple log files in the same upload time due to large log volume.

Push to HTTP Server

Last updated：2024-07-15 09:31:09

EdgeOne Real-time Log Push supports pushing logs to a custom API address. You can configure it through the console or API. EdgeOne can use an HTTP POST request to call the backend API address you provide, and transfer logs in the HTTP body to a server you specify.

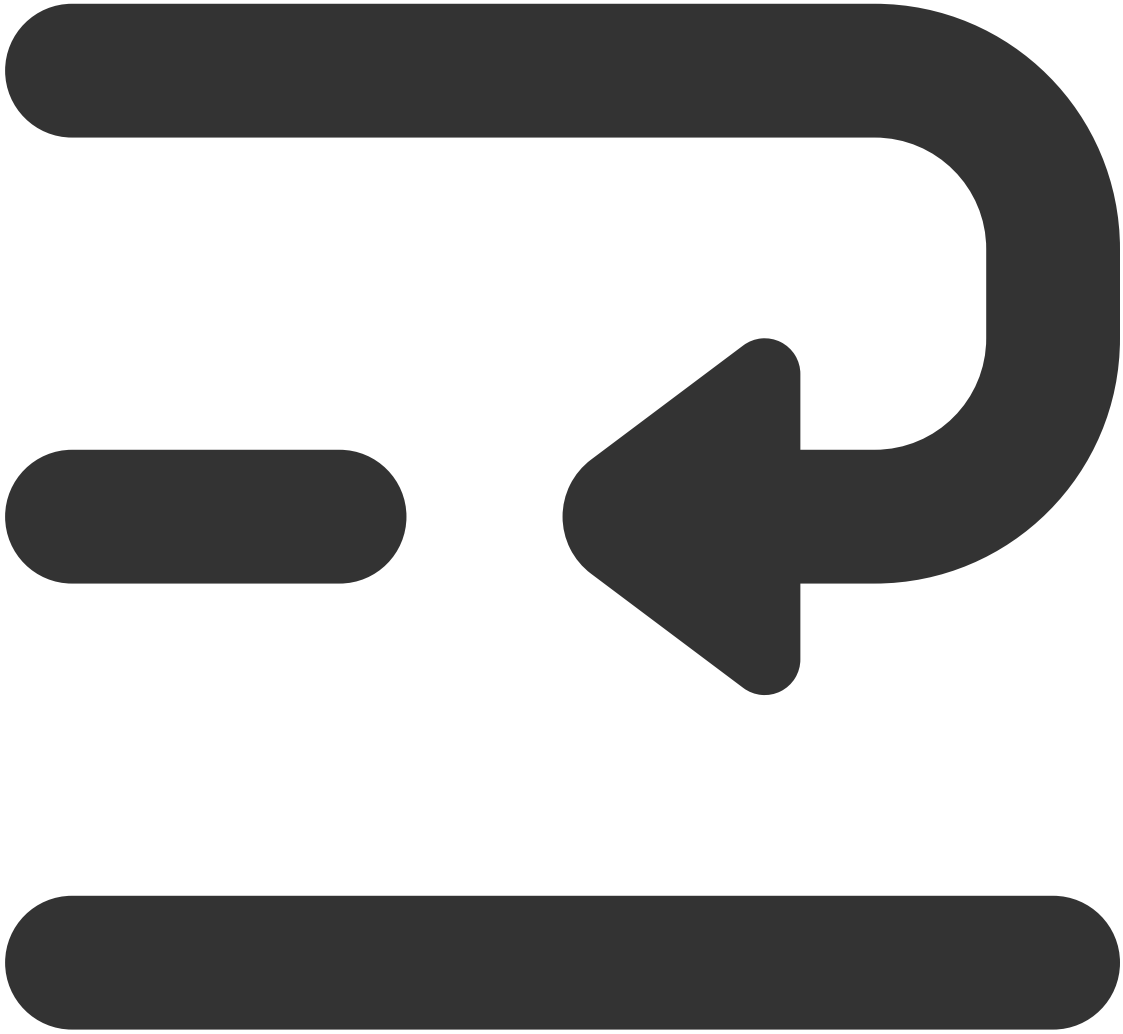
Directions

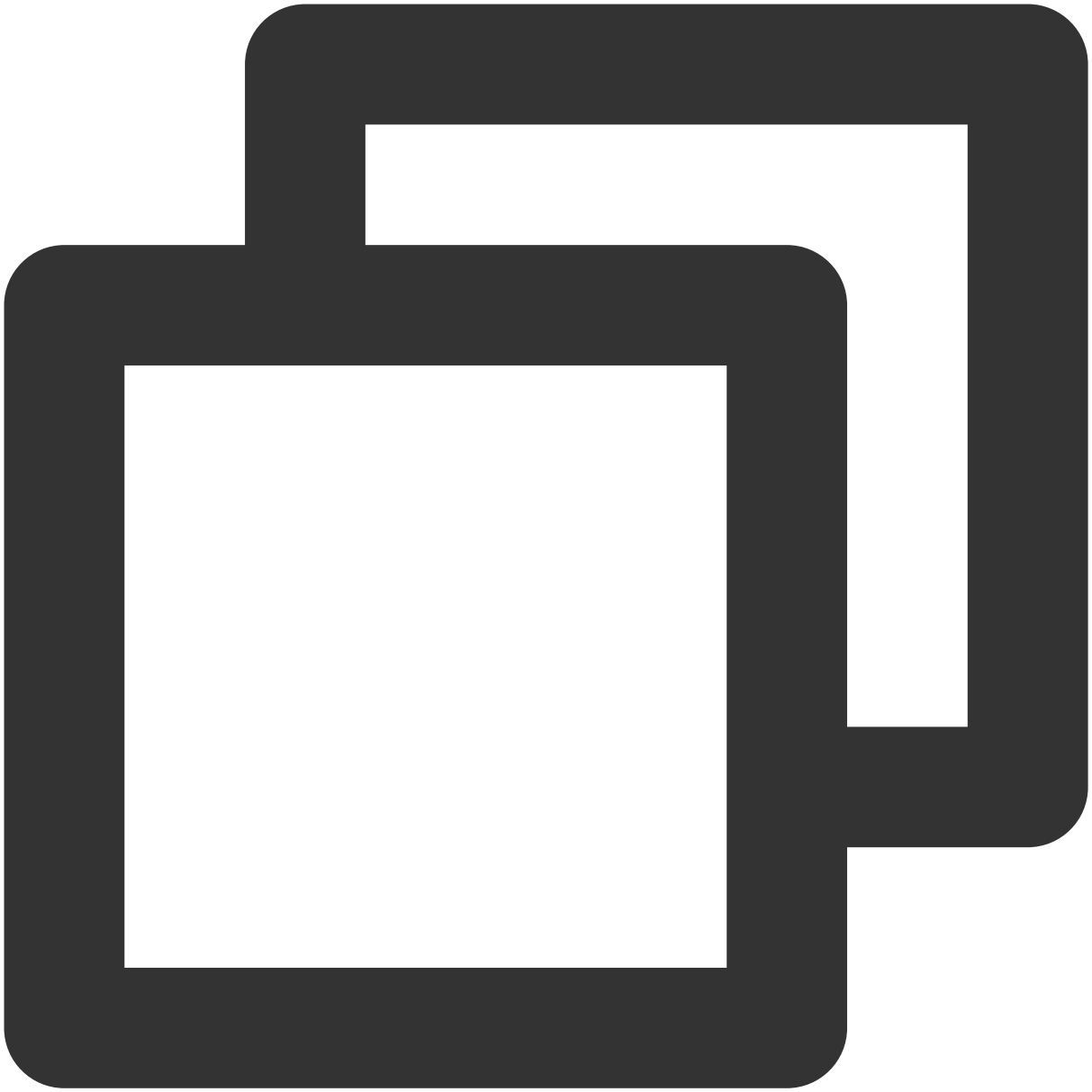
1. Log in to the EdgeOne console and click **Site List** in the left sidebar. Then click on the **site** to be configured in the site list, to enter the site details page.
2. On the site details page, click **Log Service** > **Real-time Logs**.
3. On the real-time logs page, click **Create Push Task**.
4. On the log source selection page, enter a task name, select a log type, service area, and domain name/L4 proxy instance requiring log push, and click **Next**.
5. On the push content definition page:
(Required) Check the log fields to be pushed from the predefined field list.
(Optional) Add a custom log field, which supports extracting specified field names from the request headers, response headers, and Cookie headers.
(Optional) Configure the log push filter conditions. Full logs are pushed by default.
(Optional) In advanced configuration, set the sampling ratio. By default, sampling is not enabled and 100% of logs are pushed to the destination.
(Optional) In advanced configuration, set the log output format. The default format is JSON Lines.
6. On the destination selection page, select **HTTP (POST)** and click **Next**.
7. On the destination information page, enter the related destination and parameter information.

Parameter Name	Description
API Address	Enter your log receiving API address, for example: `https://www.example.com/edgeone-logs`
Content Compression	To reduce the size of log content and save the traffic costs, you can enable content compression by checking **Compress log files with gzip**. EdgeOne will compress the logs in gzip format and then transmit them. Meanwhile, it will add an HTTP header `Content-Encoding: gzip` to indicate the compression format.
Origin Authentication	When encrypted authentication is selected, the pushed logs will carry authentication information for verification by the origin server, to ensure the security of the data source identity. For the authentication algorithm, see Authentication Algorithm Reference.

Custom HTTP Header	Add the HTTP headers to be carried when EdgeOne initiates a request. For example: Add the header `log-source: EdgeOne` , to identify the log source as EdgeOne. Add the header `BatchSize: ${batchSize}` , to obtain the number of log entries pushed in each POST request. **Note** If the header name you enter is a default header carried for EdgeOne log push, such as Content-Type, the header value you enter will override the default value.

8. Click **Push**, confirm the related cost tips in the pop-up window, and click **Confirm Creation**.
9. During the configuration phase of the real-time log push task, test data will be sent to the API address to verify the API connectivity. The data format is as follows:





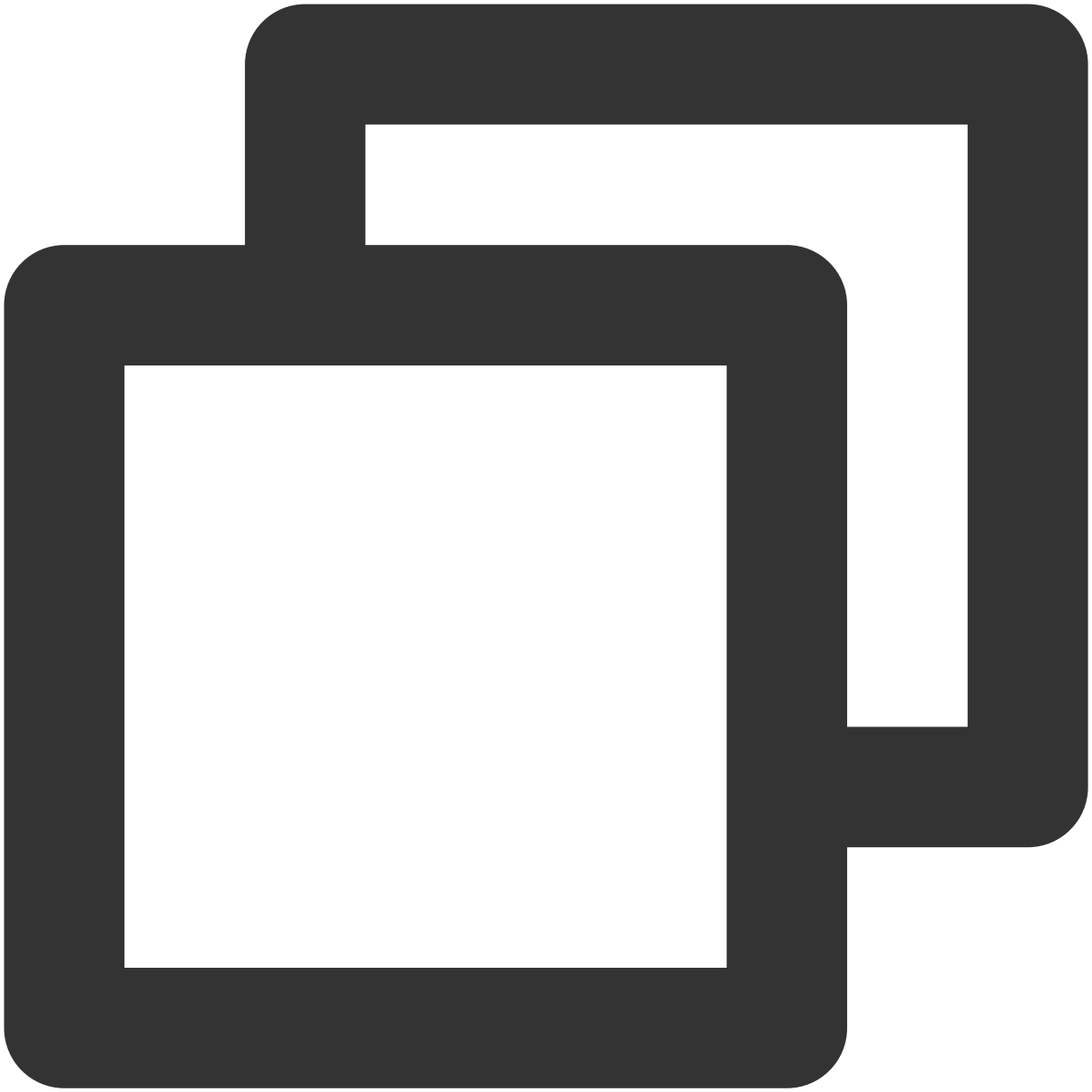

```
{
    "ClientState": "CH-AH",
    "EdgeResponseTime": 366,
    "RequestID": "13515444256055847385",
    "ClientRegion": "CN",
    "RemotePort": 443,
    "RequestHost": "www.tencent.com",
    "RequestMethod": "GET",
    "RequestUrlQueryString": "-",
    "RequestUrl": "/en-us/about.html",
    "RequestProtocol": "HTTP/2.0",
```

```
    "EdgeServerID": "336d5ebc5436534e61d16e63ddfca327-d41d8cd98f00b204e9800998ecf84
    "RequestTime": "2022-07-01T02:37:13Z",
    "EdgeCacheStatus": "-",
    "EdgeResponseBytes": 39430,
    "EdgeResponseStatusCode": 200,
    "ClientIP": "0.0.0.0",
    "RequestReferer": "https://www.tencent.com/",
    "RequestUA": "Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS X) AppleWebKi
    "EdgeServerIP": "0.0.0.0",
    "RequestRange": "0-100/200",
    "EdgeInternalTime": 334,
    "RequestBytes": 237
}
```


Related References

Code Example for Server-side Log Parsing

When origin server authentication is not enabled, you can refer to the following Python code for parsing the log content in the request body on the server side.



```
# Import modules from the Python standard library.
import time  # Used to get the current time.
import gzip  # Used to handle data compressed with gzip.


# Import HTTPServer and BaseHTTPRequestHandler classes from the http.server module.
from http.server import HTTPServer, BaseHTTPRequestHandler
import json  # Used to handle JSON data.


# Define a class inheriting from BaseHTTPRequestHandler, used to handle HTTP reques
```

```
class Resquest(BaseHTTPRequestHandler):
    # Override the do_POST method, which is called when the server receives a POST
    def do_POST(self):
        # Print the request header information.
        print(str(self.headers))
        # Print the HTTP request command (e.g., POST).
        print(self.command)
        # Read the request body content. The reading length is determined according
        req_datas = self.rfile.read(int(self.headers['content-length']))
        try:
            # Attempt to decode the request body content and print it.
            print(req_datas.decode())
        except Exception as e:
            # If an exception occurs during decoding, print the exception informati
            print(e)
            # Check whether the request header contains Content-Encoding: gzip. If
            if self.headers['Content-Encoding'] == 'gzip':
                data = gzip.decompress(req_datas)
                # Print the decompressed gzip content
                print('---------------decompress gzip content----------------------
                print(data.decode())
        # Check whether the request path is '/edgeone-logs'. If not, return a 404 e
        if self.path != '/edgeone-logs':
            self.send_error(404, "Page not Found!")
            return
        # If the request path is correct, prepare the response data.
        data = {
            'result_code': '1',
            'result_desc': 'Success',
            'timestamp': int(time.time())  # Respond with the current timestamp
        }
        # Send an HTTP response status code 200, indicating the request succeeded.
        self.send_response(200)
        # Set the response header Content-type to application/json.
        self.send_header('Content-type', 'application/json')
        # End the sending of response headers.
        self.end_headers()
        # Write the response data in JSON format to the response body.
        self.wfile.write(json.dumps(data).encode('utf-8'))


# Check whether the current script is running as the main program.
if __name__ == '__main__':
    # Define the server listening address and port. You can replace 9002 with your
    host = ('', 9002)
    # Create an HTTPServer object, passing in the listening address and port, and t
    server = HTTPServer(host, Resquest)
```

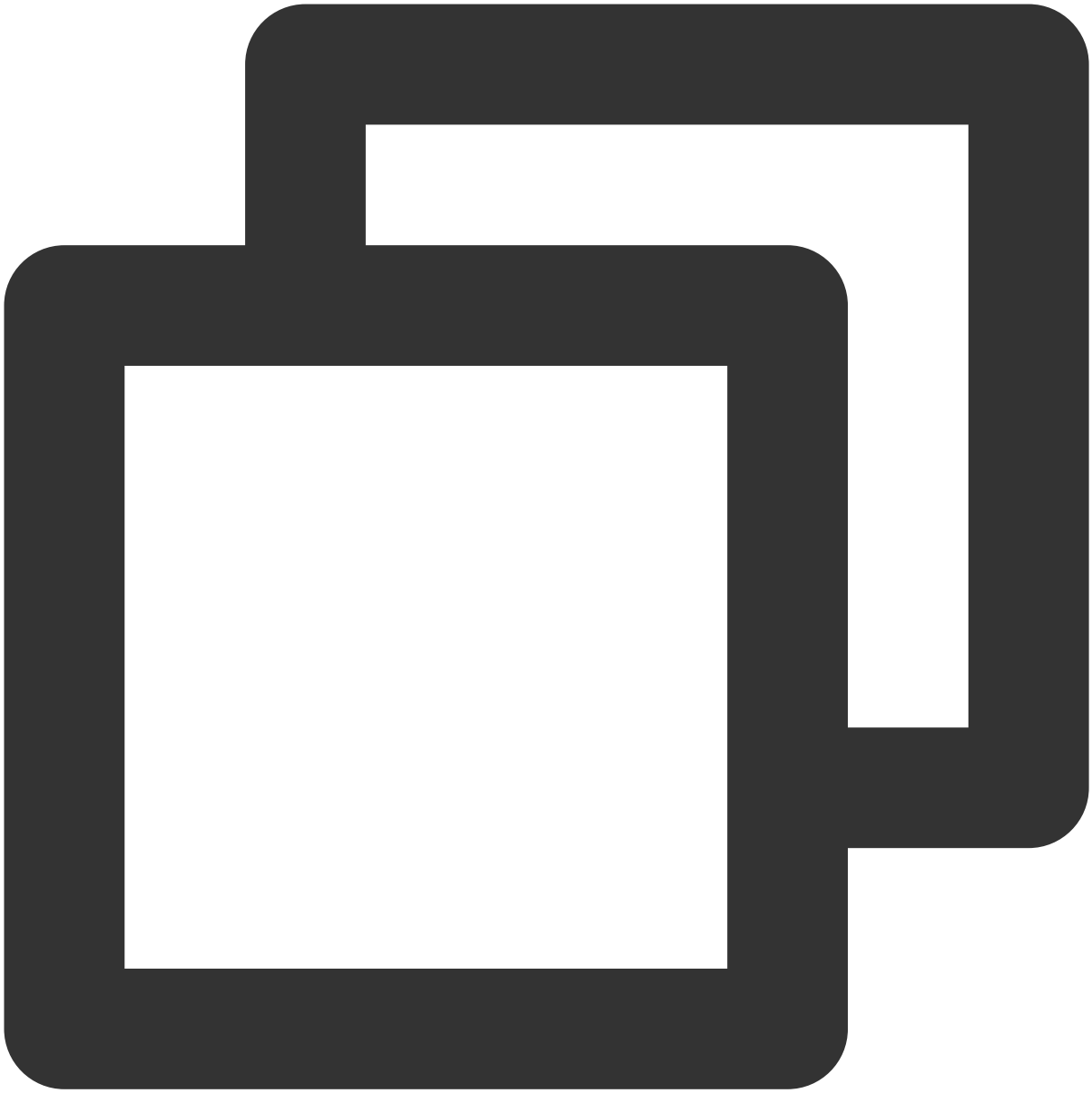
```
    # Print the server startup information.
    print("Starting server, listen at: %s:%s" % host)
    # Start the server and keep it running until externally interrupted.
    server.serve_forever()
```

Request Authentication Algorithm

If you select **Encrypted Signature** for origin server authentication in the push destination information, you can enter a custom SecretId and SecretKey. EdgeOne will add `auth_key` and `access_key` of signature to the request URL. The details of the signature algorithm are as follows:

1. **Request URL Composition**

As shown below, the request URL carries `auth_key` and `access_key` after `?` .



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

Parameter description:

timestamp: Current request time, in the format of Unix 10-digit timestamp in seconds.

rand: Random number.

access_key: Custom SecretId, used to identify the identity of the API requester.

SecretKey: Custom SecretKey, with a fixed length of 32 characters.

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

md5hash: md5hash = `md5sum(string_to_sign)` , where string_to_sign = `"uri-timestamp-rand-SecretKey"` . It is a verification string calculated through the MD5 algorithm, consisting of digits 0-9 and lowercase letters a-z, with a fixed length of 32 characters.

2. **Calculation Example**

Assume the parameters entered are as follows:

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

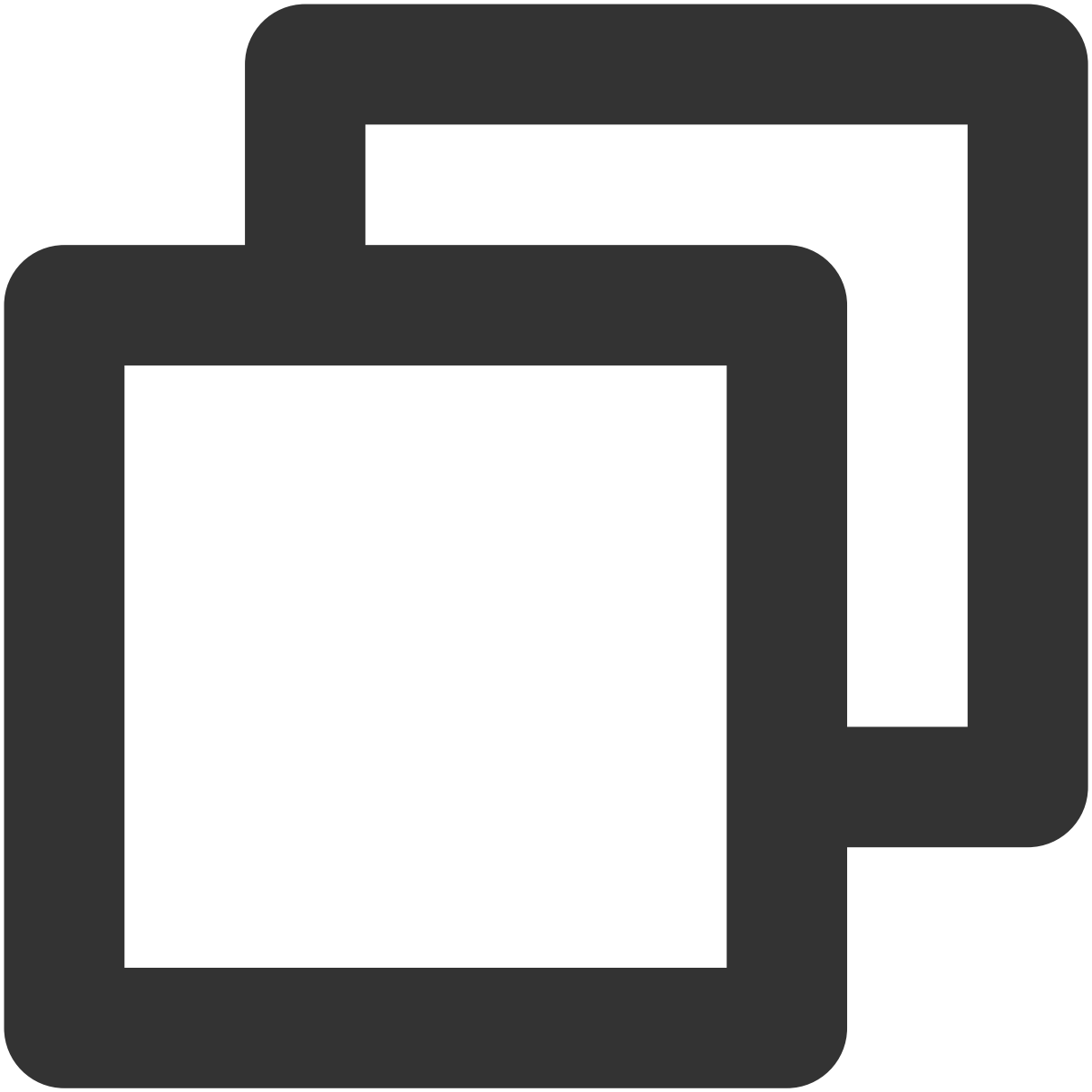
SecretId = `YourID`

SecretKey = `YourKey`

uri = `/access_log/post`

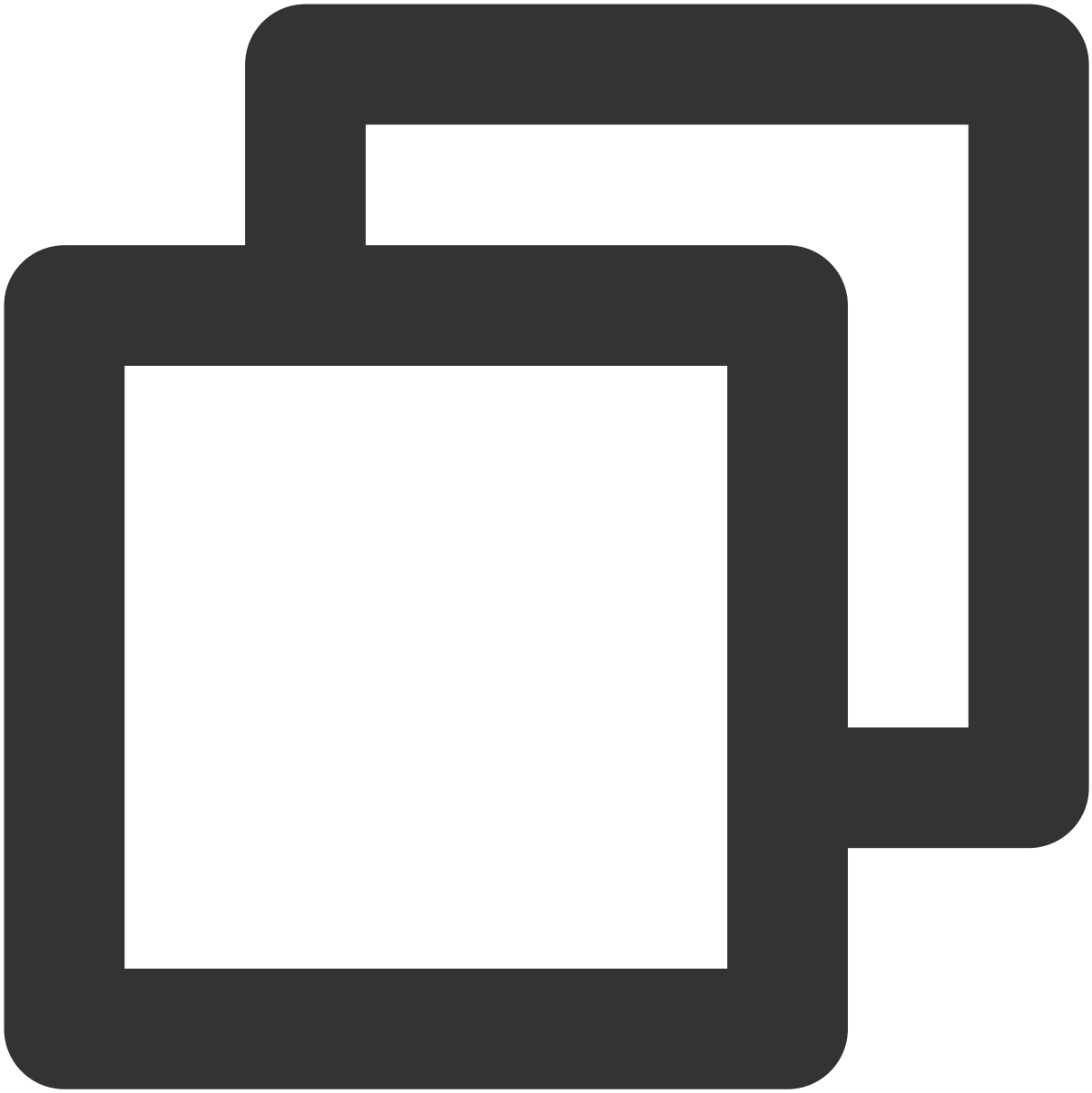
timestamp = `1571587200`

rand = `0`



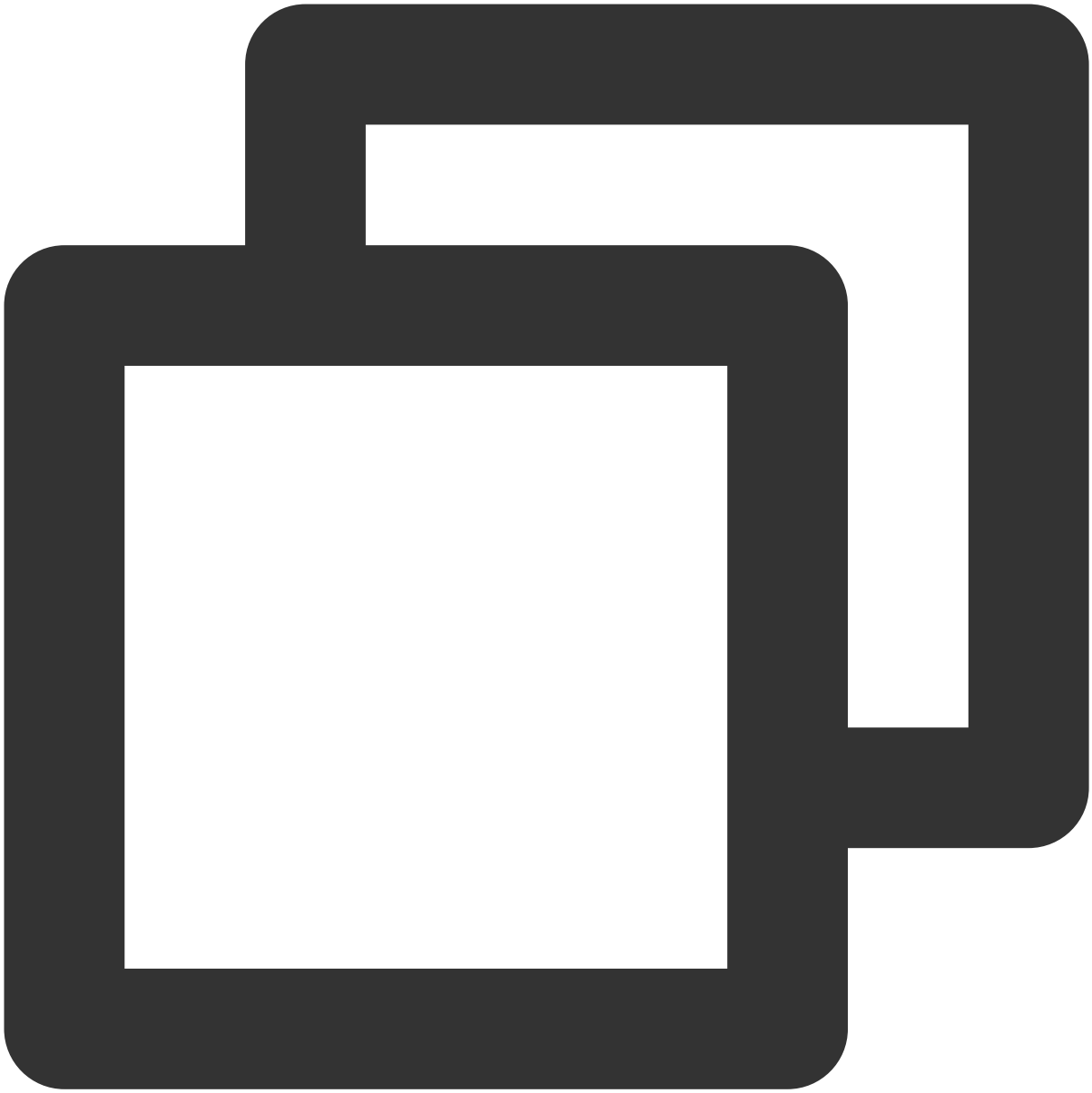
```
string_to_sign = "/access_log/post-1571587200-0-YourKey"
```

By calculation based on this string, the following result is obtained:



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

The request URL in final push is:



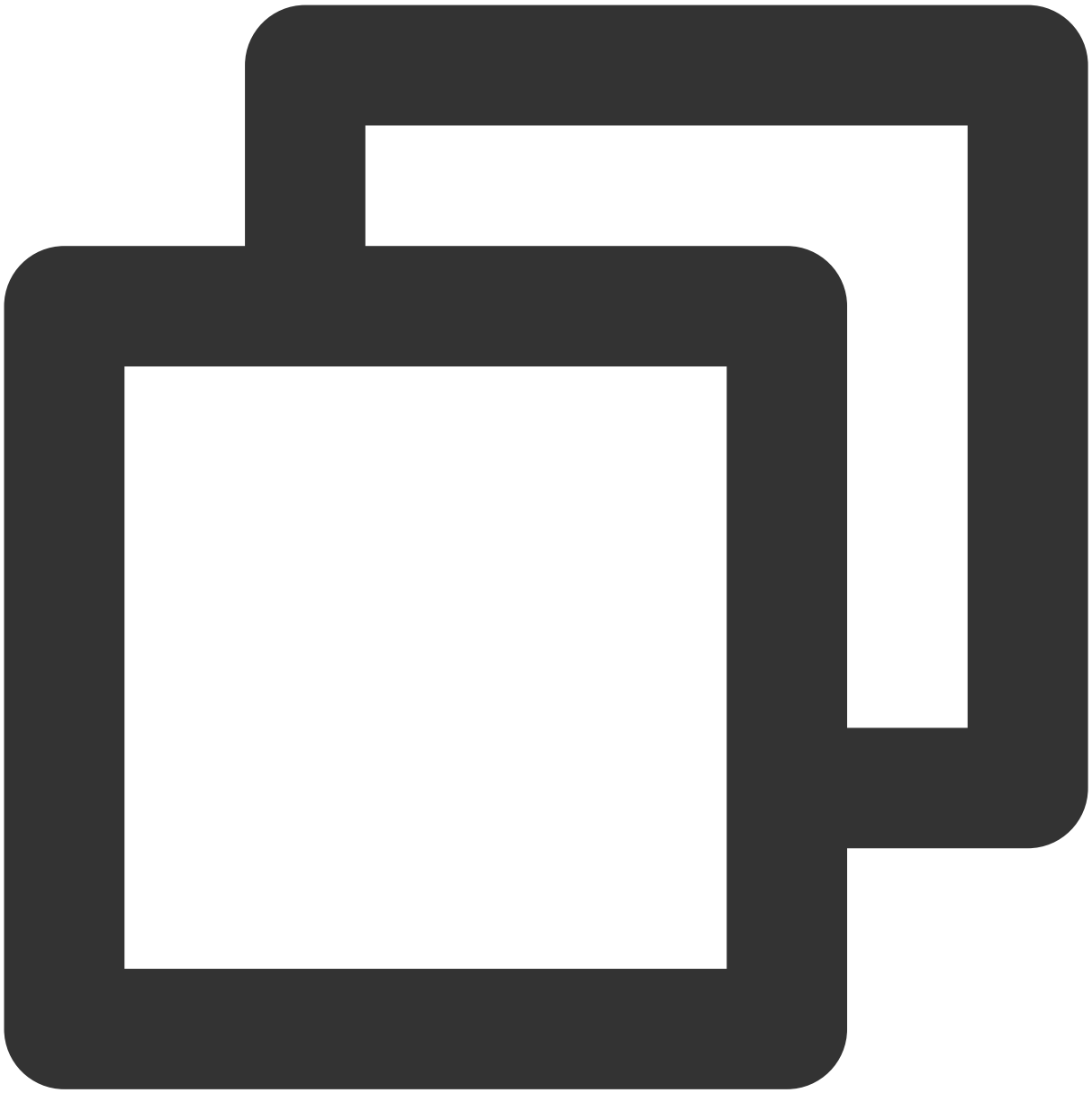
```
https://www.example.com/cdnlog/post?auth_key=1571587200-0-1f7ffa7bff8f06bbfbe2ace0f
```

After the server receives the push request, it extracts and splits the value of `auth_key` to obtain `timestamp`, `rand`, and `md5hash`. The server can first check whether the `timestamp` has expired. The recommended validity time is `300s`. Then it assembles a string to be encrypted with the SecretKey based on the aforementioned rules. After encryption, the string is compared with the `md5hash` value in `auth_key`. If consistent, it indicates authentication succeeded.

3. **Code Example for Server-Side Authentication Request Parsing**

Python

Golang



```
import hashlib

from flask import Flask, request

app = Flask(__name__)


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

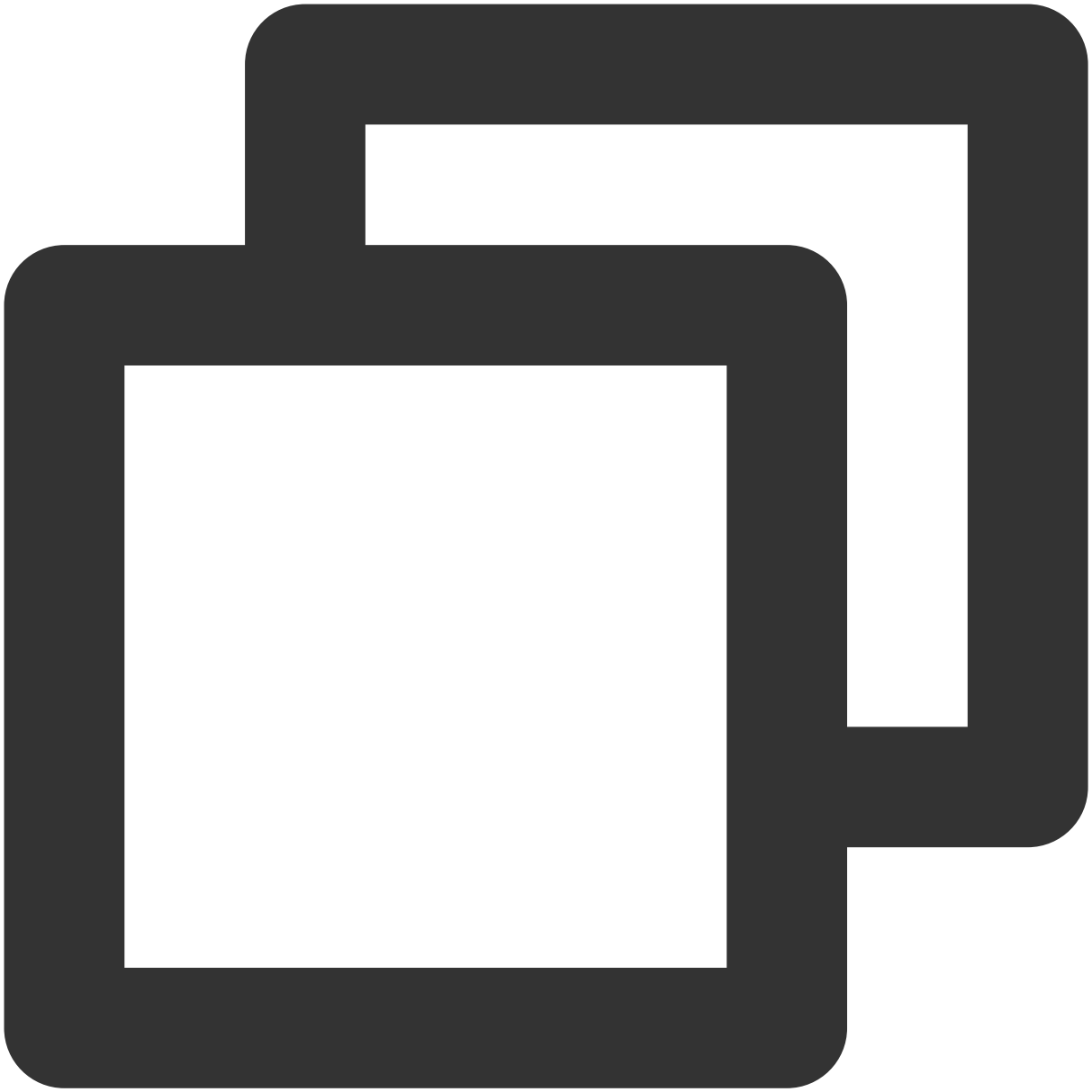
```
        "respCode": code,
        "respMsg": msg,
        "result": result
    }


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 request 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")
            # Get the secret_key using 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 succeeded.
                if request.headers['content-encoding'] == 'gzip':
                    # Data decompression
                    pass
                # Data handling
            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)
```



```
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 a 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 prov
        authKeys := strings.Split(authKey, "-")
        if len(authKeys) == 3 {
            currentTimeTs := authKeys[0]

            // Judge whether the timestamp is within the validity period.
            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) // Converted to a string for comparis
            if authMd5 == md5Hash {
                // TODO authentication succeeded.
                if r.Header.Get("Content-Encoding") == "gzip" {
                    // Data decompression
                }
                // Data handling
            }
        } else {
            // Exception handling
        }
    }
}

// Get SecretKey.
func getSecretKey(accessKey string) string {
    if accessKey != "" {
        // Get Secret_Key using Access_key (SecretId).
        return "secret_key"
    }
    return ""
}
```

Offline Logs

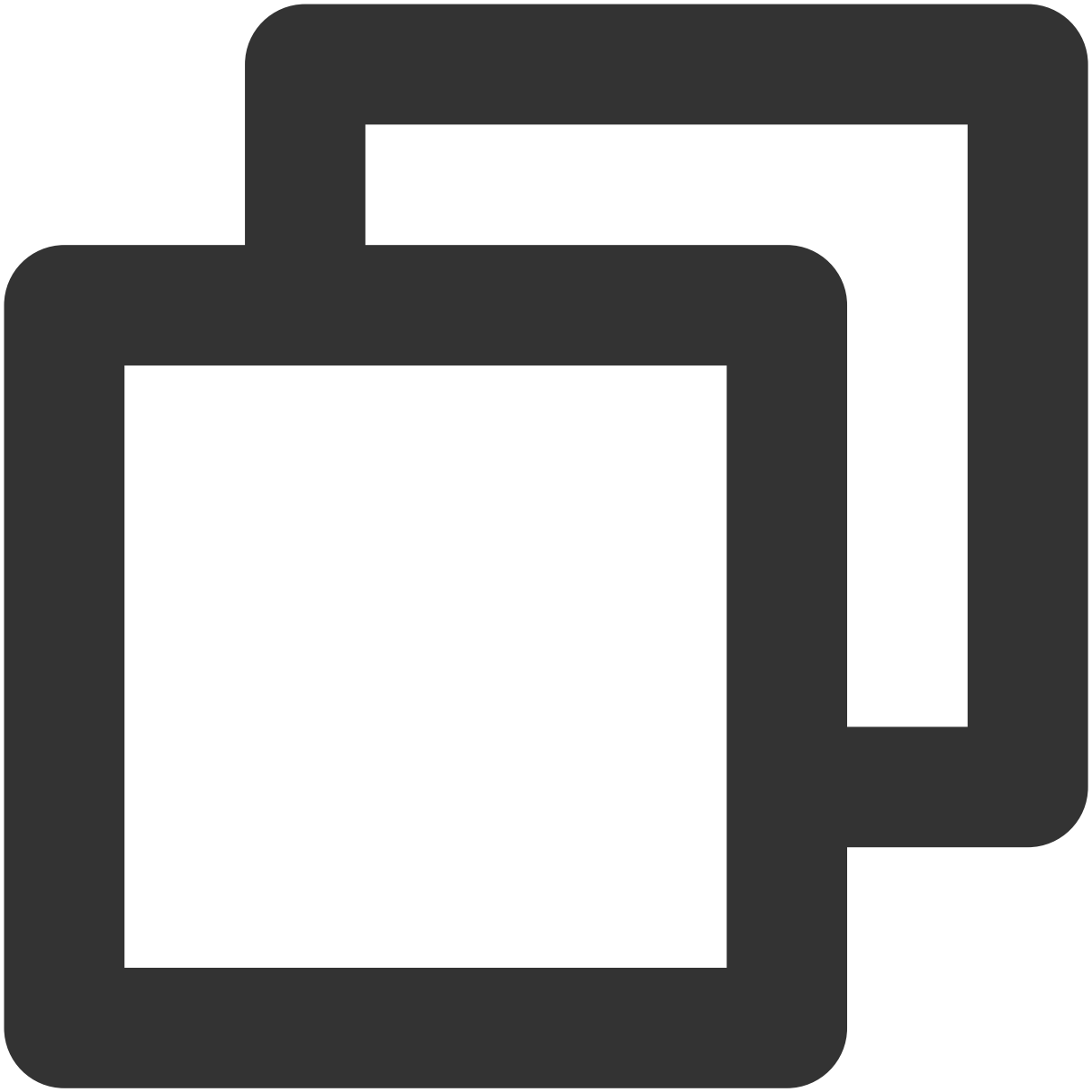
Last updated：2024-07-15 09:31:09

Feature Overview

To facilitate user access analysis by customers, EdgeOne packages access logs in hourly granularity, retains the logs for 30 days by default, and provides download services.

Offline Log Format

Logs are stored in JSON Lines format by default. Each JSON line represents a single log.
Log packages are compressed in .gz format with gzip. Due to the directory system limitations in MacOS, double-click for decompression may cause an error. In this case, you can navigate to the directory containing the logs, and use the following Terminal command for decompression.



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

Log Packaging Rules

Packaging in hourly granularity is adopted by default. If there are no requests for accessing your business within an hour, no log packages will be generated for the time interval.

Since EdgeOne nodes are distributed globally, the storage time of offline logs (the time in log package filenames) is set to UTC +00:00 by default in order to synchronize all time zones.
Offline logs are collected from various EdgeOne nodes so that they are different in latency. Generally, logs can be queried and downloaded after a delay of around 3 hours. The log packages will increase continuously and typically stabilize after around 24 hours.

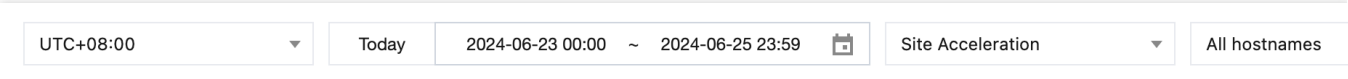
Example: Querying Offline Logs for a Specified Domain Name within a Specified Time Period

Sample Scenario

After you add an acceleration domain name and add `www.example.com` to the EdgeOne service, you shall download all site acceleration logs for `www.example.com` from June 23, 2024 to June 25, 2024 to perform data analysis. You can refer to the following directions.

Directions

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. Then click the **site** of your concern in the site list, to enter the site details page.
2. On the site details page, click **Log Service** > **Offline Logs**.
3. On the offline logs page, select the dates from June 23, 2024 to June 25, 2024 to filter by time range. On the right side, select Site Acceleration Logs as the log type and www.example.com as the domain name. The page will automatically display the query results of logs meeting the conditions after filtering.



4. In the log list obtained through query, you can download log packages as needed using the following 3 methods:
Click **Download** in the **Operation** column, to download the log package for the corresponding domain name/L4 proxy instance and the corresponding time period.
Click **Get Download URLs**, to copy the download link for the corresponding log package.
Select the required log packages, and click **Batch Get Download URLs** to copy the download links for all required log packages in batch.

Related APIs

DownloadL7Logs
DownloadL4Logs

Related References
Field description
L7 Access Logs

Last updated：2024-07-15 09:31:09

The following are detailed field descriptions for L7 access logs (Site Acceleration Logs, Rate Limiting and CC Attack Protection Logs, Custom Rule Logs, Bot Management Logs, and Managed Rule Logs).

Note

The feature of Real-time Logs - Site Acceleration Logs to record full L7 request logs (including L7 protection block logs) is in beta testing. If needed, please contact us.

Rate Limiting and CC Attack Protection Logs, Custom Rule Logs, and Bot Management Logs will be deactivated on July 31, 2024. It is recommended to obtain full L7 protection logs by using the Site Acceleration Logs.

General Fields

Field Name	Data Type	Description	Supported by Offline Logs or Not	Supported by Real-Time Logs or Not
EdgeEndTime	Timestamp ISO8601	The time to complete the response to the client request.	×	✓
EdgeFunctionSubrequest	Integer	Indicates whether this log entry belongs to a sub-request initiated by an edge function. Valid values include: 1: sub-request initiated by an edge function. 0: sub-request not initiated by an edge function.	✓	✓
EdgeServerID	String	Unique identifier of the EdgeOne server accessed by the client.	✓	✓
EdgeServerIP	String	IP address of the EdgeOne server obtained through DNS resolution of the host.	✓	✓

EdgeSeverRegion	String	Country resolved from the IP address of the responding EdgeOne node. For the format standard, refer to ISO 3166-1 alpha-2.	×	✓
LogTime	Timestamp ISO8601	Generation time of the logs.	×	✓
ParentRequestID	String	If this request is initiated using edge functions, it is recorded as the RequestID of the parent request; otherwise, it is recorded as -.	✓	✓
RequestID	String	Unique identifier of the client request.	✓	✓

Client Information

Field Name	Data Type	Description	Supported by Offline Logs or Not	Supported by Real-Time Logs or Not
ClientDeviceType	String	Client request device type. Valid values include: TV: Television Tablet: Tablet PC Mobile: Mobile phone Desktop: Computer Other: Others	×	✓
ClientIP	String	Client IP address connected to EdgeOne nodes.	✓	✓
ClientISP	String	ISP information resolved from the Client IP address. For data within the Chinese mainland, it is recorded as the ISP's Chinese name. For data in global availability zones (excluding the Chinese mainland),	✓	✓

		it is recorded as Autonomous System Number (ASN).		
ClientRegion	String	Country/Region resolved from the Client IP address. Format standard: ISO 3166-1 alpha-2.	✓	✓
ClientState	String	Administrative region below the country level, resolved from the Client IP address. Currently, it only supports data within the Chinese mainland. Format standard: ISO-3166-2.	✓	✓

Request Information

Field Name	Data Type	Description	Supported by Offline Logs or Not	Supported by Real-Time Logs or Not
RemotePort	Integer	Port for establishing a connection between the client and the node under the TCP protocol.	✓	✓
RequestBytes	Integer	Total traffic sent from the client to the EdgeOne node during the request process, in bytes. It is obtained from statistics based on the request header size, request body size, and data sent from the client to the EdgeOne node during the SSL handshake.	✓	✓
RequestHost	String	Host of the client request.	✓	✓
RequestMethod	String	HTTP method of the client request. Valid values include: GET POST HEAD PUT DELETE CONNECT	✓	✓

		OPTIONS TRACE PATCH		
RequestProtocol	String	Application layer protocol of the client request. Valid values include: HTTP/1.0 HTTP/1.1 HTTP/2.0 HTTP/3 WebSocket	✓	✓
RequestRange	String	Range parameter information of the client request.	✓	✓
RequestReferer	String	Referer information of the client request.	✓	✓
RequestSSLProtocol	String	SSL (TLS) protocol used by the client. If the value is -, it indicates no SSL handshake in the request. Valid values include: TLS 1.0 TLS 1.1 TLS 1.2 TLS 1.3	×	✓
RequestStatus	Integer	Status of the client request. For WebSocket requests, EdgeOne will periodically print logs. This field can be used to determine the connection status. Valid values include: 0: Request does not end. 1: Request ends normally. 2: It indicates the first log entry of the same connection under the WebSocket protocol. 3: It indicates a log entry that is neither the first nor the last of the same connection under the WebSocket protocol.	✓	✓
RequestTime	Timestamp ISO8601	Time when the EdgeOne node receives the client request. Time	✓	✓

		zone: UTC +00:00.		
RequestUA	String	User-Agent information of the client request.	✓	✓
RequestUrl	String	URL path of the client request, excluding query parameters.	✓	✓
RequestUrlQueryString	String	Query parameter carried in the client request URL.	✓	✓

Response Information

Field Name	Data Type	Description	Supported by Offline Logs or Not	Supported by Real-Time Logs or Not
EdgeCacheStatus	String	Whether the client request hits the node cache. Valid values include: hit: The resource is provided by the node cache. miss: The resource can be cached, but provided by the origin server. dynamic: The resource cannot be cached. other: The cache status cannot be recognized.	✓	✓
EdgeInternalTime	Integer	Duration from the time when EdgeOne receives the client-initiated request to the time when the first byte is responded to the client, in ms.	✓	✓
EdgeResponseBodyBytes	Integer	Size of the response body returned by the node to the client, in bytes.	✓	✓
EdgeResponseBytes	Integer	Total traffic returned by the node to the client, in bytes. It is obtained from statistics based	✓	✓

		on the response header size, response body size, and data sent by the EdgeOne node to the client during the SSL handshake.		
EdgeResponseStatusCode	Integer	Response status code returned to the client by the node.	✓	✓
EdgeResponseTime	Integer	Duration from the time when EdgeOne receives the client-initiated request to the time when the client receives the server-side response, in ms.	✓	✓

Origin Server Information

Field Name	Data Type	Description	Supported by Offline Logs or Not	Supported by Real-Time Logs or Not
OriginDNSResponseDuration	Float	Time consumed to receive the DNS Resolution response from the origin server, in ms. If there is no origin-pull, it is recorded as -1.	×	✓
OriginIP	String	IP address of the origin server accessed for origin-pull. If there is no origin-pull, it is recorded as -.	×	✓
OriginRequestHeaderSendDuration	Float	Time consumed to send the request header to the origin server, in ms. It is generally 0. If there is no origin-pull, it is recorded as -1.	×	✓
OriginResponseHeaderDuration	Float	Duration from sending the request header to the origin server to receiving	×	✓

		the response header from the origin server, in ms. If there is no origin-pull, it is recorded as -1.		
OriginResponseStatusCode	Integer	Response status code of the origin server. If there is no origin-pull, it is recorded as -1.	×	✓
OriginSSLProtocol	String	SSL protocol version used for requesting the origin server. If there is no origin-pull, it is recorded as -. Valid values include: 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 server, in ms. If there is no origin-pull, it is recorded as -1. **Note: It is 0 when the connection is reused.**	×	✓
OriginTLSHandshakeDuration	Float	Time consumed to complete the TLS handshake when requesting the origin server, in ms. If there is no origin-pull, it is recorded as -1. **Note: It is 0 when the connection is reused.**	×	✓

Fields Related to Security Protection

Field Name	Data Type	Description	Supported by Offline Logs or Not	Supported by Real-Time

				Logs or Not
BotCharacteristic	String	Characteristics of this request identified by EO Bot Intelligent Analysis Engine, only available for domains with Bot Management - Bot Intelligent Analysis enabled.	×	✓
BotClassAccountTakeOver	String	Risk level of the requesting client's IP address with malicious cracking logins and account takeover attacks, based on the recent IP intelligence data. Valid values include: high: high risk medium: medium risk low: low risk -: No historical data or the domain has not enabled the Client Reputation feature.	×	✓
BotClassAttacker	String	Risk level of the requesting client's IP address with attacks (e.g., DDoS, high-frequency malicious requests, and site attacks), based on the recent IP intelligence data. Valid values include: high: high risk medium: medium risk low: low risk -: No historical data or the domain has not enabled the Client Reputation feature.	×	✓
BotClassMaliciousBot	String	Risk level of the requesting client's IP address with malicious crawlers, brushing, and brute force attacks, based on the recent IP intelligence data. Valid values include: high: high risk medium: medium risk low: low risk -: No historical data or the domain has not enabled the Client Reputation feature.	×	✓

BotClassProxy	String	Risk level of the requesting client's IP address opening suspicious proxy ports and being used as a network proxy (including second-level dialing IP), based on the recent IP intelligence data. Valid values include: high: high risk medium: medium risk low: low risk -: No historical data or the domain has not enabled the Client Reputation feature	×	✓
BotClassScanner	String	Risk level of the requesting client's IP address with scanner actions of exploiting known vulnerabilities, based on the recent IP intelligence data. Valid values include: high: high risk medium: medium risk low: low risk -: No historical data or the domain has not enabled the Client Reputation feature.	×	✓
BotTag	String	Comprehensive evaluation and classification of the request by the EO Bot Intelligent Analysis Engine based on factors such as the request rate and the IP intelligence database. It is only available for domains with Bot Management - Bot Intelligent Analysis enabled. Valid values include: evil_bot (malicious Bot request) suspect_bot (suspected Bot request) good_bot (normal Bot request) normal (normal request) - (unclassified)	×	✓
JA3Hash	String	MD5 hash value of the JA3 fingerprint, used to analyze the SSL/TLS clients. It is only available for domains with Bot Management enabled.	×	✓
SecurityAction	String	Final handling action after a request	×	✓

		matches the security rules. Valid values include: -: unknown/not matched Monitor: observation JSChallenge: JavaScript challenge Deny: block Allow: pass BlockIP: IP banning Redirect: redirect ReturnCustomPage: returning custom pages ManagedChallenge: managed challenge Silence: Silence LongDelay: response after a long delay ShortDelay: response after a short delay		
SecurityModule	String	Name of the security module finally handling the request, corresponding to `SecurityAction`. Valid values include: -: unknown/not matched CustomRule: Web Protection - Custom Rules RateLimitingCustomRule: Web Protection - Rate Limiting Rules ManagedRule: Web Protection - Managed Rules L7DDoS: Web Protection - CC Attack Protection BotManagement: Bot Management - Bot Basic Management BotClientReputation: Bot Management - Client Reputation BotBehaviorAnalysis: Bot Management - Bot Intelligent Analysis BotCustomRule: Bot Management - Custom Bot Rules BotActiveDetection: Bot Management - Proactive Feature Recognition	×	✓
SecurityRuleID	String	ID of the security rule for final request handling, corresponding to SecurityAction.	×	✓

Note:

In the site acceleration logs, for long connections using the WebSocket protocol, EdgeOne will periodically record logs and the last log entry is recorded at the end of the final request. Requests can be identified through the `RequestID` field, that is, logs with the same `RequestID` represent the same connection. Additionally, the `RequestStatus` field can be used to determine the connection status at the time of logging.

L4 Proxy Logs

Last updated：2024-07-15 09:31:09

The following are detailed descriptions for the fields in L4 proxy logs.

Note:

In a long TCP connection scenario, EdgeOne records logs periodically and the last log entry is recorded when the connection ends. You can judge the connection status by checking whether the `DisconnetReason` field is empty. Additionally, you can use the `SessionID` to identify the connection. The logs with the same `SessionID` record the actions of the same connection.

Under the L4 Proxy Logs type, real-time logs and offline logs record the same fields.

Field Name	Data Type	Description
ClientRealIP	String	Real IP address of the client.
ClientRegion	String	2-letter country/region code of the client, compliant with ISO-3166 alpha-2 standard.
ConnectTimeStamp	Timestamp ISO8601	Connection time, UTC +0 time zone by default.
DisconnetReason	String	Disconnection reason. If not disconnected during the current log cycle, the value is -. The format is **Direction: Reason**. Valid values for the direction include: up: origin server direction down: client direction Valid values for the reason include: net_exception_peer_error: Read/Write peer error. net_exception_peer_close: The peer has closed connection. create_peer_channel_exception: Failed to create a channel to the next hop. channel_eof_exception: Channel has ended (when the request ends, the node ending the request will send channel_eof to the adjacent node, informing it that the request has ended). net_exception_closed: Connection has closed. net_exception_timeout: Read/Write timed out.
DisconnetTimeStamp	Timestamp ISO8601	Disconnection time, UTC +0 time zone by default. If not disconnected during the current log cycle, the value is -.
EdgeIP	String	IP address of the accessed EdgeOne server.
ForwardPort	Integer	Customer-configured forwarding port.

ForwardProtocol	String	Customer-configured forwarding protocol TCP/UDP.
LogTimeStamp	Timestamp ISO8601	Log generation time, UTC +0 timezone by default.
ReceivedBytes	Integer	Outbound traffic generated from the recording time of the previous log entry to the recording time of this log entry, in bytes.
SentBytes	Integer	Inbound traffic generated from the recording time of the previous log entry to the recording time of this log entry, in bytes.
ServiceID	String	Unique identifier ID of the L4 proxy service.
SessionID	String	Unique identifier ID of the TCP connection or UDP session.

Real-Time Log Push Filter Conditions

Last updated：2024-07-15 09:31:09

Real-time Log Push supports configuring the filter conditions to help you filter out specific types of logs and reduce the volume of downstream log processing. The following are the supported log fields and comparison operators.

Note

Currently, only Real-time Logs - **Site Acceleration Logs** support configuring the log push filter conditions.

The Real-time Log Push Filter Conditions feature is in beta testing. If needed, please contact us.

Supported Log Fields

Field Name	Data Type	Description
SecurityAction	String	Final handling action after a request matches the security rules. Valid values include: -: unknown/not matched Monitor: observation JSChallenge: JavaScript challenge Deny: block Allow: pass BlockIP: IP banning Redirect: redirect ReturnCustomPage: returning custom pages ManagedChallenge: managed challenge Silence: Silence LongDelay: response after a long delay ShortDelay: response after a short delay
SecurityModule	String	Name of the security module finally handling the request, corresponding to `SecurityAction`. Valid values include: -: unknown/not matched CustomRule: Web Protection - Custom Rules RateLimitingCustomRule: Web Protection - Rate Limiting Rules ManagedRule: Web Protection - Managed Rules L7DDoS: Web Protection - CC Attack Protection BotManagement: Bot Management - Bot Basic Management BotClientReputation: Bot Management - Client Reputation BotBehaviorAnalysis: Bot Management - Bot Intelligent Analysis BotCustomRule: Bot Management - Custom Bot Rules

		BotActiveDetection: Bot Management - Proactive Feature Recognition
EdgeResponseStatusCode	Integer	Response status code returned to the client by the node.
OriginResponseStatusCode	Integer	Response status code of the origin server. If there is no origin-pull, it is recorded as -1.

Supported Comparison Operators

Comparison Operator Name	Supporting the Data Type or Not	
	String	Integer
Equals (matching any value in the list)	✓	✓
Greater than	×	✓
Less than	×	✓
Greater than or equal to	×	✓
Less than or equal to	×	✓

Example: Filtering out Logs with HTTP Status Codes of 4xx/5xx

Sample Scenario

In a large e-commerce platform's IT Ops team, you are responsible for monitoring and analyzing real-time logs of the website. Due to the high volume of site visits and the enormous amount of log data, you wish to reduce unnecessary log data push by setting up filtering rules, thus avoiding unnecessary burden on the analysis platform. For instance, you can perform configuration to push only the access logs with HTTP status codes of 4xx/5xx, which usually indicate some kind of error. In this way, you can focus on logs that may point to user experience issues or system failures requiring immediate attention. You can follow the directions below for configuration.

Directions

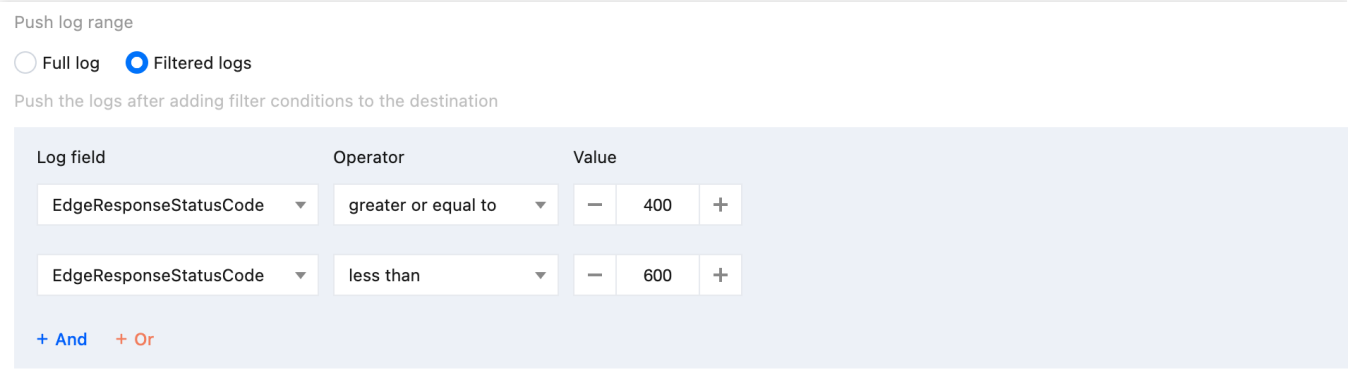
1. Log in to the EdgeOne console and click **Site List** in the left sidebar. Then click on the **site** to be configured in the site list, to enter the site details page.
2. On the site details page, click **Log Service** > **Real-time Logs**.
3. On the real-time logs page, click **Create Push Task**.

4. On the log source selection page, enter a task name, select a log type, service area, and domain name/L4 proxy instance requiring log push, and click **Next**.

5. On the push content definition page, configure the log push range.

5.1 Select **Filtered logs**.

5.2 Enter the filtering conditions, as shown in the figure below:



6. After configuring the destination, click **Push**, confirm the related cost tips in the pop-up window, and click **Confirm Creation** to save the configuration.

Custom Log Push Fields

Last updated：2024-07-15 09:31:09

If you need to push certain field values in HTTP request headers, HTTP response headers, or Cookies, you can precisely record such information in logs through the Custom Log Field feature.

Note:

The Custom Log Field feature is applicable only to real-time logs.

Use Restrictions

In the same real-time log push task, custom field names must not be duplicate.

Up to 200 custom fields can be configured.

Field names are case-sensitive and must exactly match the original field names in HTTP actions.

Field names must contain 1-100 characters, beginning with a letter and ending with a letter or a digit. The middle part may contain letters, digits, and hyphens (-).

Currently, only **Site Acceleration Logs** support adding custom fields.

Example: Recording the Value of a Specified Response Header in Logs

Sample Scenario

In some business scenarios, understanding the size of the response body is crucial for monitoring the network traffic and optimizing the performance. For this purpose, custom log fields can be configured to record the value of the `Content-Length` header for each response.

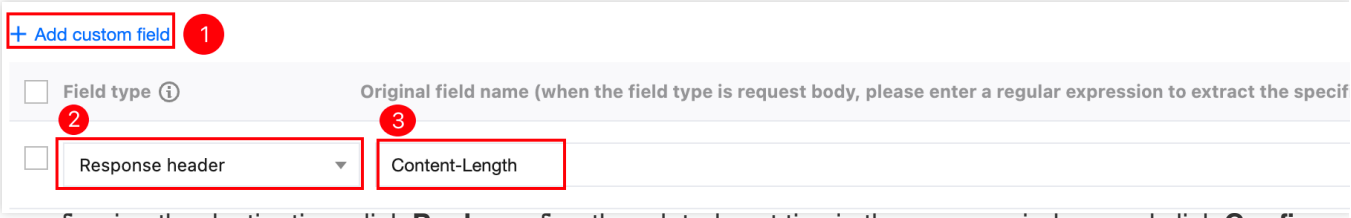
Directions

1. Log in to the EdgeOne console and click **Site List** in the left sidebar. Then click on the **site** to be configured in the site list, to enter the site details page.
2. On the site details page, click **Log Service** > **Real-time Logs**.
3. On the real-time logs page, click **Create Push Task**.
4. On the log source selection page, enter a task name, select a log type, service area, and domain name/L4 proxy instance requiring log push, and click **Next**.
5. On the push content definition page, click **Add Custom Field**.

5.1 Select **Response header** as the field type.

5.2 Enter `Content-Length` as the field name.

5.3 Click **Save**.



6. After configuring the destination, click **Push**, confirm the related cost tips in the pop-up window, and click **Confirm Creation** to save the configuration.

References

If you wish to understand the meanings of various HTTP request and response headers for deciding whether to record them in logs, refer to HTTP Standard Header Explanation.

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

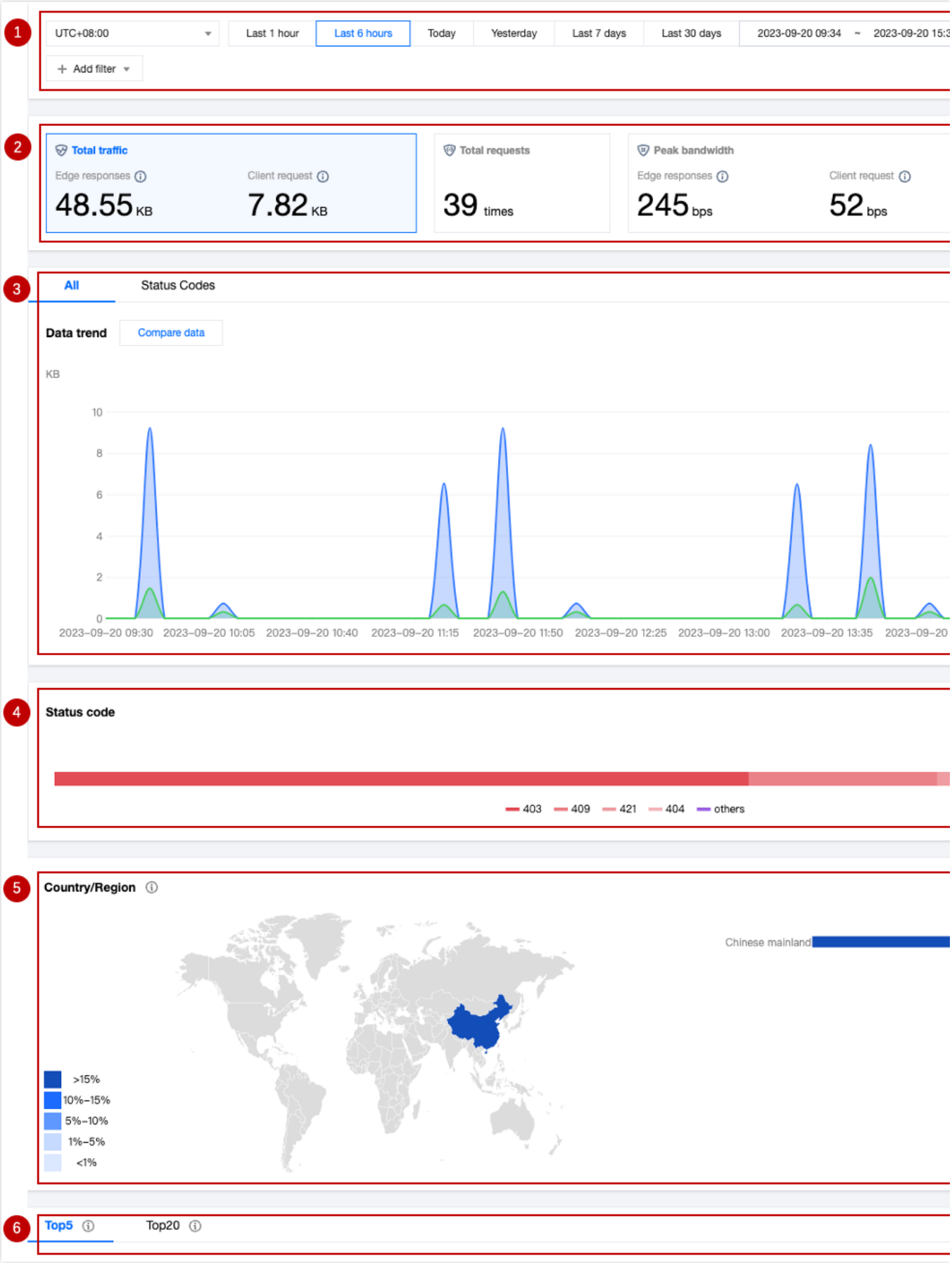
EdgeOne Service analyzes L7 (application layer) access log data to provide you with multi-dimensional, visualized traffic analysis, including time trend curves of traffic, requests, and other indicators, as well as country/region distribution and TOP rankings.

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

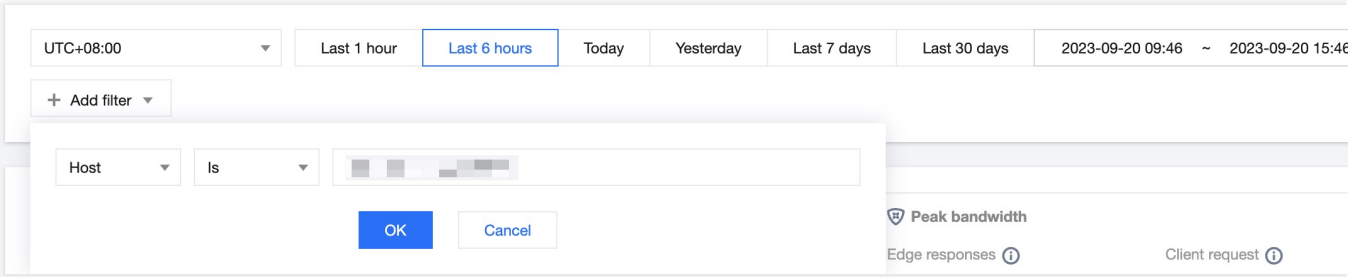
Scenario Example

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

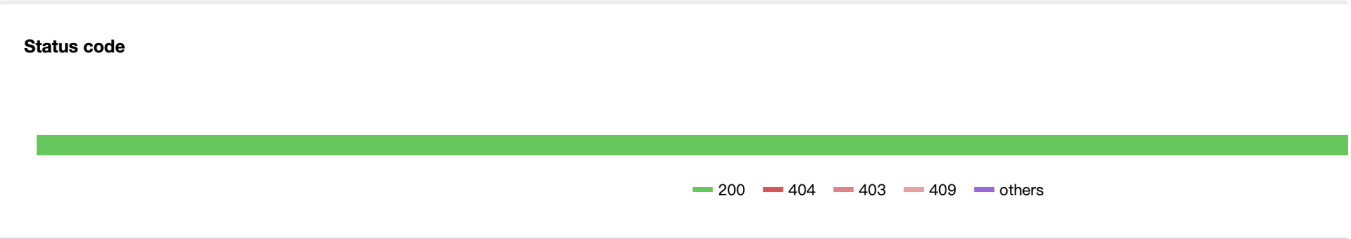
the following operations in the **Data Analysis** > **Traffic Analysis** page.

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.

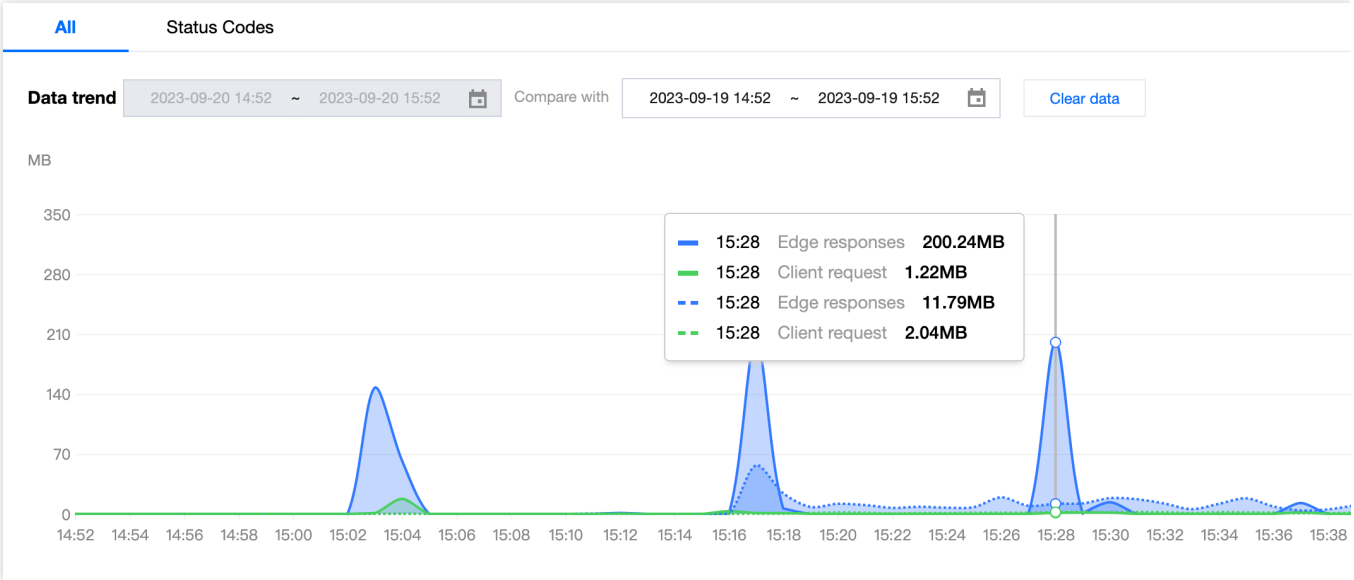
Scenario 2: Monitoring the traffic trend of all sites under the account

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

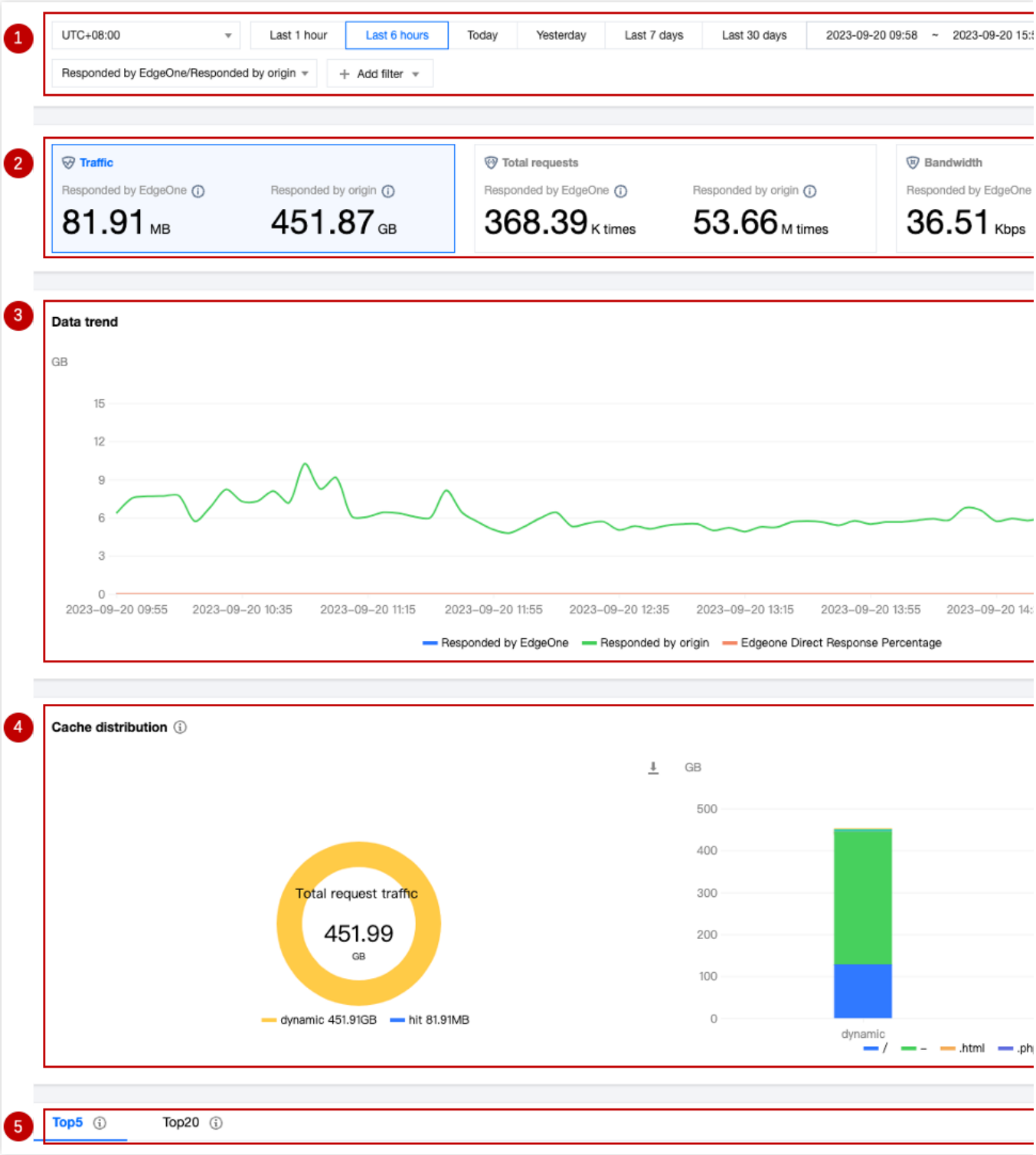
Last updated：2023-11-24 14:55:36

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

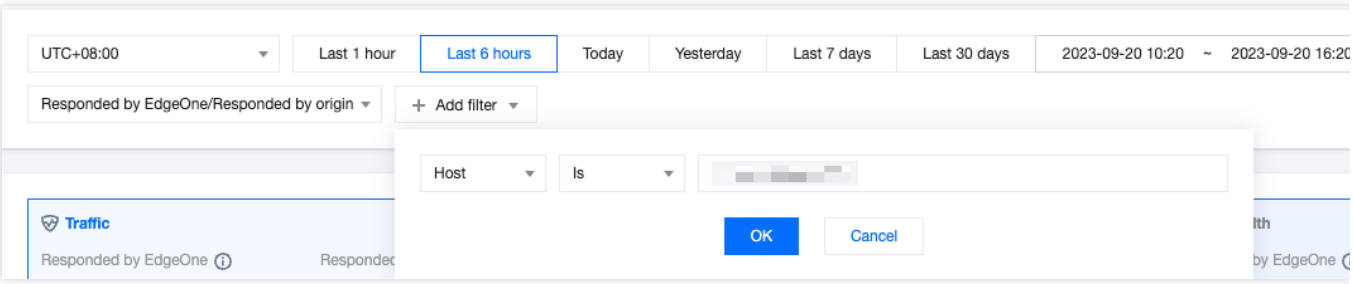
Continuously monitor the cache hit rate of the specified domain through the trend chart in cache analysis, combined with different filter items.

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

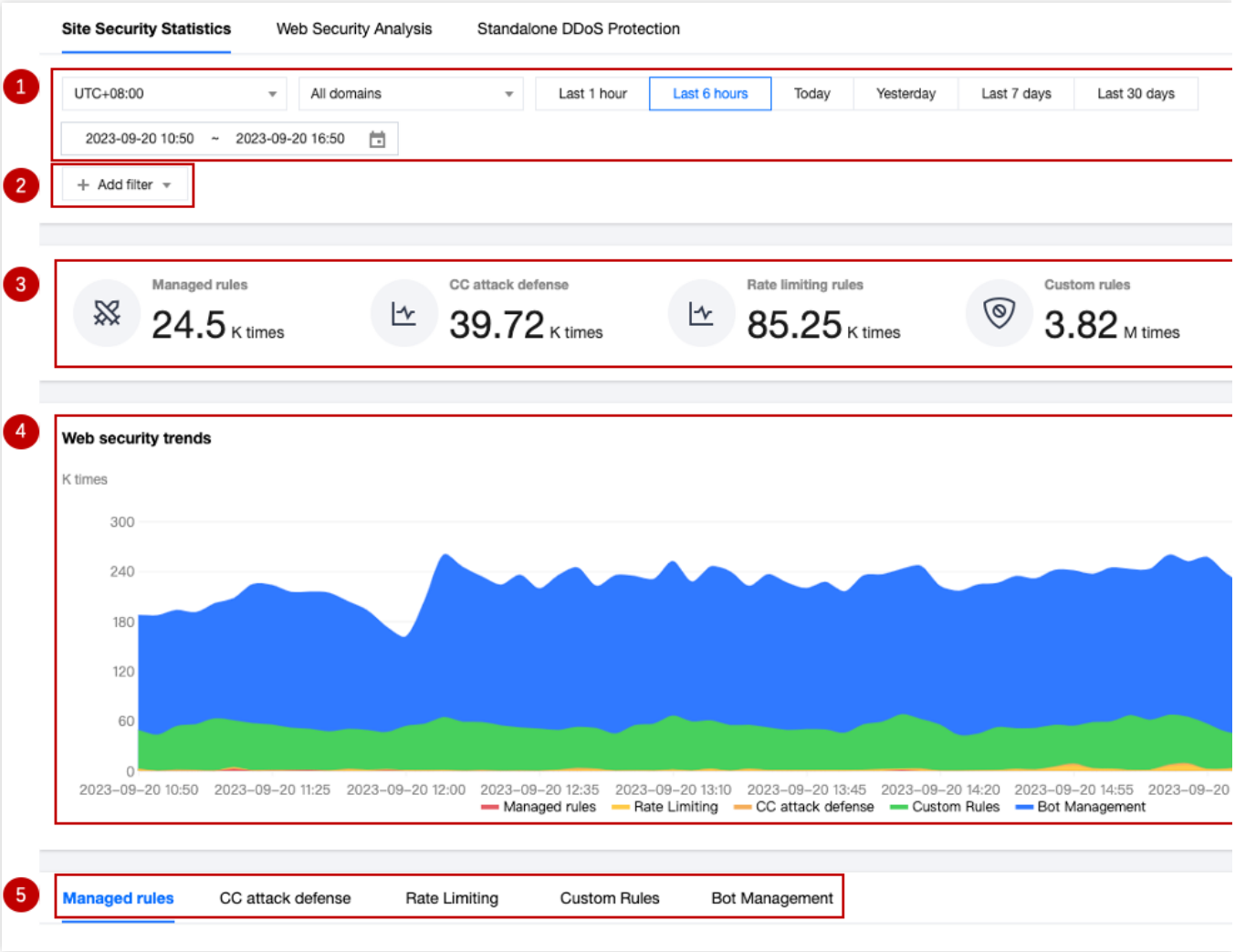
Last updated：2023-09-21 15:07:19

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:

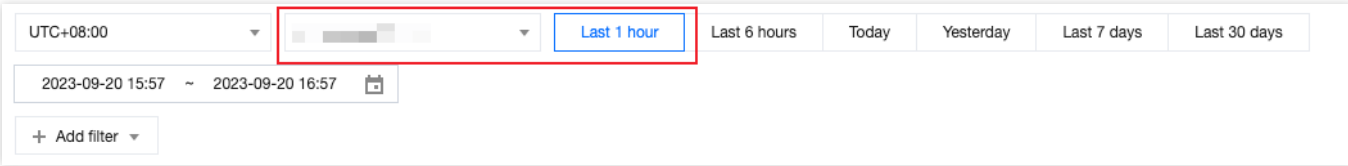
When the number of intercepted malicious clients exceeds 2000, it usually means that the attacker has invested more resources and called one or more botnet networks. Please consider upgrading to the Enterprise version and purchasing independent DDoS protection to ensure that there are sufficient protection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

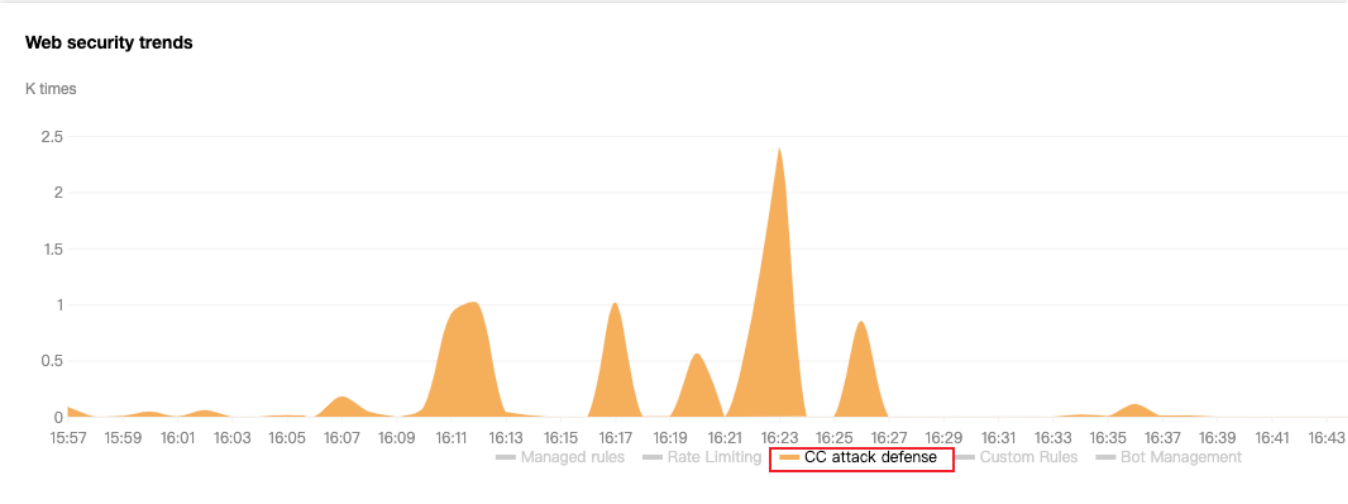
Directions

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.

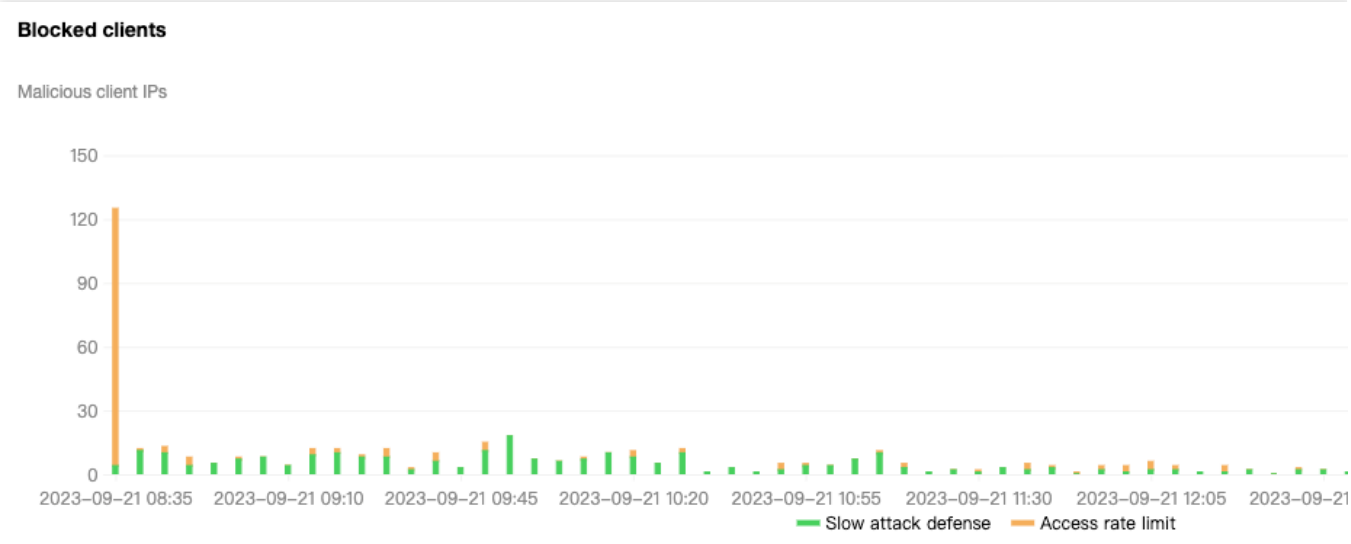


4. After filtering, the security analysis data will be automatically queried according to the filtering results. View the Web Protection trend, and you can click on the indicator value below the legend to close the display of other indicators and

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

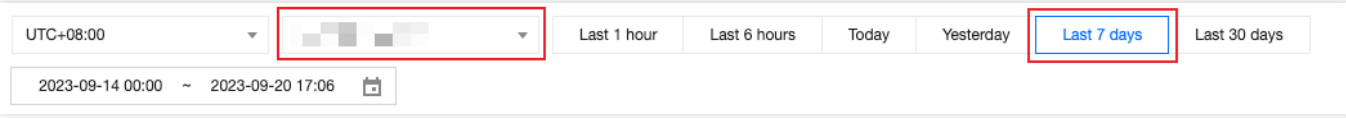
When using Managed rules to protect against vulnerability attacks, it is necessary to test and fine-tune to avoid false-positive rate. At this time, the Site Security Overview can help you evaluate the overall recognition of the rules and quickly identify rules that may have false alarms.
In general, 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

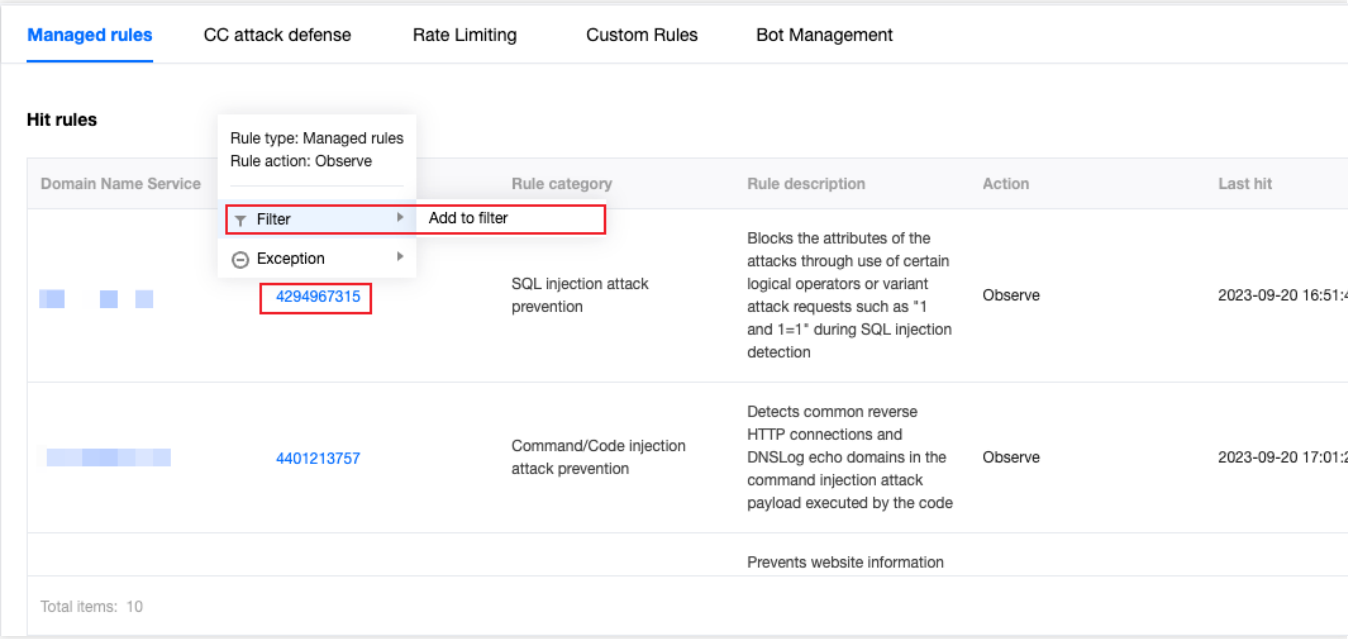
When you continuously receive feedback from different users that their current requests are blocked and they cannot access the content of the domain www.example.com within the site example.com, you need to check whether the user's request is blocked due to hitting the security protection rule and needs 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

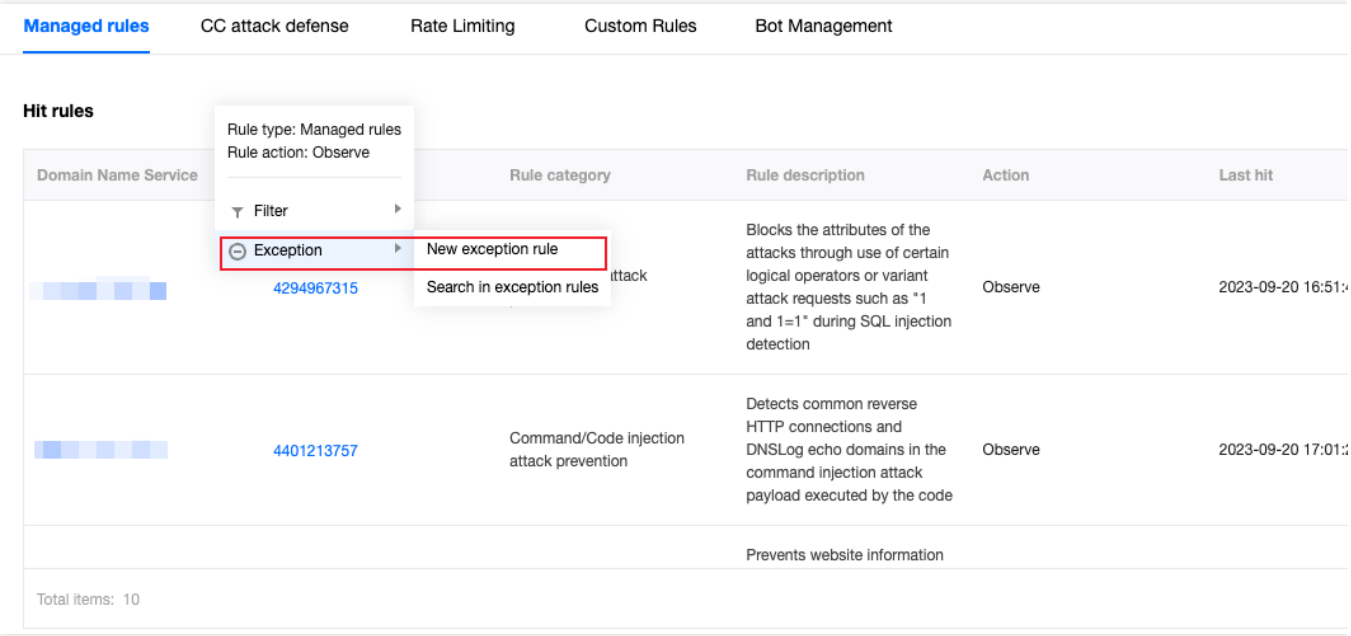
1. Log in to the EdgeOne console, click on the Site List in the left menu bar, click on the site to be configured in the Site List, and enter the Site Details Page.
2. In the Site Details Page, click Data Analysis > Security Protection, and enter the Site Security Overview analysis page by default.
3. 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.

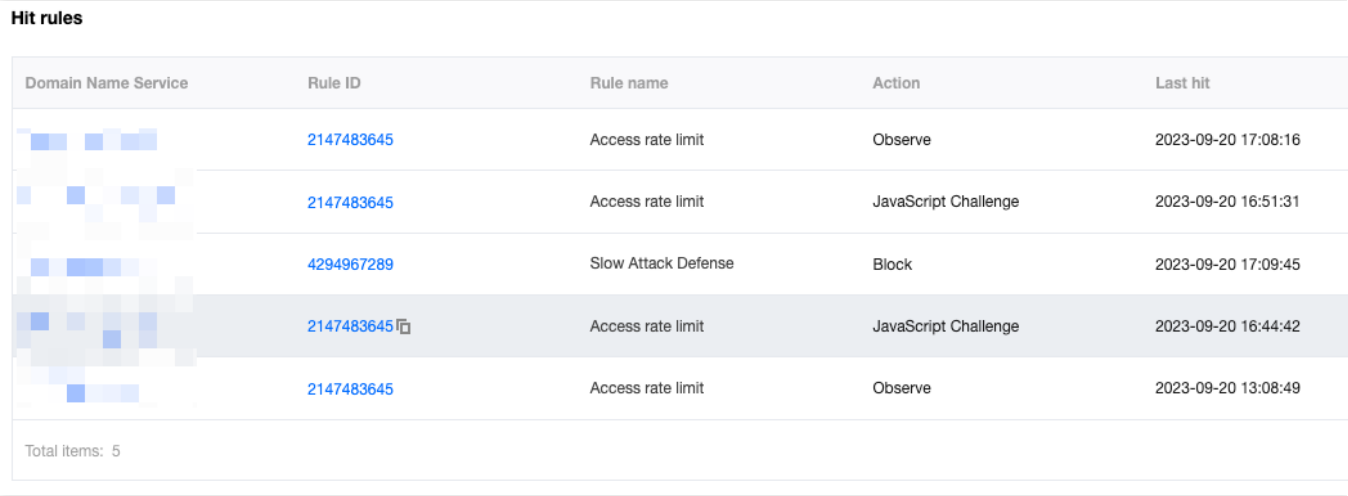
Scenario 3: Viewing the Overall Security Trend of All Sites

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.



Hit rules

Domain Name Service	Rule ID	Rule name	Action	Last hit
	2147483645	Access rate limit	Observe	2023-09-20 17:08:16
	2147483645	Access rate limit	JavaScript Challenge	2023-09-20 16:51:31
	4294967289	Slow Attack Defense	Block	2023-09-20 17:09:45
	2147483645	Access rate limit	JavaScript Challenge	2023-09-20 16:44:42
	2147483645	Access rate limit	Observe	2023-09-20 13:08:49

Total items: 5

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

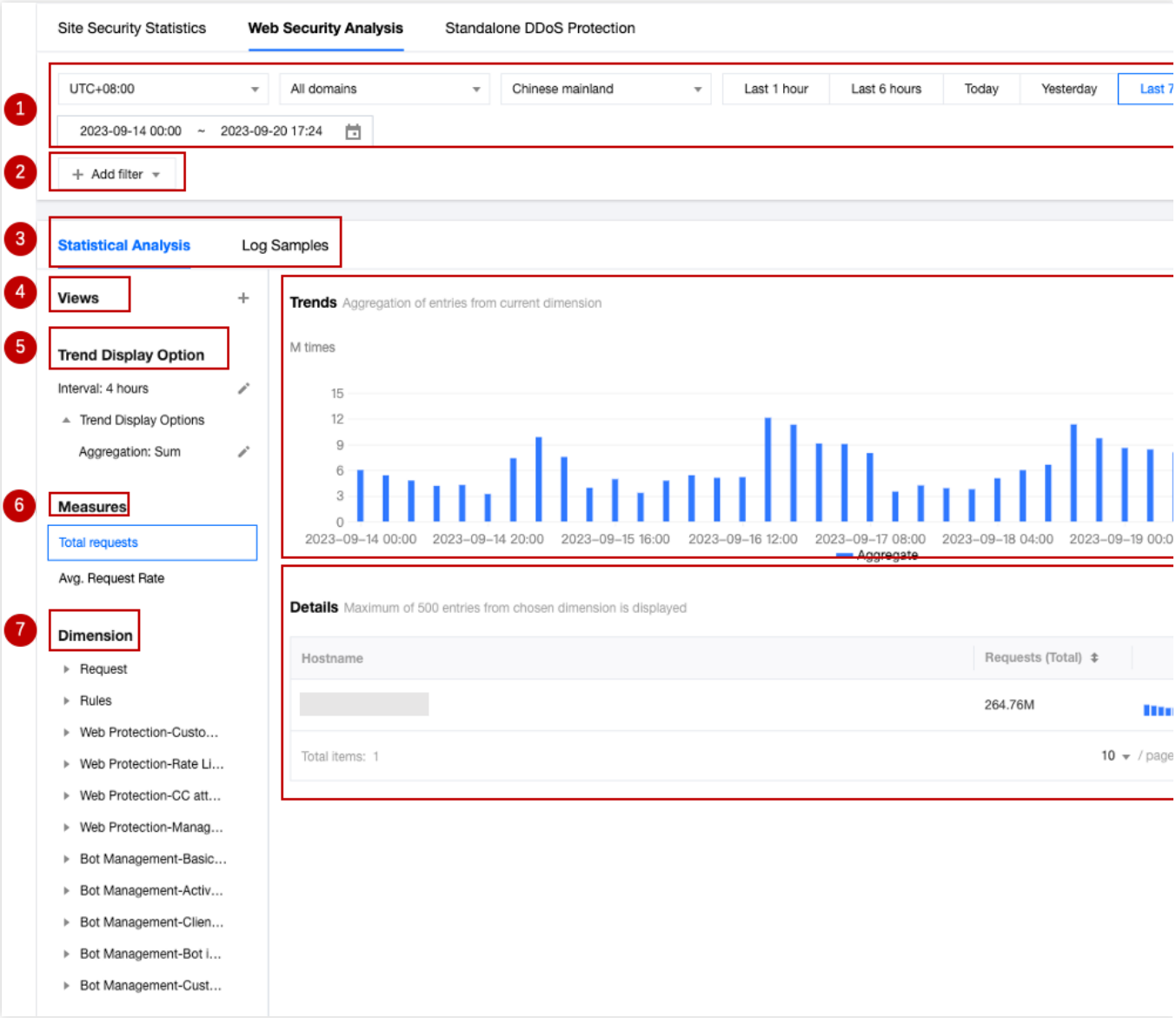
Last updated：2023-09-21 15:03:49

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

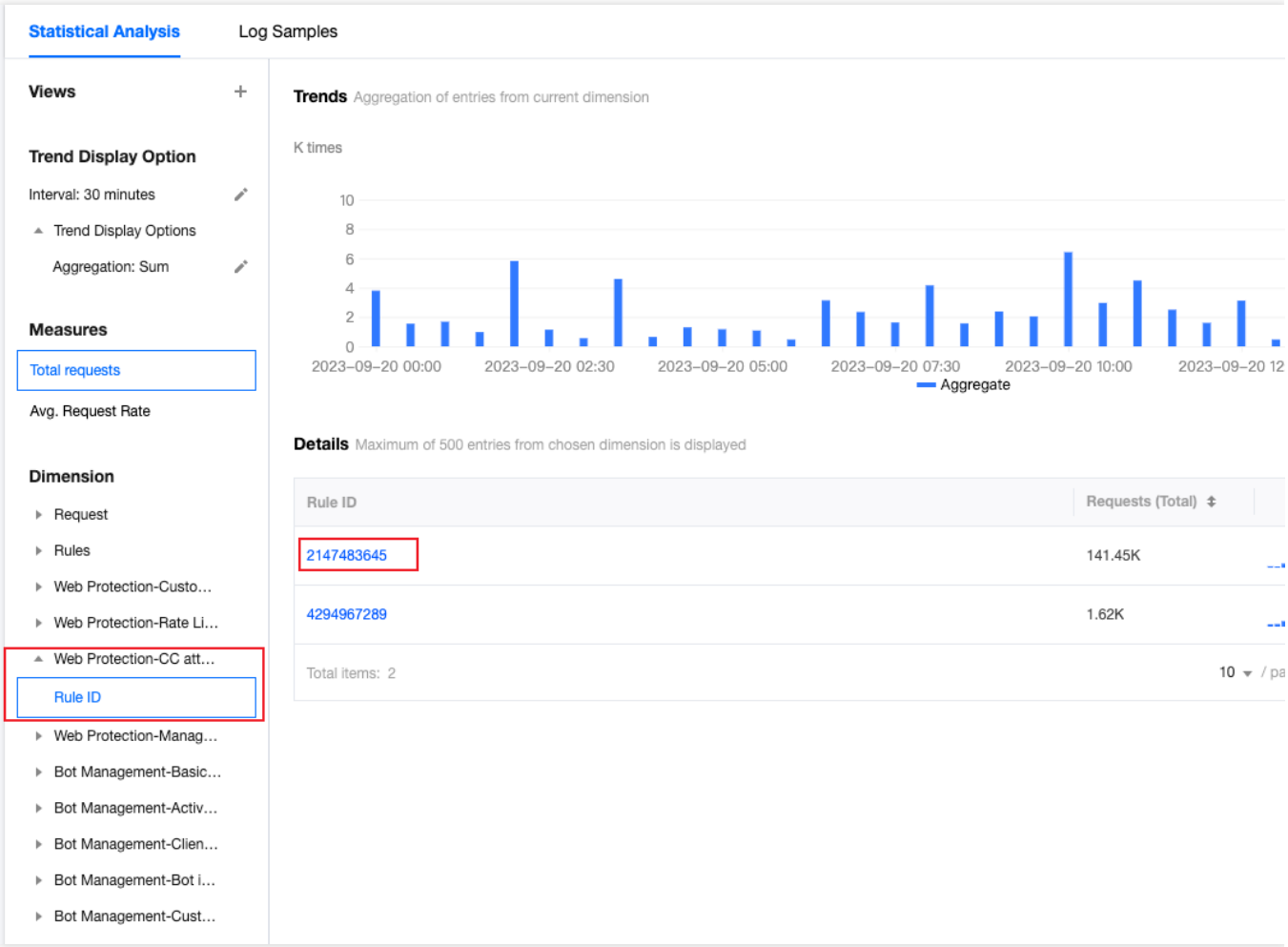
Scenario 1: Analyze the request trend of CC attack defense in the past 1 day

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.

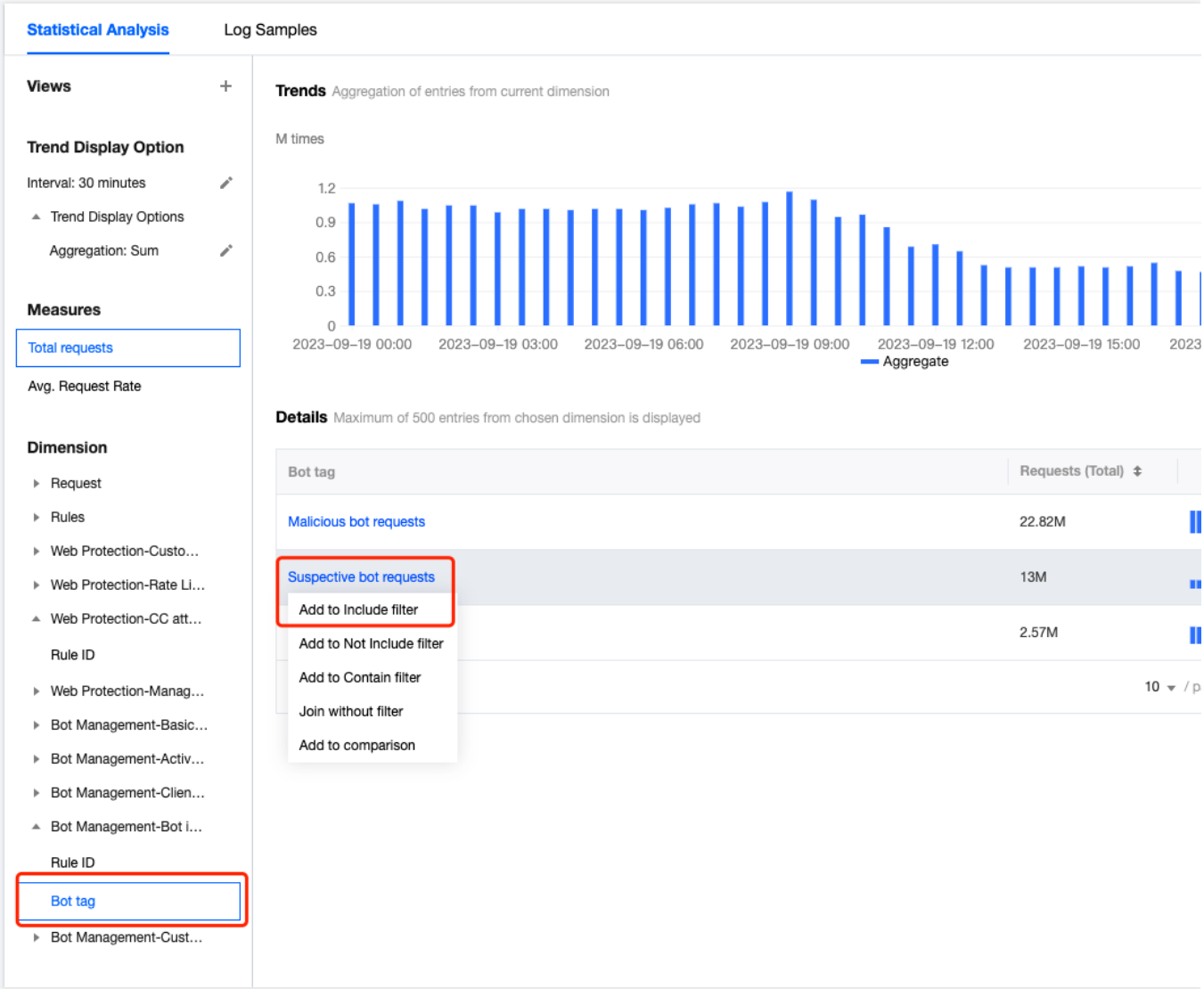
Scenario 2: Analyze whether there are abnormal requests in suspicious bot requests within the last 1 day

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 Filter** 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

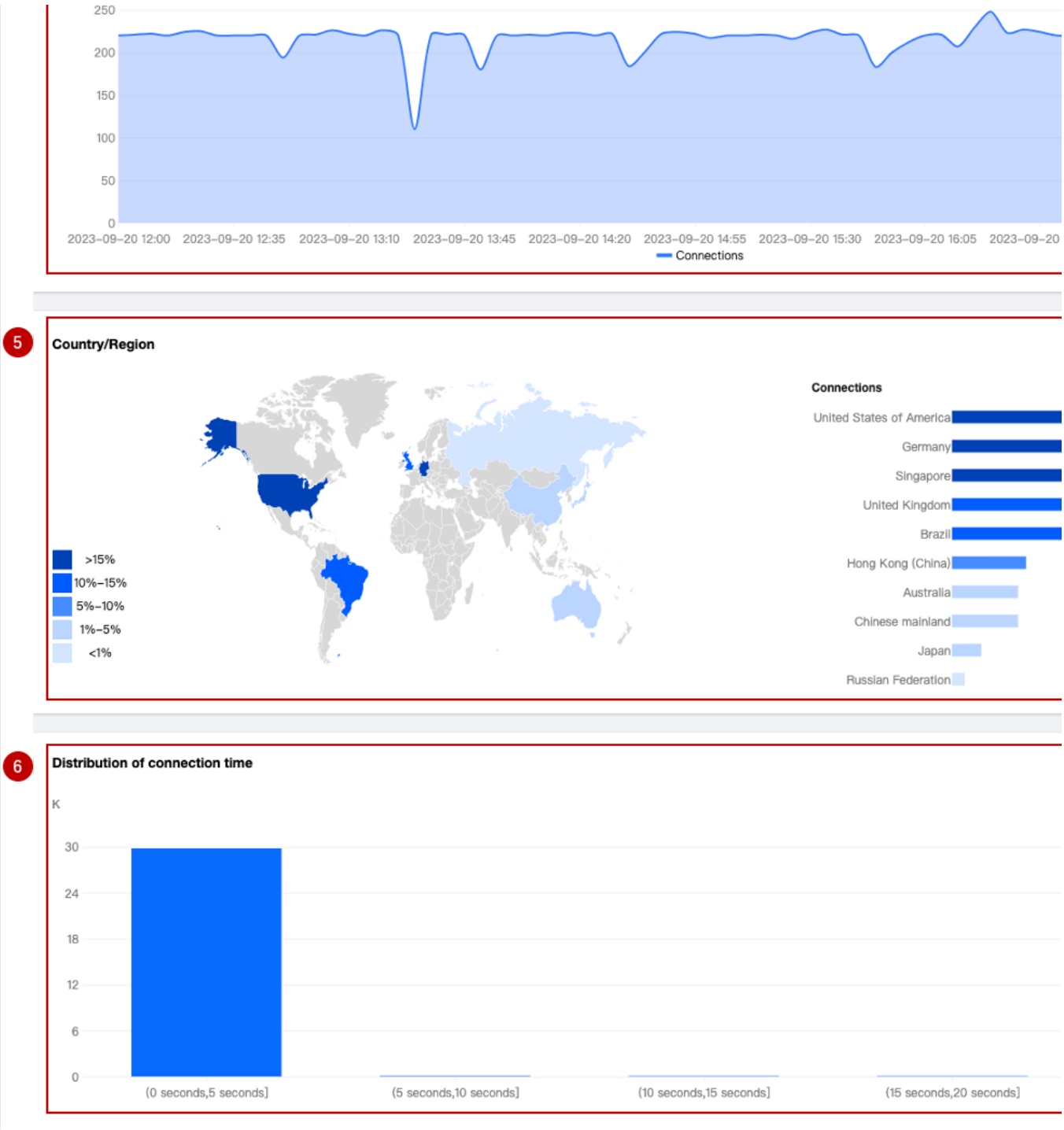
Last updated：2023-09-21 11:36:39

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.

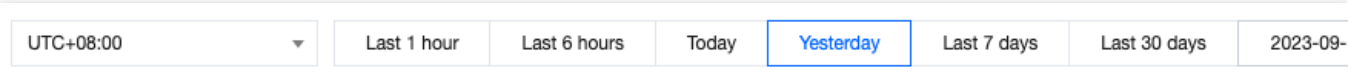
2 hours < Time Range ≤ 48 hours: 5 minutes.

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

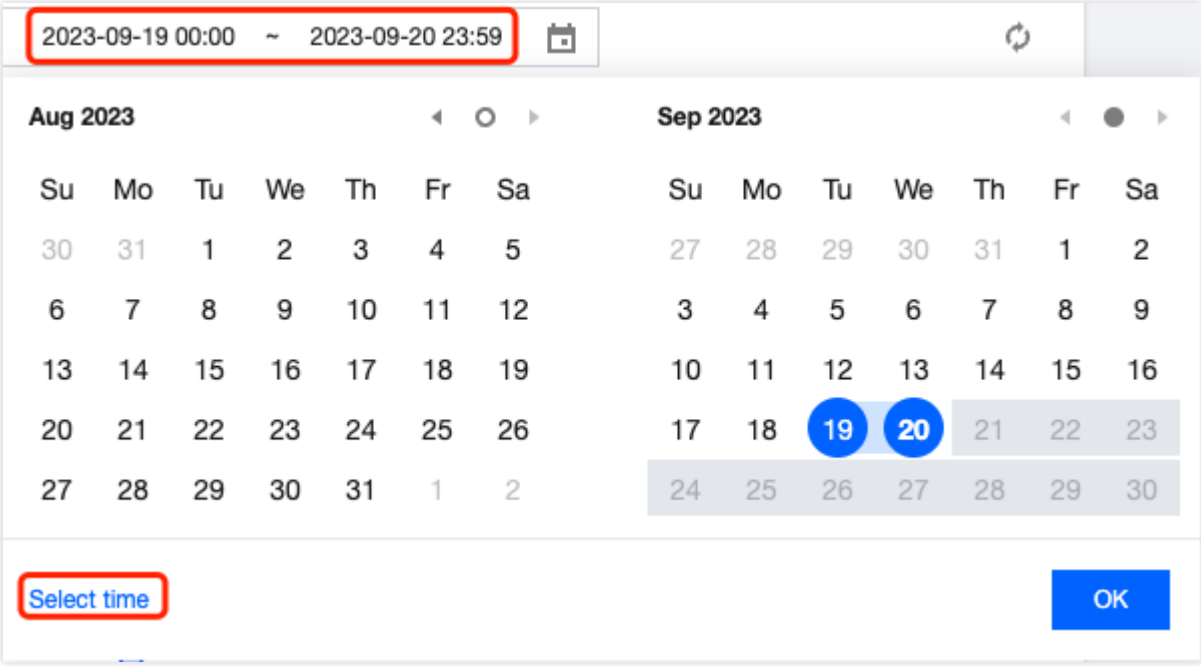
Time Range > 7 days: 1 day.

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.

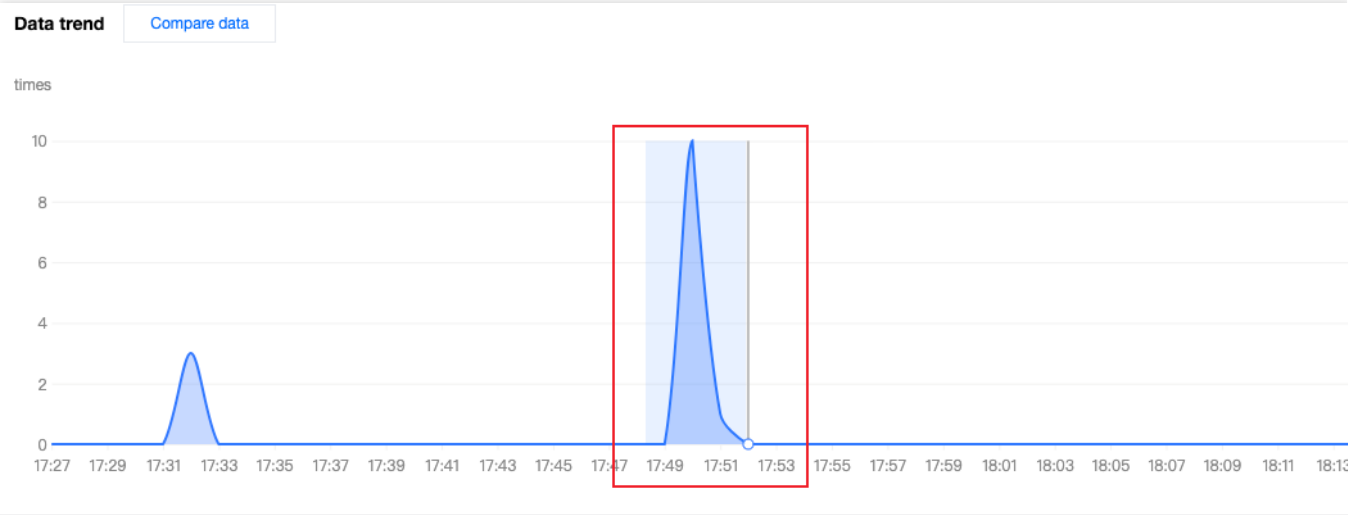


Note:

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

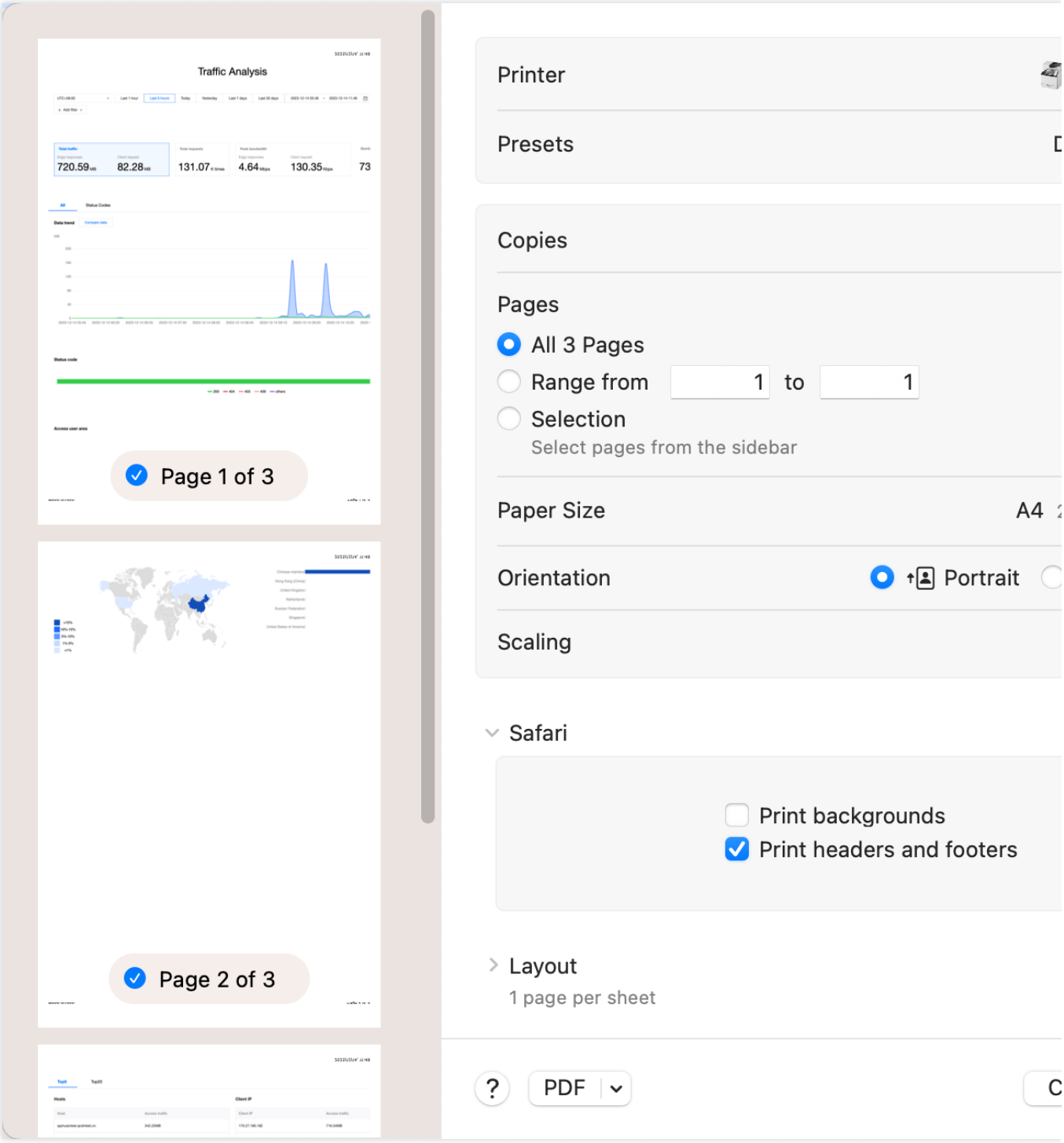
1. Log in to the EdgeOne Console and enter any **Data Analysis** page.
2. Click

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.



Analytics

Last updated：2024-07-23 18:38:12

Overview

Analysis is a powerful data analysis service provided by the EdgeOne platform. It aims to help users gain deep insights into business operations and security status. By monitoring and analyzing key indicators in nearly real-time, users can quickly identify issues, optimize resource configurations, and enhance the stability and security of their business.

Supported metrics

Analytics allows users to customize displaying data metrics, including the following operations:
1. **Display and sort metrics**: Users can choose whether to display a certain metric in the **Metric settings** and sort metrics by dragging to determine the display order on the dashboard.
2. **Select time range**: Users can choose different time ranges to view data, such as the last 30 minutes, the last hour, today, etc. The time span for a single filter does not exceed 31 days.
3. **Set filters**: Users can add filters to refine the data viewed, such as filtering by domain name, status codes, country/region, etc.

Note:
Support for historical time ranges and filters may vary depending on your plan version. For details, please refer to the Comparison of EdgeOne Plans.
Analytics supports the following metrics:

Domain related

L7 client traffic: traffic statistics between the client and EdgeOne; after clicking **EdgeOne response traffic**, you can view data by client IP locations, hosts, client IPs, Referers, URL Paths, resource types, status codes, client browser types, client device types, client operating systems and more.
L7 client bandwidth: bandwidth statistics between the client and EdgeOne;
L7 client requests: statistics of the number of client HTTP(s) requests received by EdgeOne;
L7 security policy hits: statistics of the number of times requests hit EdgeOne Web Security rules; after clicking a certain type of security rule (e.g., Custom Rules), you can view more detailed data, such as top matched rules, client IPs, URL Paths, client IP locations, recent events, and more.
L7 origin traffic: traffic statistics between EdgeOne and the origin server;
L7 origin bandwidth: bandwidth statistics between EdgeOne and the origin server;

L7 origin requests: statistics of the number of requests EdgeOne initiated to the origin server;
DNS queries: number of resolution requests received by EdgeOne DNS. Only data from sites accessed in NS mode are supported.

TCP/UDP application related

L4 client traffic: traffic statistics between the client and EdgeOne;
L4 client bandwidth: bandwidth statistics between the client and EdgeOne;
L4 concurrent connections: number of transport layer connections simultaneously established between the client and EdgeOne. Supports viewing the regional distribution of concurrent connections.

L3/4 DDoS protection

L3/4 DDoS attack bandwidth: blocked bandwidth, packet rate, and number of attack events for network and transport layer DDoS attacks. Supports viewing protocol ranking of blocked traffic and packets. Supports viewing latest attacks, attacker distribution, and attack types.

EdgeOne Shield

EdgeOne Shield served traffic: traffic responded by the EdgeOne Shield service;
EdgeOne Shield served requests: the number of requests responded by the EdgeOne Shield service.