边缘安全加速平台 EO

数据分析与日志服务

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

版权所有：腾讯云计算（北京）有限责任公司

数据分析与日志服务
日志服务
实时日志
概述

最近更新时间：2023-08-16 16:02:20

功能概述

当您的站点接入 EdgeOne 后，EdgeOne 为您提供了丰富的预制报表，帮助您监控、分析业务的运行情况，包括流量分析、缓存分析、四层代理、安全分析等。但是在数据分析中，您可能会存在更加个性化的数据分析诉求，例如以下数据分析场景：

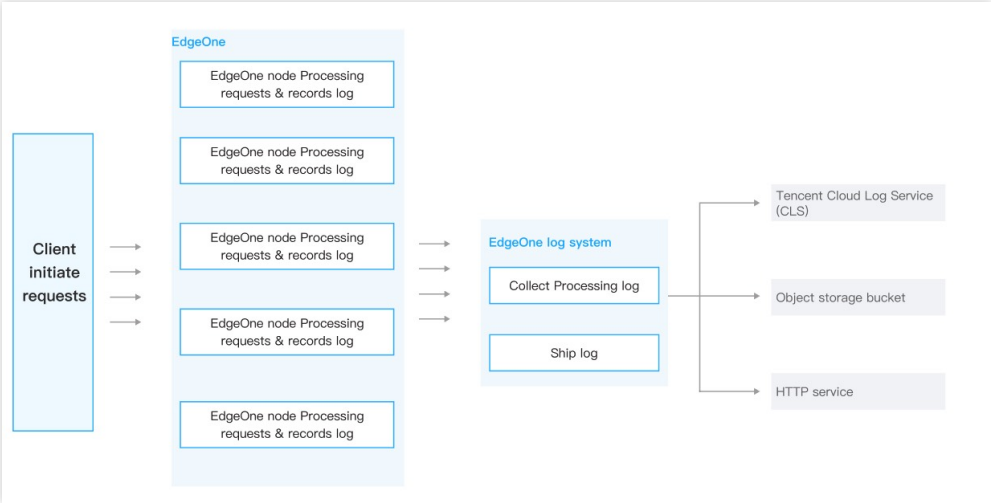
场景	场景诉求
深度数据分析	需要指定一个或者多个条件，查找符合条件的日志。例如： 通过指定客户端 IP 查询指定时间范围内的访问统计（访问 URL、访问次数等）。 通过筛选状态码、时间、URL 细化分析状态码的分布情况。 通过筛选处置方式为观察的日志，汇总携带的请求头内容及其他请求特征信息，调整安全策略。
监控服务指标	分析 EdgeOne 服务的质量以及用户的访问效率，以便及时发现异常。访问效率包括 EdgeOne 整体响应耗时、下载速度、回源响应耗时等。
鉴别盗刷	通过分析流量异常、访问模式、访问频率，鉴别存在盗刷等行为客户端 IP 。
统一多厂商监控数据	自建数据大屏，统一监控多个云厂商的应用数据。
存储日志	需要用户相关访问日志保留30天以上。

针对以上场景诉求，EdgeOne 实时日志服务提供了日志的实时采集与推送的能力，可将您的日志推送到腾讯云日志服务（CLS）或您自建的数据中心内，帮助您自行实现对日志数据的灵活检索与分析。目前 EdgeOne 支持将站点日志、四层代理日志及安全服务日志推送到以下目的地：

腾讯云日志服务（CLS）：推送至腾讯云提供的一站式日志处理服务（CLS），可用于在 CLS 上进一步对日志做检索分析。

对象存储：兼容 AWS Signature V4 鉴权方法的存储桶。

HTTP 服务（POST）：通过 HTTP POST 请求将日志推送到指定的后端服务器。



说明：

1. 通常情况下，日志投递的延迟在 2 - 5 分钟内。为了确保日志投递的实时性，EdgeOne 将固定的日志数量或者固定时间周期为一个批次，将日志推送到相应的目的地。
2. 实时日志推送至 CLS 服务时，可能在 CLS 产生流量、存储等费用，相关费用由 CLS 产品收取，详情请参见 日志服务计费说明。

计费和配额说明

计费说明：实时日志推送是一项增值服务，计费方式基于推送的日志数量，详细请查看 增值服务用量单元费用（后付费）。

配额说明：实时日志推送任务数量根据套餐不同会有不同的任务配额，具体配额请查看 套餐选型对比。

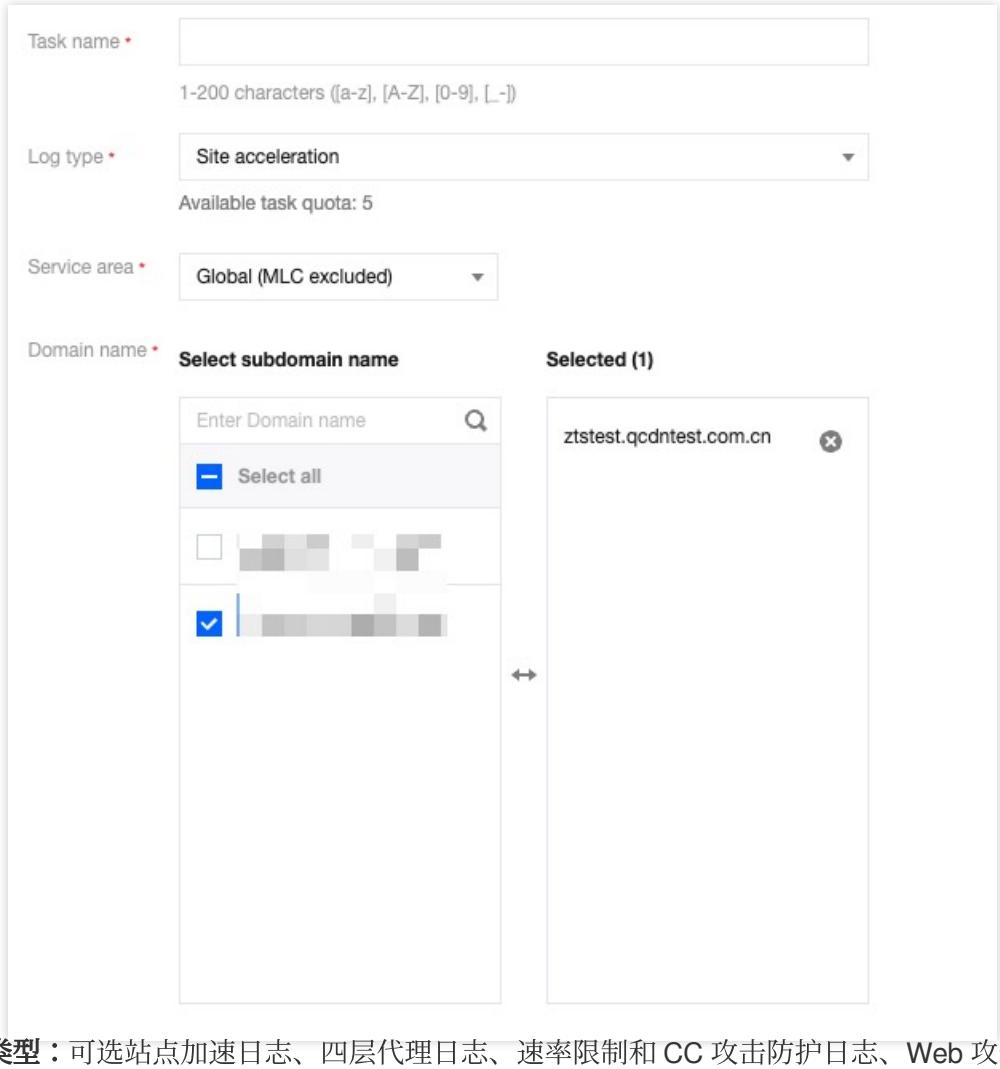
推送实时日志

最近更新时间：2024-01-02 10:24:58

本文档将指引您如何将日志推送到指定的服务内。

步骤1：选择日志源

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**日志服务 > 实时日志。**
3. 在实时日志页面，单击**新建推送任务。**
4. 在选择日志源页面，选择需要推送的日志源信息，配置相关参数，单击**下一步**。



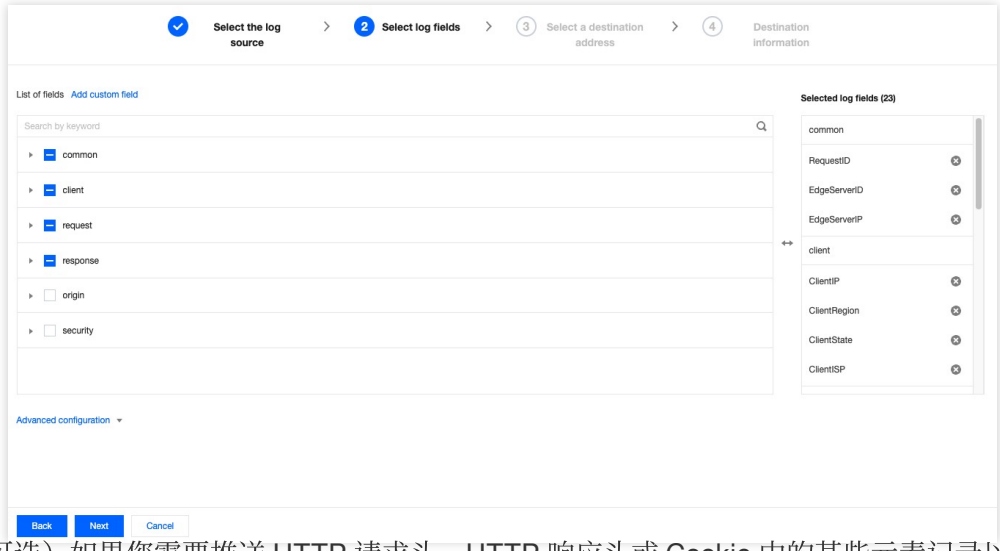
日志类型：可选站点加速日志、四层代理日志、速率限制和 CC 攻击防护日志、Web 攻击防护日志、自定义规则日志、Bot 管理日志；

服务区域：选择需要推送的日志区域，EdgeOne 实时日志推送任务可分别推送「中国大陆可用区」或「全球可用区（不包括中国大陆）」的日志，但无法直接推送「全球可用区」的日志。如果您需要推送「全球可用区」的日志，

请建立两个推送任务，一个针对「中国大陆可用区」，另一个针对「全球可用区（不包括中国大陆）」。
域名：选择需要推送日志的子域名或四层实例。同一份日志不支持配置多个推送任务，即相同地域下子域名/四层代理实例的日志仅支持配置一个推送任务，例如：`www.example.com` 的「中国大陆可用区」站点加速日志配置了日志推送任务 A，此时日志推送任务 B 无法选择到 `www.example.com` 。

步骤2：选择日志字段

1. 在选择日志字段中，配置需要推送的字段内容，您可以在字段列表中，通过勾选进行选择；相关字段说明请参考：实时日志字段说明。
说明：
目前仅 **站点加速日志** 和 **四层代理日志** 支持自定义选择需要推送的日志。



2. （可选）如果您需要推送 HTTP 请求头，HTTP 响应头或 Cookie 中的某些元素记录以进行分析时，您可以点击添加自定义字段，配置需要推送的 HTTP 请求头、HTTP 响应头或 Cookie 名称。您可以通过键值对形式将此类信息精确记录在日志中。以 `Accept-Language` 头为例，其对应的信息可以直接通过日志中的 `Accept-Language` 字段获取。
说明：
1. 字段默认区分大小写，因此需要与原始字段完成匹配；
2. 目前仅**站点加速日志**支持添加自定义字段。
3. （可选）如果您的日志量非常大，实时日志推送后仅用于监控及分析，不需要全量的日志数据，您可以点击高级配置，配置采样比例来降低日志推送的数量。配置后，EdgeOne 将按照设定的百分比随机抽取日志，然后将其推送到您指定的目的地。

4. 配置完成日志字段后，点击下一步，进入步骤3。

步骤3：选择推送目的地

选您可以根据需要推送的实时日志目的地，选择推送至腾讯云 CLS、S3 兼容存储桶或者指定的 HTTP 服务器内，参考如下步骤进行配置：

推送至腾讯云 CLS

推送至 S3 兼容存储

推送至指定 HTTP 服务器

如果当前您还未自建数据分析系统，腾讯云提供了日志服务（CLS）可帮助您一站式完成实时日志的采集、推送与检索分析，减少您的开发及维护成本。您可以参考以下步骤将实时日志推送至腾讯云 CLS 服务内：

前提条件

当前已开通先开通 日志服务（CLS） 并授权腾讯云 EdgeOne 以创建日志集。

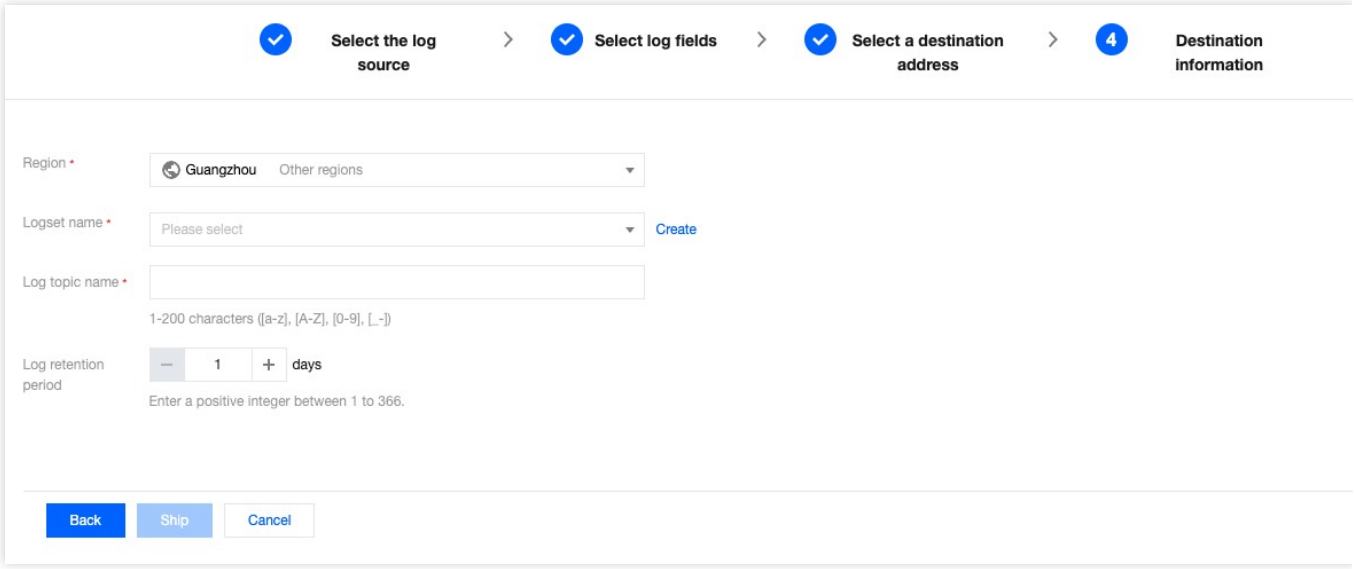
说明

1. 日志服务（CLS）为付费服务，相关费用请参考：日志服务计费概述。
2. 建议您使用主账号启用服务，若为子账号或协作者，您需要为其授权相关权限。

操作步骤

创建推送任务

1. 在 **第 ③ 步** 中选择目的地为 **腾讯云日志服务（CLS）**，并点击 **下一步** 。
2. 填写相关参数信息，参数说明如下：



地域：选择需要推送的目标地域。

目标集名称：选择目标地域下的日志集。

说明

若此处为空或需要新建日志集，请单击**创建**，在所选地域下创建日志集。

日志主题名称：可输入1-200个字符，允许的字符为 `a-z, A-Z, 0-9, _, -` 。

日志保存时间：请输入1-366间正整数。

相关参考

日志检索

日志检索支持多种类型的检索分析方式及图表分析形式，详细说明可见 日志检索。

EdgeOne 以推送任务为单元进行日志检索。在 实时日志页面，选择您需要检索的推送任务，单击**检索**，进入日志检索页面。

您可后续通过 日志服务（CLS） 侧管理日志集等模块，如修改日志集名称。

日志集

日志集（Logset）是腾讯云日志服务（CLS）的项目管理单元，用于区分不同项目的日志，一个日志集对应合集。腾讯云 EdgeOne 日志集有以下基本属性信息：

地域：日志集所属 地域 。

日志集名称：日志集命名。

日志保留时间：当前日志集里数据的保存时间周期。

创建时间：日志集创建时间。

日志主题

日志主题（Topic）是腾讯云日志服务（CLS）的基本管理单元，一个日志集可以包含多个日志主题。一个日志主题对应一类应用或服务，建议将不同机器上的同类日志收集到同一个日志主题中。例如，一个业务项目有三种日志：

操作日志、应用程序日志、访问日志，每种类型可以创建对应日志主题。

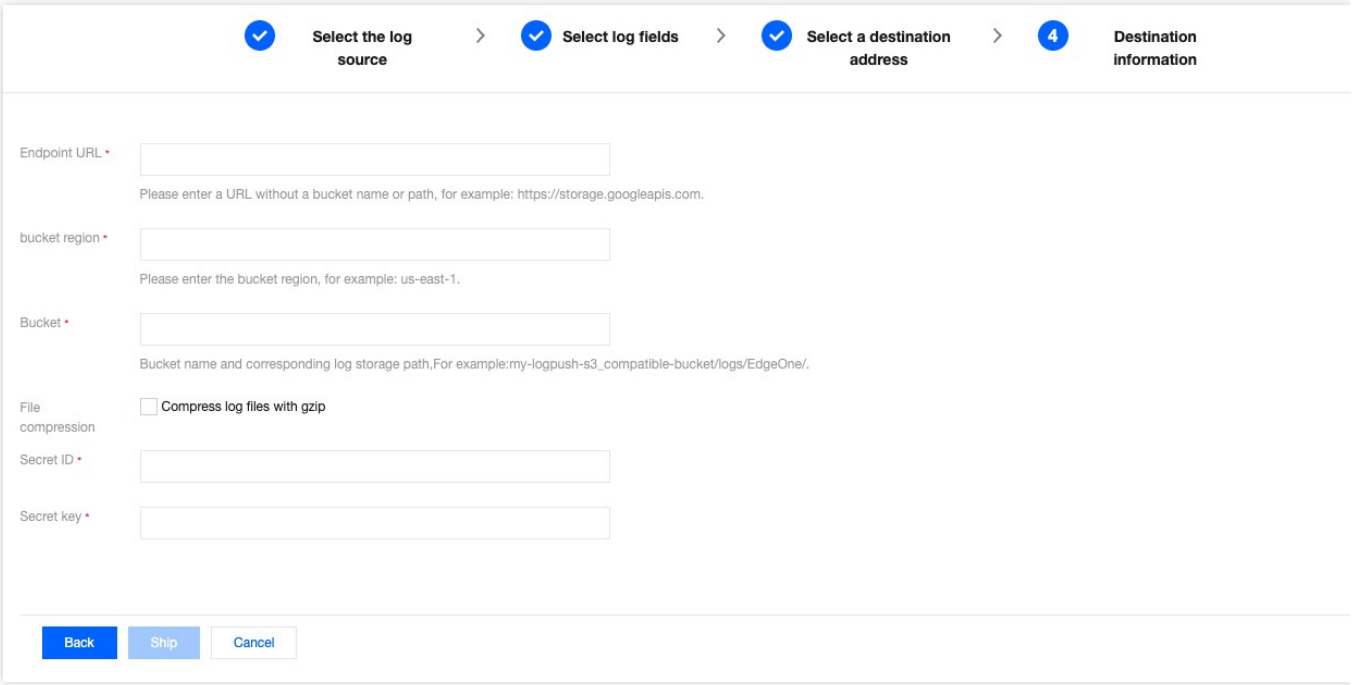
日志服务系统以日志主题为单位，区分管理用户不同的日志数据，每个日志主题都可以配置不同的数据源、不同的索引规则和投递规则。因此，日志主题是日志服务配置、管理日志数据的基本单元，创建日志主题后需配置相关规则，才能如期有效地进行日志采集，并使用检索分析和投递等功能。

从场景功能上理解，日志主题主要提供：
采集日志到日志主题。
以日志主题为单元存储管理日志。
以日志主题为单元检索分析日志。
以日志主题为单元投递日志到其他平台。
从日志主题下载、消费日志。
说明
以上信息摘自 日志服务（CLS） 产品文档，请以日志服务（CLS）侧的说明为准。
每一个推送到腾讯云日志服务（CLS）的实时日志推送任务会将所选子域名的日志推送到一个对应的日志主题。

如果您当前已有自建的数据源，需要将实时日志推送到兼容 S3 存储桶，您可以参考以下步骤操作继续操作：
说明：
目前仅支持将站点加速日志、四层代理日志推送至兼容 S3 存储桶。
推送日志格式为 JSON Lines。

操作步骤

1. 在 **第 ③ 步** 中选择目的地为 **S3 兼容**，并点击 **下一步** 。
2. 填写对应的目的地参数：
端点 URL：不包含存储桶名称或路径的 URL，例如：`https://storage.googleapis.com` 、 `https://s3.ap-northeast-2.amazonaws.com` 。
存储桶地域：存储桶所在的地域，例如： `ap-northeast-2` 。
存储桶：存储桶名称和对应的日志存储路径：例如： `your_bucket_name/EO-logs/` 。
文件压缩：是否使用 gzip 压缩日志文件，勾选后，推送的日志文件将使用 gzip 压缩，文件名称将改为 `filename.log.gz` 。
SecretId：访问存储桶使用的 Access Key ID。
SecretKey：访问存储桶使用的 secret key。



说明：

1. 存储桶需要兼容 AWS Signature Version 4 鉴权算法，具体兼容情况请参考您的存储桶提供方的说明。
2. 文件名称说明：日志将会在指定存储桶路径下以 `UploadTime_Random.log` 格式存储，且会以日期（UTC +00:00）为一个文件夹归档日志，例如：`logs/20230331/20230331T185917Z_2aadf5ce.log` 。

UploadTime：日志文件上传时间，使用 ISO-8601 格式，UTC+00:00 时区。

Random：随机字符，当日志量较大的情况，可能会出现同一个上传时间有多个日志文件，通过此串随机字符来标识不同的文件。

3. 单击**推送**，下发实时日志推送任务后，EdgeOne 将推送一个测试文件至目标存储桶路径以校验连通性，例如 `1699874755_edgeone_push_test.txt` ，文件内容为固定字符串“test”。

如果您当前已有自建的数据源，EdgeOne 可通过 HTTP POST 请求调用您提供的后端接口地址，将日志在 HTTP body 中传输到您指定的服务器上。

说明：

1. HTTP 是明文传输，因此接口地址建议您使用 HTTPS 加密后地址。
2. 为了进一步加强请求来源的安全性验证，我们提供了请求鉴权方案，可在配置推送目的地信息中填写相关鉴权信息，鉴权算法见：鉴权算法参考。
3. 推送日志格式为多个 JSON 对象组成的数组，每个 JSON 对象为一条日志。

操作指引

创建推送任务

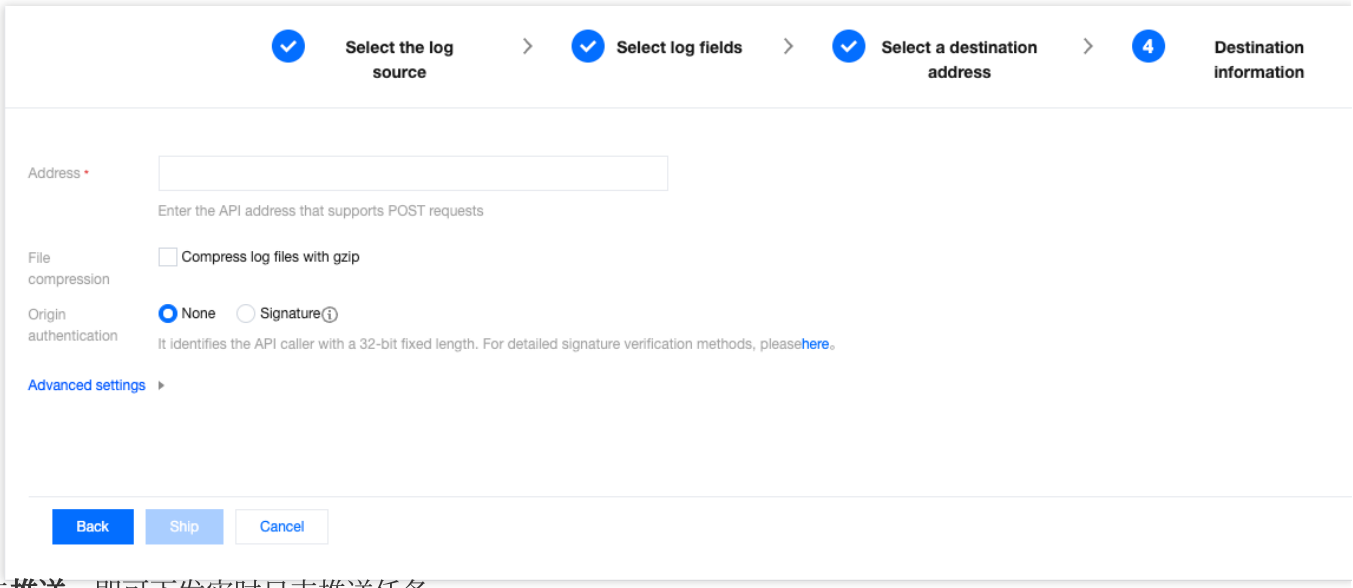
1. 在 **第 ③ 步** 中选择目的地为 **HTTP 服务（POST）**，并点击 **下一步** 。
2. 填写相关目的地及参数信息，参数说明如下：

接口地址：填入您的数据源接口地址，例如：`https://www.example.com/log`

文件压缩：为减少日志文件的大小，节约流量开销，您可以通过勾选 **使用 gzip 压缩日志文件** 开启文件压缩，EdgeOne 将会使用 gzip 格式压缩日志后再传输日志，并且会增加 HTTP 头部 `content-encoding = gzip` 来标明压缩格式。

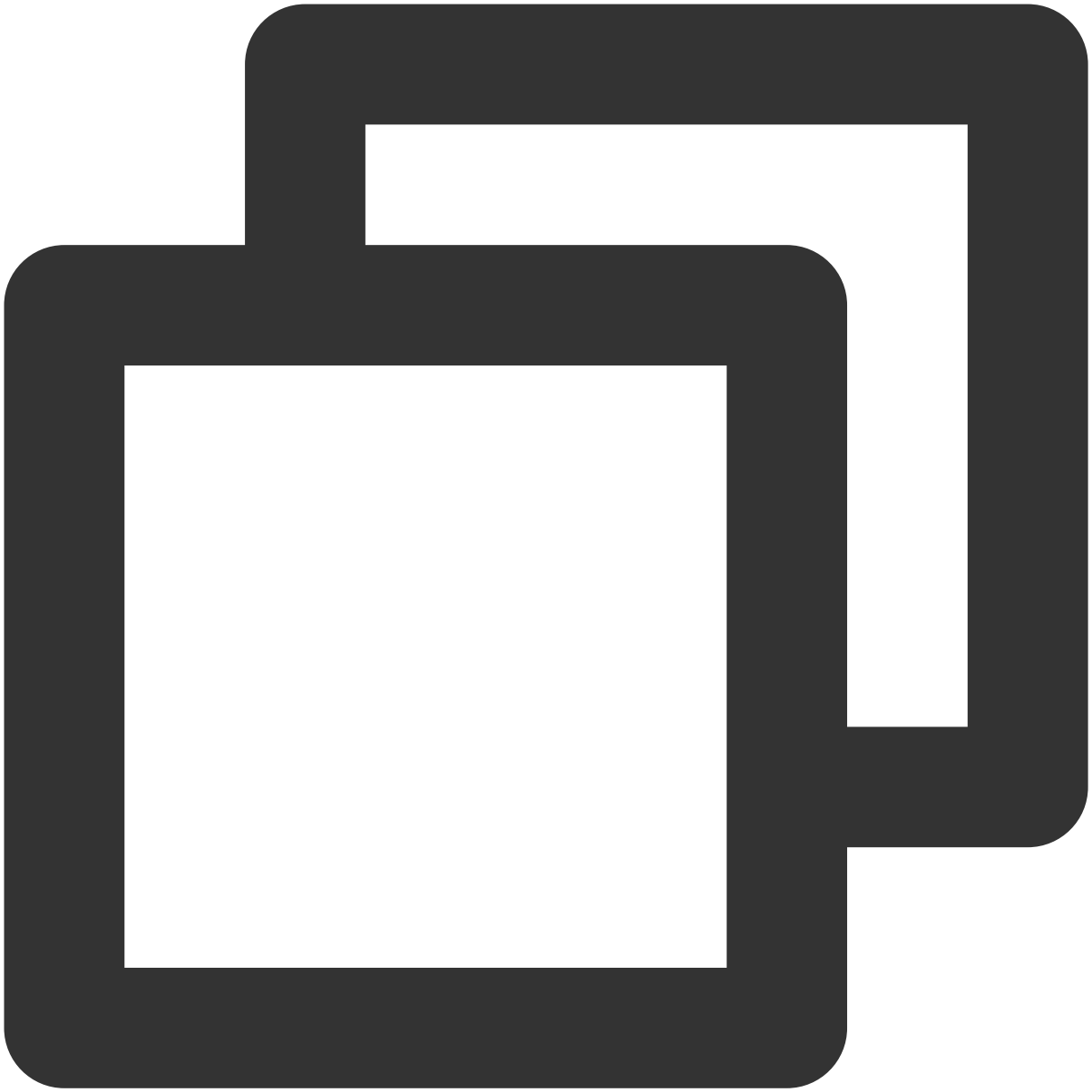
源站鉴权：选择为加密鉴权时，推送日志时将携带鉴权信息供源站进行验证，保证数据来源身份的安全性。

自定义 HTTP 请求头：添加需要 EdgeOne 发起请求时携带的 HTTP 头部。例如：您需要通过头部识别日志来源的厂商是 EdgeOne，您可以添加一个头部 `log-source = EdgeOne` 来识别日志是来源。



3. 单击**推送**，即可下发实时日志推送任务。

4. 实时日志推送任务在配置阶段为了校验接口连通性，将向接口地址发送一个空数据进行验证，数据格式如下所示：




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

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

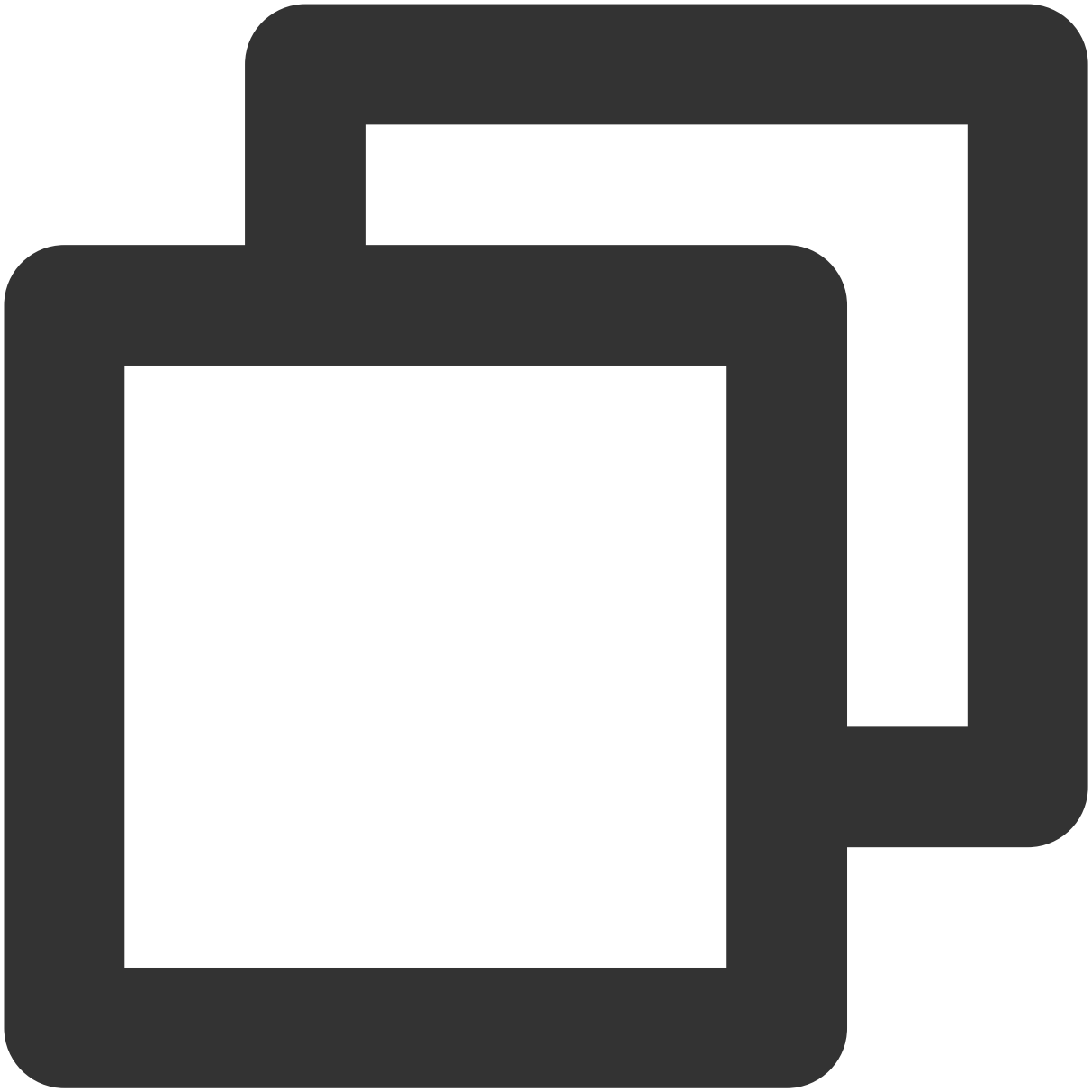
相关参考

请求鉴权算法

如果您在推送目的地信息中，源站鉴权内选择了**加密签名**，可自定义输入您自定义配置 SecretId 和 SecretKey，EdgeOne 将在请求 URL 中增加签名 `auth_key` 和 `access_key`，签名算法详情如下：

1. **请求URL构成**

如下所示，请求 URL 将在？后携带 `auth_key` 和 `access_key` 。



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

参数说明：

timestamp：请求当前时间，使用 Unix 秒级10位时间戳。

rand：随机数

access_key：用于标识接口请求方的身份，即您所自定义配置的 SecretID。

SecretKey：固定长度32，即您所自定义配置的 SecretKey。

uri：资源标识符，例如：`/access_log/post`。

md5hash：md5hash = `md5sum(string_to_sign)`，其中 string_to_sign = `"uri-timestamp-rand-SecretKey"`。通过md5算法计算出的验证串，数字0-9和小写英文字母 a-z 混合，固定长度32。

2. **计算示例**

假定填入参数为：

接口地址：`https://www.example.com/access_log/post`

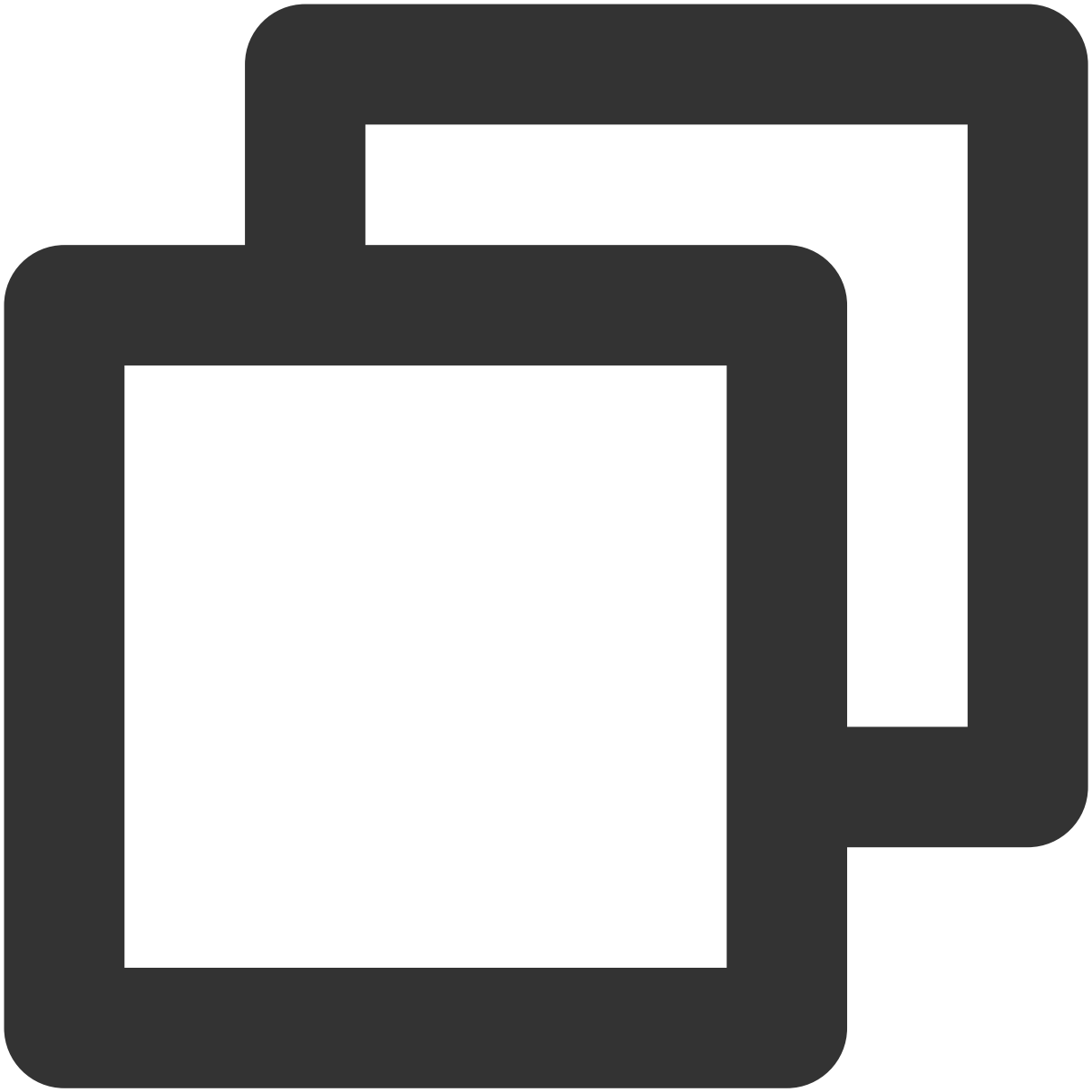
SecretID = `YourID`

SecretKey = `YourKey`

uri = `/access_log/post`

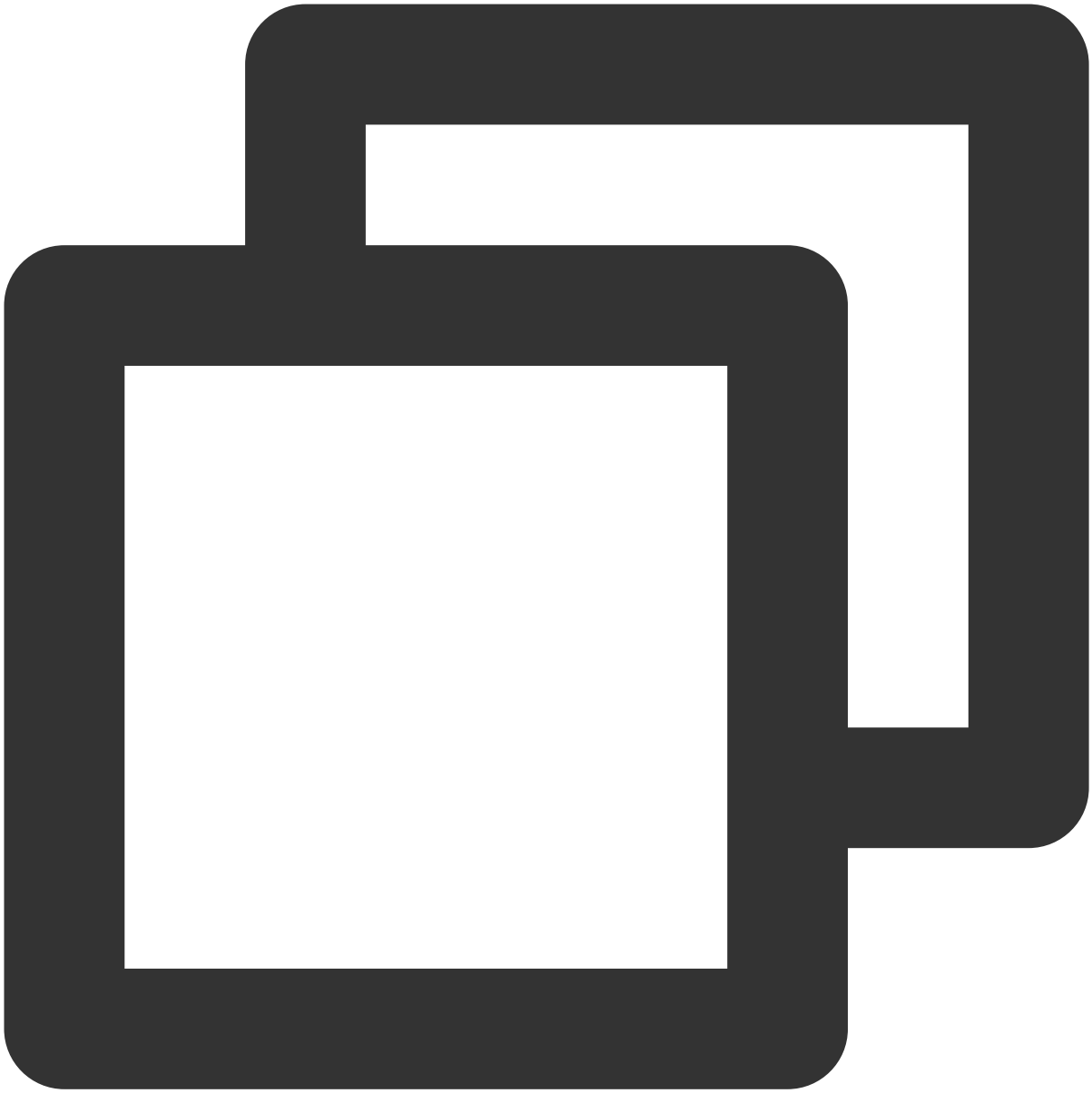
timestamp = `1571587200`

rand = `0`



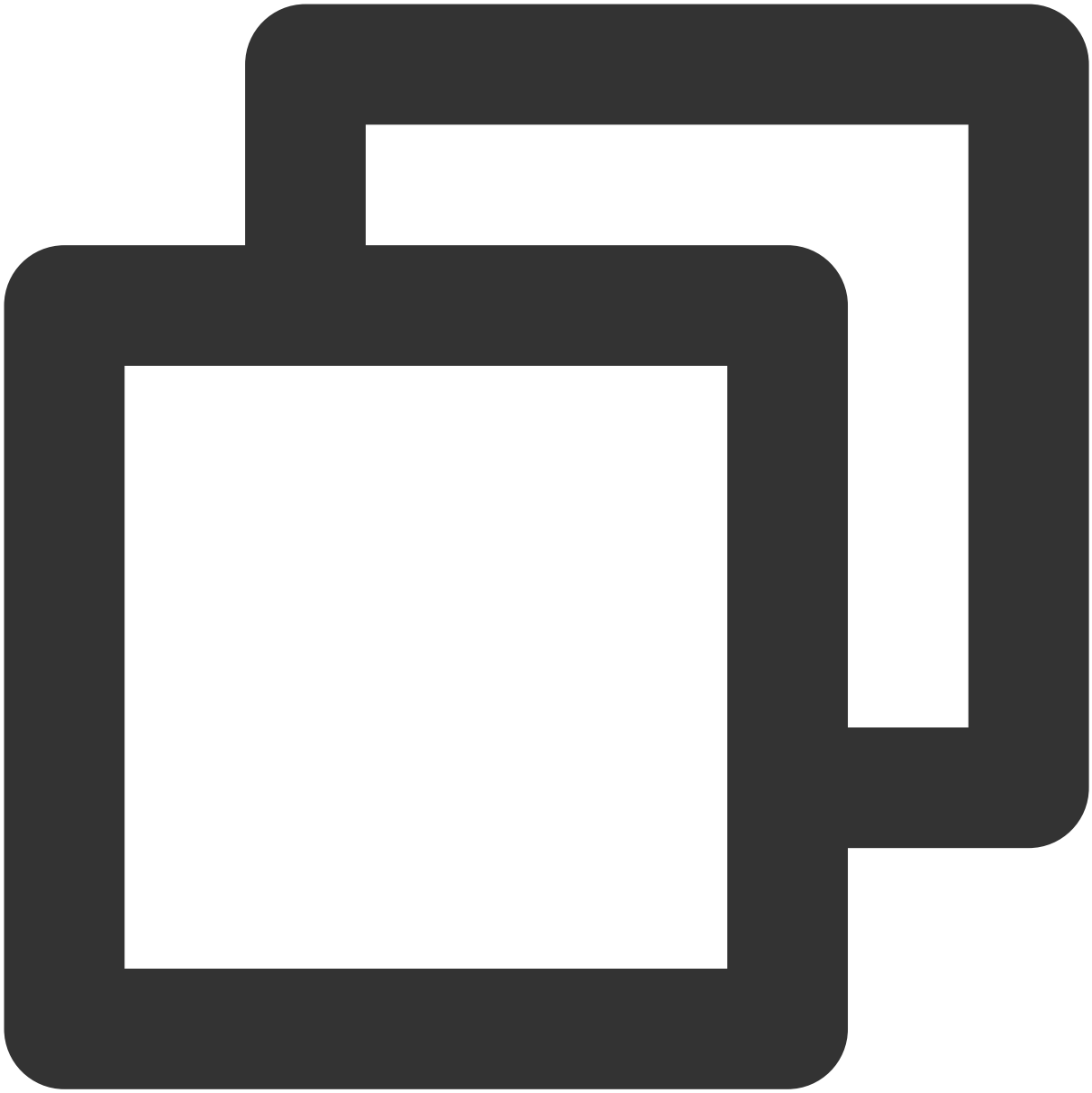
```
string_to_sign = "/access_log/post-1571587200-0-YourKey"
```

基于该字符串计算出



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

最终推送时的请求 url 为：



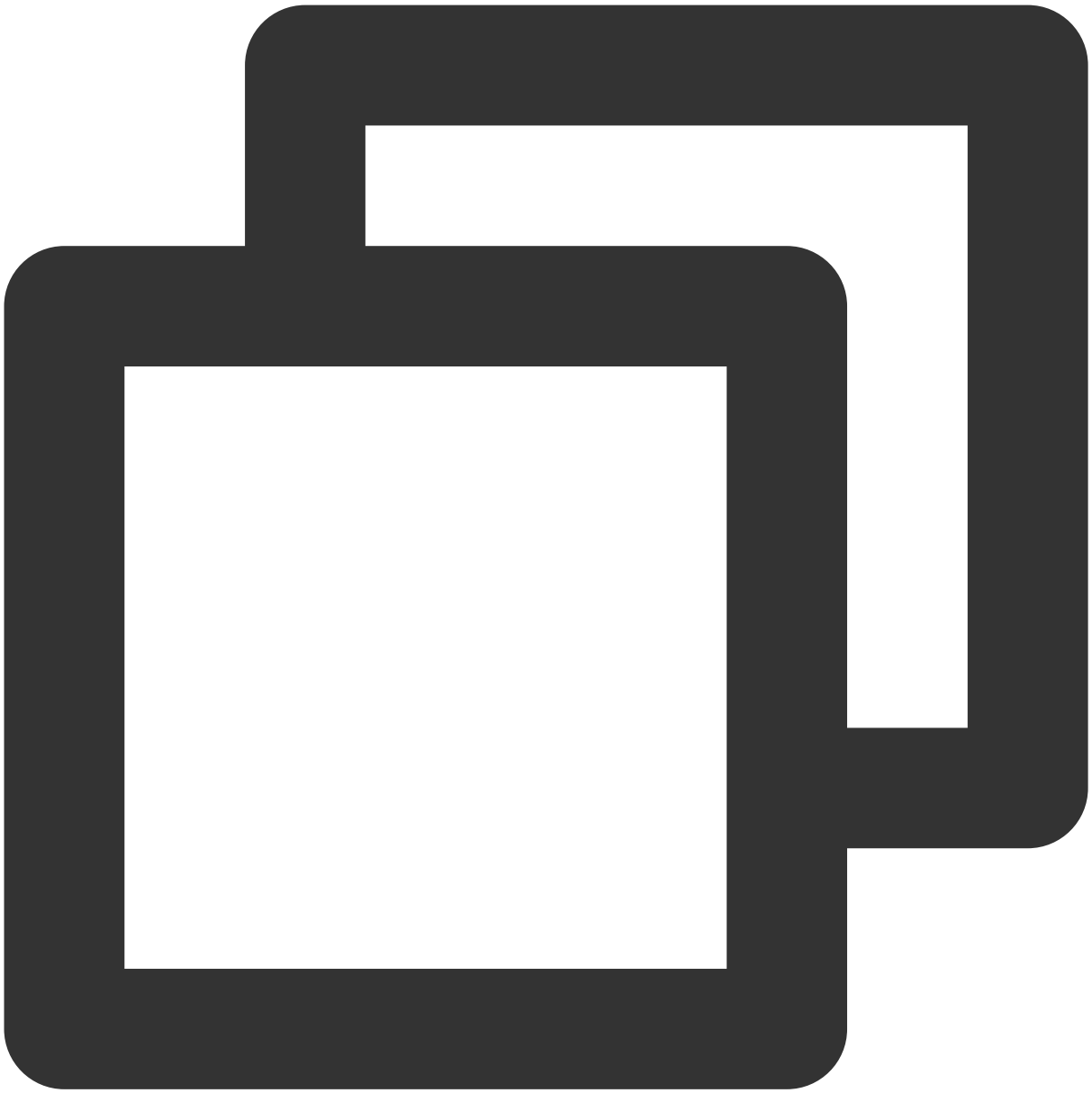
```
https://www.example.com/cdnlog/post?auth_key=1571587200-0-1f7ffa7bff8f06bbfbe2ace0f
```

服务端在接收到推送请求后，提取 `auth_key` 的值. 对auth_key的值进行拆分，获取 `timestamp` ， `rand` 和 `md5hash` 。可先检查 timestamp 是否过期，过期时间建议为 `300s` ，并基于上述规则拼装加密字符串，利用 SecretKey 拼装出需加密的字符串，加密后与 `auth_key` 中的 `md5hash` 值进行比较, 相同则说明鉴权通过。

3. 服务端解析鉴权请求代码示例

Python

Goland



```
import hashlib

from flask import Flask, request

app = Flask(__name__)


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

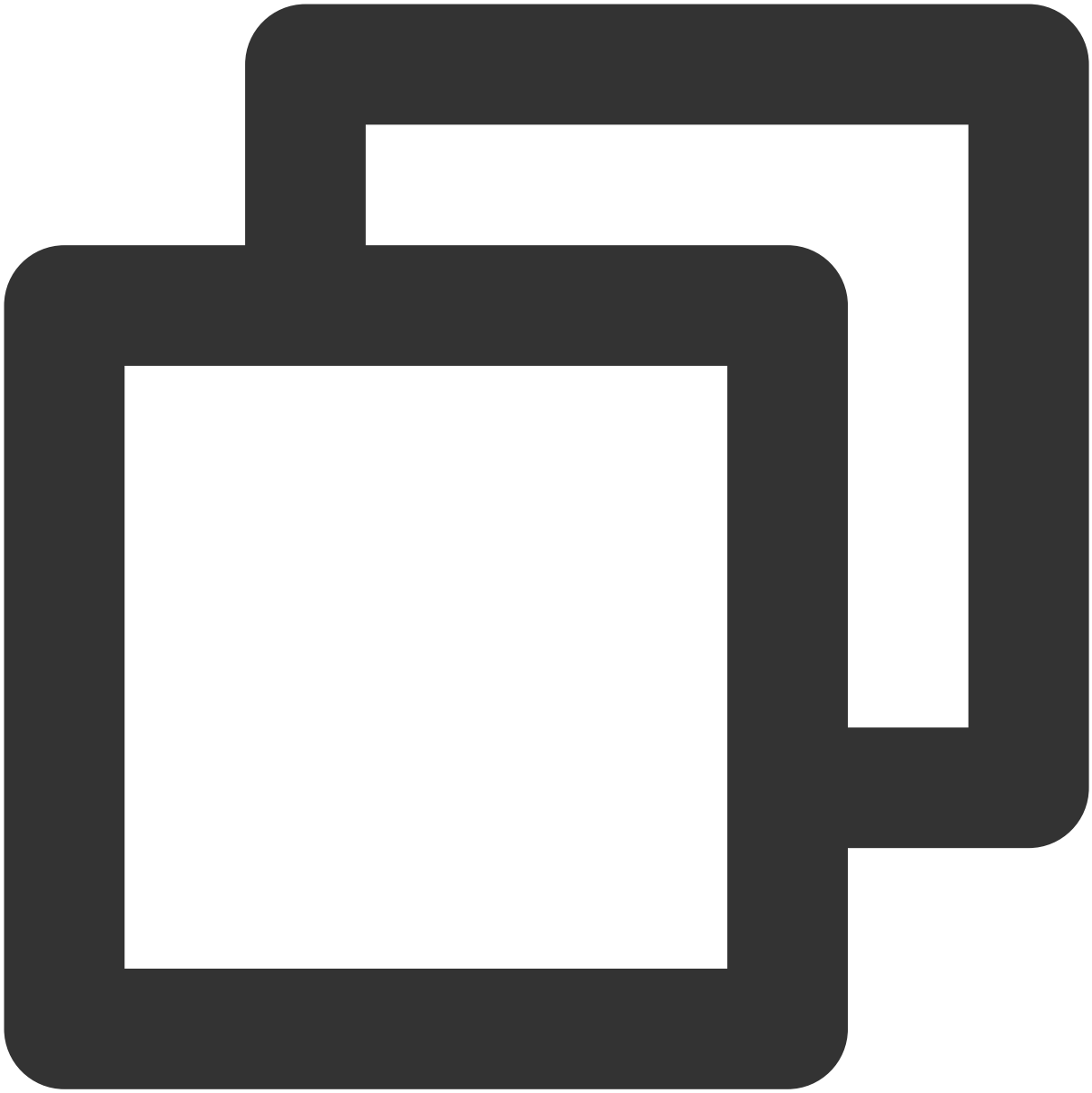
```
        "respCode": code,
        "respMsg": msg,
        "result": result
    }


def get_secret_key(access_key):
    return "secret_key"


@app.route("/access_log/post", methods=['POST'])
def access_log():
    if request.method == 'POST':
        if request.content_type.startswith('application/json'):
            current_time_ts, rand_num, md5hash = request.args.get("auth_key").split
             # 判断请求时间是否是在有效期内
            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")
            # 通过access_key(SecretID)获取secret_key
            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:
                # 认证通过
                if request.headers['content-encoding'] == 'gzip':
                    # 解压数据
                    pass
                # 数据处理
            return get_rsp("ok")
        return get_rsp(msg="Please use content_type by application/json", code=-1)
    return get_rsp(msg="The request method not find, method == %s" % request.method

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



```
package main

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

```
    "syscall"
)

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

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

    // 创建系统信号接收器
    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 即您提供的SecretID
        authKeys := strings.Split(authKey, "-")
        if len(authKeys) == 3 {
            currentTimeTs := authKeys[0]

            //进行时间戳有效期判断
            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) //转换成字符串进行比较
            if authMd5 == md5Hash {
                // todo 认证成功
                if r.Header.Get("Content-Encoding") == "gzip" {
                    //解压数据
                }
                //数据处理
            }
        } else {
            //异常处理
        }
    }
}

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

实时日志字段说明

最近更新时间：2023-12-01 10:14:13

本文介绍了实时日志中站点加速日志和四层代理日志字段解释。

说明

当某字段无值时：

字段的数据类型为 String 且字段没有数据，字段取值为："-"。

字段的数据类型为 Integer 且字段没有数据，字段取值为：-1。

站点加速日志

名称	数据类型	说明
LogTime	Timestamp ISO8601	日志生成的时间
RequestID	String	客户端请求的唯一标识 ID
ClientIP	String	客户端 IP
ClientRegion	String	客户端 IP 解析出来的国家/地域。格式标准：ISO-3166 alpha-2
ClientState	String	客户端 IP 解析出国家下一级的行政划分。目前仅支持中国大陆境内数据。格式标准：ISO-3166 alpha-2
ClientISP	String	客户端 IP 解析出的运营商信息。 中国大陆境内数据，记录为 ISP 中文名称； 全球可用区（不含中国大陆）数据，记录为：自治系统编号（ASN）
RequestTime	Timestamp ISO8601	客户端请求时间，时区：UTC +00:00
RequestStatus	Integer	客户端请求的状态，若使用 Websocket 协议的请求，EdgeOne 会周期打印日志，可以使用此字段确定连接状态 取值有： 0：未结束 1: 请求正常结束 2：异常结束
RequestHost	String	客户端请求的 Host

RequestBytes	Integer	客户端请求的大小，单位：Byte
RequestMethod	String	客户端请求的 HTTP Method，取值有： GET POST HHEAD PUT DELETE CONNECT OPTIONS TRACE PATCH
RequestSSLProtocol	String	客户端的使用的 SSL（TLS）协议，若取值为“-”，则没有请求没有 SSL 握手；取值有： TLS 1.0 TLS 1.1 TLS 1.2 TLS 1.3
ClientDeviceType	String	客户端请求设备类型，取值有： TV：电视 Tablet：平板电脑 Mobile：手机 Desktop：电脑 Other：其他
RequestUrl	String	客户端请求的 URL
RequestUrlQueryString	String	客户端请求的 URL 携带的查询参数
RequestUA	String	客户端请求的 User-Agent 信息
RequestRange	String	客户端请求的 Range 参数信息
RequestReferer	String	客户端请求的 Referer 信息
RequestProtocol	String	客户端请求的应用层协议，取值有： HTTP/1.0 HTTP/1.1 HTTP/2.0 HTTP/3 WebSocket
RemotePort	Integer	TCP 协议下客户端与节点建立连接的端口
EdgeCacheStatus	String	客户端请求是否命中节点缓存，取值有：

		hit：资源由节点缓存提供 miss:资源可缓存，但由源站提供 dynamic：资源不可缓存 other：无法被识别的缓存状态
EdgeResponseStatusCode	Integer	节点响应返回给客户端的状态码
EdgeResponseBytes	Integer	节点响应返回给客户端的大小，单位：Byte
EdgeResponseBodyBytes	Integer	节点响应返回给客户端的body大小，单位：Byte
EdgeResponseTime	Integer	从 EdgeOne 接收到客户端发起的请求开始，到客户端接收到服务器端的响应结束，这个过程所耗费的时间；单位：ms
EdgeInternalTime	Integer	从 EdgeOne 接收到客户端发起的请求开始，到响应给客户端的第一个字节，整个过程的耗时；单位：ms
EdgeServerIP	String	DNS 解析 Host 得到的 EdgeOne 服务器 IP 地址
EdgeServerID	String	客户端访问到的 EdgeOne 服务器唯一标识
EdgeSeverRegion	String	响应的 EdgeOne 节点 IP 解析出来的国家，格式标准参考：ISO-3166 alpha-2
EdgeEndTime	Timestamp ISO8601	完成响应客户端请求的时间
OriginDNSResponseDuration	Float	接收到源站DNS解析响应的耗时，若没有回源，记录为 -1，单位：ms
OriginIP	String	回源访问的源站IP，若没有回源，记录为“-”
OriginRequestHeaderSendDuration	Float	向源站发送请求头的耗时，一般是0，若没有回源，记录为 -1，单位：ms
OriginSSLProtocol	String	请求源站使用的 SSL 协议版本，若没有回源，记录为“-”；取值有： TLS 1.0 TLS 1.1 TLS 1.2 TLS 1.3
OriginTCPHandshakeDuration	Float	请求源站时，完成 TCP 握手的耗时，若没有回源，记录为 -1，单位：ms；注意：当连接重复利用时为0
OriginTLSHandshakeDuration	Float	请求源站时，完成 TLS 握手的耗时，若没有回源，记录为 -1，单位：ms；注意：当连接重复利用时为0

OriginResponseHeaderDuration	Float	向源站发送请求头到接受到源站响应头的耗时，若没有回源，记录为 -1，单位：ms
OriginResponseStatusCode	Integer	源站响应状态码，若没有回源，记录为 -1
BotClassAttacker	String	基于近期IP情报数据，请求客户端IP有攻击（如DDoS，高频恶意请求、站点攻击等）行为的风险等级，"-" 对应无历史数据，其它取值有： high：对应高风险 medium：对应中等风险 low：对应一般风险
BotClassProxy	String	基于近期IP情报数据，请求客户端IP开放可疑代理端口、并且被用作网络代理（包括秒拨IP）的风险等级，"-" 对应无历史数据，其它取值有： high：对应高风险 medium：对应中等风险 low：对应一般风险
BotClassScanner	String	基于近期IP情报数据，请求客户端IP有攻击已知漏洞的扫描器行为的风险等级，"-" 对应无历史数据，其它取值有： high：对应高风险 medium：对应中等风险 low：对应一般风险
BotClassAccountTakeOver	String	基于近期IP情报数据，请求客户端IP有恶意破解登陆，发起账号接管攻击的风险等级，"-" 对应无历史数据，其它取值有： high：对应高风险 medium：对应中等风险 low：对应一般风险
BotClassMaliciousBot	String	基于近期IP情报数据，请求客户端IP有恶意爬虫、刷量和暴力破解行为的风险等级，"-" 对应无历史数据，其它取值有： high：对应高风险 medium：对应中等风险 low：对应一般风险

说明：

站点加速日志中，使用 WebSocket 协议的长连接，EdgeOne 会在周期记录日志，并在最终请求结束时记录一条日志。可以通过 `RequestID` 字段来标识请求，相同 `RequestID` 的日志代表记录的是同一个连接；并且可以通过 `RequestStatus` 可以判断日志记录时刻的连接状态。

四层代理日志

名称	数据类型	说明
ServiceID	String	四层代理服务唯一标识 ID
SessionID	String	TCP 连接或 UDP 会话的唯一标识 ID
ConnectTimeStamp	Timestamp ISO8601	建连时间；默认UTC +0 时区
DisconnetTimeStamp	Timestamp ISO8601	断连时间；默认UTC +0 时区
DisconnetReason	String	断连原因； 格式为 「方向：原因」 方向取值有： up：源站方向 down：客户端方向 原因取值有： net_exception_peer_error：读写对端返回错误 net_exception_peer_close：对端已关闭连接 create_peer_channel_exception：创建到下一跳的 channel 失败 channel_eof_exception：channel 已结束（请求结束时，结束请求的节点会给相邻节点发送 channel_eof 告知相邻节点请求已结束） net_exception_closed：连接已关闭 net_exception_timeout：读写超时
ClientRealIP	String	客户端真实 IP
ClientRegion	String	客户端所在国家/地域2位字母编码，符合 ISO-3166 alpha-2 规范
EdgeIP	String	访问的 EdgeOne 服务器 IP 地址
ForwardProtocol	String	客户配置的转发协议 TCP/UDP
ForwardPort	Integer	客户配置的转发端口
SentBytes	Integer	上一条日志记录时间至本条日志记录期间产生的入流量，单位：Byte
ReceivedBytes	Integer	上一条日志记录时间至本条日志记录期间产生的出流量，单位：Byte
LogTimeStamp	Timestamp	日志生成时间；默认 UTC +0 时区

版权所有：腾讯云计算（北京）有限责任公司

	ISO8601	

说明：

在 TCP 长连接的场景下，EdgeOne 会周期记录日志，并且在连接结束的时候记录最后一条日志，您可以通过 `DisconnetReason` 字段是否为空来判定连接是否断开；同时也可以使用 `SessionID` 来标识连接，相同的 `SessionID` 的日志记录的是相同连接的行为。

离线日志

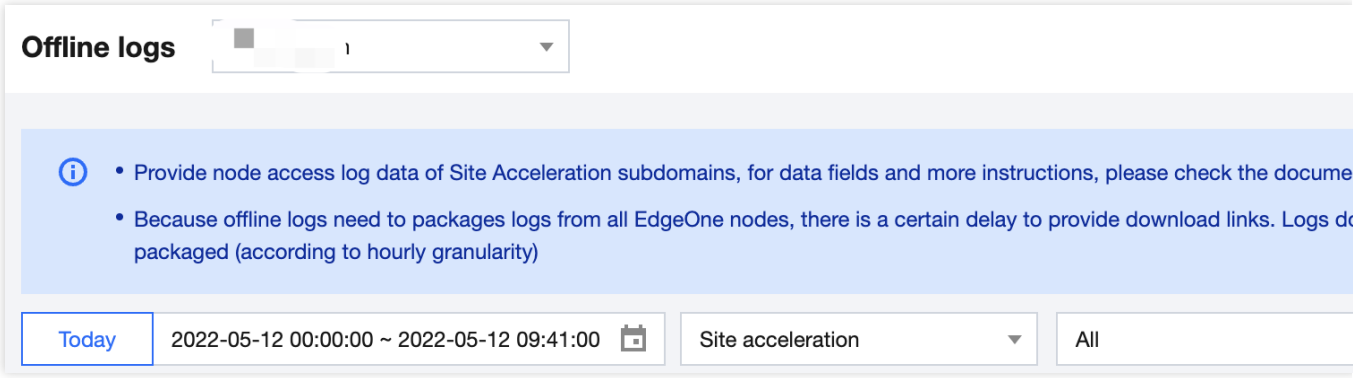
最近更新时间：2024-04-15 15:00:09

功能介绍

为了方便客户对用户访问进行分析，EdgeOne 对全网访问日志进行了小时粒度打包，默认存储 30 天，并且提供下载服务。

操作步骤

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**日志服务 > 离线日志**。
2. 在离线日志页面，可选择具体站点或具体子域名的离线日志；同时支持筛选不同时间进行离线日志查询。

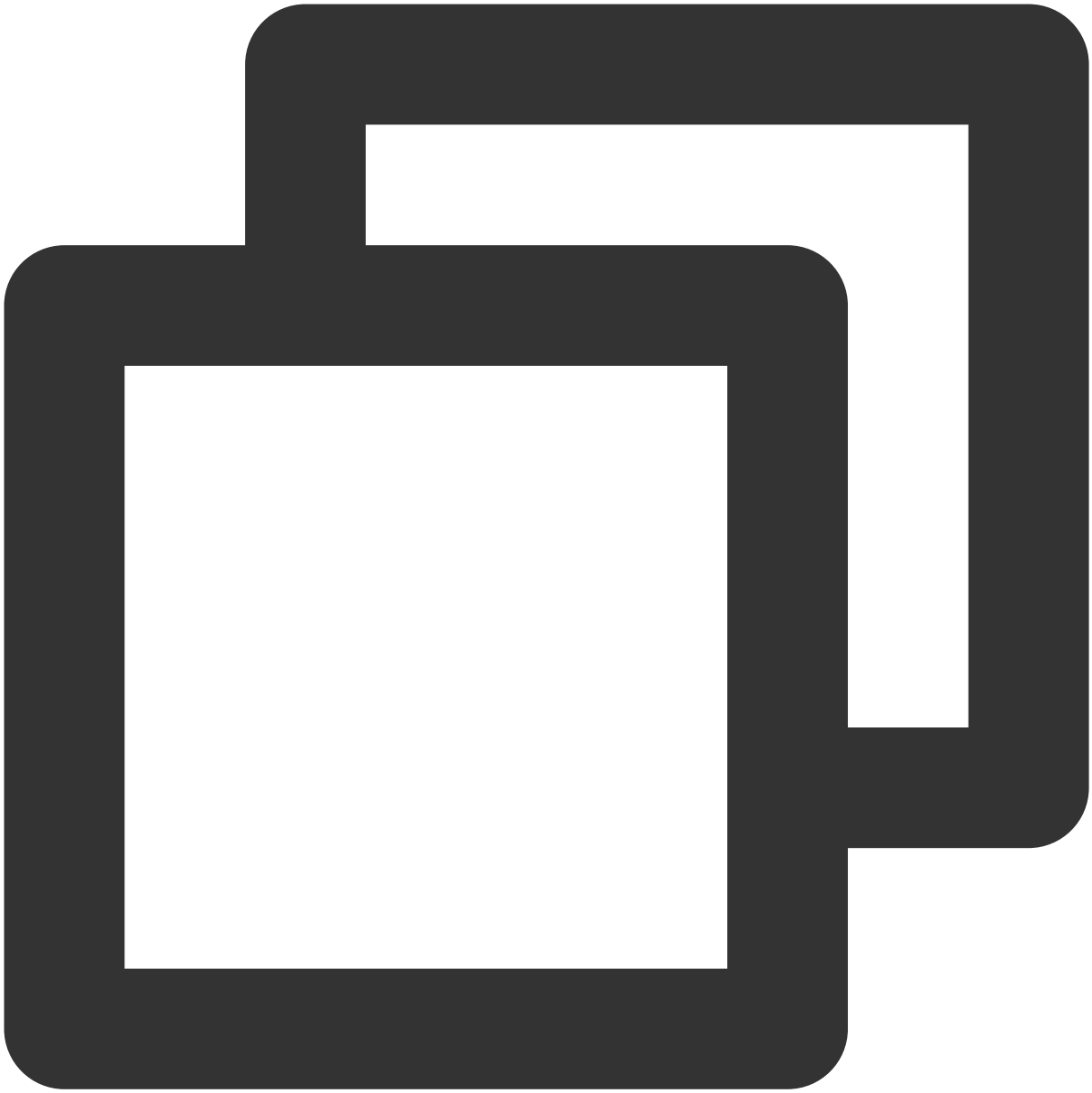


3. 通过单击**操作**列**下载**，即可下载对应域名的日志包。

注意

访问日志默认按小时打包，若某个小时里域名无任何请求，则不会产生该时间区间的日志包。

日志包通过 gzip 压缩为 .gz 格式。由于 MacOS 系统的目录系统缺陷，在MacOS 系统下双击解压可能会报错，如出现这种情况，您可以通过如下 Terminal 命令进行解压（在您存储日志的目录下）。



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

由于 EdgeOne 节点分布在各地，为同步所有时区，离线日志的存储时间和查询时间默认为：UTC +00:00。
离线日志从各 EdgeOne 节点收集而来，因此延迟上各有差异，一般情况下延迟 3 小时左右后可查询、下载日志包，日志包会不断追加，一般24小时左右趋于稳定。

字段说明

日志默认按照 json 格式存储，具体的日志字段解释如下。
当某字段无值时：
字段的数据类型为 String 且字段没有数据，字段取值为：“-”。
字段的数据类型为 Int 且字段没有数据，字段取值为：-1。

站点加速日志

名称	数据类型	说明
RequestID	String	客户端请求的唯一标识 ID
ClientIP	String	客户端 IP
ClientRegion	Sting	客户端 IP 解析出来的国家/地域。格式标准：ISO-3166 alpha-2
ClientState	String	客户端 IP 解析出国家下一级的行政划分。目前仅支持中国大陆境内数据。格式标准：ISO 3166-2
ClientISP	String	客户端 IP 解析出的运营商信息。 中国大陆境内数据，记录为 ISP 中文名称； 全球可用区（不含中国大陆）数据，记录为 自治系统编号（ASN）。
RequestTime	String	客户端请求时间，时区：UTC +00:00，格式标准：ISO-8601
RequestStatus	int	客户端请求的状态；0：未结束，1: 请求正常结束，2：异常结束
RequestHost	String	客户端请求的 Host
RequestBytes	int	客户端请求的大小，单位：Byte
RequestMethod	String	客户端请求的 HTTP Method
RequestUrl	String	客户端请求的 URL
RequestUrlQueryString	String	客户端请求的 URL 携带的查询参数
RequestUA	String	客户端请求的 User-Agent 信息
RequestRange	String	客户端请求的 Range 参数信息
RequestReferer	String	客户端请求的 Referer 信息
RequestProtocol	String	客户端请求的应用层协议：HTTP/1.0，HTTP/1.1，HTTP/2.0，HTTP/3，WebSocket
RemotePort	int	TCP 协议下客户端与节点建立连接的端口

EdgeCacheStatus	String	客户端请求是否命中节点缓存： hit：资源由节点缓存提供 miss：资源可缓存，但由源站提供 dynamic：资源不可缓存 other：无法被识别的缓存状态
EdgeResponseStatusCode	int	节点响应返回给客户端的状态码
EdgeResponseBytes	int	节点响应返回给客户端的大小，单位：Byte
EdgeResponseTime	int	从 EdgeOne 接收到客户端发起的请求开始，到客户端接收到服务器端的响应结束，这个过程所耗费的时间；单位：ms
EdgeInternalTime	int	从 EdgeOne 接收到客户端发起的请求开始，到响应给客户端的第一个字节，整个过程的耗时；单位：ms
EdgeServerIP	String	DNS 解析 Host 得到的 EdgeOne 服务器 IP 地址
EdgeServerID	String	客户端访问到的 EdgeOne 服务器唯一标识
SecurityAction	String	命中安全规则后的处置方式；取值：Monitor（观察），JSChallenge（JavaScript 挑战），Deny（拦截），Allow（放行），BlockIP（IP 封禁），Redirect（重定向），ReturnCustomPage（返回自定义页面），ManagedChallenge（托管挑战）
SecurityRuleID	String	处置请求的安全规则 ID
SecurityUserNote	String	用户自定义的标签
SecurityModule	String	命中安全规则的所对应的安全功能；取值：CustomRule（自定义规则），BotManagement（Bot管理），RateLimiting（速率限制模板），RateLimitingCustomRule（速率限制规则），ManagedRule（托管规则），BotClientReputation（客户端画像），BotBehaviorAnalysis（Bot智能防护），RateLimitingClientFiltering（智能客户端过滤）

四层代理日志

名称	数据类型	说明
ServiceID	String	四层代理服务唯一标识 ID
ConnectTimeStamp	String	建连时间；使用 ISO-8601 规范，默认UTC +0 时区

DisconnetTimeStamp	String	断连时间；使用 ISO-8601 规范，默认UTC +0 时区
DisconnetReason	String	断连原因； 格式为 「方向：原因」 方向取值：up（源站方向）/down（客户端方向） 原因： net_exception_peer_error：读写对端返回错误 net_exception_peer_close：对端已关闭连接 create_peer_channel_exception：创建到下一跳的 channel 失败 channel_eof_exception：channel 已结束（请求结束时，结束请求的节点会给相邻节点发送 channel_eof 告知相邻节点请求已结束） net_exception_closed：连接已关闭 net_exception_timeout：读写超时
ClientRealIP	String	客户端真实 IP
ClientRegion	String	客户端所在国家/地域2位字母编码，符合 ISO-3166 alpha-2 规范
EdgeIP	String	访问的 EdgeOne 服务器 IP 地址
ForwardProtocol	String	客户配置的转发协议 TCP/UDP
ForwardPort	Int	客户配置的转发端口
SentBytes	Int	本条日志持续期间产生的入流量，单位：Byte
ReceivedBytes	Int	本条日志持续期间产生的出流量，单位：Byte
LogTimeStamp	String	日志生成时间；使用 ISO-8601 规范，默认UTC +0 时区

特别说明

通过站点加速访问日志 EdgeResponseBytes 字段中记录的字节数，统计计算而来的流量、带宽数据与 EdgeOne 计费流量或带宽数据可能不一致。原因如下：
访问日志中仅可记录应用层数据，在实际网络传输中，产生的网络流量要比纯应用层流量多5% - 15%。由两部分组成：
TCP/IP 包头消耗，基于 TCP/IP 协议的 HTTP 请求，每一个包的大小最大是1500个字节，包含了 TCP 和 IP 协议的40-60个字节的包头，包头部分会产生流量，但是无法被应用层统计到，这部分的开销大致为3-4%左右。
TCP 重传，正常网络传输过程中，发送的网络包会有3% - 10%左右会被互联网丢掉，丢掉后服务器会对丢弃的部分进行重传，此部分流量应用层也无法统计，占比约为3% - 7%。
开启智能加速后，腾讯云 EdgeOne 会对客户端请求 EdgeOne 节点所产生的流量/带宽计费。详情请参见 计费概述。

数据分析
概述

最近更新时间：2023-09-21 15:07:32

腾讯云边缘安全加速平台 EdgeOne 通过分析访问日志数据，在数据分析页面中提供多种数据指标，供您多维度了解业务数据。

适用场景

场景	具体诉求
日常监控巡检	通过观察加速域名/四层代理实例的各项数据指标走势和分布，持续监控 EdgeOne 是否存在高延迟或故障等问题。
故障排查分析	通过分析访问日志，了解报障用户访问的路径、内容等信息，从而定位问题并进行排查。
业务数据洞察	通过对客户端数据进行分析和挖掘，了解用户画像。

功能详情

数据分析功能	功能介绍
流量分析	通过分析 L7（应用层）访问日志，了解用户访问网站或服务的来源、流量/带宽、延迟等数据，帮助您更好地了解用户需求和优化网络性能。
缓存分析	通过分析缓存命中率和缓存内容等数据，了解缓存策略的效果，帮助您更好地优化缓存配置。
安全分析	通过对访问日志、网络数据等进行分析，了解与您业务有关的攻击面数据，包括攻击来源、攻击方式等，帮助您更好地了解攻击情况，制定更有效的安全策略。
DNS 解析	通过对 NS 接入模式下的 DNS 解析数据进行统计，了解访问量、返回码等数据，帮助您更好地了解解析系统的运行情况。
四层代理	通过分析 L4（传输层）访问日志，了解用户访问四层代理实例的来源、流量、连接时长等数据，帮助您更好地监控四层代理实例的运行情况。

版权所有：腾讯云计算（北京）有限责任公司

流量分析

最近更新时间：2023-12-18 11:21:26

概述

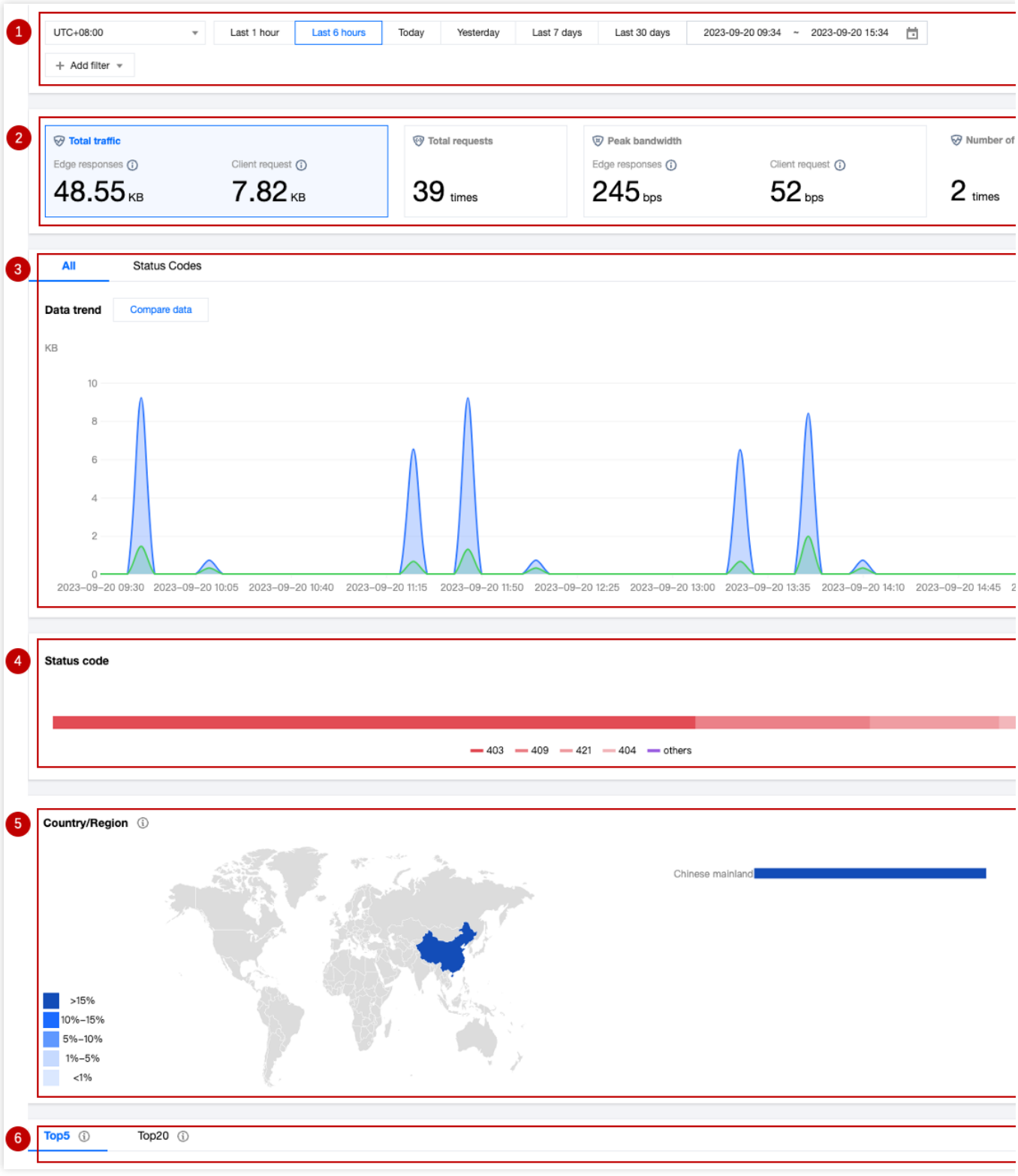
EdgeOne 通过分析 L7（应用层）访问日志数据，为您提供了多维度、可视化的流量分析展示，主要包括流量、请求数等指标的时间趋势曲线、国家/地区分布和 TOP 排行等数据。

支持的能力

流量分析支持流量、请求数、带宽下的数据统计，可以通过单击**顶部不同核心指标数据区域**来进行切换。

说明：

暂不支持切换至“独立 IP 数”指标。



1. 数据筛选与过滤

支持选择数据查询的时间范围，详情请参见 如何修改查询时间范围。

支持按照站点、Hosts、国家/地区、状态码、URL 等维度筛选过滤，详情请参见 如何使用筛选条件。

2. 核心指标

总流量：

EdgeOne 响应流量：经由 EdgeOne 向客户端传输的全部流量之和，即下行流量。

客户端请求流量：EdgeOne 接收到客户端请求的流量之和，即上行流量。

总请求数：EdgeOne 接到来自客户端的请求数。

带宽峰值：

EdgeOne 响应带宽：经由 EdgeOne 向客户端传输的全部带宽的峰值，即下行带宽峰值。

客户端请求带宽：EdgeOne 接收到客户端请求的带宽峰值，即上行带宽峰值。

独立 IP 数：针对客户端 IP 地址进行去重后得到的请求数，可以体现访问业务的 IP 地址数量。

说明：

在不同时间统计颗粒度下，带宽峰值指标的计算方式会有所区别。

1 分钟颗粒度：1 分钟内的总流量 * 8 / 60 秒。

5 分钟颗粒度：5 分钟内的总流量 * 8 / 300 秒。

1 小时颗粒度：所有的 5 分钟颗粒度带宽峰值点中的最大值。

1 天颗粒度：所有的 5 分钟颗粒度带宽峰值点中的最大值。

3. 时间趋势图

全部分页下，展示当前选中的核心指标的时间趋势曲线。

状态码分页下，展示当前选中的核心指标的、分状态码的时间趋势柱状图。

说明：

当核心指标选择**带宽峰值**时，不支持显示**状态码**分页数据。

4. 状态码分布

展示当前选中的核心指标在状态码维度上的分布。默认仅展示 Top 4，其他状态码归类为“Others”。

说明：

1. 此处使用的是 EdgeOne 节点响应给客户端的状态码。
2. 当核心指标选择**带宽峰值**时，不支持显示状态码分布。

5. 国家/地区分布

展示当前选中的核心指标在国家/地区上的分布。

说明：

1. 此处数据以客户端所在国家/地区为准，与计费数据可能有差异，计费数据的大区分布以实际服务用户客户端的 EdgeOne 节点所在区域为准。
2. 由于时延和算法的影响，国家/地区分布仅供参考，建议您以实际日志分析结果为准。

6. TOP 排行

流量分析支持的 TOP 排行维度如下：

Hosts：客户端请求的子域名。

URLs：客户端请求的具体资源路径。

资源类型：客户端请求的资源类型，例如：“.png”“.json”等。
客户端 IP 地址：客户端请求的具体来源 IP 地址。
Referers：客户端请求的 Referer 信息。
客户端设备类型：
设备类型：客户端请求所使用的硬件设备类型，取值有：
TV：电视。
Tablet：平板电脑。
Mobile：手机。
Desktop：电脑。
Other：其他。
浏览器：客户端请求使用的浏览器类型。
操作系统：客户端请求使用的操作系统类型。
说明：
1. TOP 客户端 IP 地址排行仅支持以下筛选项：Host、国家/地区、HTTP 协议版本、TLS 版本、HTTP/HTTPS。
2. 由于时延和算法的影响，TOP 排行数据仅供参考，建议您以实际日志分析结果为准。
3. 当核心指标选择“**带宽峰值**”时，不支持显示 TOP 排行。

分析示例

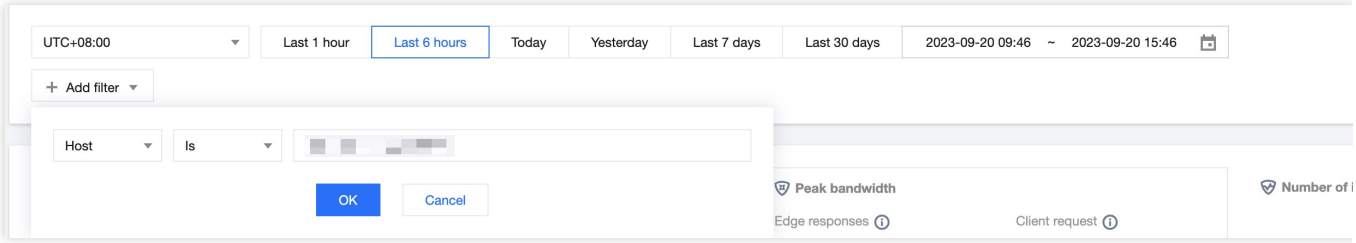
场景一：排查访问错误的 URL

场景示例

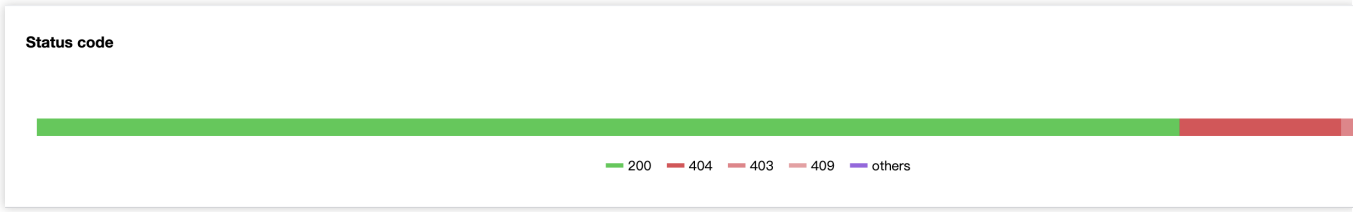
当您通过 添加加速域名 将 `www.example.com` 添加至 EdgeOne 服务后，较多终端用户反馈无法打开网页。为了分析故障原因和影响面，您可以在**数据分析** > **流量分析**页面中进行如下操作。

操作步骤

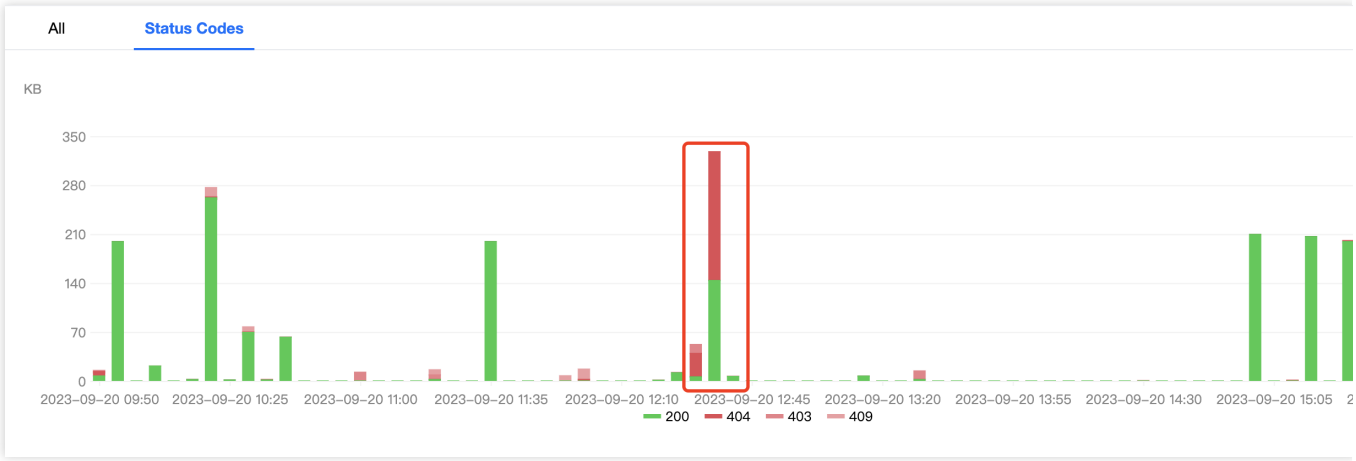
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击您关注的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**数据分析** > **流量分析**，进入流量分析页面。
3. 在流量分析页面，单击**添加筛选**，添加筛选条件 `Host=www.example.com` ，单击**确定**。



4. 查看状态码分布，观察异常状态码的占比，发现有异常状态码“404”。



5. 查看状态码的分时趋势，例如某几个时段“404”占比较高，可以排查到这段时间的业务访问失败数量高，需要重点关注。



6. 添加筛选条件 `状态码=404` ，通过查看 TOP URL，可以得到具体访问异常的 URL，下一步您可以前往源站排查此 URL 是否存在问题。

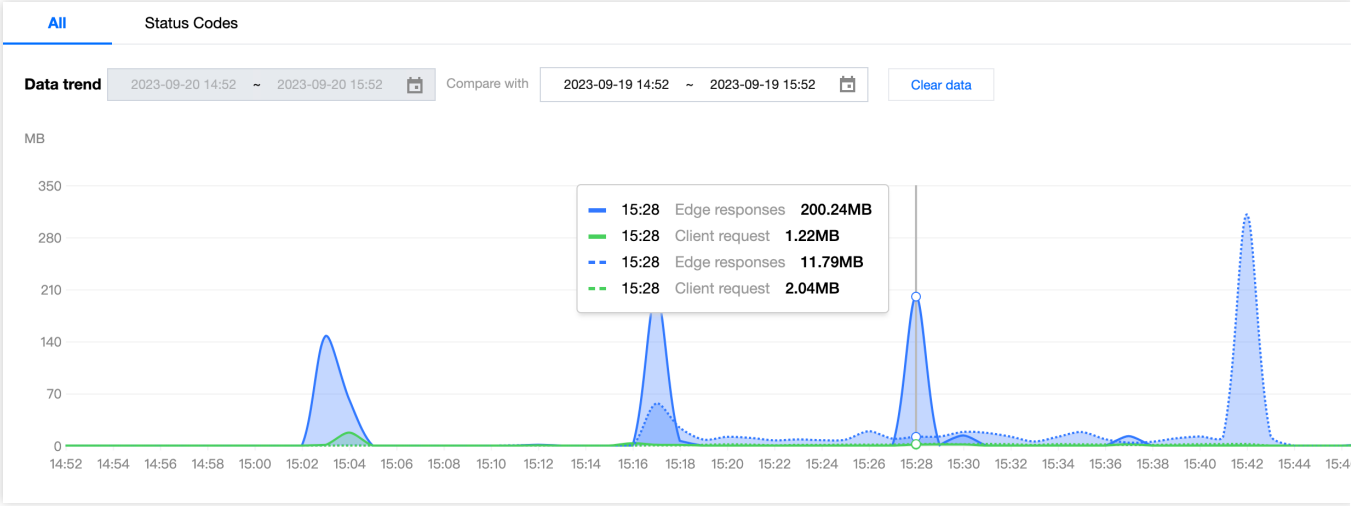
场景二：监控账号下所有站点的流量走势

场景示例

当您添加多个站点并在 EdgeOne 稳定运行一段时间后，希望在控制台定期巡检所有站点下的流量趋势，您可以参考如下步骤操作。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**数据分析** > **流量分析**，进入多站点聚合的流量分析页面。
2. 查看时间趋势图，观察流量、请求数是否有陡增或陡降，判断整体业务是否正常运行。
3. 单击**对比数据**，对比最近两天相同时间段的流量曲线，观察业务日环比是否有突增或突降。



缓存分析

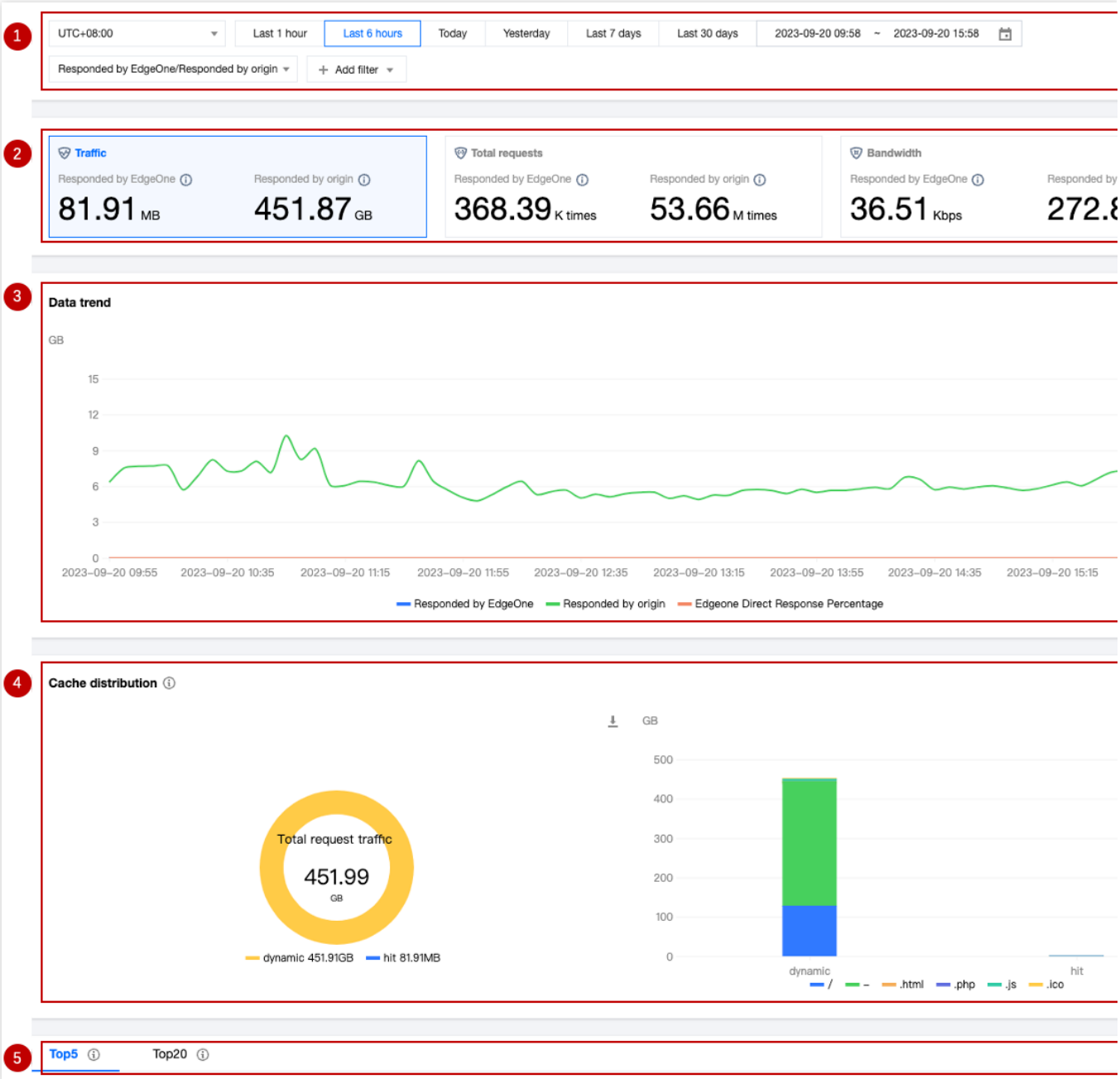
最近更新时间：2023-12-18 11:23:15

概述

EdgeOne 通过分析 L7（应用层）访问日志数据，为您提供了多维度、可视化的缓存分析展示，主要包括流量、请求数等指标的时间趋势曲线、缓存状态分布和 TOP 排行。

支持的能力

缓存分析支持流量、请求数、带宽下的数据统计，可以通过单击**顶部不同核心指标数据区域**来进行切换。



1. 数据筛选与过滤

选择数据查询的时间范围，详情请参见 修改查询时间。

支持按照站点、Host、缓存状态、状态码等维度筛选过滤，详情请参见 如何使用筛选。

支持切换页面展示的核心指标。

EdgeOne 直接响应：展示 EdgeOne 节点缓存直接响应的流量/请求数/带宽峰值。

源站响应：展示由源站响应的流量/请求数/带宽峰值。

2. 核心指标

流量：经由 EdgeOne 向客户端传输的全部流量，即下行流量。

EdgeOne 直接响应：EdgeOne 节点缓存直接响应的流量。

源站响应：由源站响应的流量。

请求数：EdgeOne 接收到来自客户端的请求数。

EdgeOne 直接响应：EdgeOne 节点缓存直接响应的请求数。

源站响应：由源站响应的请求数。

带宽峰值：经由 EdgeOne 向客户端传输的全部带宽的峰值，即下行带宽峰值。

EdgeOne 直接响应：EdgeOne 节点缓存直接响应的带宽峰值。

源站响应：由源站响应的带宽峰值。

说明：

在不同时间统计颗粒度下，带宽峰值指标的计算方式会有所区别。

1 分钟颗粒度：1 分钟内的总流量 * 8 / 60 秒。

5 分钟颗粒度：5 分钟内的总流量 * 8 / 300 秒。

1 小时颗粒度：所有的 5 分钟颗粒度带宽峰值点中的最大值。

1 天颗粒度：所有的 5 分钟颗粒度带宽峰值点中的最大值。

3. 时间趋势图

展示 EdgeOne 直接响应和源站响应的核心指标绝对值的分时趋势，以及当前核心指标下的 EdgeOne 直接响应占比（即缓存命中率）分时趋势。

4. 缓存分布

缓存状态分布，取值包括：

hit：请求命中了 EdgeOne 的缓存，资源由 EdgeOne 直接响应。

miss：资源可以缓存，但是没有命中 EdgeOne 的缓存，资源由源站响应。

dynamic：资源无法缓存，资源由源站响应。

other：无法被识别的缓存状态。

缓存状态和资源类型的交叉分析：通过柱状图展示每一类缓存状态中的资源类型分布。

说明：

当核心指标选择“带宽”时，不支持显示缓存分布。

5. TOP 排行

缓存分析支持的 TOP 排行维度如下：

资源类型：客户端请求的资源类型，例如：“.png”“.json”等。

Hosts：客户端请求的子域名。

URLs：客户端请求的具体资源路径。

状态码：EdgeOne 节点响应给客户端的状态码。

说明：

1. 由于时延和算法的影响，TOP 排行数据仅供参考，建议您以实际日志分析结果为准。
2. 当核心指标选择“带宽”时，不支持显示 TOP 排行。

版权所有：腾讯云计算（北京）有限责任公司

分析示例

场景一：监控域名的缓存命中率

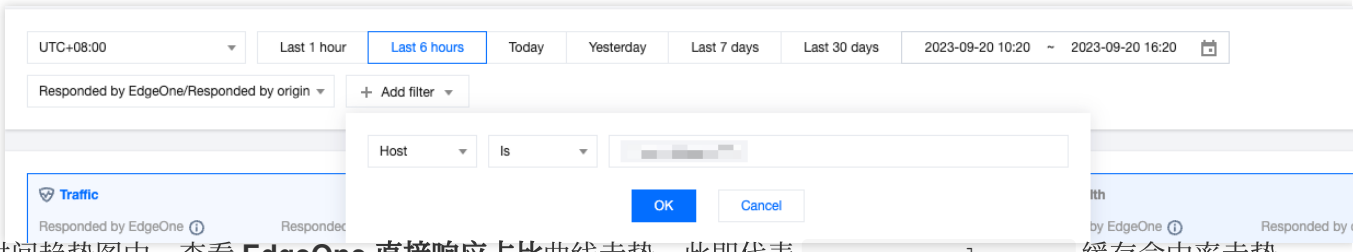
通过缓存分析中的趋势图，结合不同筛选项目，持续监控指定域名的缓存命中率。

场景示例

当您 添加加速域名 并且 配置相应缓存策略 后，希望监控域名 `www.example.com` 的缓存命中率指标以评估和优化缓存配置，您可以在**数据分析 > 缓存分析**页面中进行如下操作。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击您关注的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**数据分析 > 缓存分析**，进入缓存分析页面。
3. 在缓存分析页面，单击**添加筛选**，添加筛选条件 `Host=www.example.com` ，单击**确定**。



4. 在时间趋势图中，查看 **EdgeOne 直接响应占比**曲线走势，此即代表 `www.example.com` 缓存命中率走势。
5. 当您认为缓存命中率较低时，可以添加筛选条件 `缓存状态=miss` ，然后通过查看 TOP 排行，排查缓存命中率不及预期的原因。

例如：观察资源类型的 TOP 排行，发现大量“.mp4”文件后缀的资源没有命中缓存。您可以参考 节点缓存 TTL 配置 优化相应配置。

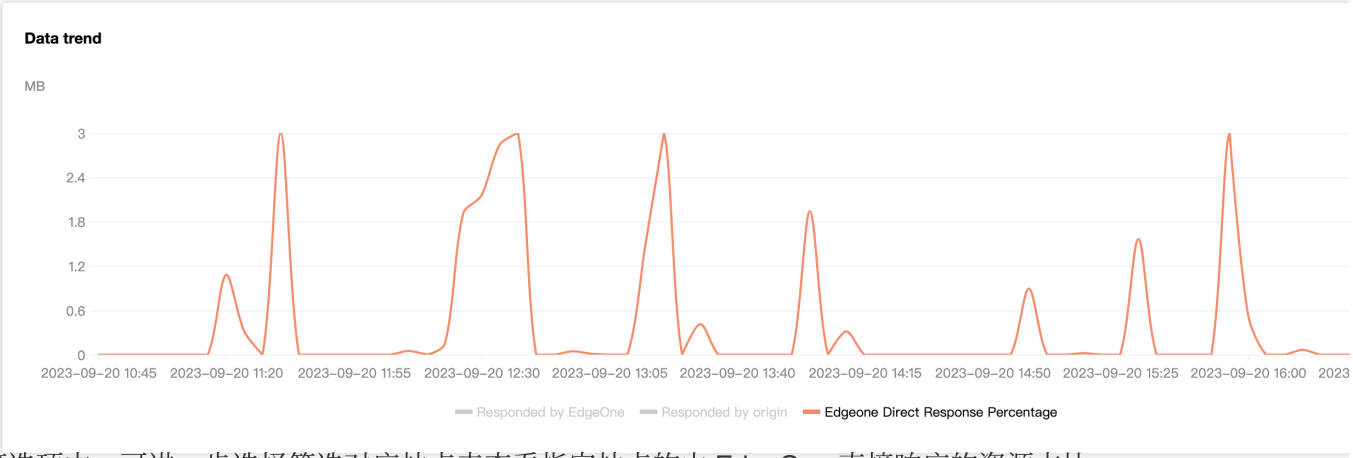
场景二：监控所有站点的缓存命中率

场景示例

当您的站点全部为静态网站，在 EdgeOne 上稳定运行一段时间后，需要监控所有站点的静态资源的缓存命中率指标，您可以参照如下步骤操作。

操作步骤

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**数据分析 > 缓存分析**，进入多站点聚合的缓存分析页面。
2. 查看趋势曲线，可查看所有站点汇总的由 EdgeOne 直接响应的资源占比数据。



3. 在筛选项中，可进一步选择筛选对应站点来查看指定站点的由 EdgeOne 直接响应的资源占比。

安全分析
站点安全概览

最近更新时间：2023-09-21 15:07:10

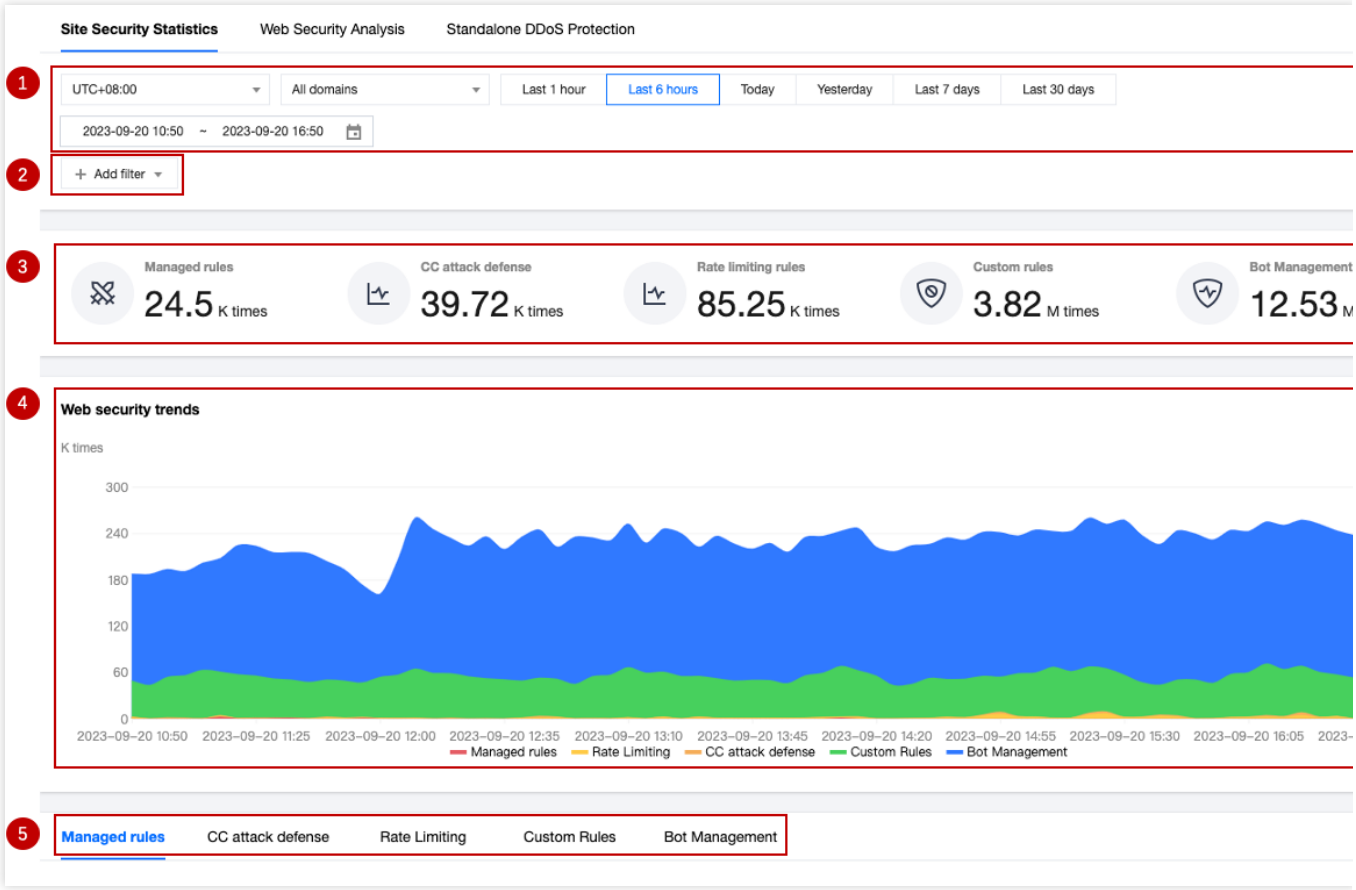
概述

站点安全概览集中展示了站点面临的主要安全风险情况。通过展示一段时间内命中 EdgeOne 安全模块的请求统计情况，包括趋势图和 TOP N 图表，站点安全概览可以为您提供多个维度安全风险参考：风险严重和紧急程度（安全事件规模与趋势）、安全风险的主要对象（攻击的主要目标域名、路径等）和风险分类（主要攻击方式，如 HTTP DDoS 攻击、漏洞攻击和爬虫访问等）。通过这些信息，您可以快速了解当前站点面临的安全威胁，并对应调整或加固安全策略。

支持的能力

站点安全概览提供了多种统计分析功能，展示命中安全规则请求的整体情况，来帮助您快速评估威胁。

版权所有：腾讯云计算（北京）有限责任公司



1. 数据范围

调整数据时间范围，展示不同时间段内的安全事件数据。

2. 过滤与筛选

说明：

筛选条件将对页面的所有数据生效，包括自定义规则、速率限制、CC攻击防护、托管规则、Bot管理分页中的统计数据。

当查询的数据量较大时，可能会消耗较长的查询时间。

站点安全概览支持的筛选项可参考 如何使用筛选条件。

3. 关键防护指标数据

托管规则：查看命中托管规则，携带漏洞攻击特征的请求。

CC 攻击防护：查看命中 CC 攻击防护，可能对站点可用性造成风险的请求。

速率限制规则：查看触发速率限制规则，可能滥用资源或应用接口的请求。

自定义规则：查看触发自定义规则的请求。您可以进一步分析请求趋势，评估您的定制安全策略。

Bot 管理：查看来自自动化程序（Bot）的请求，包括搜索引擎和自动化工具在内的各类爬虫请求。

4. 安全事件趋势图

趋势图帮助您理解某一段时间内的外部安全风险趋势，并通过堆叠图方式展示整体风险规模和各个风险分类的规模趋势，帮助您快速评估风险的严重程度和优先级，以采取合适的流程应对。

说明：

趋势图为叠加面积图，其中：

纵轴展示了命中各个安全模块，包括命中自定义规则、速率限制、CC 攻击防护、托管规则和 Bot 管理模块的请求数。

横轴展示了时间戳，对应计数窗口的起始时间。例如：当数据按1分钟颗粒度展示时，16:05:00的数据点对应了16:05:00-16:05:59的请求数总和。

5. 安全事件分类统计展示

指标	指标说明
命中规则统计	命中安全防护规则的 TOP 10 规则统计，包含命中规则的Host、规则ID、处置方式以及命中时间、命中请求数信息
请求路径统计	命中安全防护规则的请求路径 TOP 10 数据
客户端 IP 统计	命中安全防护规则的请求客户端 IP TOP 10 统计
客户端分布统计	命中 Web 防护规则的客户端分布地区 TOP 10 统计
已拦截恶意客户端统计	统计 CC 攻击防护内已拦截恶意客户端 IP 数量
Bot 标签趋势	统计已拦截的 Bot 标签趋势

在安全事件中，您也可以通过单击对应的域名、请求路径、规则 ID、客户端 IP 快速加入为筛选条件，查看更细致维度的统计分析数据；

如果在安全概览中发现某规则 ID 拦截了正常请求，可单击该**规则 ID**，单击**新建防护例外规则**，快速新建一条防护例外规则。

分析示例

场景一：查看正在进行的 CC 攻击活动

使用站点安全概览中的趋势图，趋势图的峰值对应着各类攻击总量，CC 攻击规模通常对应了速率限制和 CC 攻击防护的命中请求数。

用于 CC 攻击的客户端数量往往对应着攻击强度和攻击方的成本投入，您可以在 CC 攻击防护分页中查看已拦截的恶意客户端数量，来判断攻击方投入的资源，作为防护参考。

说明：

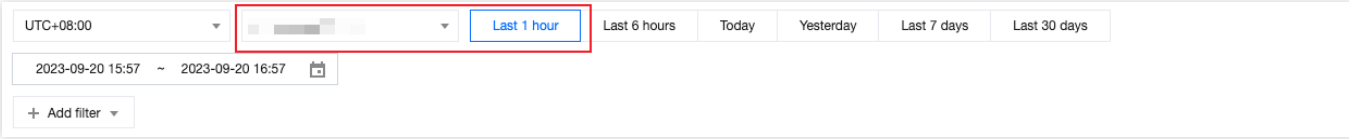
当已拦截的恶意客户端数量超过2000个时，通常意味着攻击方投入了较多资源，并调用了一个或多个 Botnet 网络，请考虑升级企业版并购买独立 DDoS 防护，以确保有足够防护资源进行对抗，避免攻击造成业务损失。

场景示例

当您的站点 `example.com` 内域名 `www.example.com` 在近1小时内遭受了大规模 CC 攻击时，您需要第一时间了解关于该威胁的信息，以便制定针对性的防护策略或评估已有策略。除了在流量分析页面查看状态码比例，检查是否对业务造成影响外，您也可以在**安全分析 > 站点安全概览页**中查看安全模块的统计情况。

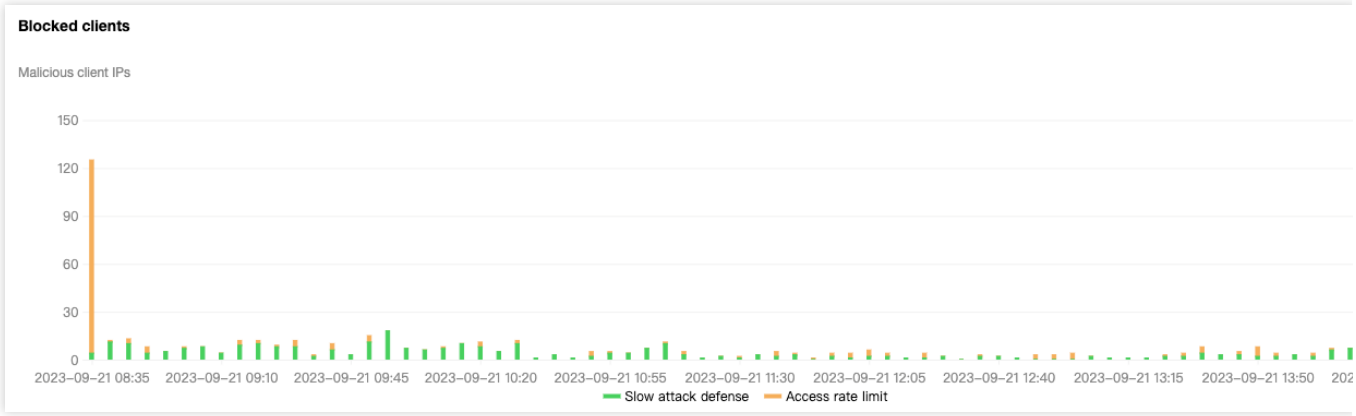
操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**数据分析 > 安全防护**，默认进入站点安全概览分析页内。
3. 修改查看需分析的站点域名和时间范围。以本场景为例，选择业务域名为 `www.example.com` 的域名在近1小时内的安全防护数据。



4. 筛选后，会自动根据筛选结果查询安全分析数据。查看 Web 防护趋势，您可以通过点击图例下方的指标值，关闭其余指标展示，只展示 CC 攻击防护的攻击规模和趋势。

5. 在下方安全分类事件统计中，单击 **CC 攻击防护**，查看已拦截恶意客户端统计，可查看当前已出发拦截的客户端 IP 数量和趋势分布，确认发起攻击的客户端 IP 数量。



6. 分别切换至 CC 攻击防护和速率限制分页中，可以查看该域名命中次数最多的 TOP 规则列表，从而明确攻击的主要目标和对应方式。根据分析结果，您可以前往 CC 攻击防护 和 速率限制 内配置调整相应的防护策略。

场景二：评估漏洞攻击防护策略

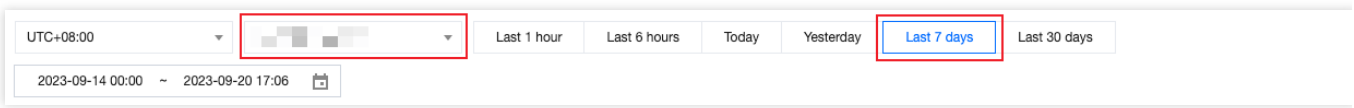
使用托管规则防护漏洞攻击时，需要进行测试调优避免误拦截。此时，站点安全概览可以帮助您评估规则的整体识别情况，并快速识别出可能误报的规则。
通常情况下，漏洞攻击具有偶发性特点，仅有少数场景（如：扫描站点漏洞）可能存在持续命中托管规则的情况。因此，当观察到持续命中固定规则时，需要排除规则误报的情况。

示例场景

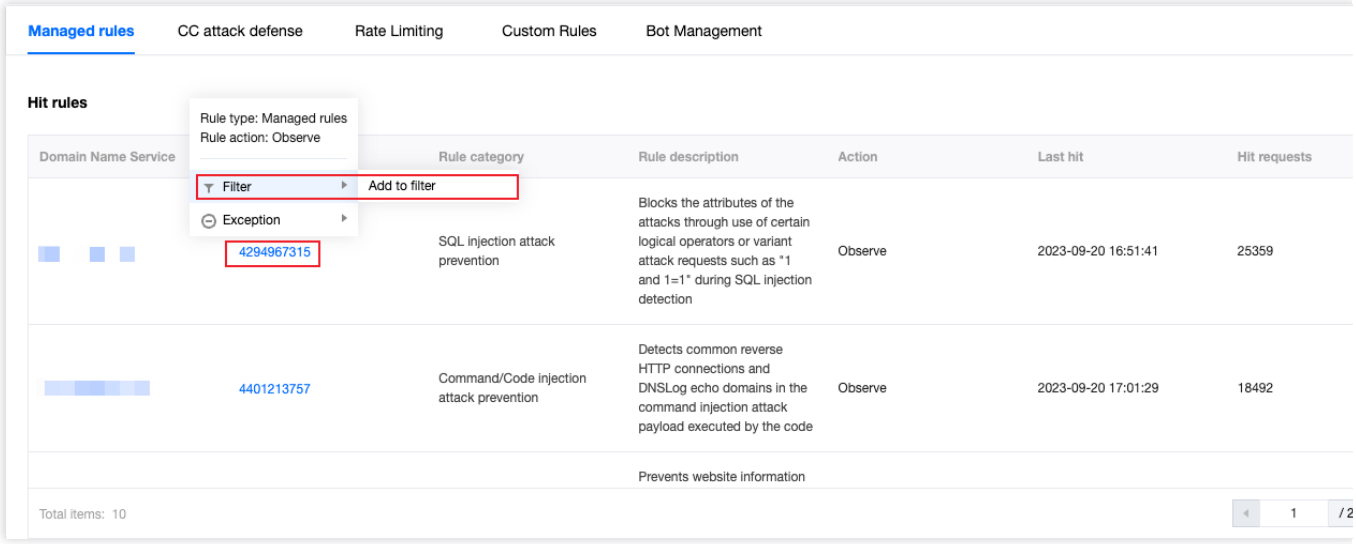
当您持续接受到不同的用户反馈当前请求被拦截导致无法访问站点站点 `example.com` 内域名 `www.example.com` 的内容时，需要查看是否因为该用户请求命中了安全防护规则导致被拦截，需要对规则进行调优。其中，客户端 IP 为1.1.1.1用户为可信任的内部测试用户，也遭到了拦截。

操作步骤

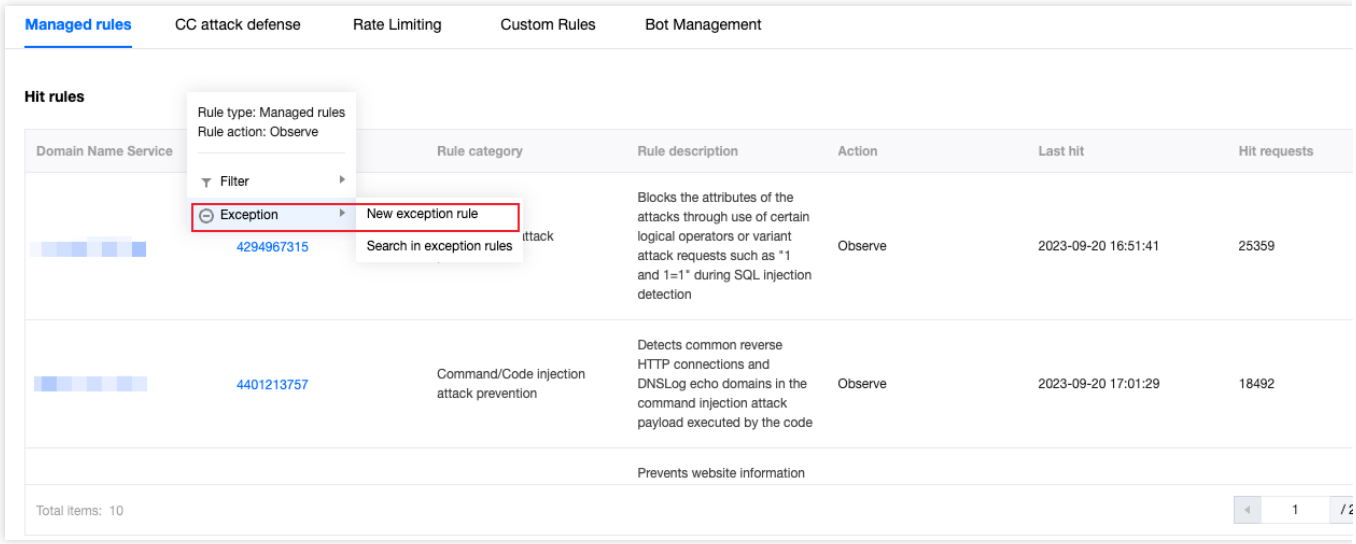
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**数据分析** > **安全防护**，默认进入站点安全概览分析页内。
3. 筛选查看需分析的站点域名、时间范围。以本场景为例，选择业务域名为 `www.example.com` 的域名在近7天内的安全防护数据。



4. 在托管规则分页中，查看所有命中规则统计，当有规则 ID 大量命中请求时，可单击该**规则 ID**，选择**筛选** > **加入筛选**，将该规则 ID 加入筛选条件，查看所有命中该规则 ID 的请求，触发的详细请求路径、客户端 IP 以及命中趋势信息。



5. 分析后，如果您发现该规则确实拦截了正常的路径请求或客户端 IP，但是也拦截了部分非正常的业务请求，您可以单击该**规则 ID**，选择**规则例外 > 新建防护例外规则**，快速新建一条 Web 防护例外规则。以本场景为例，新建一条规则，将受信任的客户端 IP `1.1.1.1` 加入防护例外规则，跳过该规则 ID 扫描。



6. 如果需要查看更详细的规则命中日志，您可以记录该规则 ID，使用 Web 安全分析来进一步查看命中该规则 ID 的请求样本来判断是否为正常请求。

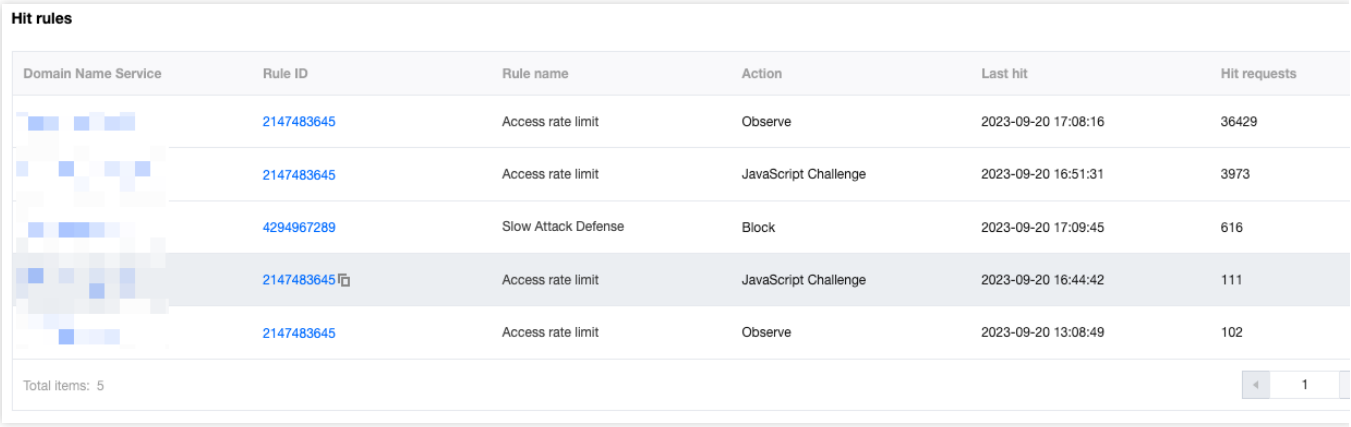
场景三：查看所有站点的整体安全趋势

场景示例

当您添加多个站点并在 EdgeOne 稳定运行一段时间后，为查看所有站点的安全防护趋势，找出其中频繁遭遇 CC 攻击的站点及域名，用于进一步对该站点域名加强防护，可以参照如下步骤操作。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**数据分析** > **安全分析**，进入多站点聚合的缓存分析页面，默认为站点安全概览页面。
2. 在该页面内可查看所有站点汇总的安全防护统计数据，在下方的安全事件分类统计展示中，单击 **CC 攻击防护**，查看命中规则统计，可以看到命中 CC 规则最多的域名、规则名称、处置方式以及命中的请求数。


Hit rules

Domain Name Service	Rule ID	Rule name	Action	Last hit	Hit requests
	2147483645	Access rate limit	Observe	2023-09-20 17:08:16	36429
	2147483645	Access rate limit	JavaScript Challenge	2023-09-20 16:51:31	3973
	4294967289	Slow Attack Defense	Block	2023-09-20 17:09:45	616
	2147483645	Access rate limit	JavaScript Challenge	2023-09-20 16:44:42	111
	2147483645	Access rate limit	Observe	2023-09-20 13:08:49	102

Total items: 5 1

3. 您可以进一步点击对应域名，将该域名添加为筛选项后，进一步分析该域名触发的 CC 防护规则触发次数趋势以及客户端分布。之后参考 CC 攻击防护配置文档来进一步优化防护策略。

Web 安全分析

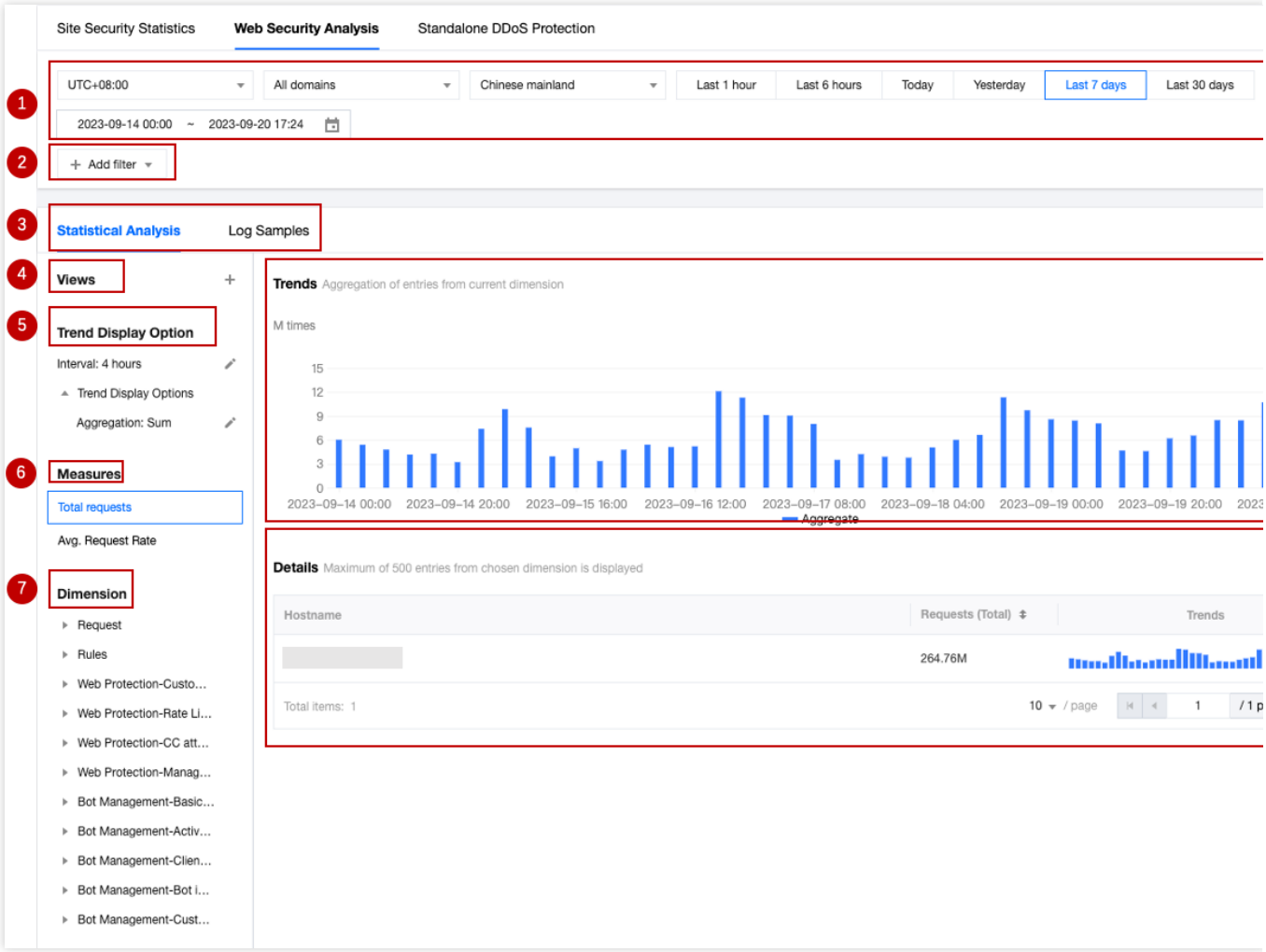
最近更新时间：2023-09-21 15:03:26

概述

Web 安全分析提供了安全事件精细化分析工具，为您制定或调整安全策略提供参考。您不仅可以查看近期安全事件在数十个维度下的统计分析和分布趋势，并通过查看样本日志，进一步了解某一事件的具体内容和详细信息。Web 安全分析为 EdgeOne 的 web 安全功能提供了多个分析维度，帮助您制定高效的安全策略。

支持的能力

说明：
由于一个安全事件中，单个请求可能命中多个安全规则。在进行筛选或选择统计维度时，请注意区分规则的处置方式和请求的处置结果。
例如：一个请求命中了多条**处置方式**为观察的规则，同时命中了一条**处置方式**为拦截的规则，导致该请求最终的**处置结果**为拦截。



1. 数据时间范围

通过调整查询时间范围，您可以查询某一特定时间段的安全事件。

说明：

不同版本套餐可支持的查询时间范围请参见 套餐选项对比。

2. 添加筛选

支持的根据请求特征、规则 ID 等多种维度筛选需要统计的 Web 安全数据，Web 安全分析支持的筛选项可参考 如何使用筛选条件。

说明：

1. 同一个请求可能命中多条规则，因此当使用规则 ID 筛选时，会展示同时命中的其他规则的统计详情和趋势分布。
2. 您可以在统计详情中点击需要筛选的特征值，快速添加到筛选。

3. 分析维度

统计分析：帮助您按所选维度展示指标排名，发现异常访问量和异常访问趋势。例如：当您选择按 User-Agent 头部维度展示时，您可以查看访问的设备分布和访问指标趋势，从而鉴别出访问量异常的设备类型，以及匀速周期访问

的可疑访问行为。

样本日志：帮助您进一步查看安全事件详情，判断请求命中的安全策略是否符合预期。例如：您可以通过样本日志查看请求命中的托管规则，以及托管规则匹配的字段内容，从而帮助您判断是否为误杀，并据此调优安全策略。

4. 常用视图

您可以根据需要，将当前视图选项保存为常用视图，便于后续快捷使用。您可以为常用视图命名，视图将保存当前趋势展示选项、统计指标和 统计维度信息。

5. 趋势展示统计方式

说明：

当调整数据筛选时间范围时，数据颗粒度会对应调整，以确保有合适的趋势图表展示。

您可以按需要调整趋势图的展示选项：

数据颗粒度：趋势图中每个柱对应的数据统计时长。

汇聚方式：趋势图中每个柱对应数据的计算方式。

总和：展示按所选维度过滤数据后，该时间段段内所有统计项的指标总和。例如：趋势图中一个柱对应的统计时段中，有 6000 个请求，则该柱展示数据为 6000。

平均值：展示按所选维度过滤数据后，该时间段段内所有统计项指标的平均值。例如：按 Host 维度展示统计数据时，数据共包含 5 个 Host 数据，趋势图中一个柱对应的统计时段中，有 6000 个请求，则该柱展示数据为 6000 / 5 = 1200。

最大值：展示按所选维度分拆数据后，该时间段内的最大数据项。

99 分位值：展示按所选维度分拆数据后，该时间段内大于 99% 数据项的最小数值，即：该值大于其他 99% 的统计项指标值。

99.9 分位值：展示按所选维度分拆数据后，该时间段内大于 99.9% 数据项的最小数值，即：该值大于其他 99.9% 的统计项指标值。

6. 统计指标

您可以选择展示 `请求数` 或者 `平均请求速率` 指标，来展示需要的统计特征（如：速率特征或请求数特征）。

请求数：按当前统计维度展示总请求数，用于区分大量请求的访客特征。例如：按 `请求 Host` 维度分析，可以区分出访问较集中的业务域名。

平均请求速率：按当前统计维度统计平均请求速率，用于区分访问频次较高的访客特征。例如：按 `User-Agent` 头部维度分析，可区分出访问频率异常的设备类型。

7. 统计维度

Web 安全分析提供了下列分析维度分类，您可以选择按所选维度调整统计对象和分组方式：

按**请求**属性分类的统计维度有：

客户端 IP：统计来自不同客户端 IP 的请求数。

客户端 IP（XFF 头部优先）：统计来自不同客户端 IP 的请求数。如果客户端经过 Web 代理访问，将按 XFF 头部中最近一跳的 IP 统计。

User-Agent：统计来自不同设备类型（通过 HTTP User-Agent 头部区分）的请求。
请求 URL：统计访问不同 URL （包括访问路径和查询参数）的请求。
域名 Host：统计访问不同域名（通过 HTTP 头部 Hostname 区分）的请求。
来源 Referer：统计使用不同引用方式（通过 HTTP Referer 头部区分）访问资源的请求。
按**规则**属性分类的统计维度有：
类型：统计命中不同安全模块（如：自定义规则、托管规则等）的请求。
规则 ID：统计命中不同规则的请求。
说明：
1. 您可以使用规则分类中规则 ID 选项合并展示命中所有安全防护规则的请求。
2. 您也可以使用具体安全功能分类中的规则 ID 选项，仅查看命中该模块中规则的情况。如：按命中 Web 防护自定义规则的规则 ID 来统计请求。
3. 不同版本套餐可支持的统计维度不同，详情请参见 套餐选项对比。
您也可以选择其他按防护功能提供的分析选项。如：托管规则的命中字段、Bot 智能分析的 Bot 标签等，来进行统计分析。

8. 统计趋势图

统计趋势图将根据您的趋势展示选项和筛选条件，展示对应的汇聚数据柱状图。

9. 统计详情

根据您的统计维度和统计指标选项，展示不同维度的请求特征值，以及对应的指标。例如：当选择了 `请求数` 指标和 `User-Agent` 分析维度时，统计详情部分将展示不同客户端设备类型（User-Agent 头部取值）的请求数，按请求数从大到小排列展示，并展示各个设备类型的请求趋势。

分析示例

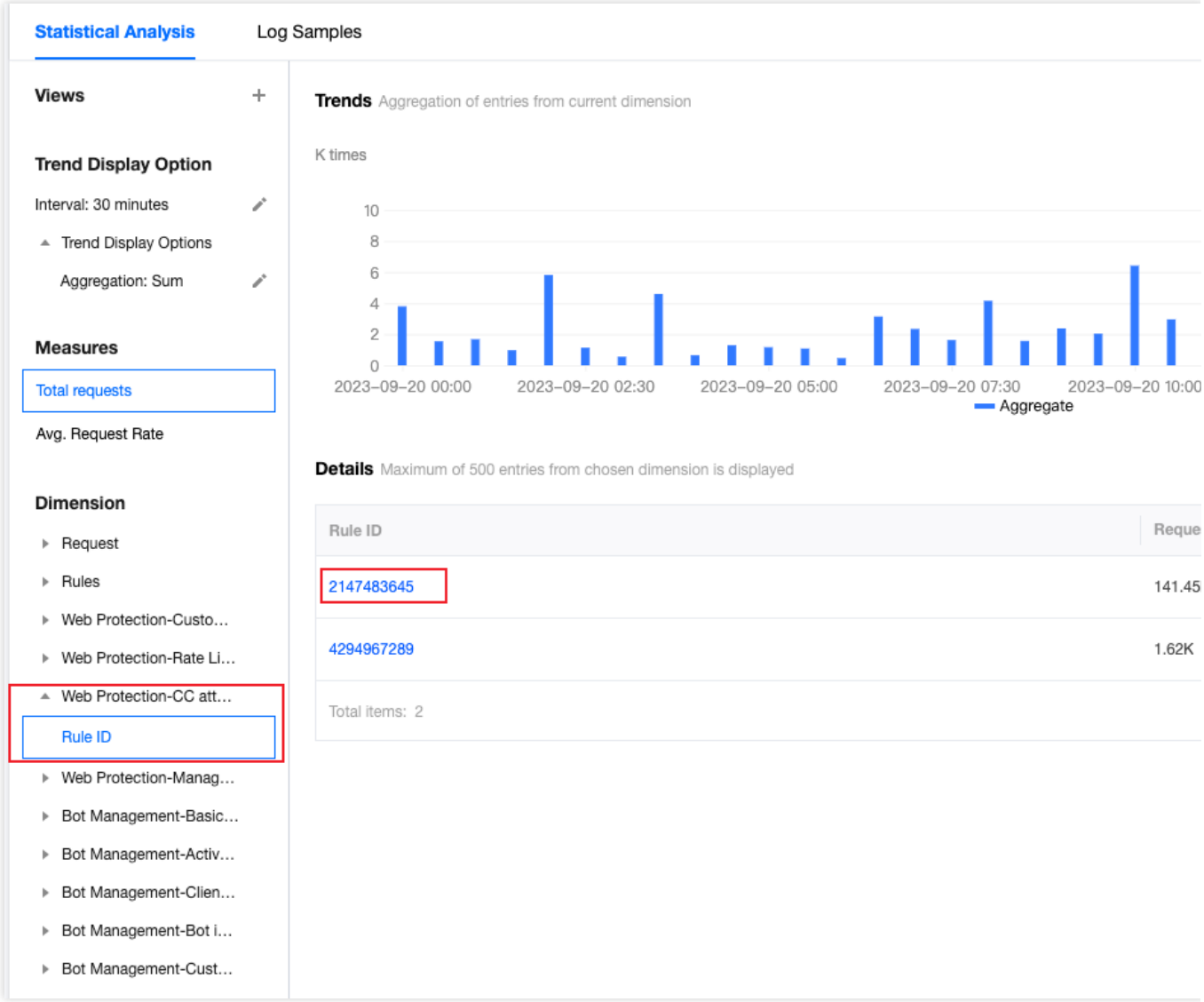
场景一：分析近 1 天内 CC 攻击防护的请求趋势

场景示例

假设您的站点 `example.com` 发现可疑的访问量突增，命中了 CC 攻击防护规则。需要分析在近 1 天内所有命中 CC 攻击防护的请求是否为正常请求，您可以参考以下步骤进行分析。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**数据分析** > **安全防护**，默认进入站点安全概览分析页内，在上方单击 **Web 安全分析**。
3. 筛选查看需要分析的站点域名、时间范围以及聚合条件，以当前场景为例，可选择过去 1 天的时间范围内。
4. 在统度分析中，单击 **Web 防护-CC 攻击防护** > **规则 ID**。



5. 查看数据结果，以上图为例，智能客户端过滤触发的请求数非常高（规则 ID：4294967293）可单击该**规则 ID** 加入筛选。然后单击左侧统计维度内的**请求 > User Agent，**即可查看命中该规则的所有 User Agent 头部汇总信息。您可以根据 User Agent 值判断是否符合您正常客户端预期。您也可以在统计维度中继续添加其它统计维度，例如：客户端 IP 和 请求 URL 来进一步缩小筛选范围。

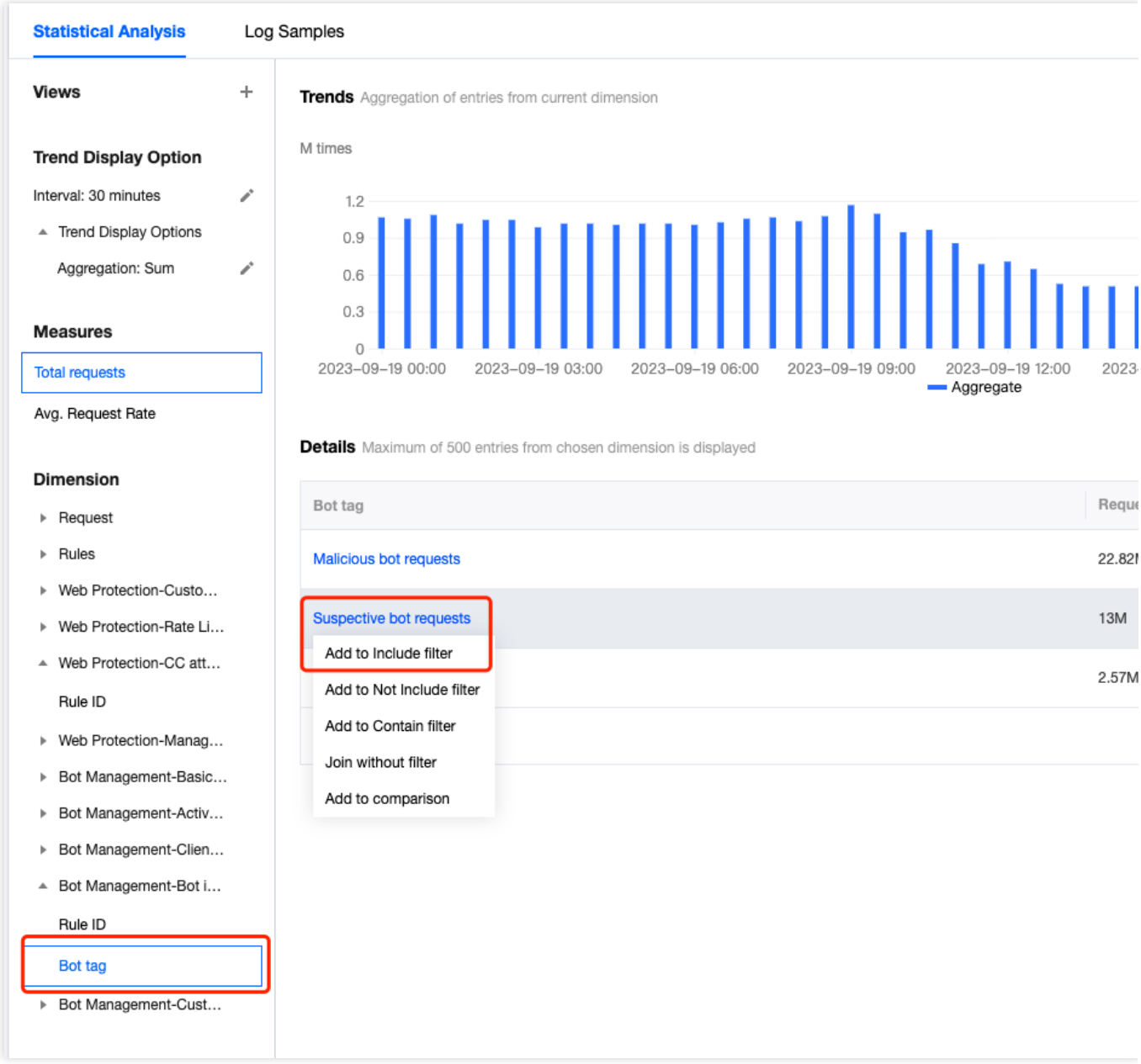
场景二：分析近 1 天内疑似 Bot 请求是否存在异常请求

场景示例

假设您的站点 `example.com` 近期频繁遭遇疑似 Bot 访问，需要分析在过去1天内所有疑似 Bot 请求访问的是否为正常请求，您可以参考以下步骤进行分析。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**数据分析** > **安全防护**，默认进入站点安全概览分析页内，在上方单击 **Web 安全分析**。
3. 筛选查看需要分析的站点域名、时间范围以及聚合条件，以当前场景为例，可选择过去 1 天的时间范围内。
4. 在统计分析中，单击 **Bot 管理-Bot 智能分析** > **Bot 标签**。
5. 查询数据结果，在统计详情内，可以看到相应 Bot 标签的请求次数。以当前场景为例，可以单击**疑似 Bot 请求** > **加入等于筛选**做进一步分析，加入筛选条件后，您也可以在统计维度中继续添加其它统计维度，例如：User-Agent 来进一步缩小筛选范围。



6. 单击**样本日志**，切换至详细样本日志分析，单击每条日志左侧的箭头可展开查看详细的请求头以及命中规则情况，来用于判断该请求是否为正常请求。

四层代理

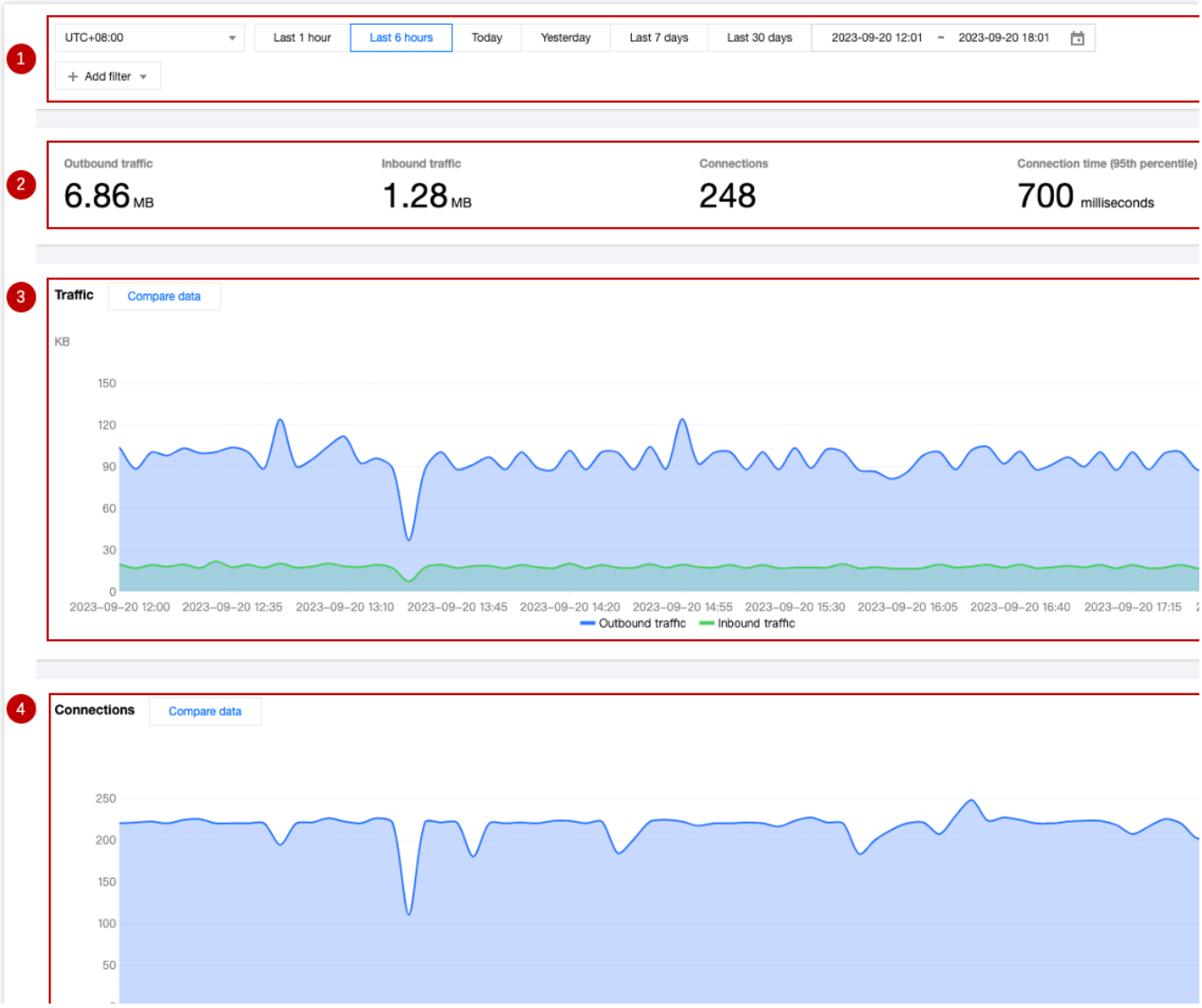
最近更新时间：2023-09-21 11:36:15

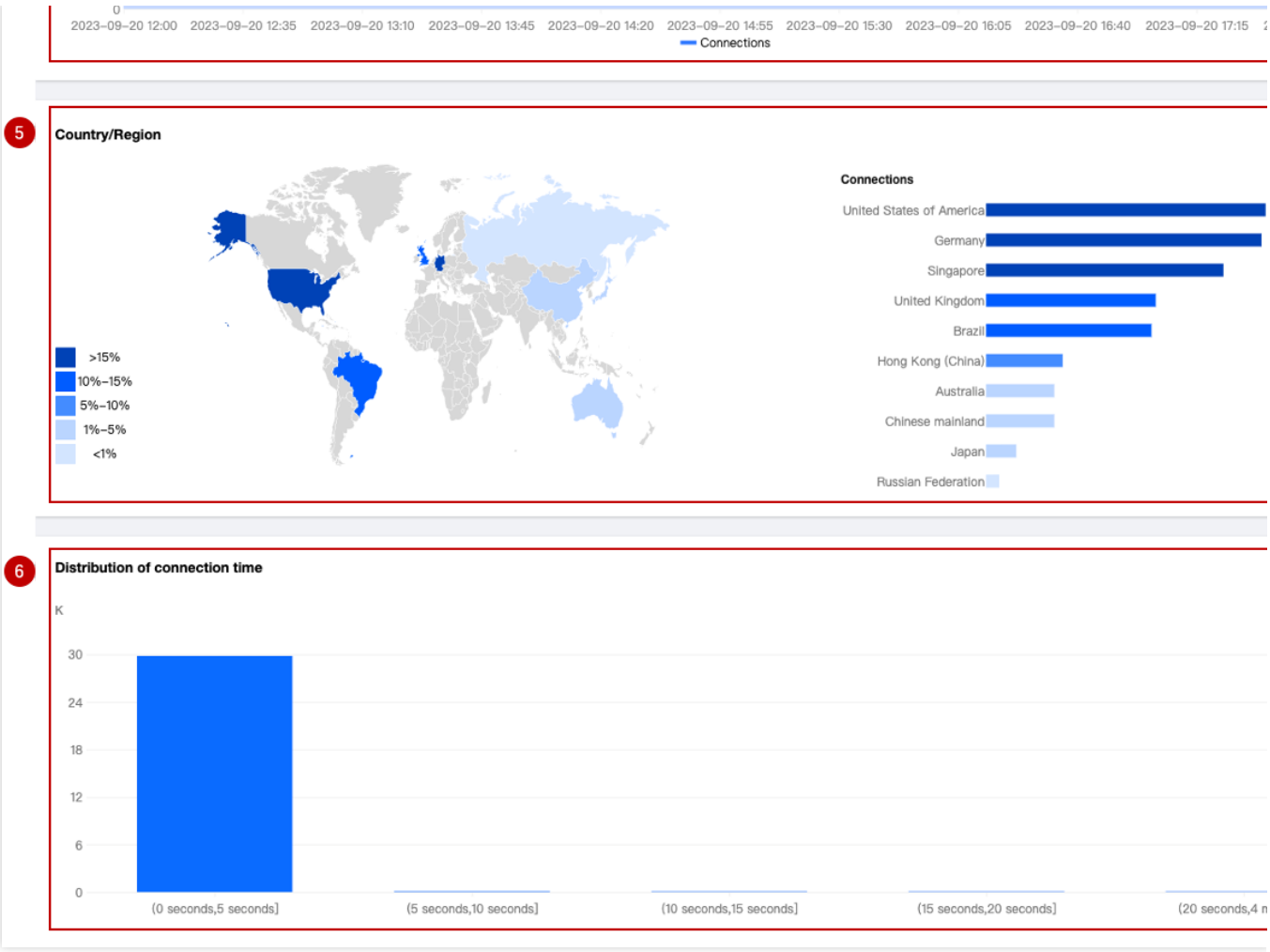
概述

EdgeOne 通过分析 L4（传输层）访问日志，为您提供用户访问四层代理实例的数据分析展示，主要包括流量、连接数、连接时长等数据，帮助您更好地监控四层代理实例的运行情况。

支持的能力

四层代理分析页面支持对四层代理实例的流量、连接数、连接时长等数据进行统计展示，支持添加筛选过滤条件。





1. 数据筛选与过滤

支持选择数据查询的时间范围，详情请参见 如何修改查询时间范围。
支持按照站点、服务名称、转发规则、国家/地区等维度筛选过滤，详情请参见 如何使用筛选条件。

2. 核心指标

出流量：经由 EdgeOne 节点向客户端传输的流量。
入流量： EdgeOne 节点接收到客户端请求的流量。
连接数：在所选时间范围内存在的连接数量。
连接时长（95 分位）：针对在所选时间范围内存在的连接，统计其连接时长的 95 分位值，即：该值大于其他 95% 的连接时长。

3. 时间趋势图-流量

展示出流量、入流量的分时趋势曲线。

4. 时间趋势图-连接数

展示连接数的分时趋势曲线。

版权所有：腾讯云计算（北京）有限责任公司

5. 国家/地区分布

展示连接数在国家/地区上的分布。

说明：

1. 此处数据以客户端所在国家/地区为准，与计费数据可能有差异，计费数据的大区分布以实际服务用户客户端的 EdgeOne 节点所在区域为准。
2. 由于时延和算法的影响，国家/地区分布仅供参考，建议您以实际日志分析结果为准。

6. 连接时长分布

展示连接时长的直方图分布。

分析示例

场景一：监控四层代理实例，在某国家的流量和连接数指标

在一定筛选条件下，通过四层代理分析页面的时间趋势图，监控四层代理实例的运行情况。

场景示例

当您 新建四层代理实例 后，希望监控四层代理实例名称为 `example` 的业务在新加坡的流量和连接数指标，可以在**数据分析 > 四层代理**页面中进行如下操作。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击您关注的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**数据分析 > 四层代理**，进入四层代理页面。
3. 在四层代理页面，单击**添加筛选**，添加筛选条件 `服务名称=example` `国家/地区=新加坡`，单击**确定**。
4. 查看流量和连接数的时间趋势图，观察是否有陡增或陡降，判断您关注的业务是否正常运行。

场景二：查看所有站点的四层代理实例整体运行趋势

场景示例

当您有多个站点添加了四层代理实例并在 EdgeOne 稳定运行一段时间后，希望在控制台定期巡检所有站点下的四层代理服务使用功能流量趋势，您可以参考如下步骤操作。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**数据分析 > 四层代理**，进入多站点聚合的数据分析页面。
2. 查看时间趋势图，观察流量、连接数是否有陡增或陡降，判断整体业务是否正常运行。
3. 在连接数卡片中，单击**对比数据**，可对比最近两天相同时间段的流量曲线，观察业务日环比是否有突增或突降。

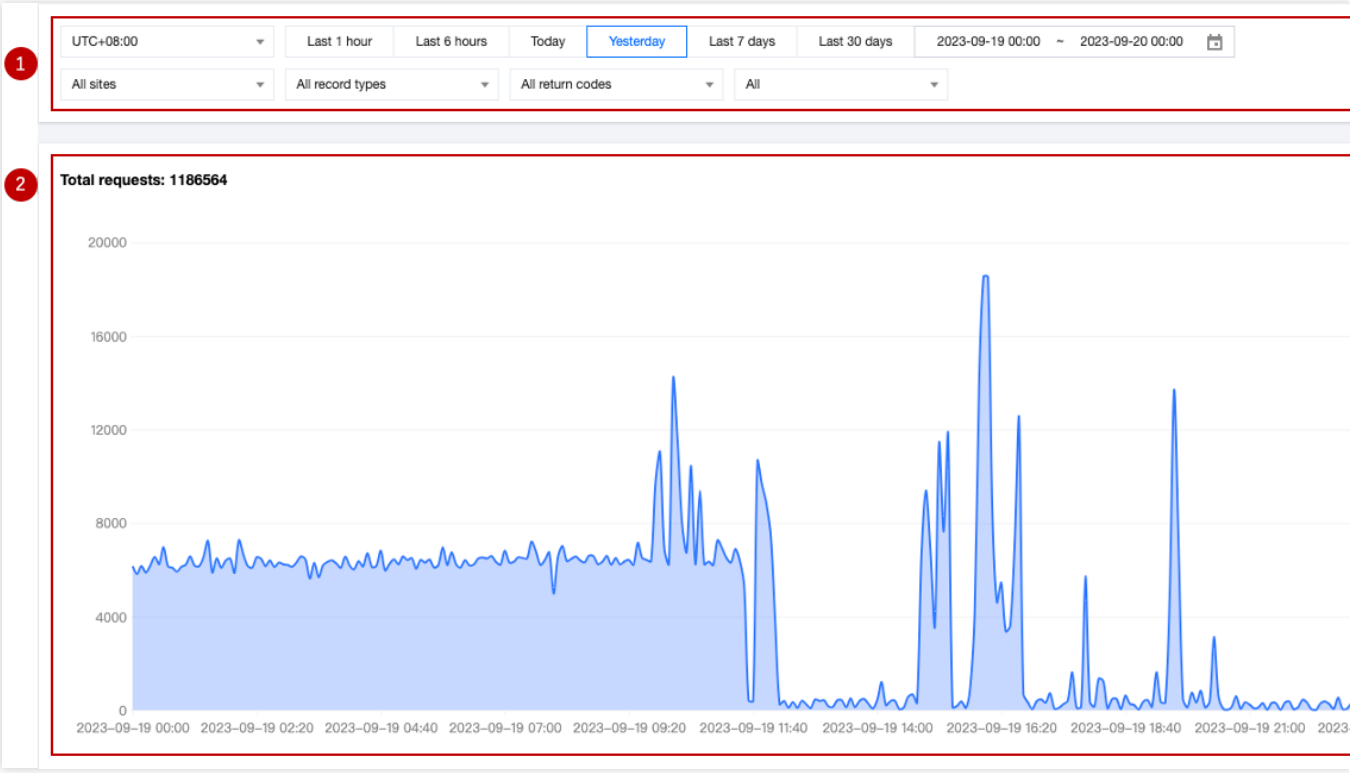
DNS 解析

最近更新时间：2023-09-21 11:37:21

概述

本页面主要展示 EdgeOne DNS 接收到解析请求的数量。仅支持 NS 模式接入的站点数据。

支持的能力



1. 数据筛选与过滤

支持选择数据查询的时间范围，详情请参见 如何修改查询时间范围。
支持按照站点、子域名、记录类型、返回码、客户端请求地域等维度筛选过滤，详情请参见 如何使用筛选条件。

2. 时间趋势图

展示 EdgeOne DNS 请求数量的分时趋势曲线。

分析实例

场景1：查看指定站点的 DNS 解析性能

示例场景

站点 `example.com` 通过 NS 的方式接入 EdgeOne 后，需要查看相关 DNS 解析请求次数，可参照如下步骤操作。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击您关注的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**数据分析** > **DNS 解析**，进入 DNS 解析分页面。
3. 在 DNS 解析分页面，可以查看到站点下所有解析请求次数趋势，您也可以通过筛选条件，进一步根据子域名、记录类型、返回码以及地区维度过滤统计数据。

场景2：查看所有站点的 DNS 解析性能

示例场景

当您的站点均使用 NS 的方式接入 EdgeOne 后，如需查询所有站点的 DNS 解析请求次数及变化趋势，可参照如下步骤操作。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**数据分析** > **DNS 解析**，进入多站点聚合的数据分析页面。
2. 在该页面内即可查看所有站点下的所有解析请求次数及趋势，您也可以通过筛选条件，进一步根据站点、记录类型、返回码以及地区维度过滤统计数据。

相关参考
如何使用筛选条件

最近更新时间：2023-09-21 11:31:49

目前 EdgeOne 数据分析支持的筛选条件分为两种类型：
1. 时间筛选条件（必选）：查看所选的时间范围内的数据，详情请参见 如何修改查询时间范围。
2. 其他筛选条件：根据每个页面支持的筛选项，自定义筛选需要的数据。下文针对这部分详细说明。

支持的运算符

运算符	说明
等于	查询筛选项等于任一指定值的数据
不等于	查询筛选项不等于任一指定值的数据
包含	查询 URL、Referer、资源类型包含指定字符串的数据（例如：查询 `URL 包含/example` 数据）
不包含	查询 URL、Referer、资源类型不包含指定字符串的数据（例如：查询 `URL 不包含/example` 的数据）
开始于	查询 URL、Referer、资源类型的前缀匹配指定字符串的数据
不开始于	查询 URL、Referer、资源类型的前缀不匹配指定字符串的数据
结尾是	查询 URL、Referer、资源类型的后缀匹配指定字符串的数据
结尾不是	查询 URL、Referer、资源类型的后缀不匹配指定字符串的数据

多个筛选条件之间的关系

多个筛选条件之间的关系为“且”关系，同一个筛选条件内的多个取值之间的关系为“或”关系。
例如：同时添加筛选条件 `国家/地区=新加坡;泰国` 和 `状态码=404`，意味着查询满足**来自新加坡或泰国客户端的访问**且**边缘响应状态码为 404** 的数据。

不同数据分析页面支持的筛选项

流量分析

站点：筛选归属不同站点的数据，支持多选，仅在多站点聚合数据分析下可选。
Host：客户端请求的 host，支持多选，仅在单站点数据分析下可选。
国家/地区：客户端请求来源的国家或地区，支持多选。
状态码：EdgeOne 响应客户端的状态码，支持多选，仅在单站点数据分析下可选。
HTTP 协议版本：客户端请求使用的 HTTP 版本，支持多选，取值有：
HTTP/1.0
HTTP/1.1
HTTP/2.0
HTTP/3.0（QUIC 协议）
Websocket Over HTTP/1.1（由 HTTP/1.1 发起的 Websocket 协议）
TLS 版本：客户端请求使用的 TLS 协议版本，支持多选，仅在单站点数据分析下可选。取值有：
TLS 1.0
TLS 1.1
TLS 1.2
TLS 1.3
URL：客户端请求的 URL 路径（path），仅在单站点数据分析下可选。支持填入多个值，不同值使用半角分号进行分隔。例如：`/example1;/example2`
Referer：客户端请求的 referer，仅在单站点数据分析下可选。支持填入多个值，不同值使用半角分号进行分隔。
资源类型：客户端请求的资源类型，仅在单站点数据分析下可选。支持填入多个值，不同值使用半角分号进行分隔。例如：`.txt;.jpg`
设备类型：客户端请求的设备类型，由 HTTP 请求头中的 User-Agent 解析得出，支持多选，仅在单站点数据分析下可选。取值有：
TV：电视
Tablet：平板电脑
Mobile：手机
Desktop：电脑
Other：其他
Empty：空
浏览器类型：客户端请求使用的浏览器类型，仅在单站点数据分析下可选。支持多选。
系统类型：客户端请求使用的操作系统类型，仅在单站点数据分析下可选。支持多选。
IP 版本：客户端请求使用的 IP 地址版本，仅在单站点数据分析下可选。取值有：
IPv4
IPv6
HTTP/HTTPS：客户端请求使用的 HTTP 协议类型，取值有：
HTTP
HTTPS

省份：客户端请求来源的省份，仅在单站点数据分析下可选。仅中国大陆可用区站点支持。
运营商：客户端请求来源的运营商，仅在单站点数据分析下可选。仅中国大陆可用区站点支持。
说明：
1. 当核心指标选择“带宽峰值”时，仅支持「国家/地区」「Host」「HTTP/HTTPS」「HTTP 协议版本」筛选项。
2. 不同套餐支持的筛选条件可能不同，详情请参见 套餐选型对比。

缓存分析

站点：筛选归属不同站点的数据，支持多选，仅在多站点聚合数据分析下可选。
Host：客户端请求的 host，支持多选，仅在单站点数据分析下可选。
缓存状态：客户端请求的缓存状态，仅在单站点数据分析下可选。取值有：
Hit：请求命中 EdgeOne 节点缓存，资源由节点缓存提供。
Miss：请求未命中 EdgeOne 节点缓存，资源由源站提供。
Dynamic：请求的资源无法缓存/未配置被节点缓存，资源由源站提供。
状态码：EdgeOne 响应客户端的状态码，支持多选。
URL：客户端请求的 URL 路径（path），仅在单站点数据分析下可选。支持填入多个值，不同值使用半角分号进行分隔。例如：`/example1;/example2`
资源类型：客户端请求的资源类型，仅在单站点数据分析下可选。支持填入多个值，不同值使用半角分号进行分隔。例如：`.txt;.jpg`

安全分析

站点安全概览

请求处置结果：仅查看命中安全规则并按指定方式处置的请求（不包括放行或例外规则）。
请求路径：仅查看访问指定请求路径的请求数据。
规则 ID：仅查看命中指定规则的请求数据。
客户端 IP：仅查看来自某客户端 IP 的请求数据。
Host：仅查看访问某一域名服务的请求数据。

Web 安全分析

支持的根据请求特征、规则特征以及各详细的 Web 防护规则和 Bot 管理策略特征来进行筛选，其中请求特征的相关筛选项说明如下：
客户端 IP：仅查看来自某客户端 IP 的请求数据，支持输入多个值，不同值使用回车进行分隔。
客户端 IP（XFF 头部优先）：仅查看来自某客户端 IP 的请求数据，如果客户端经过 Web 代理访问，将按 XFF 头部中第一个 IP 进行筛选。支持输入多个值，不同值使用回车进行分隔。
User Agent：客户端请求中携带的 User Agent 头部信息,支持输入多个值，不同值使用回车进行分隔。
请求 url：仅查看访问某一特定URL（不包括Host，仅包含请求路径和查询参数）的请求数据，支持输入多个值，不同值使用回车进行分隔。
域名 host：客户端请求的 host，支持输入多个值，不同值使用回车进行分隔。

版权所有：腾讯云计算（北京）有限责任公司

来源 referer：客户端请求携带的 referer，支持输入多个值，不同值使用回车进行分隔。
处置结果：仅查看指定命中安全规则并按指定方式处置的请求，支持多选，详细的请求处置结果说明请参考：Web 防护处置方式 及 Bot 管理处置方式。
请求路径（Path）：仅查看访问某一特定路径（HTTP请求路径，不包括Host和查询参数）的请求数据。支持填入多个值，不同值使用回车进行分隔。
请求 JA3 指纹：查看匹配某一特定JA3 指纹的请求数据。
请求方式（Method）：仅查看使用指定HTTP Method 方式访问站点的请求数据，支持多选。
请求 ID：仅查看指定请求（请求 ID 即为拦截页面和日志中的请求 ID，可对应到唯一请求）。

DNS 解析

站点：筛选归属不同站点的数据，支持多选，仅在多站点聚合数据分析下可选。
子域名：客户端请求的 host，支持多选，仅在单站点数据分析下可选。
记录类型：DNS 记录类型，取值请参考 记录类型。
返回码：DNS 解析应答状态码。取值有：
NOError：无错误，成功响应
NXDomain：不存在的记录
NotImp：未实现，DNS 服务器不支持所请求的查询类型；已实现的请求查询类型参考 记录类型。
Refused：拒绝，DNS 服务器由于策略拒绝执行指定的操作。
地区：客户端请求来源的大洲，目前支持如下选项：
亚洲
欧洲
非洲
大洋洲
美洲

如何修改查询时间范围

最近更新时间：2023-09-21 12:13:20

EdgeOne 数据分析页面支持用户自定义筛选时间范围，下文主要介绍筛选时间范围的两种方式。

说明：

为了提升查询效率，不同时间范围的数据颗粒度如下：

时间范围 ≤ 2 小时：1 分钟。

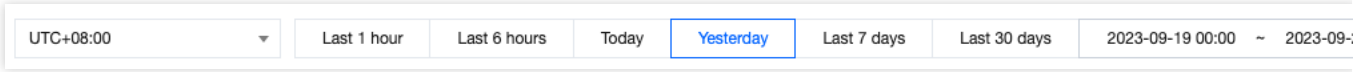
2 小时 < 时间范围 ≤ 48 小时：5 分钟。

48 小时 < 时间范围 ≤ 7 天：1 小时。

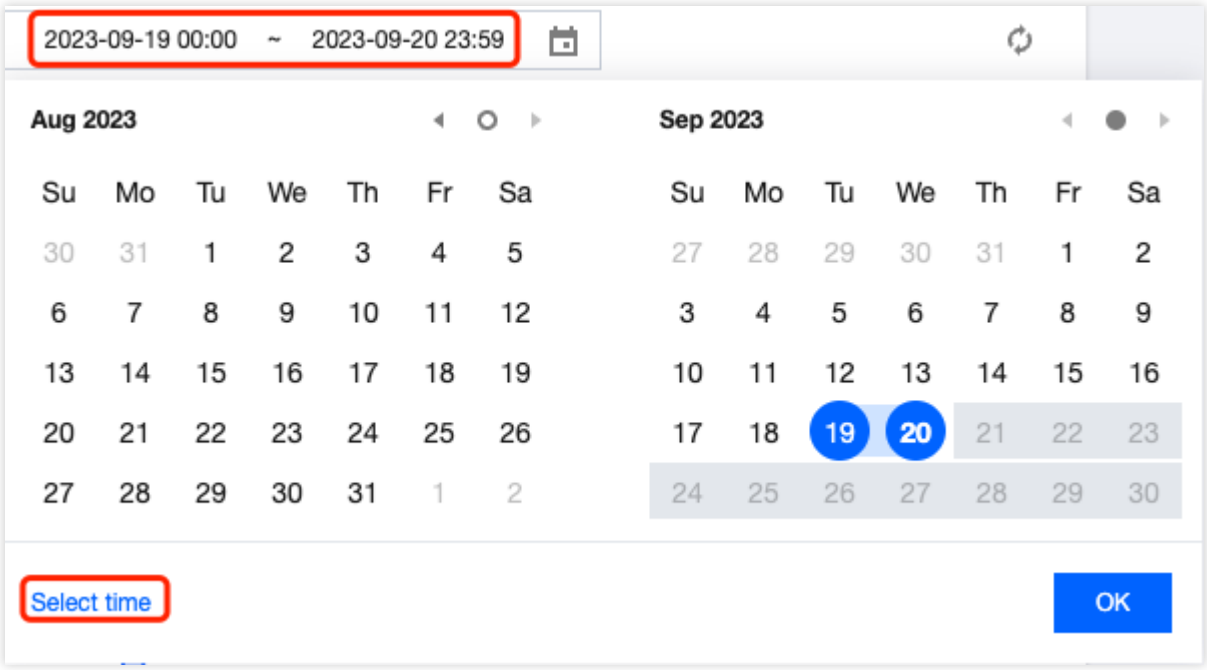
时间范围 > 7 天：1 天。

方式 1：通过筛选栏设置查询时间范围

快速查询：通过单击**近 1 小时**、**近 6 小时**、**今日**、**昨日**等按钮快速查询对应的时间范围数据。



自定义查询：您可以通过选择具体的日期和时间范围，查询自定义时间范围内的数据。

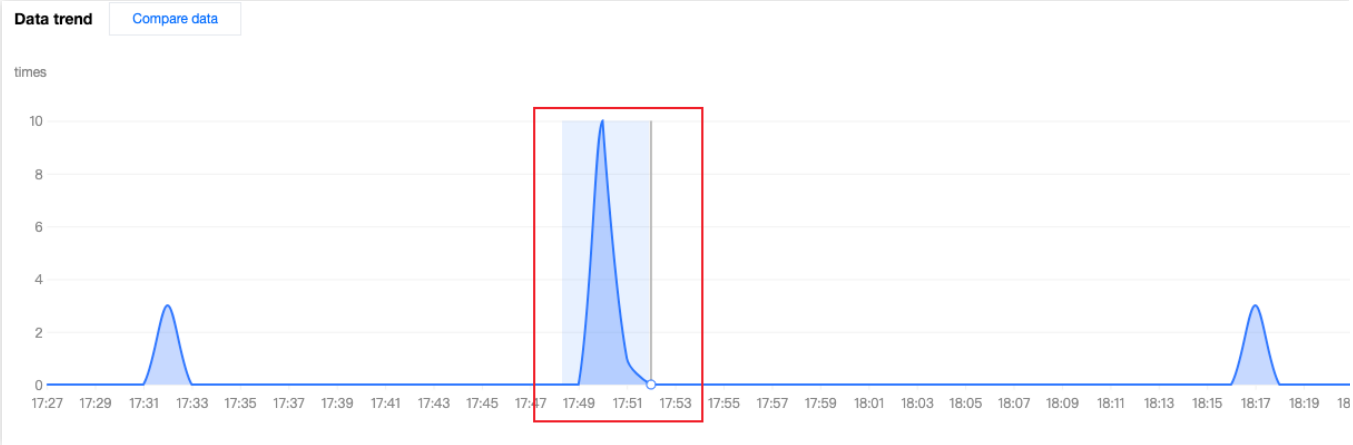


说明：

1. 当您选择“近 1 小时”“近 6 小时”“今日”时，页面会显示最近 1 小时、6 小时、当日（从 00:00 开始）的数据，并以每5分钟的频率刷新。
2. 单次最大查询时间范围为 31 天。
3. 由于套餐版本不同，不同站点可能支持查询的数据范围不同，具体请参见 套餐选型对比。
4. 为兼容不同套餐的数据查询，直接点击左侧一级导航栏中的**数据分析**查询数据时，仅支持查询最近 61 天的数据。

方式 2：在时间趋势图上选择查询时间范围

若您想查看曲线上特定的时间段，如下图所示，可以通过鼠标在曲线上点击滑动选取曲线的特定区域。该区域所对应的时间范围将会回填至顶部筛选栏，并影响页面中其他数据统计。



如何导出统计数据与报告

最近更新时间：2024-01-02 10:31:06

本文档介绍了 EdgeOne 数据分析页面如何导出统计数据和报告，具体操作步骤如下。

导出统计数据

1. 登录 边缘安全加速平台 EO 控制台，进入任意**数据分析**页面。
2. 单击

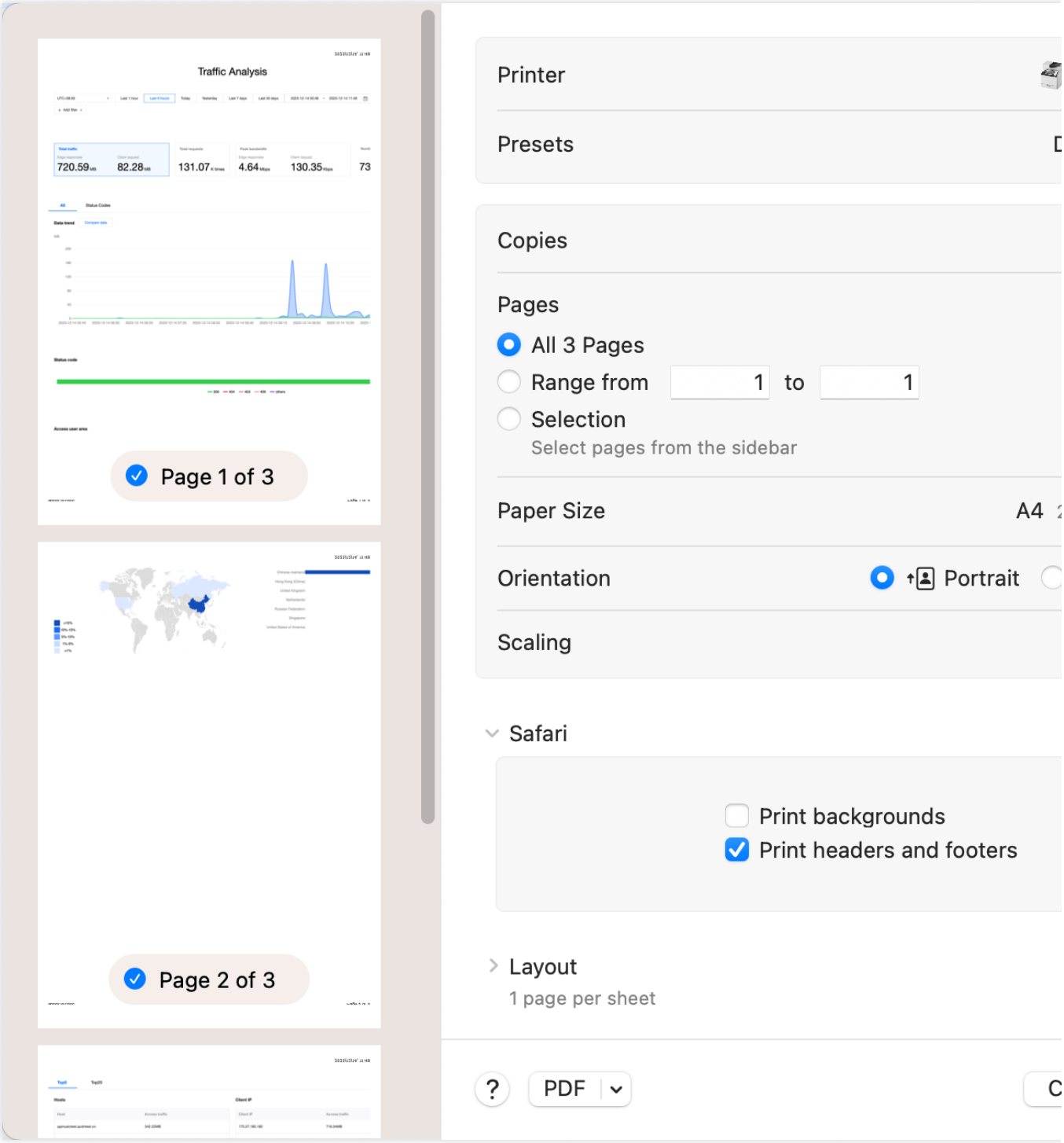
即可下载相应统计数据表，文件格式为 .csv，当前页面上的筛选条件将会应用到导出的数据上。

导出报告

1. 登录 边缘安全加速平台 EO 控制台，进入任意**数据分析**页面。
2. 单击筛选栏右上角的

，EdgeOne 将会唤起浏览器的打印窗口，您可选择打印或另存为 PDF 报告。当前页面上的筛选条件将会同步打印在报告中。

版权所有：腾讯云计算（北京）有限责任公司


Traffic Analysis
720.59
82.28
131.07
4.64
130.35
73
Page 1 of 3
Page 2 of 3
Printer
Presets
Copies
Pages
All 3 Pages
Range from
1
to
1
Selection
Select pages from the sidebar
Paper Size
A4
Orientation
Portrait
Scaling
Safari
Print backgrounds
Print headers and footers
Layout
1 page per sheet
PDF