边缘安全加速平台

操作指南

产品文档

腾讯云

文档目录

操作指南
站点概览

最近更新时间：2022-07-29 17:41:23

功能简介

EdgeOne 服务整体概览页，供您快速查看当前站点的整体情况，通过各类快捷入口前往功能页面或产品文档。含加速及安全服务数据，站点管理，服务状态，常见问题和文档资源模块。

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**服务概览**。
2. 在服务概览页面，默认选中“全部站点”，您可按需选择一个具体的站点查看。

3. 在服务概览页面，可查看工作流、站点管理、数据总览、常见问题和文档资源。

工作流

在页面顶部，您可以看到站点不同服务模块，其核心功能，及其接入状态。您可以快速查看所选站点已使用哪些产品服务，尚未使用哪些产品服务，并通过快捷入口前往其核心功能页配置。

> **说明**
> 选择“全部站点”时， 不同服务模块的接入状态无动态变化，只有选择一个具体的站点时，才有动态变化。

站点管理

1. 在站点管理模块中，可查看站点的状态和套餐信息。
   - 状态：
     - 已启用：成功检测到接入站点的 NS 或 CNAME 已更新，指向 EdgeOne。
     - 未生效：已添加站点但未更新 NS 或 CNAME。
     - 已停用：已对历史启用中的站点停用 EdgeOne 所有服务（DNS，加速和安全防护服务）。
   - 套餐信息：各站点对应的套餐版本及到期时间。
2. 在站点管理模块中，可以单击**管理**，对站点进行启用、停用和删除。
   - 启用：对已停用的站点重新启用 EdgeOne 所有服务。

     > **注意**
     > 启用后请关注服务是否生效（可能需要修改 NS 或 CNAME）。

   - 停用：对已启用的站点停用 EdgeOne 所有服务。

     > **注意**
     > 请您关注并确认您的站点解析。

- 删除：删除站点。删除后，站点的所有配置数据将被清空。如需使用，请重新接入。

> **注意**
> 删除前必须先停用站点服务。

数据总览

在数据总览模块中，展示了站点的业务访问、与安全防护相关数据概览；由于数据汇总存在延迟，所有数据仅作参考；详细数据请前往 数据分析 文档查看。

> **注意**
> 所有的数据仅为客户端访问日志数据（即应用层数据），与实际产生计费的数据有一定出入。在实际网络传输，实际产生的数据会大于纯应用层数据，具体计费用量，以实际计费账单为准。

常见问题

在常见问题模块中，展示了一些产品服务相关的常见问题。

文档资源

在文档资源模块中，罗列了一些产品服务相关的产品文档。

数据分析
流量分析

最近更新时间：2022-08-01 10:37:37

功能简介

通过分析业务访问日志数据，提供多种数据指标，供您多维度了解业务数据。受时延和算法影响，分布、排行类数据仅供参考，请以实际日志数据分析为准。

操作步骤

查询条件

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** > **流量分析**。
2. 在流量分析页面，选择所需站点，可查看相关指标；并支持按照时间筛选数据，或单击**添加筛选**，按照国家/地区、Host、设备类型等条件筛选数据。

参数说明：

- 站点：支持查看全部站点或单个站点的数据分析结果。
- 统计指标：单击*总流量*、*总请求数*，可展示根据流量、请求数所统计的 Hosts、客户端 IP 地址、urls、Referes 等指标。单击**带宽峰值**，可以查看带宽峰值展示的趋势曲线和国家/地区分布。

  > **注意**
  > - 带宽统计指标仅有 Host、国家/地区、HTTP 协议筛选指标。
  > - 调整时区会对整个**数据分析**功能生效。
  > - 单次查询起始时间与结束时间之间不能超过30天。

- 时间颗粒度：
  - 近1小时：1分钟。
  - 超过近1小时 ~ 1天内：5分钟。
  - 7天内 ：1小时。
  - 超过7天：天维度。
- 筛选条件：
  - 国家/地区：访问来源的国家/地区，支持多选。
  - Host：站点下的子域名。
  - 状态码：访问状态码。
  - 设备类型：访问来源的硬件设备类型，目前支持：Empty、TV、Tablet、Mobile、Desktop、Others。
  - 浏览器类型：用户访问使用的浏览器类型。
  - 操作系统类型：用户访问使用的操作系统类型。
  - 网络协议：用户访问时使用的网络协议，目前支持：http/2.0、http/1.1、https/2.0、https/1.1。
  - TLS版本：TLS协议版本，目前支持：TLS1.0、TLS1.1、TLS1.2、TLS1.3。
  - URL：访问URL，例如：/content。

- Referer：Referer 信息，例如：example.com。
- 资源类型：请求的资源类型，例如：png、json 等。

数据总览

在总览模块中，可根据设置的筛选条件与数据统计指标，展示这一时间段的趋势曲线。

国家/地区

在国家/地区模块中，可根据设置的筛选条件与数据统计指标，通过统计客户端 IP 识别访问用户所在国家/地区，汇总出访问客户端的国家/地区分布，并且排列统计指标前10的国家/地区。

状态码

在状态码模块中，展示了不同客户端访问返回的状态码的数量及分布。

数据排行

在数据排行模块中，可根据所选筛选条件，为您统计 Hosts（子域名）、客户端 IP 地址、URLs、Referers、资源类型、客户端设备类型等的 Top5、Top10 数据；如需更多详细数据，您可以通过下载完整统计数据查看，供您分析实际业务，如需更详细的数据，请查看具体日志。

缓存分析

最近更新时间：2022-07-29 17:43:28

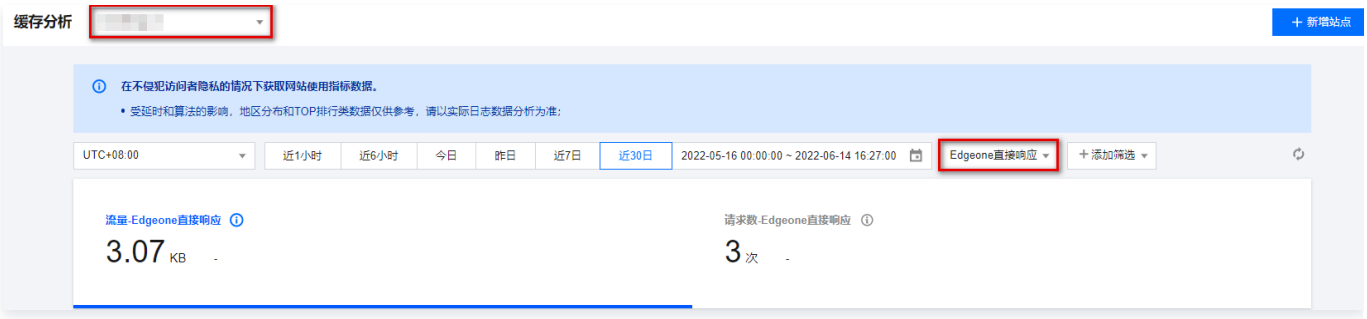
功能简介

通过分析业务访问日志数据和客户端的请求的缓存状态，提供多维度的缓存分析，助力优化配置。您可通过缓存分析，直观的查看流量值或请求由 EdgeOne 节点的缓存直接响应，提升了客户端的资源获取速度，且降低了您的源站压力。

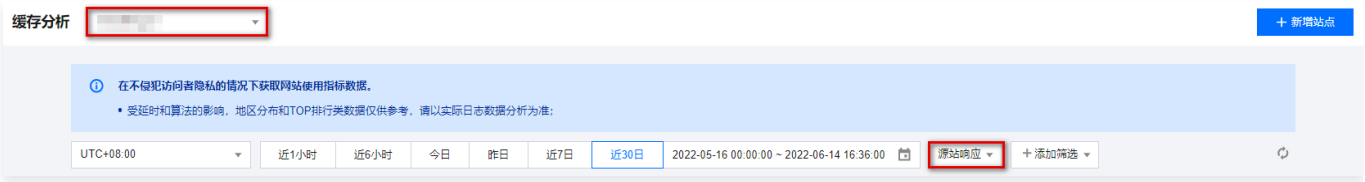
操作步骤

查询条件

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**。
2. 在流量分析页面，选择所需站点，您可根据实际需要选择正确的查询条件查询数据：
   - EdgeOne 直接响应：客户端请求的资源由 EdgeOne 的边缘节点缓存直接响应。

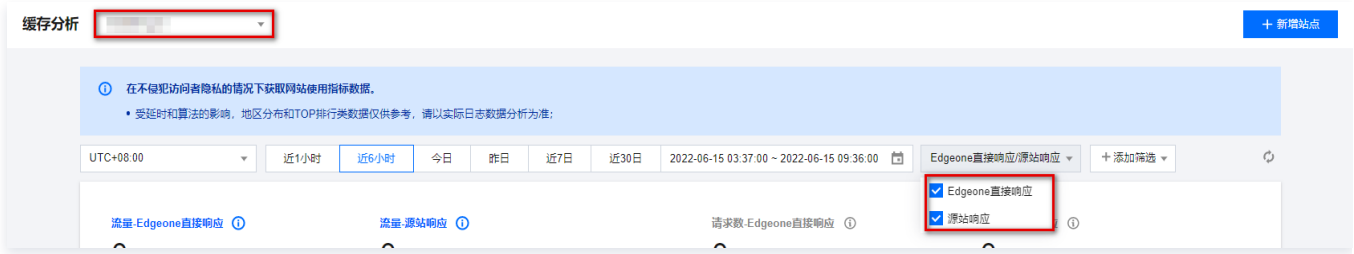


   - 源站响应：客户端请求的资源由源站响应提供。



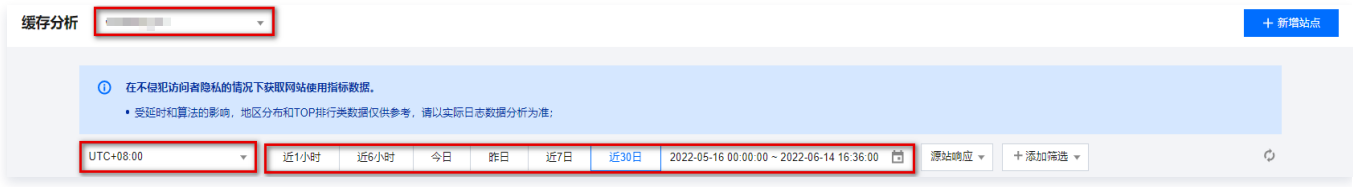
   - 根据 EdgeOne 直接响应和源站响应的流量、请求数，统计 Hosts、urls 等指标。

> **说明**
> - 您可以选择 **EdgeOne 直接响应**或**源站响应**，单独查看仅由源站/ EgdeOne 节点提供的数据。
> - 流量仅统计腾讯云 EdgeOne 向客户端提供的数据。



   - 时间选择：要查询的时间范围。

> **注意**
> - 调整时区会对整个**数据分析**功能生效。
> - 单次查询起始时间与结束时间之间不能超过30天。



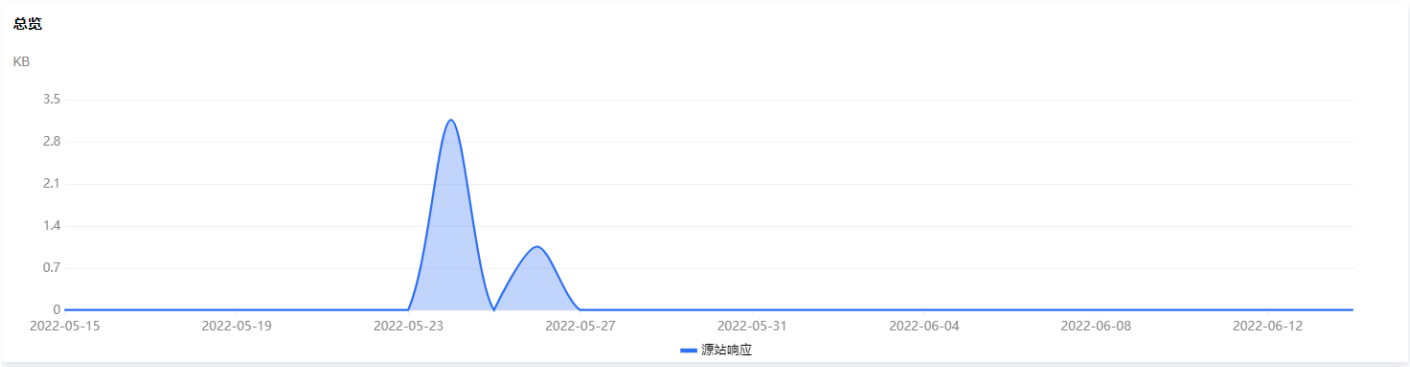
- 时间颗粒度：
  - 近1小时：1分钟。
  - 超过近1小时 ~ 1天内：5分钟。
  - 7天内 ：1小时。
  - 超过7天：天维度。
- 筛选条件：单击**添加筛选**，可以根据 Hosts、URL、资源类型、缓存状态来筛选数据。

字段说明：

- Hosts：站点下的子域名。
- URL：请求资源的 URL，例如：/content。
- 资源类型：请求的资源的资源类型，例如：png。
- 缓存状态：请求的命中缓存的状态。
  - 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/未配置被节点缓存，资源由源站提供。

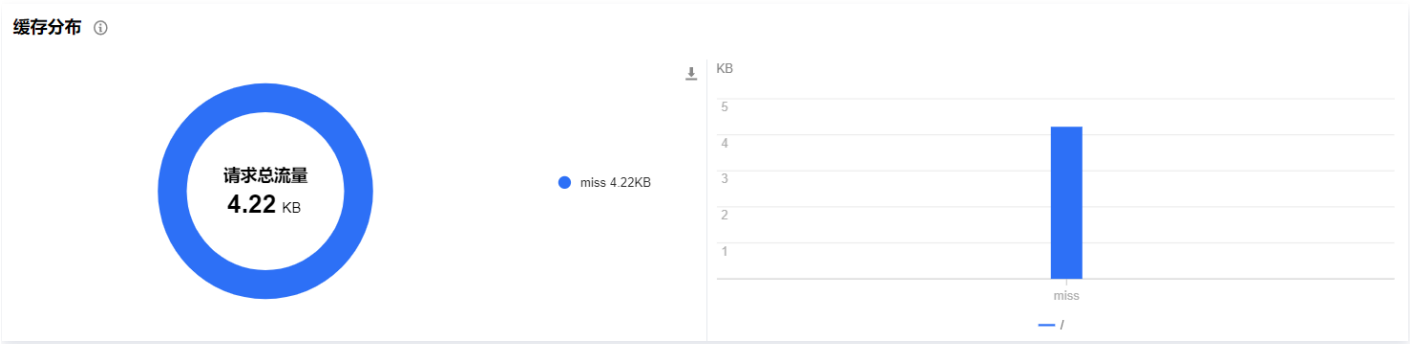
数据总览

根据设置的筛选条件与数据统计指标，展示这一时间段的趋势曲线。



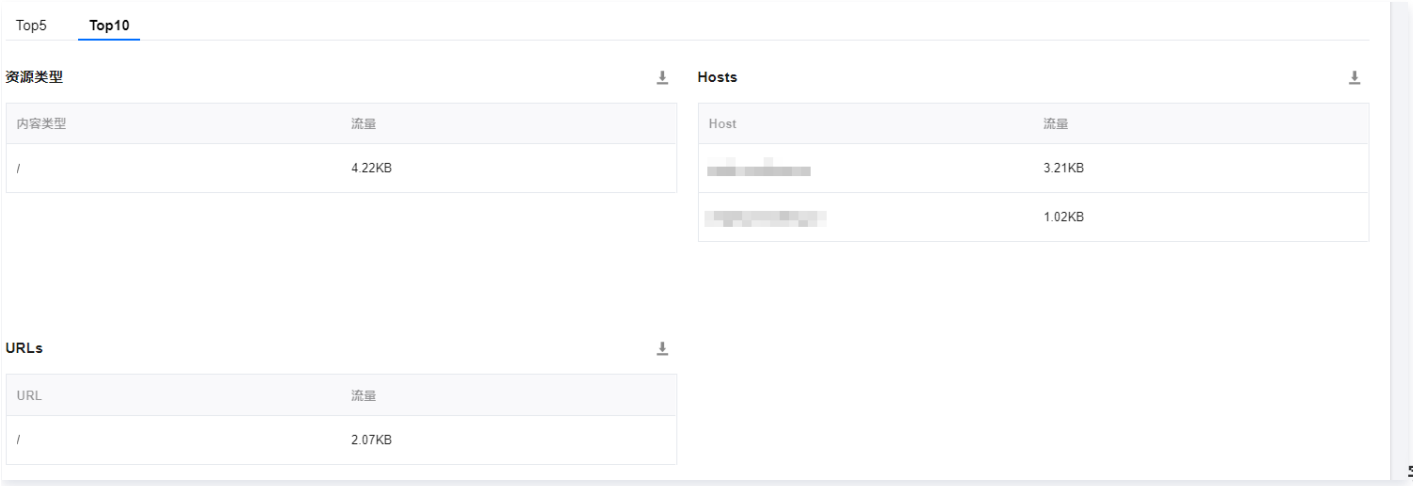
缓存分布

根据请求数据的缓存状态，展示这一时间段的缓存分布，同时展示不同缓存状态的资源类型分布。



数据排行

根据所选筛选条件，为您统计 Hosts（子域名）、客户端 IP 地址、URLs、Referers、资源类型（暂时不支持）、客户端设备类型等的 Top 5、Top 10数据；如需更多详细数据，您可以通过下载完整统计数据查看；供您分析实际业务，如需更详细的数据，请查看日志。



字段说明：

- 资源类型：请求的资源的文件后缀。
- Hosts：访问站点下的子域名。
- URLs：客户端访问的具体资源 URLs。

日志服务
实时日志

最近更新时间：2022-12-28 16:14:29

功能介绍

EdgeOne 实时日志服务功能通过对访问日志的实时采集与推送，实现对日志数据的快速检索与分析。您可通过 EdgeOne 控制台一站式快捷接入，享受从日志采集、日志存储到日志检索等全方位稳定可靠的日志服务。

适用场景

通过访问日志数据实时地多维度查看或分析业务情况。

前提条件

目前仅支持推送实时日志到腾讯云日志服务（CLS），为在腾讯云 EdgeOne 使用 CLS，需先开通 日志服务（CLS） 并授权腾讯云 EdgeOne 以创建日志集。

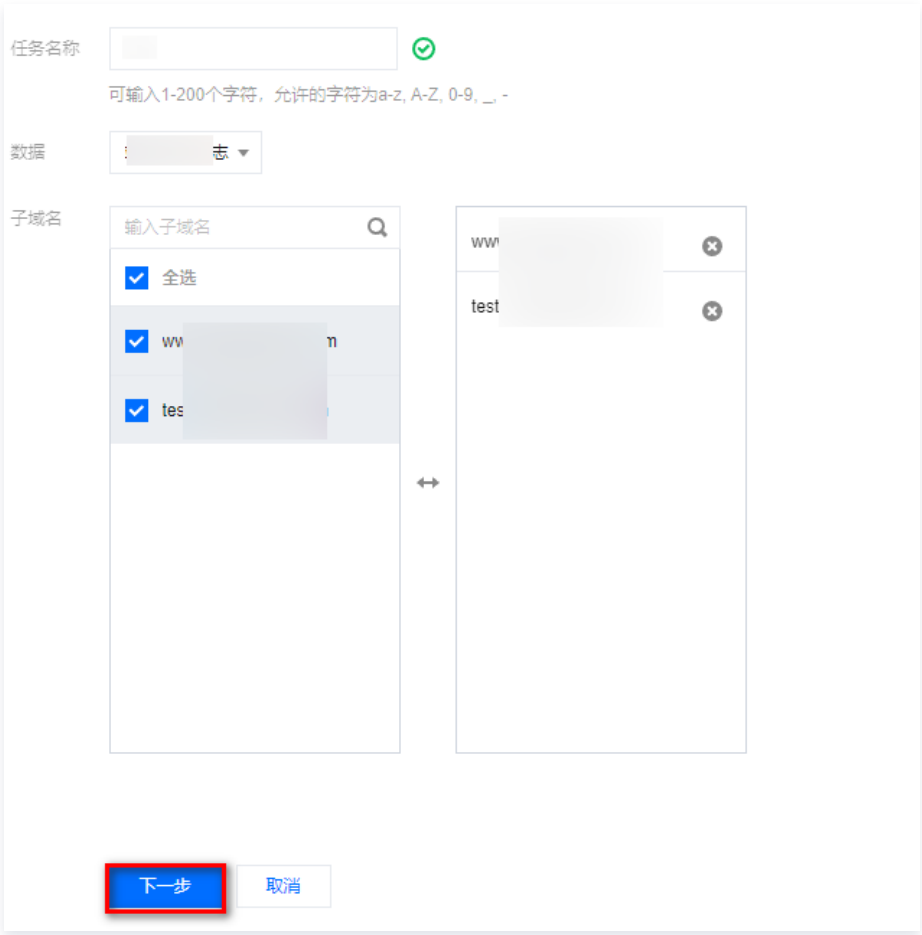
> **说明**
> 建议您使用主账号启用服务，若为子账号或协作者，您需要为其授权相关权限。

创建推送任务

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**日志分析** > **实时日志**。
2. 在实时日志页面，选择所需站点，单击**新建推送任务**，为当前站点新建实时日志推送任务。

> **说明**
> 目前仅支持推送实时日志到腾讯云日志服务（CLS）。

3. 在新建推送任务页面，输入任务名称，并且选择需要推送的数据和当前站点下需要推送日志的子域名，单击**下一步**。



参数说明：

- 任务名称：可输入1-200个字符，允许的字符为 `a-z, A-Z, 0-9, _, -` 。
- 数据：目前仅支持推送站点加速数据。
- 子域名：当前站点下需要推送日志的子域名。

> **说明**
> 同一个推送任务仅支持添加在一个推送任务中。

4. 选择所需参数，单击**推送**。

参数说明：

- 目标地址：默认选择腾讯云日志服务（CLS），不可更改。
- 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。

管理推送任务

编辑推送任务

1. 在 实时日志页面，选择所需推送任务，单击操作列的**编辑**。

2. 在编辑任务页面，可修改推送任务的名称、子域名列表，推送数据、推送任务的日志主题名称、日志保存时间，单击**保存**。

停用推送任务

停止日志推送任务投递到日志主题。

1. 在 实时日志页面，选择所需推送任务，单击操作列的**更多 > 停用**。

2. 停止后，该推送任务下的子域名的日志将不再继续投递至该日志主题，已经投递的日志将会继续保留。

启用推送任务

启动日志推送任务，投递日志到日志主题。

1. 在 实时日志页面，选择所需推送任务，单击操作列的**更多 > 启用**。

2. 启动后，该推送任务下的子域名的日志将继续投递至对应日志主题。

删除推送任务

1. 在 实时日志页面，选择所需推送任务，单击操作列的**更多 > 删除**。

2. 删除后，该推送任务下的子域名的日志将不再继续投递至对应日志主题，对应的日志主题将会被删除，已经投递的日志将会被全部清空。

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。

名词解释

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。

实时日志字段说明

日志字段	原始日志类型	说明
RequestID	string	客户端请求的唯一标识 ID
ClientIP	string	客户端 IP
ClientCountry	string	客户端所在国家2位字母编码，符合3166-2规范
RequestTime	int	客户端请求时间，UNIX 时间戳，单位为：秒
RequestHost	string	客户端请求的 Host
RequestBytes	int	客户端请求的大小（包含文件本身大小及请求 header 头部大小）
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 HTTP 协议：HTTP, HTTPS, HTTP/3
RemotePort	int	TCP 协议下客户端与节点建立连接的端口，若无则为 -
EdgeCacheStatus	string	客户端请求是否命中节点缓存：HIT，MISS，Dynamic
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
EdgeResponseTime	int	指的是从请求端发起请求开始，到请求端接收到服务器端的返回结束，这个过程所耗费的时间

热点问题

为什么腾讯云日志服务（CLS）控制台的部分日志主题在腾讯云 EdgeOne 控制台看不到?

因为腾讯云 EdgeOne 控制台仅支持和展示以腾讯云 EdgeOne 服务角色创建的日志信息，即专属腾讯云 EdgeOne 的实时日志服务，其他日志集及日志主题不会同步过来。

为什么实时日志检索不到数据，出现了丢数据的情况?

可能由于您的日志数据量较大，但日志主题是单分区或关闭了自动分裂。创建日志主题时，分区数量默认为1 ，默认开启自动分裂。

建议您按照自己的日志量预估所需的分区，前往 日志服务（CLS） 在日志主题的高级选项里面配置，详细可参考 主题分区 。

是否支持删除 CLS 的日志集吗?

支持，您需前往 日志服务（CLS）控制台 删除该日志集，删除前需先删除日志集下所有的日志主题。腾讯云 EdgeOne 侧会同步此删除状态，若您后续有需要，可于腾讯云 EdgeOne 控制台重新创建日志集和日志主题。

离线日志

最近更新时间：2022-12-20 17:28:14

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。

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。

```
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30分钟左右后可查询、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-3166-2
RequestTime	int	客户端请求时间，时区：UTC +00:00，格式标准：ISO-8601
RequestStatu	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

s		
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，若无则为 -
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）
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 向源站发起请求到收到源站返回第一个响应字节的耗时；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-3166-2 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	Int or 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 。

安全防护
DDoS 防护

最近更新时间：2022-08-12 17:13:49

本文将介绍 DDoS 防护功能的 DDoS 防护等级、IP 黑白名单、区域封禁、协议封禁等功能以及相关配置操作。

> **说明**
> DDoS 防护功能和相关配置可能根据您选购的 EdgeOne 产品套餐有所不同。

前提条件

您需要成功 购买 边缘安全加速平台（EdgeOne）产品（企业版），并完成 接入站点 或 接入四层代理 。

DDoS防护等级

针对 DDoS 攻击，EdgeOne 提供不同防护等级的相关操作及应用场景，并为您介绍如何在控制台中设置 DDoS 防护等级。

应用场景

EdgeOne 提供防护策略调整功能，针对 DDoS 攻击提供三种防护等级供您选择，各个防护等级的具体防护操作如下：

防护等级	防护操作	描述
宽松	• 过滤明确攻击特征的 SYN、ACK 数据包。 • 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 • 过滤具有明确攻击特征的 UDP 数据包。	• 清洗策略相对宽松，仅对具有明确攻击特征的攻击包进行防护。 • 建议在怀疑有误拦截时启用，遇到复杂攻击时可能会有攻击透传。
适中	• 过滤明确攻击特征的 SYN、ACK 数据包。 • 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 • 过滤具有明确攻击特征的 UDP 数据包。 • 过滤常见基于 UDP 的攻击数据包。 • 对部分访问源 IP 进行主动验证。	• 清洗策略适配绝大多数业务，可有效防护常见攻击。 • 默认为适中模式。
严格	• 过滤明确攻击特征的 SYN、ACK 数据包。 • 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 • 严格检查过滤具有明确攻击特征的 UDP 数据包和基于 UDP 的攻击数据包。 • 对部分访问源 IP 进行主动验证。 • 过滤 ICMP 攻击包。	清洗策略相对严格，建议在适中模式出现攻击透传时使用。

> **说明**
> - 如果您的业务有遭受大规模攻击的历史，或者需要使用 UDP，建议您联系 腾讯云技术支持 进行策略定制，以免严格模式影响业务流程。
> - 默认情况下，您所购买的 EdgeOne（企业版）采用适中防护等级，您可以根据实际业务情况自由调整 DDoS 防护等级。
> - 默认情况下，您所购买的EdgeOne（标准版）采用适中防护等级。

操作步骤

1. 登录 边缘安全加速平台控制台，在左侧导航中，单击**安全防护 > DDoS 防护**。
2.在 DDoS 防护页面的左侧，选中防护业务对象，如“企业版 DDoS 防护”或“企业版 DDoS 防护 – 四层代理”实例。

3.在 DDoS 防护等级卡片中，默认在开启“防护状态”的情况下，业务刚接入的 EdgeOne 站点采用适中防护等级，您可以根据实际业务防护需求自由调整 DDoS 防护等级。

IP 黑白名单

EdgeOne 支持通过配置 IP 黑名单和白名单的方式，控制对 EdgeOne 站点的访问，基于客户端源 IP 封禁或者放行访问请求。

> **说明**
>
> IP 黑白名单规则保存后，将在5–10秒内生效。
>
> - 白名单中的 IP，访问时请求将被直接放行，不再经过其他 DDoS 防护策略过滤。
> - 黑名单中的 IP，访问时请求将被直接丢弃。

1. 登录 边缘安全加速平台控制台，在左侧导航中，单击**安全防护** > **DDoS 防护**。
2.在 DDoS 防护页面的左侧，选中防护业务对象，如“企业版 DDoS 防护”或“企业版 DDoS 防护 – 四层代理”实例。

3.在 IP 黑白名单卡片中，单击**设置**，进入 IP 黑白名单页面。

4. 在 IP 黑白名单页面中，单击**新建**，创建 IP 黑白名单规则，输入需要匹配规则的 IP，并选择黑白名单类型，单击**保存**。

5. （可选）新建完成后，IP 黑白名单列表将新增一条 IP 黑白名单规则，可以在右侧操作列，单击**删除**，删除 IP 黑白名单规则。

区域封禁

EdgeOne 支持通过指定区域列表的方式，禁止源 IP 归属指定区域的客户端访问 EdgeOne 站点。支持多地区、国家进行流量封禁。

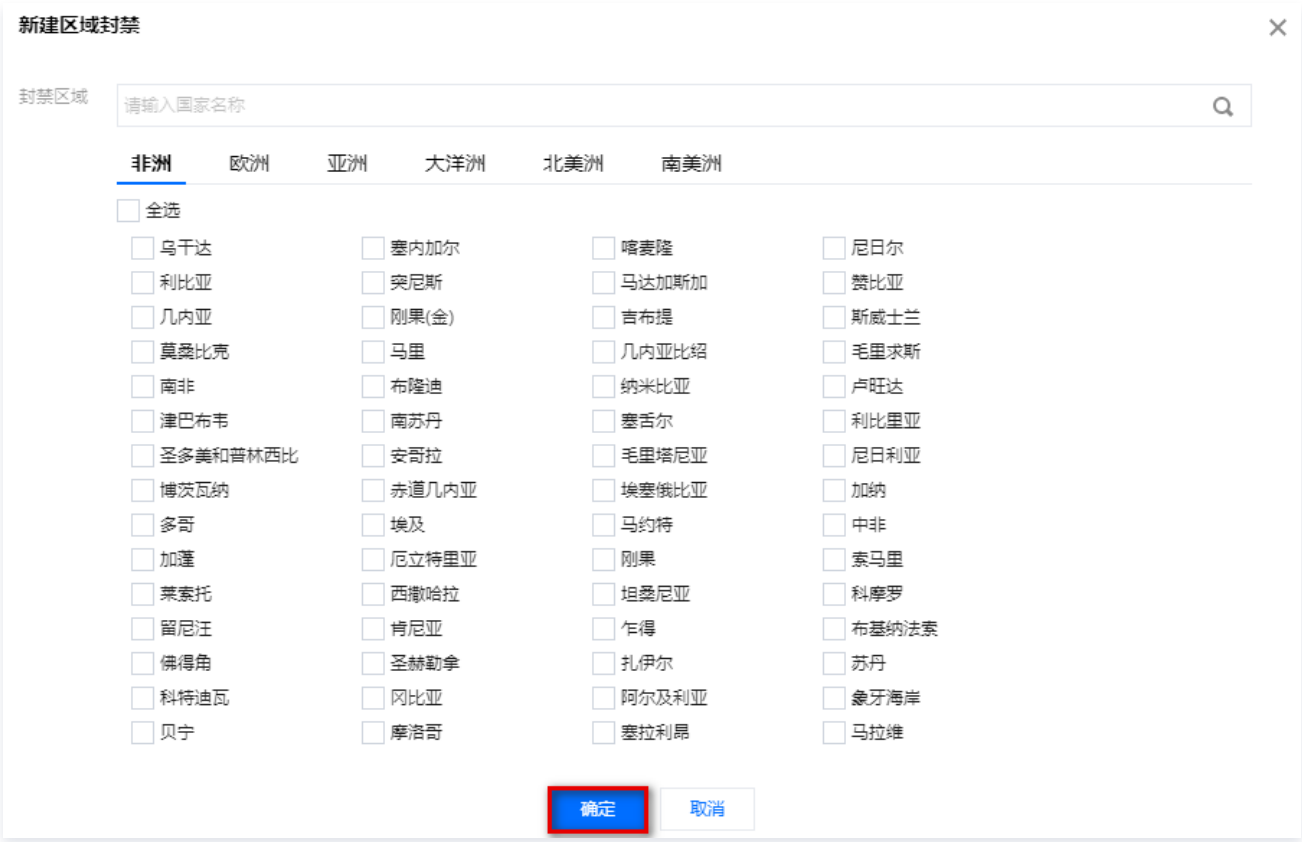
> **说明**
> 在配置了区域封禁后，该区域的攻击流量依然会被平台统计和记录，但不会流入业务源站。

1. 登录 边缘安全加速平台控制台，在左侧导航中，单击**安全防护** > **DDoS 防护**。
2. 在 DDoS 防护页面的左侧，选中防护业务对象，如“企业版 DDoS 防护”或“企业版 DDoS 防护 – 四层代理”实例。

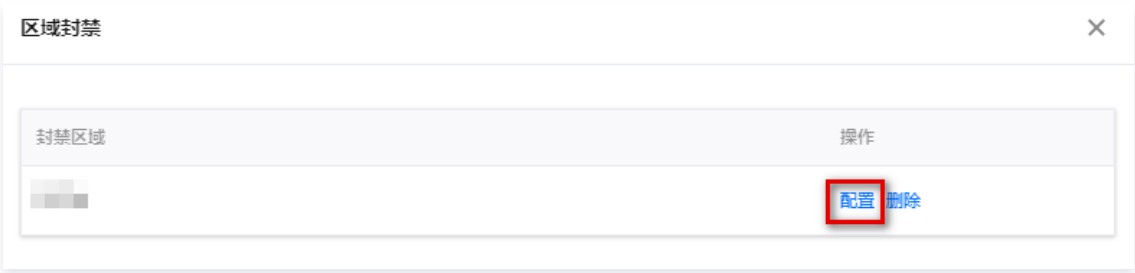
3.在区域封禁卡片中，单击**设置**，进入区域封禁页面。

4. 在区域封禁页面，单击**新建**。

5. 在新建区域封禁对话框中，选择封禁区域，单击**确定**，创建区域封禁规则。



6. （可选）新建完成后，在区域封禁列表，将新增一条区域封禁规则，可以在右侧操作列，单击**配置**，修改区域封禁规则。



端口过滤

EdgeOne 支持通过指定端口和协议的方式，管控客户端访问 EdgeOne 站点。开启端口过滤后，可以根据需求自定义协议类型、源端口范围、目的端口范围的组合，并对匹配中的规则进行设置丢弃、、继续防护的策略动作。端口过滤可以针对源端口的访问流量，进行精准制定防护策略。

1. 登录 边缘安全加速平台控制台，在左侧导航中，单击**安全防护** > **DDoS 防护**。

2.在 DDoS 防护页面的左侧，选中防护业务对象，如“企业版 DDoS 防护”或“企业版 DDoS 防护 – 四层代理”实例。

3.在端口过滤卡片中，单击**设置**，进入端口过滤页面。

4. 在端口过滤页面中，单击**新建**，创建端口过滤规则，根据需求，选择不同防护动作并填写相关字段，单击**保存**。

> **说明**
> - 支持选择多个实例资源批量创建，未绑定防护资源的实例，不允许创建规则。
> - 优先级：请填写一个介于1-1000的数字，数字越小优先级越高，该条规则排列位置越靠前，默认优先级为10。

5.（可选）新建完成后，在端口过滤列表将新增一条端口过滤规则，可以在右侧操作列，单击**配置**，可以修改特征端口规则。

特征过滤

EdgeOne 支持针对 IP、TCP 及 UDP 报文头或载荷中的特征自定义拦截策略。开启特征过滤后，您可以将源端口、目的端口、报文长度、IP 报文头或荷载的匹配条件进行组合，并对命中条件的请求设置丢弃、放行、丢弃并拉黑、继续防护等策略动作，特征过滤可以精准制定针对业务报文特征或攻击报文特征的防护策略。

1. 登录 边缘安全加速平台控制台，在左侧导航中，单击**安全防护 > DDoS 防护**。

2.在 DDoS 防护页面的左侧，选中防护业务对象，如“企业版 DDoS 防护”或“企业版 DDoS 防护 – 四层代理”实例。

3.在特征过滤卡片中，单击**设置**，进入特征过滤页面。

4. 在特征过滤页面中，单击**新建**。

5. 在新建特征过滤对话框中，创建特征过滤规则，根据需求，选择不同防护动作并填写相关字段，单击**确定**。

6.（可选）新建完成后，特征过滤列表将新增一条特征过滤规则，可以在右侧操作列，单击**配置**，可以修改特征过滤规则。

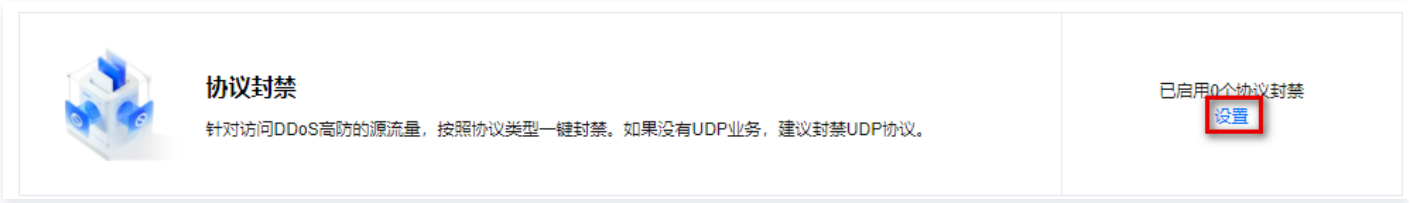
协议封禁

EdgeOne 支持对访问站点的源流量按照协议类型一键封禁。您可配置 ICMP 协议封禁、TCP 协议封禁、UDP 协议封禁和其他协议封禁，配置后相关访问请求会被直接截断。由于 UDP 协议无连接的特点（不像 TCP 具有三次握手过程）具有天然的安全性缺陷。若您没有 UDP 业务，建议封禁 UDP 协议。

1. 登录 边缘安全加速平台控制台，在左侧导航中，单击**安全防护** > **DDoS 防护**。

2.在 DDoS 防护页面的左侧，选中防护业务对象，如“企业版 DDoS 防护”或“企业版 DDoS 防护 – 四层代理”实例。

3.在协议封禁卡片中，单击**设置**，进入协议封禁页面。



4. 在协议封禁页面，单击封禁所需协议开关 。

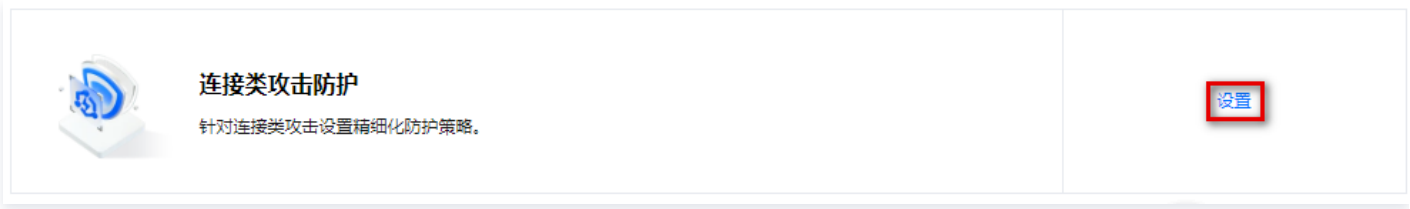
连接类攻击

EdgeOne 支持对连接型攻击进行防护，对连接行为异常的客户端自动封禁。在源 IP 最大异常连接数开启防护后，当边缘安全加速平台检测到同一个源 IP 短时间内频繁发起大量异常连接状态的报文时，会将该源 IP 纳入黑名单中进行封禁惩罚，封禁时间为15分钟，等封禁解除后可恢复访问。

1. 登录 边缘安全加速平台控制台，在左侧导航中，单击**安全防护 > DDoS 防护**。

2.在 DDoS 防护页面的左侧，选中防护业务对象，如“企业版 DDoS 防护”或“企业版 DDoS 防护 – 四层代理”实例。

3.在连接类攻击防护卡片中，单击**设置**，进入连接类攻击防护页面。



4. 在连接类攻击防护页面中，单击**配置**，配置连接类攻击防护。

5. 在配置连接类攻击防护对话框中，开启异常连接防护，单击**确定**。

6.（可选）新建完成后，连接类攻击防护列表将增加一条连接类攻击防护规则，可以在右侧操作列，单击**配置**，修改异常连接规则。

Web 防护

最近更新时间：2023-03-13 11:05:37

功能简介

概述

Web 防护功能提供对 http/https 协议的应用层防护，保护站点安全。包括内含500余条托管规则的规则库和 AI 引擎。

Web/Bot 安全执行动作说明

Web 防护与 Bot 防护具有较多复杂的安全处置方式，可以依据实际业务场景进行选择。具体执行动作介绍如下：

- 阻断：该流量被拦截，不会向后转发，返回拦截页面，同时记录攻击日志。
- 观察：该流量被放行，同时记录攻击日志。
- 放行：该流量被放行，不会记录攻击日志。

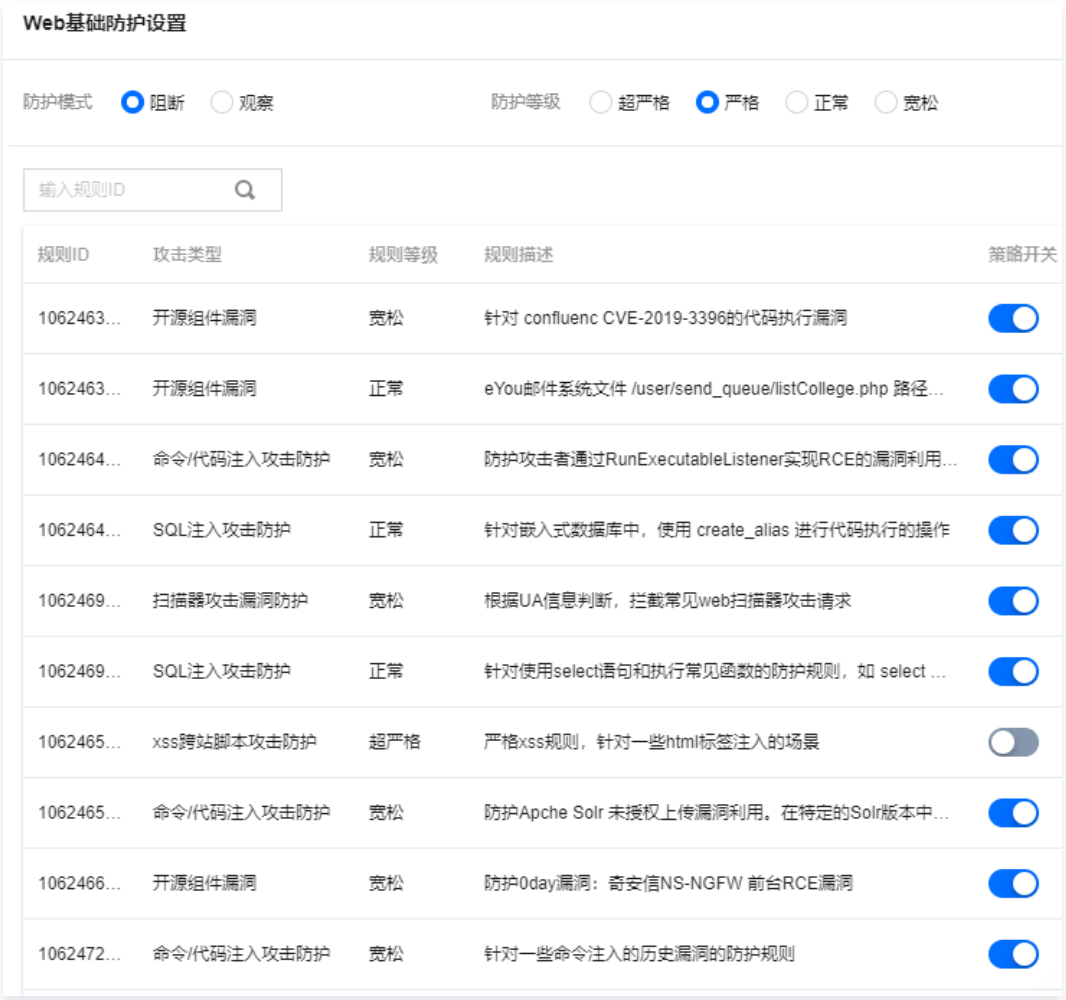
Web 基础防护设置

主要用于提供腾讯云多年积累的托管规则，具有极低的漏报、误报率，和快速的0day 响应机制。

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**安全防护** > **Web 防护**。
2. 在 Web 防护页面，选择所需站点，单击 Web 基础防护设置模块中的开关，可以快速的将本防护策略设置为“不可用”，此时该模块将不检测的放行全部流量。该开关不会删除“设置”中的配置。

3.在 Web 基础防护设置模块中，单击**设置**，可以对此防护模块进行配置和调整。

4. 在 Web 基础防护设置页面，可修改防护模式、防护等级和规则列表。



参数说明：

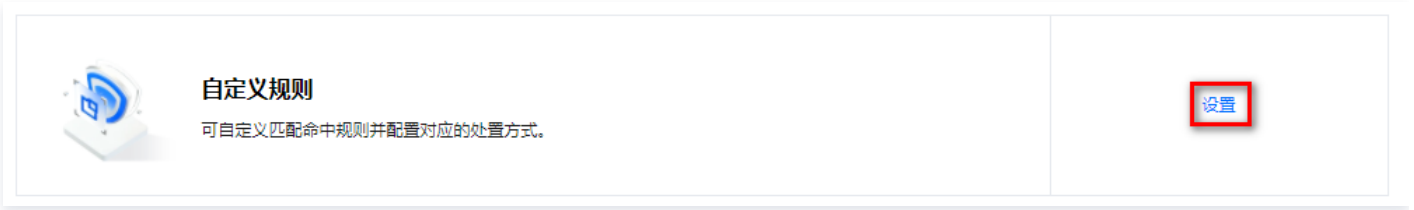
- 防护模式：可以选择“阻断”或“观察”。
  - 阻断模式下，当本模块检测到攻击流量，将会拦截该流量，并记录攻击日志。当开启 Web 基础防护配置时，默认为拦截模式。
  - 观察模式下，当本模块检测到攻击流量，仍然会放行流量，并记录攻击日志。主要用于配置策略调整时对误拦截情况的观察。该模式下不具备拦截攻击流量能力，调试完成后强烈建议变更为阻断模式。
- 防护等级：策略的严格程度调整，由“超严格、严格、正常、宽松”四种级别。越严格的模式，对疑似攻击流量的判断越多，拦截能力越强，容易造成误报。越宽松的模式，对疑似攻击流量的判断越少，只有非常明显的攻击流量会被拦截，不容易造成误报，但安全性较低。
- 规则列表包含：规则 ID、攻击类型、规则等级、规则描述、策略开关。
  - 规则 ID ：为记录对应规则的唯一 ID 号，用于追溯攻击日志进行分析。
  - 攻击类型：用于描述该攻击所属的攻击手法。
  - 规则等级：用于说明该条规则的严格程度，对应配置防护等级可以批量的开关对应等级的策略。
  - 规则描述：用于介绍防护规则包含的防护内容。
  - 策略开关：可以手动启用或禁用单条规则。

自定义规则

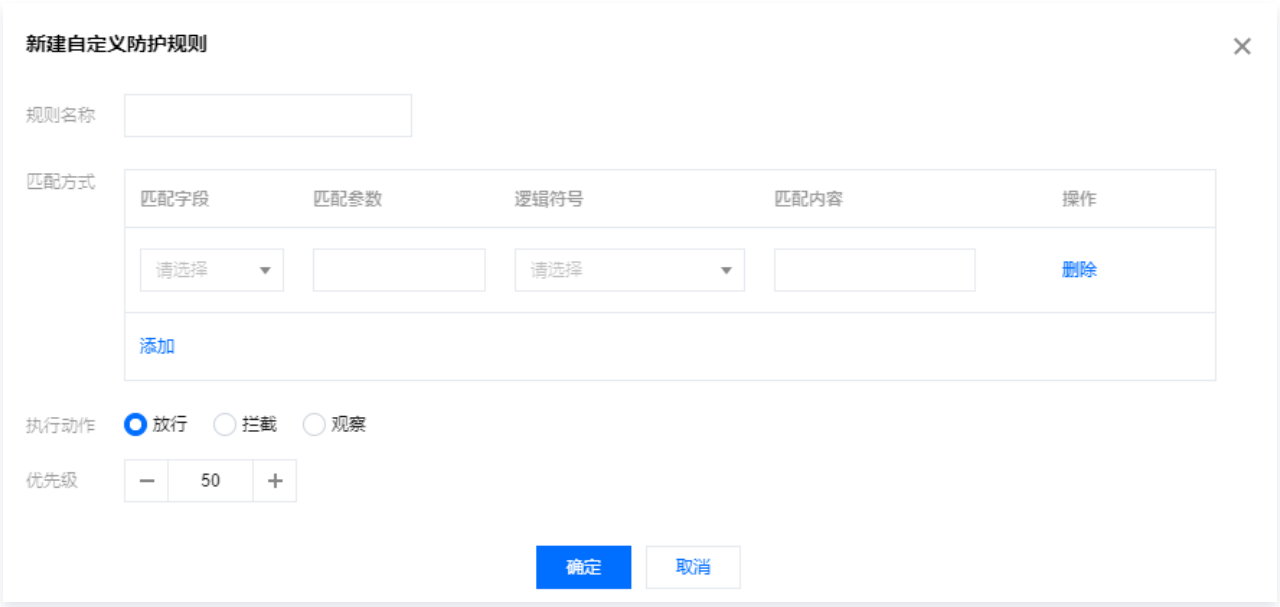
当业务与某些规则极度相似，或需要放行/阻止某些特定流量时，可使用本模块进行策略配置。

添加规则

1. 在 Web 防护页面，选择所需站点，单击自定义规则模块中的**设置**。



2. 在自定义规则页面，单击**添加规则**，输入规则名称、匹配方式、执行动作和优先级。



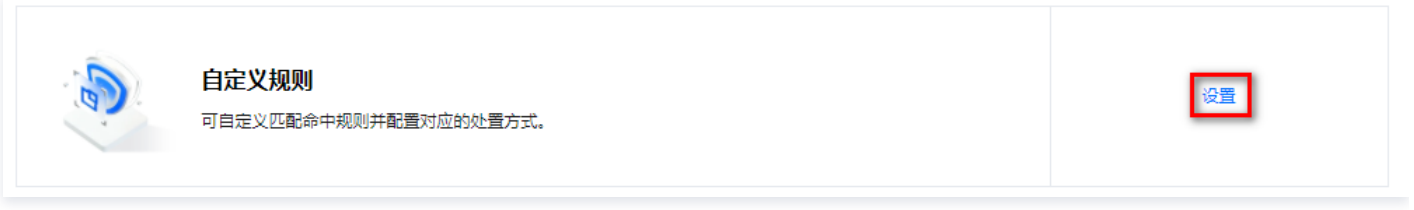
参数说明：

- 规则名称：采用字母、数字和下划线组成，不填写则会自动生成一个规则名称，规则名应当唯一。
- 匹配方式：包含若干 http/https 协议字段，可以通过包含、等于等方式进行匹配。一个防护规则的每一行匹配条件之间为“并且”关系（最多5条），相同的字段只能配置一次。
- 执行动作：放行、拦截和观察三种。
  - 放行：表示命中后会直接放行，不再执行检测。
  - 拦截：表示命中后直接阻断，记录攻击日志并返回拦截页面。
  - 观察：表示命中后会放行，但是会记录攻击日志。
- 优先级：表示该条目的执行顺序。**自定义规则将优先以配置的优先级由大到小顺序执行，当优先级相同时，以修改时间由近到远顺序执行。**

3. 单击**确定**，即可完成添加规则。

启用规则

1. 在 Web 防护页面，选择所需站点，单击自定义规则模块中的**设置**



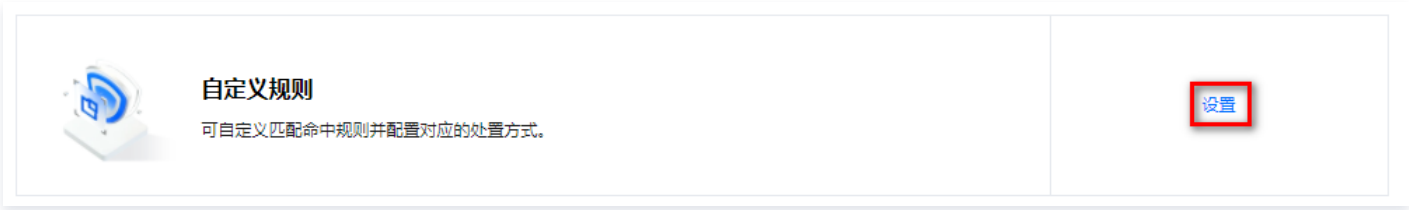
2. 在自定义规则页面，支持单个启用规则或批量启用规则。

- 单个：选择所需规则 ID，单击策略开关的  ，即可开启对应规则。

- 批量：勾选所需规则，单击**启用**，即可开启所选规则。

禁用规则

1. 在 Web 防护页面，选择所需站点，单击自定义规则模块中的**设置**。

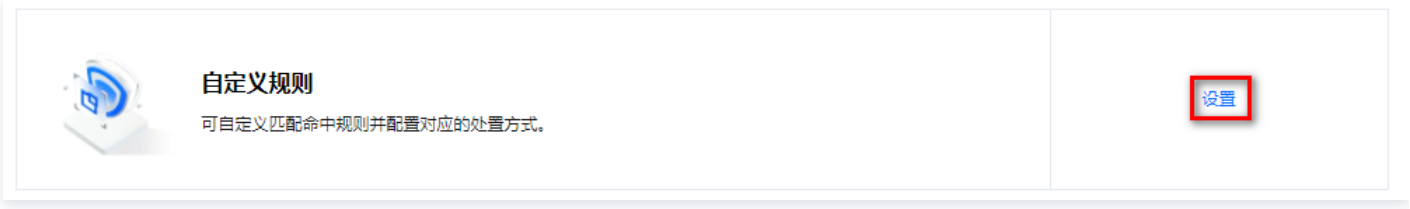


2. 在自定义规则页面，支持单个禁用规则或批量禁用规则。

- 单个：选择所需规则 ID，单击策略开关的，即可关闭对应规则。
- 批量：勾选所需规则，单击**禁用**，即可关闭所选规则。

删除规则

1. 在 Web 防护页面，选择所需站点，单击自定义规则模块中的**设置**。



2. 在自定义规则页面，选择所需规则，单击操作列的**删除**。

3. 在删除规则弹窗中，单击**删除**，即可删除对应规则。

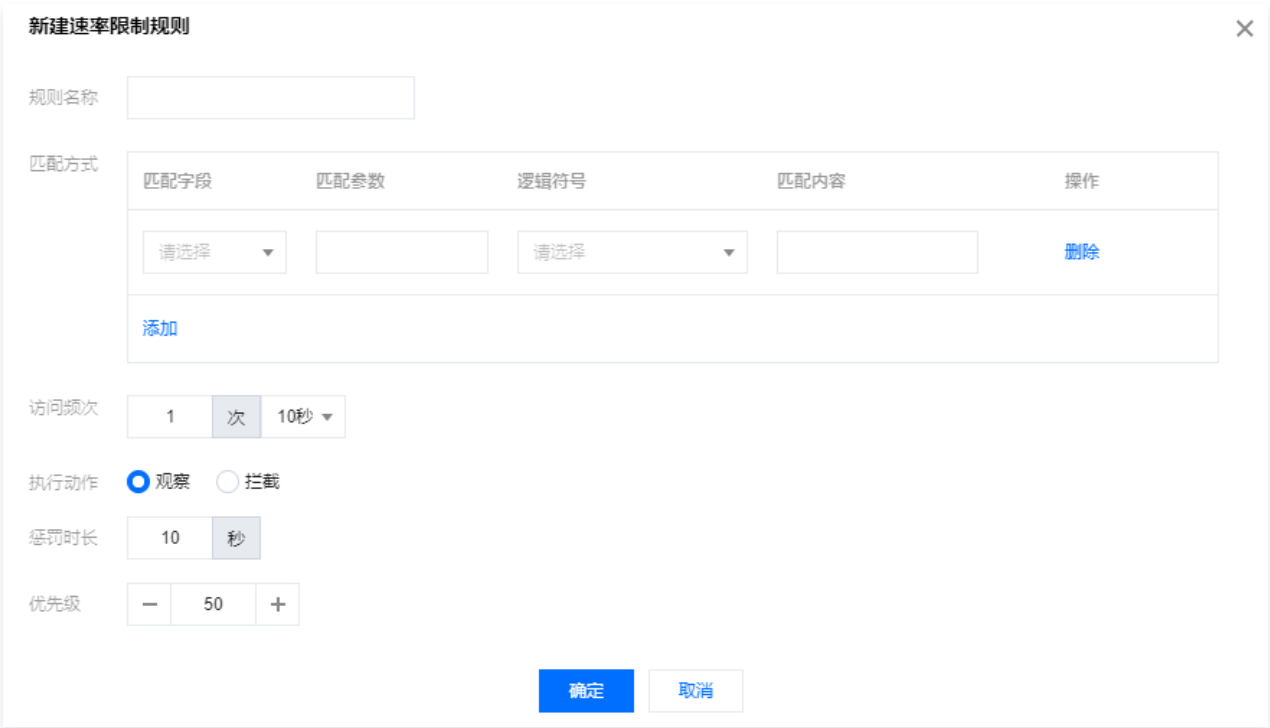
速率限制

此功能用于限制源 IP 访问对应三级域名时，命中规则后的访问频率，在一定时间内不能超过固定的访问次数，否则封禁该源 IP 一段时间。

添加规则

1. 在 Web 防护页面，选择所需站点，单击速率限制模块中的**设置**。

2. 在速率限制页面，单击**添加规则**，输入规则名称、匹配方式、访问频次、执行动作、惩罚时长和优先级。



参数说明：

- 规则名称：用于命名规则名称，采用字母、数字和下划线组成，不填写则会自动生成一个规则名称。规则名应当唯一。
- 匹配方式：包含若干 http/https 协议字段，可以通过包含、等于等方式进行匹配。一个防护规则的每一行匹配条件之间为“并且”关系（最多5条），相同的字段只能配置一次。
- 访问频次，用于描述一个源 IP 访问当前三级域名时，命中当前匹配方式频率，在XX秒内XX次，如果达到该阈值，将依据执行动作对后续该源 IP 的流量进行处置。
- 执行动作：包括观察、拦截。

- 拦截：表示命中后直接阻断，记录攻击日志并返回拦截页面。
- 观察：表示命中后会放行，但是会记录攻击日志。

- 惩罚时长：当触发执行动作后，对源 IP 的观察/拦截时间。
- 优先级表示该条目的执行顺序。**自定义规则将优先以配置的优先级由大到小顺序执行，当优先级相同时，以修改时间由近到远顺序执行。**

3. 单击**确定**，即可创建新的速率限制规则。

启用规则

1. 在 Web 防护页面，选择所需站点，单击速率限制模块中的**设置**。
2. 在速率限制页面，支持单个启用规则或批量启用规则。
   - 单个：选择所需规则 ID，单击策略开关的，即可开启对应规则。
   - 批量：勾选所需规则，单击**启用**，即可开启所选规则。

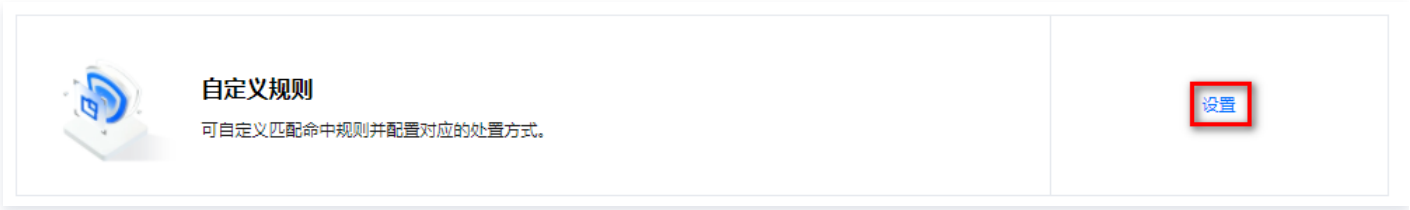
禁用规则

1. 在 Web 防护页面，选择所需站点，单击自定义规则模块中的**设置**。

2. 在速率限制页面，支持单个禁用规则或批量禁用规则。
   - 单个：选择所需规则 ID，单击策略开关的，即可关闭对应规则。
   - 批量：勾选所需规则，单击**禁用**，即可关闭所选规则

删除规则

1. 在 Web 防护页面，选择所需站点，单击自定义规则模块中的**设置**。



2.在速率限制页面，选择所需规则，单击操作列的**删除**。

3. 在删除规则弹窗中，单击**删除**，即可删除对应规则。

Bot 管理

最近更新时间：2022-08-12 17:13:38

功能简介

基于请求和会话特征、客户端画像情报和智能行为分析，识别并管控机器人客户端（包括代理、爬虫、扫描器、搜索引擎机器人、API 客户端等非浏览器客户端）访问，识别处置恶意高危请求（如恶意扫描、僵尸网络设备、ATO 攻击源、高危代理、暴力破解客户端等），同时降低对低风险爬虫、合法 API 误报和误拦截的概率。

调优 Bot 管理规则，调试优化规则配置时，建议按如下步骤部署策略：

1. 将规则或规则分类的处置方式调整为观察，此时 Bot 管理功能对匹配规则的请求将放行，但是会记录规则匹配日志。
2. 发起已知为正常（或明确需要拦截）的请求。
3. 查看 Bot 管理匹配规则日志，对于明确为正常的请求匹配的规则，配置为观察或忽略。对于明确需要拦截的请求，配置人机挑战（JavaScript 挑战或托管挑战）或者拦截。

Bot 基础防护设置

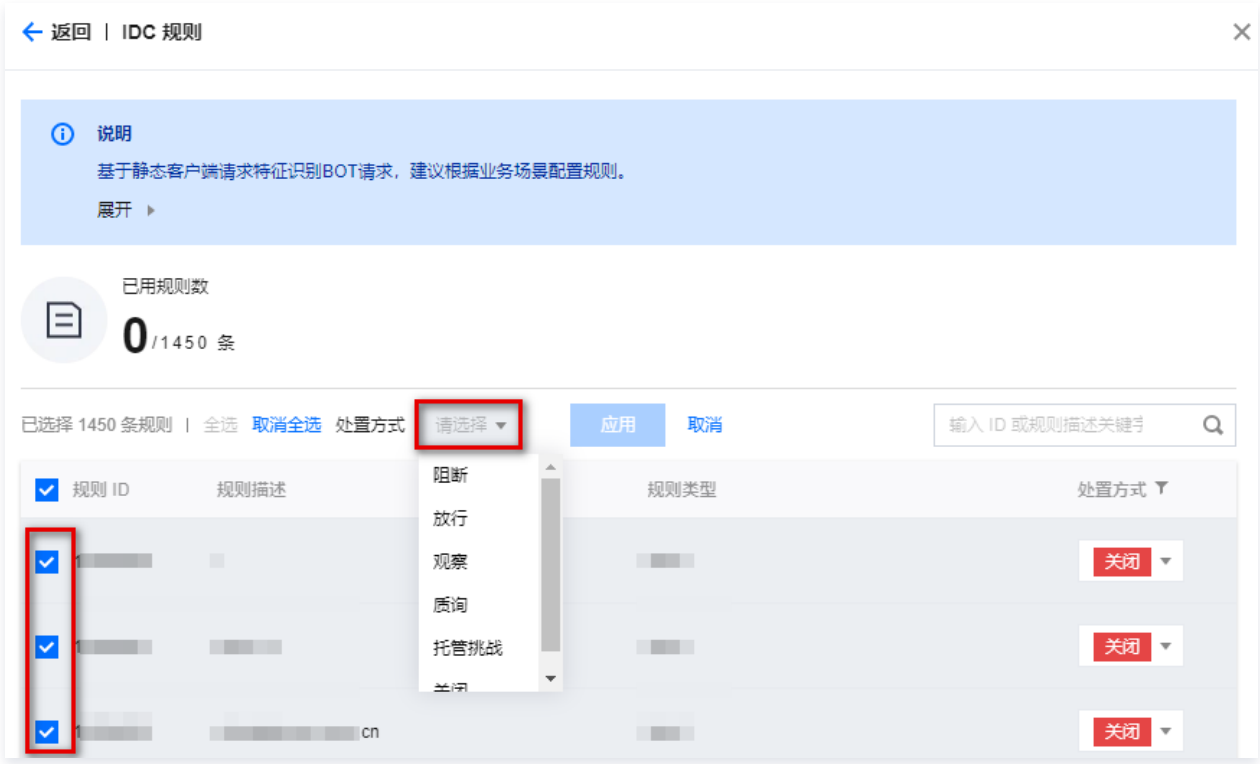
基于请求特征，如 UA、搜索引擎特征、IDC 等分类，对匹配具体特征规则或匹配特征分类的请求进行处置。

> **说明**
>
> 配置建议：该功能基于静态客户端请求特征识别 BOT 请求，建议根据业务场景配置规则。
>
> - UA 特征规则：覆盖场景较多，识别特定类型客户端，针对性强。建议业务按实际情况启用特定规则，并结合观察处置方式调试优化。
> - 搜索引擎规则：针对搜索引擎使用的 Bot 客户端识别。对于网站等搜索引擎可达的业务场景建议关闭，对于非页面类型站点（如 API 服务等）建议开启。
> - IDC 规则：针对数据中心或特定运营商客户端识别。建议结合业务需要配置指定运营商或IDC规则，并结合观察处置方式调试优化。

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**安全防护** > **Bot管理**，并选择所需站点和子域名。

2. 在 Bot 基础防护设置卡片中，单击**设置**，调整规则配置。
3. 在 Bot 基础防护设置页面上，可以单个或批量设置规则分类。
   3.1 单个设置规则分类
      3.1.1 所需要配置的规则分类上，单击**详细规则**，对该类别规则进行配置。

3.1.2 选择**规则 ID**，单击**处置方式**下拉框，选择需要配置的处置方式。



3.1.3 单击**应用**，配置生效。

3.2 批量设置规则分类

3.1.1 在 Bot 基础防护设置页面上，单击**批量设置**，选择一个或多个分类规则进行批量设置处置方式。

3.1.2 在批量设置模式下，逐个单击需要包含的分类卡片，直至所有需要配置的分类卡片都已勾选。

> **说明**
> 在批量设置模式下，可以单击**全选**快速选择全部分类卡片，或者单击**取消全选**快速取消选择全部分类卡片。

3.1.3 单击**处置方式**下拉框，选择需要配置的处置方式。

3.1.4 单击**应用**，配置生效。

4. 完成全部配置调整后，单击页面底部**确定**，配置生效。

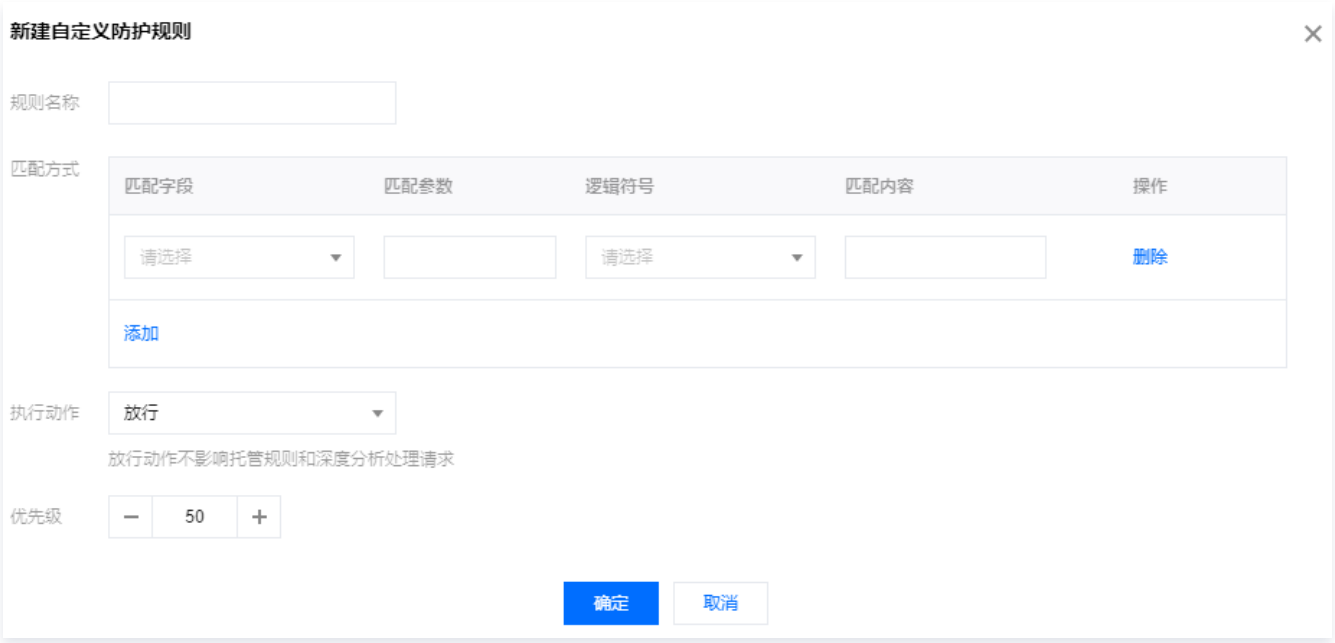
自定义规则

当业务与某些规则极度相似，或需要放行/阻止某些特定流量时，可使用本模块进行策略配置。

添加规则

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**安全防护** > **Bot管理**，并选择所需站点和子域名。

2. 在自定义规则卡片中，单击**设置**。
3. 在自定义规则页面，单击**添加规则**，输入规则名称、匹配方式、执行动作和优先级。



参数说明：

- 规则名称：由字母、数字和下划线组成，不填写则会自动生成一个规则名称，规则名应当唯一。
- 匹配方式：包含若干 http/https 协议字段，可以通过包含、等于等方式进行匹配。一个防护规则的每一行匹配条件之间为“并且”关系（最多5条），相同的字段只能配置一次。
- 执行动作：根据实际需求选择。
- 优先级：表示该条目的执行顺序。**自定义规则将优先以配置的优先级由大到小顺序执行，当优先级相同时，以修改时间由近到远顺序执行。**

4. 单击**确定**，即可完成添加规则。

启用规则

在自定义规则页面，支持单个启用规则或批量启用规则。

- 单个：选择所需规则 ID，单击策略开关，即可开启对应规则。

- 批量：勾选所需规则，单击**启用**，即可开启所选规则。

禁用规则

在自定义规则页面，支持单个禁用规则或批量禁用规则。

- 单个：选择所需规则 ID，单击策略开关的，即可关闭对应规则。
- 批量：勾选所需规则，单击**禁用**，即可关闭所选规则。

删除规则

1. 在自定义规则页面，选择所需规则，单击操作列的**删除**。

2. 在删除规则对话框中，单击**删除**，即可删除对应规则。

客户端画像

基于近期采集的大量恶意访问数据和情报数据，对客户端 IP 信誉画像分析。可根据恶意客户端置信度配置相应处置方式。

> **说明**
>
> 客户端画像置信度：对于各个类别的客户端画像规则，每个置信度对应了一个客户端地址列表，置信度反应了该列表内的客户端地址近期进行该类别恶意行为的频率和一致性。
>
> - 较高置信度：该客户端地址近期稳定、高频率进行该类别的恶意行为。来自该类地址的请求几乎确定为恶意行为，建议拦截。

- 中等置信度：该客户端地址近期有过显著频率进行该类别的恶意行为。来自该类地址的请求较大概率为恶意行为，偶尔会有误报，建议配置为 JavaScript 挑战 或 托管挑战。
- 一般置信度：该客户端地址近期有过稳定进行该类别的恶意行为记录。来自该地址的客户端相比其他地址有更大可能性发起恶意行为，但有一定误报可能，建议配置为观察，并通过调优步骤，按需要调整为 JavaScript 挑战或托管挑战。

1.登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**安全防护** > **Bot管理**，并选择所需站点和子域名。

2. 在客户端画像分析卡片中，单击右侧“开关”，可以快速开启或关闭该功能。

说明

- 关闭客户端画像分析功能后，功能内规则不生效，将默认放行请求，也不会记录相关日志。
- 首次开启客户端画像分析功能时，建议先配置详细规则，再开启规则。以避免未配置的规则影响正常业务访问。

3. 在客户端画像分析卡片中，单击**设置**，对模块内规则进行配置。
4. 在客户端画像分析配置页面，在需要调整配置的恶意行为分类框内，单击不同置信度对应的**处置方式**下拉框，选择需要配置的处置方式。

5. 完成全部配置后，单击页面底部**确定**，配置生效。

源站防护

最近更新时间：2022-10-12 16:18:11

功能简介

获取四层代理和站点加速服务最新的回源 IP 信息，更新业务源站防火墙规则，仅允许经过固定 IP(s) 的流量回源至源站，实现源站防护。

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**安全防护** > **源站防护**。
2. 在源站防护页面，单击源站防护状态的**启用**，选择站点加速/四层代理服务，单击**确认启用**为所选资源启用源站防护。

> **说明**
> 选择站点加速/四层代理服务：请绑定需要使用源站防护服务的资源。

3. 成功启用后：
   - 您可查看到这些资源目前使用的回源 IP 列表，请将其更新至您的源站防火墙规则中。
   - 后续如果回源 IP 列表有更新，我们将发出消息通知，直到您确认并反馈后，再为绑定的资源正式使用更新后的回源 IP 列表。

注意事项

为了您的业务能正常运行，当收到 IP 列表更新的消息，请您及时前往控制台确认并更新。

> **说明**
> 如未及时更新至最新的回源 IP，则可能影响正常业务，如延时不能达到最优，高并发时可能不稳定等。

热点问题

为什么有些域名无法绑定?

源站防护为安全防护功能，仅支持绑定开启了“安全加速”业务模式的域名。

如何为域名开启“安全加速”业务模式?

若站点所属套餐支持“安全加速”业务模式，请前往 安全防护 > **防护功能配置**为域名开启“高级防护”即可。

非“安全加速”的资源支持使用源站防护吗?

不支持。若站点所属套餐不支持“安全加速”业务模式，目前不支持此功能。

告警通知推送

最近更新时间：2023-01-11 10:54:54

功能简介

当检测到针对企业版 DDoS 防护（站点接入和四层代理）的 DDoS 攻击，且攻击数据速率超过配置阈值时，边缘安全加速平台将通过消息中心推送通知。您可在控制台配置推送通知的 DDoS 攻击规模范围（最小攻击速率），并在消息中心配置订阅。

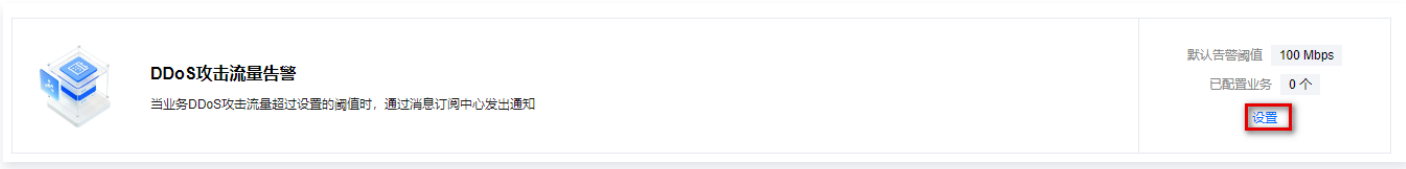
说明：

- 边缘安全加速平台持续检测外部访问流量，并识别其中的 DDoS 攻击。当检测到攻击时，无需人工介入，将自动进行流量清洗，过滤恶意攻击流量。
- 仅支持针对企业版 DDoS 防护（站点接入和四层代理）的 DDoS 攻击推送告警通知，其他业务暂不支持 DDoS 攻击流量告警功能。

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**安全防护** > **告警通知推送**，并选择所需站点。

2.在 DDoS 攻击流量告警卡片中，单击**设置**。



3. 在 DDoS 攻击流量告警页面，支持对当前站点调整全局默认 DDoS 攻击告警阈值，仅对攻击数据速率超过配置阈值的攻击事件推送消息中心通知。单击默认告警阈值的**编辑**，修改默认告警阈值，单击**保存**。

说明：

DDoS 攻击流量告警页面展示了全部支持 DDoS 攻击流量告警的业务，和对应的 DDoS 攻击告警阈值。对于未启用自定义阈值的业务，可通过调整

默认告警阈值，调整对应 DDoS 攻击告警阈值。

4. 在 DDoS 攻击流量告警页面，支持单独配置安全加速或四层代理业务项目的告警阈值。

说明：

建议根据被攻击频率和历史调整，默认100Mbps，最小可调节至10Mbps。

4.1 设置单个告警阈值

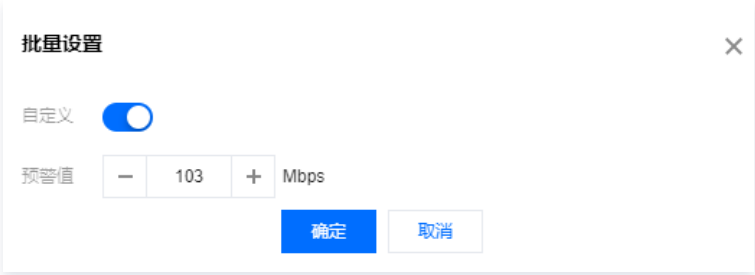
4.1.1 选择所需业务，单击对应告警阈值列的**编辑**，可调整该业务推送DDoS攻击通知的攻击规模范围（最小攻击速率）。

4.1.2 修改告警阈值，单击**保存**，自定义阈值自动开启。

4.2 批量设置告警阈值

4.2.1 选择一个或多个业务，单击**批量设置**。

4.2.2 单击开启自定义开关，调整预警值，单击**确定**。



证书管理
边缘节点证书

最近更新时间：2022-07-29 17:44:15

功能简介

EdgeOne 为站点加速提供一站式证书申请、上传、管理、部署服务，实现边缘 SSL 证书集中管理和快速部署。EdgeOne 的证书类型分为以下3种：

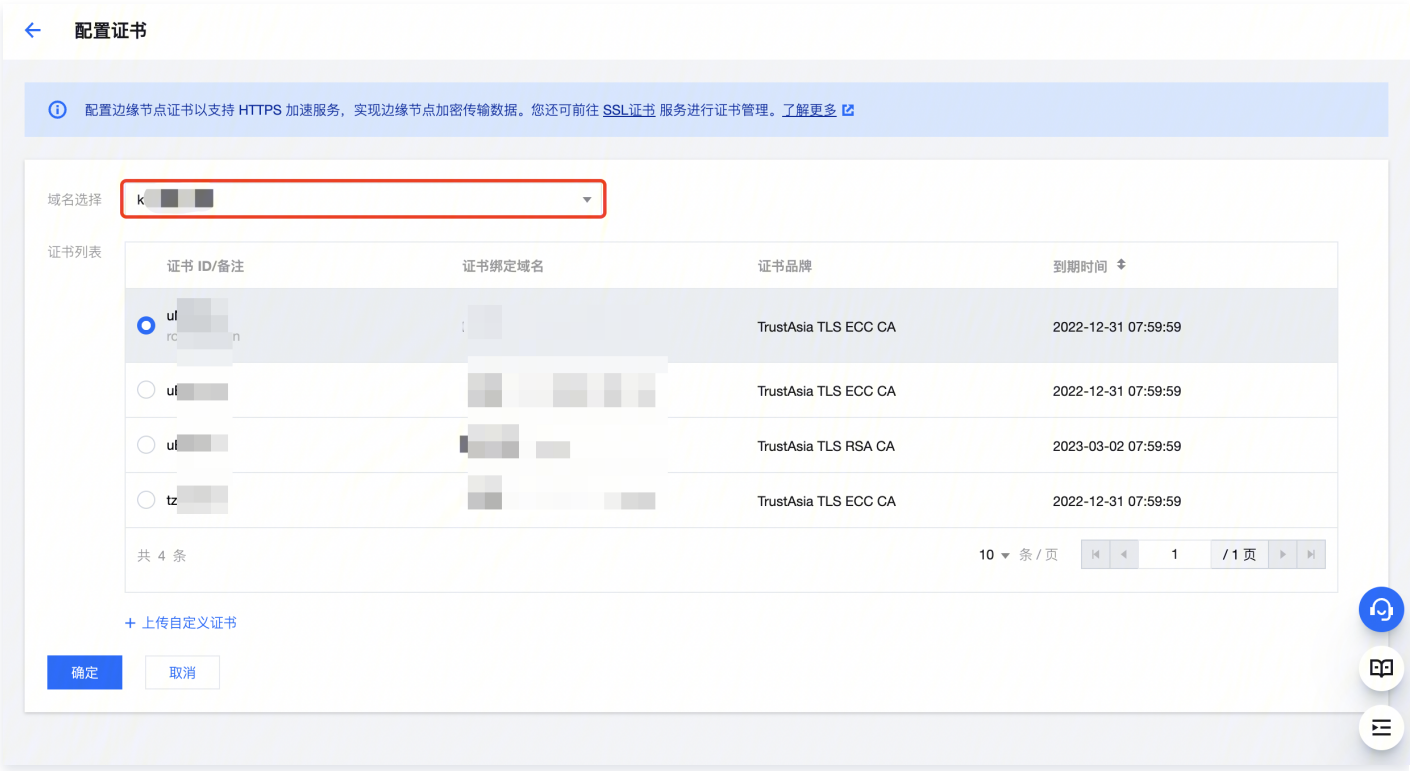
- 通用证书：NS 接入方式下，一旦站点生效，系统会为站点的根域名 (example.com) 及三级泛域名 (*.example.com) 生成一本通用证书，并自动部署、更新。
- 自定义上传证书：通过 EdgeOne 控制台 或者 SSL 证书控制台 自行上传的证书。
- 腾讯云托管证书：通过 证书中心控制台 购买或者免费申请的证书。

> **说明**
> - 通用证书为 NS 接入方式特有证书，CNAME 接入方式下系统不会提供该证书。
> - 用户从 NS 接入切换至 CNAME 接入后，通用证书会保留但不会更新，到期后会自动删除。
> - EdgeOne 上的自定义上传/腾讯云托管证书与 SSL 证书控制台 互相同步。

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**证书管理 > 边缘节点证书**。
2.在边缘节点证书页面，选择所需站点，单击**配置证书**。

3.在配置证书页面，选中需绑定证书的域名，则证书列表自动展示 SSL 证书控制台 中该域名可关联的证书。



4. 如果暂无可关联的证书，您可以单击**上传自定义证书**上传该域名的证书。

5. 选择要关联的证书，单击**确定**，证书将自动部署到 EdgeOne 加速节点。

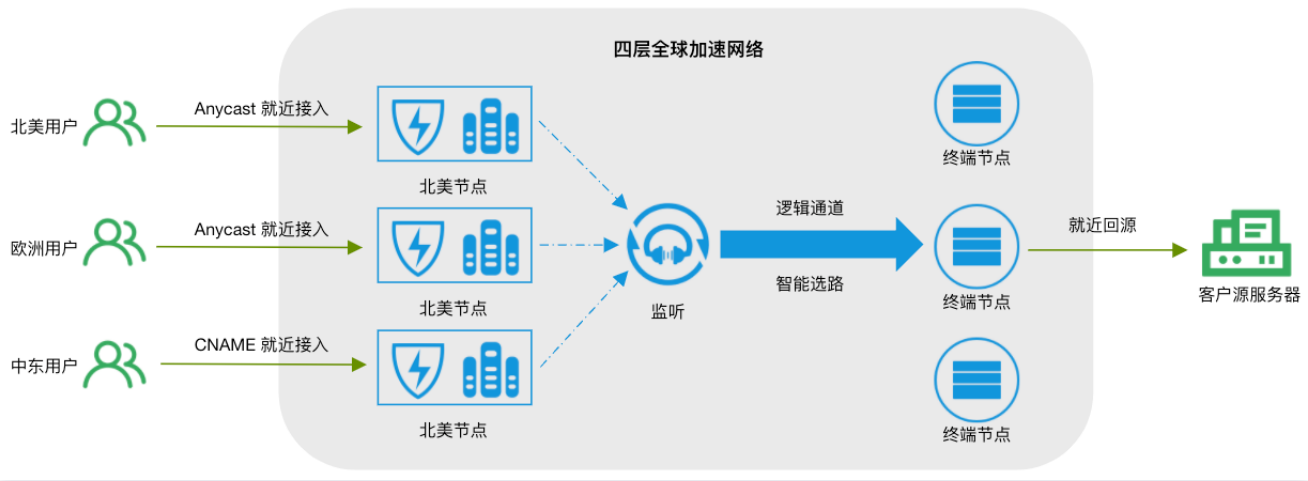
> **说明**
> 如果域名已关联过证书，重新关联将会覆盖旧的证书。

四层代理

最近更新时间：2023-03-22 14:53:06

功能简介

四层代理为 TCP/UDP 应用提供客户级 DDoS 防护和四层加速服务，依赖 EdgeOne 平台分布广泛的四层代理节点、独有的 DDoS 防护模块和智能路由技术，实现终端用户就近接入、边缘流量清洗和端口监听转发，为四层应用提供高可用低延迟的安全加速服务。



说明

- 目前每个站点底下仅允新建1个四层代理服务，如需扩容，请 联系我们 。
- 四层代理默认提供客户级别 DDoS 防护能力，不可关闭。
- 四层代理暂不支持 IPv6。

新建四层代理服务

1. 登录 边缘安全加速平台控制台 ，在左侧菜单栏中，单击**四层代理**。
2. 在四层代理页面，选择所需站点，单击**新建四层代理服务**。
3. 在新建四层代理服务页面，配置**服务配置**参数。

参数说明：

- 服务名称：四层代理服务的实例名称，可创建的实例数量取决于所属站点的套餐。
- 调度模式：选择四层代理服务的接入方式。
  - CNAME（推荐）：采用 CNAME 作为接入地址，DDoS 防护能力更强，支持就近接入加速及四层转发加速。
  - Anycast IP：采用 Anycast IP 作为接入地址，支持 DDoS 防护及四层转发加速。

> **说明**
> 如果 Host 同时开启了站点加速，调度模式只能选择 CNAME。

- 代理模式：配置四层代理模式。
  - DDoS 高防：三四层 DDoS 防护能力。默认启用，无法关闭，您可前往 DDoS防护 页面修改默认 DDoS 策略。
  - 四层加速：四层转发加速功能，降低网络传输时延。可选择开启/关闭。

4. 在新建四层代理服务页面，单击**添加规则**，配置**转发规则**参数。

> **说明**
> 每个四层代理服务可添加2000条转发规则。

参数说明：

- 转发协议：支持选择 TCP/UDP。
- 转发端口：支持端口范围1-64999（除去36000和56000），支持输入多个端口，用分号隔开，支持连字符输入端口段，一个转发规则最多可输入20个端口。

  > **说明**
  > 如果 Host 同时开启了站点加速，则转发端口不能包含 80/443。

- 源站类型/源站信息：
  - 单一源站：手动以**源站地址:端口**的格式输入源站信息，支持输入多个源站，用分号隔开。
  - 源站组：从已有的 源站组 中选择源站，只能选中带有回源端口信息的源站组，也可以在此新建源站组。
- 传递客户端 IP：选择四层代理节点回源时，真实客户端 IP 的携带方式。
  - TOA：通过 TCP Option (type 200) 传递客户端 IP。支持 TCP 协议，不支持 UDP 协议。
  - Proxy Protocol V1（推荐）：PP 协议通过 TCP Header 传递客户端 IP，V1版本采用明文传递。支持 TCP 协议，不支持 UDP 协议。
  - Proxy Protocol V2：通过 Header 传递客户端 IP，V2版本采用二进制格式，支持 TCP/UDP 协议。TCP 每个数据包都会携带 PPv2 头部，UDP 只有数据流的第一个报文会携带。
  - 不传递：配置不传递真实客户端 IP。
- 会话保持：源站 IP 不变的情况下，同一个客户端 IP 始终回到同一个源站 IP。

批量导入转发规则

新建或查看四层代理服务时，支持批量导入转发规则。

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**四层代理**。
2. 在四层代理页面，选择所需站点，单击**新建四层代理服务**。
3. 在新建四层代理服务页面的转发规则模块中，单击**批量导入**。

4. 在批量导入转发规则窗口中，输入所需规则，单击**提交**。

- 批量导入格式说明：
  - 一行对应一条转发规则，最多可输入 100 条。
  - 每行包含 4 个字段，字段之间以空格分开，不区分大小写。
  - 字段含义从左到右依次为：
  - 转发协议:端口，如 tcp:123。
  - 源站信息，单一源站输入格式为 test.origin.com:456，源站组输入格式为 og:OriginGroupName。
  - 会话保持状态，可输入 on/off。
  - 传递 IP 方式，可输入 TOA/PPv1/PPv2/off。
- 输入示例：

```
tcp:123 test.origin.com:456 on ppv1
udp:2330 og:l4testkb off ppv2
```

配置等同于下图：


转发协议
转发端口
源站类型
源站信息
传递客户端 IP
会话保持
TCP
123
单一源站
test.origin.com:456
Proxy Protocol V1
是
UDP
2330
源站组
l4testkb 源站：origin.cc
Proxy Protocol V2
否

站点加速
访问控制
Token 鉴权

最近更新时间：2022-11-29 16:20:24

功能简介

Token 鉴权为一种访问控制策略，通过配置鉴权规则进行访问校验，过滤不合法的访问请求。可有效防止站点资源被恶意盗刷，保护您的业务内容。

Token 鉴权如何做到访问控制?

客户端用户在发起请求时，其访问请求 URL 需按鉴权规则生成鉴权 URL，当且仅当鉴权 URL 中的鉴权信息（例如：时间戳）通过节点校验，即鉴权通过时，该访问请求才会被视为合法请求，节点正常响应。若校验失败，则节点拒绝该访问，直接返回403。

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**规则引擎**。
2. 在规则引擎页面，选择所需站点，可按需配置 Token 鉴权规则。如何使用规则引擎，请参见 规则引擎 。

配置项	说明
鉴权方式	目前支持4种鉴权签名计算方式，请您根据访问 URL 格式选择合适的方式。详情请参见 鉴权方式 。
密钥（主）	鉴权方式对应的主用密码，由6-40位大小写英文字母或数字组成。
密钥（备）	鉴权方式对应的备用密码，由6-40位大小写英文字母或数字组成。
鉴权参数	鉴权参数名称，节点将校验此参数名对应的值。由1 - 100位大小写字母、数字或下划线组成。
有效时长	配置的鉴权 URL 的有效时长，单位：秒（1 - 630720000），用于判断客户端访问请求是否过期： 若当前时间超过”timestamp + 有效时长“时间，则为过期请求，直接返回403。 若当前时间未超过”timestamp+ 有效时长“时间，则请求未过期，继续校验。

鉴权方式

方式 A

鉴权 URL 格式

```
http://Hostname/Filename?sign=timestamp-rand-uid-md5hash
```

鉴权字段说明

字段	说明
Hostname	站点加速域名。
Filename	资源访问路径，鉴权时 Filename 需以 `/` 开头。
sign	自定义设置的鉴权参数名称。
timestamp	时间戳参数

	格式：十进制整型正数的 Unix 时间戳，是从 UTC 时间1970年01月01日00时00分00秒到现在的总秒数，其定义与所在时区无关。
rand	0 – 100位随机字符串，由大小写字母与数字组成。
uid	用户 ID，暂未使用，默认为0。
md5hash	通过 MD5 算法计算出的固定长度为32位的字符串： • 算法：MD5（/Filename-timestamp-rand-uid-密钥）。 • 鉴权逻辑：若请求未过期，则节点比较此字符串值与请求 URL 中携带的 `md5hash` 值：两值相同，鉴权通过，响应请求；两值不同，鉴权失败，返回403。

方式 B

鉴权 URL 格式

```
http://Hostname/timestamp/md5hash/Filename
```

参数说明

字段	说明
Hostname	站点加速域名。
Filename	资源访问路径，鉴权时 Filename 需以 `/` 开头。
timestamp	时间戳参数。 格式：YYYYMMDDHHMM，UTC+8 时间，例如201807301000。
md5hash	通过 MD5 算法计算出的固定长度为32位的字符串： • 算法：MD5（密钥 + timestamp + /Filename）。 • 鉴权逻辑：若请求未过期，则节点比较此字符串值与请求 URL 中携带的 `md5hash` 值：两值相同，鉴权通过，响应请求；两值不同，鉴权失败，返回403。

方式 C

鉴权 URL 格式

```
http://Hostname/md5hash/timestamp/Filename
```

参数说明

字段	说明
Hostname	站点加速域名。
Filename	资源访问路径，鉴权时 Filename 需以 `/` 开头。
timestamp	时间戳参数。 格式：十六进制整型正数的 Unix 时间戳，是从 UTC 时间1970年01月01日00时00分00秒到现在的总秒数，其定义与所在时区无关。
md5has	通过 MD5 算法计算出的固定长度为32位的字符串：

h	• 算法：MD5（密钥+ /Filename + timestamp ）。注：计算时，十六进制的 timestamp 需过滤掉进制数标识0x。 • 鉴权逻辑：若请求未过期，则节点比较此字符串值与请求 URL 中携带的 `md5hash` 值：两值相同，鉴权通过，响应请求；两值不同，鉴权失败，返回403。

方式 D

鉴权 URL 格式

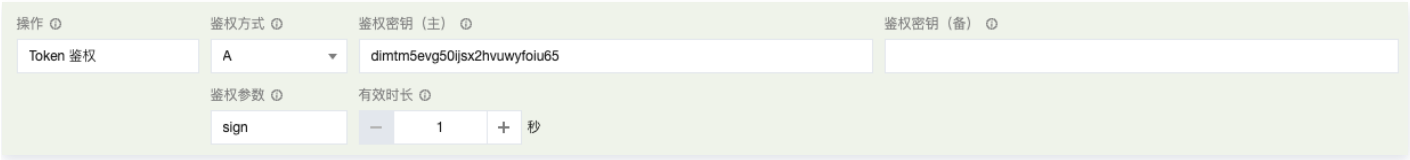
```
http://Hostname/Filename?sign=md5hash&t=timestamp
```

参数说明

字段	说明
Hostname	站点加速域名。
Filename	资源访问路径，鉴权时 Filename 需以 `/` 开头。
sign	自定义设置的鉴权参数名称。
t	自定义设置的时间戳参数名称
timestamp	时间戳参数。 格式：十进制整型正数的 Unix 时间戳，是从 UTC 时间1970年01月01日00时00分00秒到现在的总秒数，其定义与所在时区无关；或十六进制整型正数的 Unix 时间戳，是从 UTC 时间1970年01月01日00时00分00秒到现在的总秒数，其定义与所在时区无关。
md5hash	通过 MD5 算法计算出的固定长度为32位的字符串： • 算法：MD5（密钥 + /Filename + timestamp）。注：计算时，十六进制的 timestamp 需过滤掉进制数标识0x。 • 鉴权逻辑：若请求未过期，则节点比较此字符串值与请求 URL 中携带的 `md5hash` 值：两值相同，鉴权通过，响应请求；两值不同，鉴权失败，返回403。

配置示例

假设请求 `http://www.example.com/test.jpg` 符合鉴权方式 A，则可配置如下：



获取鉴权参数

- /Filename：`/foo.jpg` 。
- imestamp：服务端生成鉴权URL的时间为2022年03月15日10:30:32（UTC+8），转换为十进制的整形数值为 `1647311432` 。
- rand：生成随机数为 `J0ehJ1Gegyia2nD2HstLvw` 。
- uid：`0` 。
- 密钥：`3C9mxSGzc8ZadmGNzE` 。
- md5hash：MD5（/Filename-timestamp-rand-uid-密钥）= MD5（ `/foo.jpg` - `1647311432` - `J0ehJ1Gegyia2nD2HstLvw` - `0` - `3C9mxSGzc8ZadmGNzE` ）= ecce3150cbdaac83b116d937777ca77f。

鉴权 URL

`http://www.example.com/foo.jpg?sign=1647311432-J0ehJ1Gegyia2nD2HstLvw-0-ecce3150cbdaac83b116d937777ca77f` 。

节点鉴权

当节点服务器接受到客户端通过加密 URL 发出的请求时，解析出 URL 中的 timestamp 参数，加上配置的“有效时长 – 1秒”，与当前时间比较：

1. 若当前时间超过”timestamp + 有效时长“时间，则为过期请求，直接返回403。
2. 若当前时间未超过”timestamp + 有效时长“时间，则请求未过期，继续第3步。
3. 节点服务器通过获取的鉴权参数计算 md5hash 值，与请求 URL 中携带的 md5hash 值做比较：两值相同，鉴权通过，响应请求；两值不同，鉴权失败，返回403。

注意事项

1. 鉴权通过后，节点会自动忽略 URL 中鉴权相关的参数再将其作为缓存标识（Cache key），提高缓存命中率，减少回源。
2. 鉴权通过后，若未命中节点缓存，则会继续回源，实际回源 URL 将与 鉴权 URL 格式一致，保留鉴权参数。源站可按需忽略或二次校验，或使用 回源请求参数设置 操作配置回源是忽略相关鉴权参数。
3. URL 中不能包含中文。

视频拖拽

最近更新时间：2022-11-25 17:55:07

功能简介

开启视频拖拽功能后，可通过 start 指定视频播放的开始位置，支持 mp4、flv 与 ts 文件格式。

适用场景

在视频点播业务场景中，当用户拖拽视频播放进度时，会向服务端发起类似如下请求：

```
http://www.test.com/test.flv?start=10
```

此时会返回第10字节开始的数据，由于点播类视频文件均缓存在节点上，开启此项配置，各节点可直接响应此类请求。

注意事项

- 业务源站需同步支持 Range 请求，否则可能会导致回源失败。
- 请同步关注 “查询字符串”配置，优化节点缓存，减少回源。因为视频请求 URL(s) 中可能会携带不同的查询字符串，若未忽略查询字符串进行缓存，即使请求的是同一份资源内容，也会产生多份缓存标识（因查询字符串不同），可能导致请求多次回源，节点缓存多份相同资源。详情可查看 查询字符串 。
- 目前支持的视频文件格式为：mp4、flv 与 ts。

文件类型	meta 信息	start 参数说明	请求示例
MP4	源站视频的 meta 信息必须在文件头部，不支持 meta 信息在尾部的视频	start 参数表示的是时间，单位是秒，支持小数以表示毫秒（如 start = 1.01，表示开始时间是1.01s），节点会定位到 start 所表示时间的前一个关键帧（如果当前 start 不是关键帧）	http://www.test.com/demo.mp4?start=10 表示从第10秒开始播放
FLV	源站视频必须带有 meta 信息	start 参数表示字节，节点会自动定位到 start 参数所表示的字节的前一个关键帧（如果 start 当前不是关键帧）	http://www.test.com/demo.flv?start=10 表示从第10个字节开始播放
TS	无特殊要求	start 参数表示字节，节点会自动定位到 start 参数所表示的字节	http://www.test.com/demo.ts?start=10 表示从第10个字节开始播放

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**规则引擎**。
2. 在规则引擎页面，选择所需站点，可按需配置视频拖拽规则。如何使用规则引擎，请参见 规则引擎 。

智能加速

最近更新时间：2023-02-08 16:46:06

功能简介

智能加速，即动态智能路由加速。启用此功能后，我们将实时检测节点网络延迟，通过智能算法选择最佳传输路径，以更快、更稳定、更安全的方式处理客户端用户的请求，不论是静态资源还是动态资源请求。

通过智能动态路由，将最大限度降低网络延迟、连接错误和请求失败等问题。

什么是静态资源，什么是动态资源?

- 静态资源：用户多次访问某一资源，返回**相同**内容。例如：html、css 和 js 文件、图片、视频、软件安装包、apk 文件、压缩包文件等。
- 动态资源：用户多次访问某一资源，返回**不同**内容。例如：API 接口、.jsp、.asp、.php、.perl 和 .cgi 文件等。

使用场景

动态资源加速

适用于网络游戏、电子商务、金融支付、在线教育等对时延敏感，有高频次动态资源请求的业务。

动、静态混合资源加速

动态资源同上文中的”动态资源加速“，同时，静态资源将被缓存在靠近客户端用户的边缘节点中，以便快速响应。当静态缓存资源内容过期时，可通过智能加速快速更新。

操作步骤

站点全局配置

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点加速** > **智能加速**。
2. 在智能加速页面，选择所需站点，单击智能加速的“开关”，开启或关闭智能加速功能。

差异化配置

如需针对子域名，URL Path 或文件后缀等单独配置与站点全局配置不同的规则，请前往规则引擎配置。

1. 在左侧菜单栏中，单击**规则引擎**。
2. 创建规则的详细使用说明请参见 规则引擎 。

计费说明

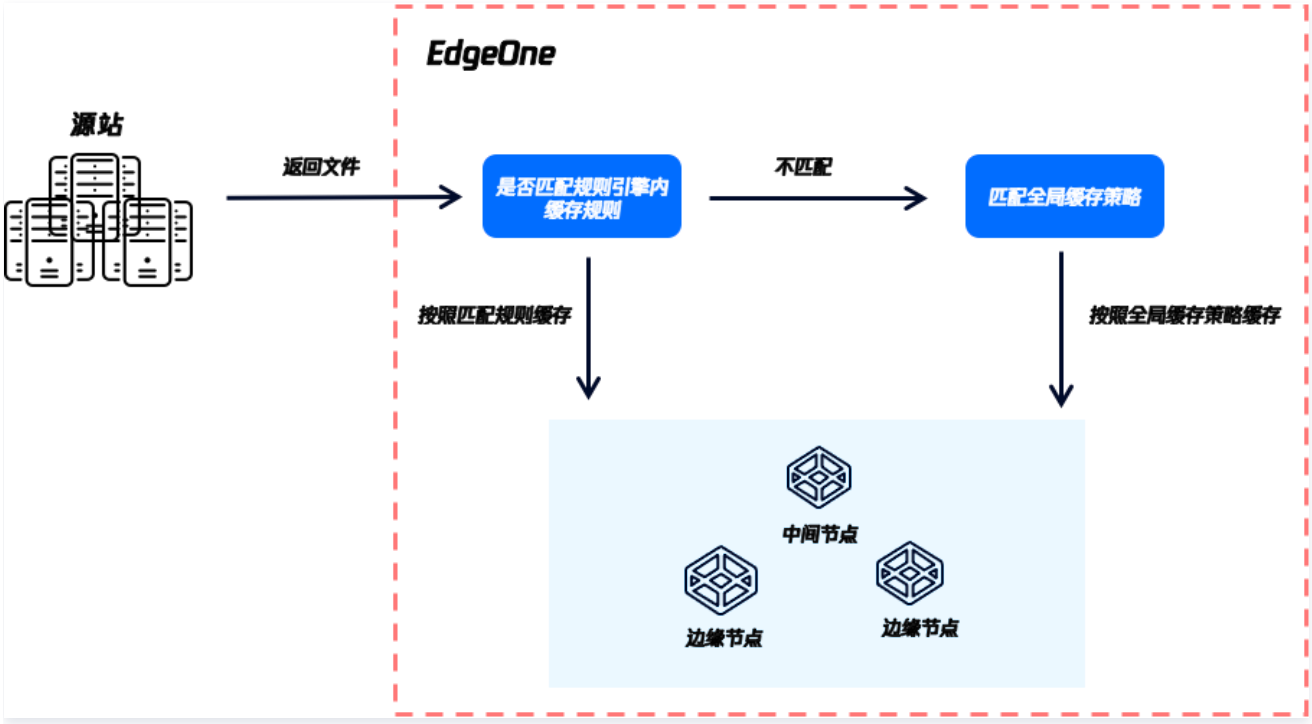
智能加速是一项增值服务，因此会产生额外的使用费用。在开启服务前，请您仔细查阅 计费概述 相关计费说明。

缓存配置
EdgeOne 内容缓存规则

最近更新时间：2023-03-02 16:06:01

概述

当客户端向 EdgeOne 边缘节点发起 HTTP 请求后，节点将判断当前文件是否命中缓存，如未命中，则回源向源站发起请求获取最新文件，在源站正确响应文件后，EdgeOne 将根据用户设置的缓存规则结合平台默认缓存策略，对文件进行缓存。您可以通过查看 如何配置缓存规则 来了解如何自定义设置您的文件缓存规则。缓存规则配置后，将按照以下顺序匹配生效：



> ⚠ **注意：**
> 缓存规则仅在源站响应状态码为200、206的情况下生效，如果源站响应为404状态码，则节点将缓存该状态码10s，其他状态码均不缓存。

1. 缓存规则将优先匹配规则引擎内缓存规则，按照从上往下的优先级顺序进行匹配，最上方规则优先级最高，如该文件在规则引擎内匹配成功，则按照该缓存规则进行缓存。
2. 规则引擎内未匹配到相应的规则时，则按照站点加速内的全局节点缓存策略进行缓存，全局缓存策略默认为 EdgeOne 的默认缓存策略，您可以根据需求自定义修改。

缓存规则

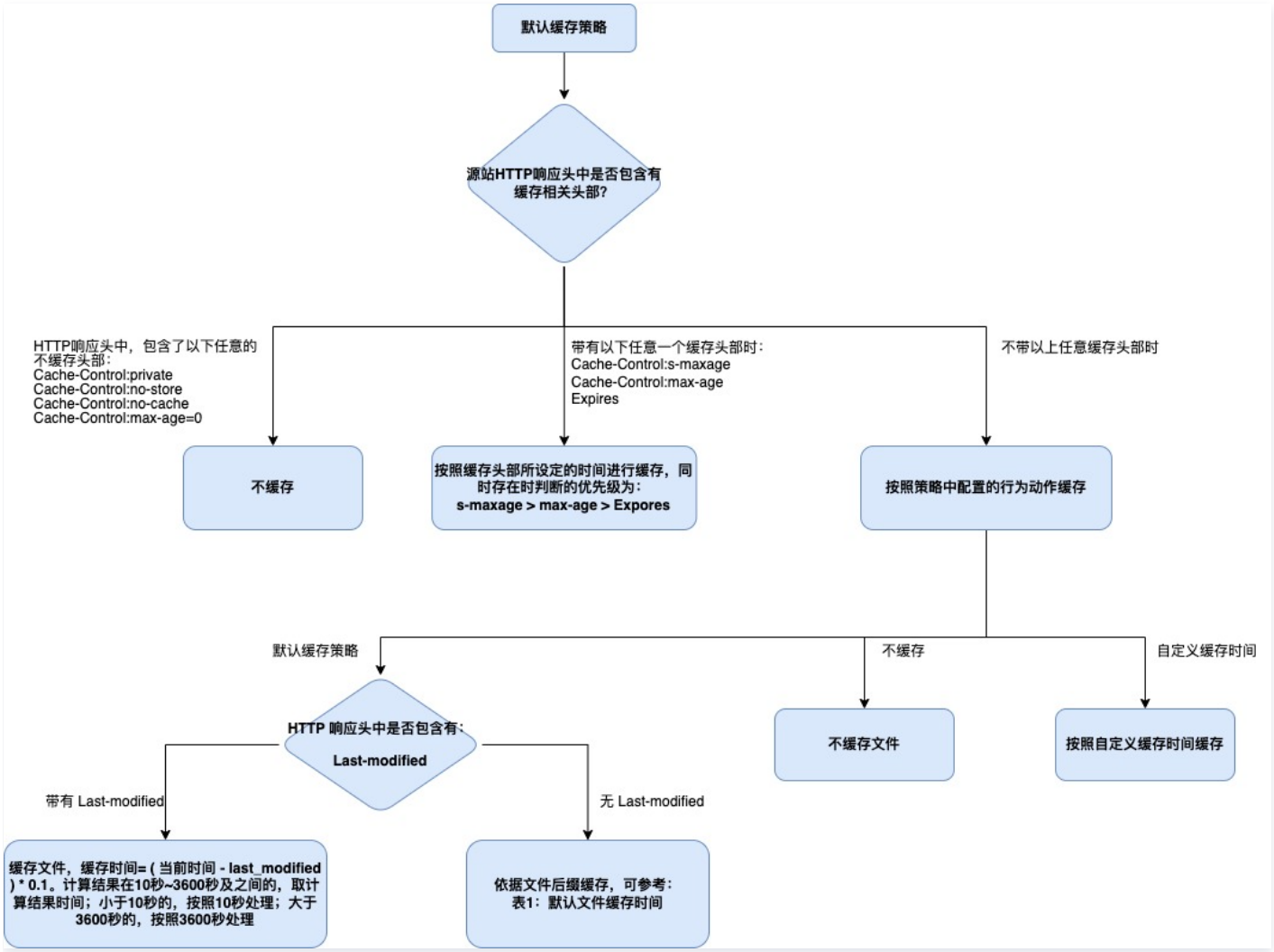
EdgeOne 支持配置三种缓存策略配置，分别为：

- **默认缓存策略：**遵循 EdgeOne 默认缓存策略，根据 HTTP 响应头内的 `Cache-Control` 及其他缓存头部来决定文件在节点内的缓存时间。
- **不缓存：**通过规则引擎内指定文件不缓存，或全局文件不缓存，适用于动态文件或更新频繁的文件内容。
- **自定义缓存时间：**按照自定义缓存时间缓存文件。

> ⚠ **注意：**
> 文件缓存在 EdgeOne 节点后，平台具有文件冷热淘汰机制，如果当前缓存文件长时间未有请求，则可能在未达到最大缓存时间时提前从节点缓存中删除。

默认缓存策略

EdgeOne 的默认缓存策略如下：



在默认缓存策略下，节点将根据源站是否携带缓存头部来控制该文件在节点的缓存动作及缓存时间，缓存规则如下：

1. 当 HTTP 响应头中，包含了以下任意的不缓存头部时，文件不缓存：
   - Cache-Control:private
   - Cache-Control:no-store
   - Cache-Control:no-cache
   - Cache-Control:max-age=0
2. 当 HTTP 响应头中，包含以下任意一个缓存头部时，文件将按照缓存头部中设定的缓存时间进行缓存：
   - Cache-Control:s-maxage
   - Cache-Control:max-age
   - Expires

   如果同时存在以上多个响应头，则缓存时间按照 s-maxage > max-age > Expires 的优先级顺序判断，按照优先级高的头部所设定时间缓存。
3. 当 HTTP 响应头不包含以上任意的缓存头部时，则会根据在规则中所配置的缓存行为执行：

- 默认缓存策略：
  - 如果 HTTP 响应头内带有 Last-Modified ，则缓存时间 =（当前时间 − Last-Modified ）* 0.1，计算结果在10秒 ~ 3600秒及之间的，取计算结果时间；小于10秒的，按照10秒处理；大于3600秒的，按照3600秒处理。
  - 如果 HTTP 响应头内无 Last-Modified ，则依据文件后缀，按照平台默认缓存规则进行缓存，不同文件后缀的缓存时间如下：

表1：默认文件缓存时间

文件类型	后缀	缓存时间
动态文件	php、aspx、asp、jsp、do、dwr、cgi、fcgi、action、ashx、axd、json	不缓存

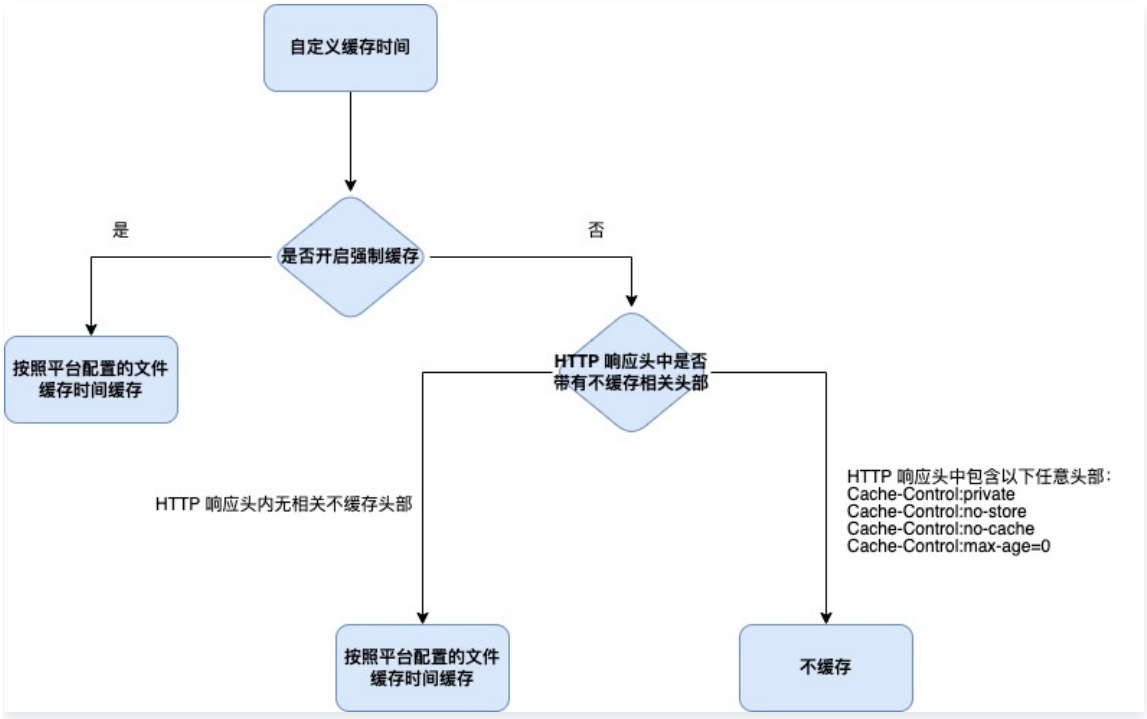
静态文件	图片	jpg、png、jpeg、webp、gif、heif、heic、kpg、ico	缓存2小时
	音视频	mp4、mp3、m3u8、ts、m4a、avi、m4s、ogg	
	网页	html、js、css	
	压缩包	zip、7z、tar、br、gz、rar、bz2	
	文档	doc、docx、xls、xlsx、pdf、ppt、pptx	
	应用程序	apk、exe、bin	
	其它	vsv、iso、jar、swf、chunk、atlas	
其他文件		N/A	不缓存

- 不缓存：HTTP 响应头中不包含以上任意缓存头部的情况下，不缓存
- 自定义时间：如果 HTTP 响应头中不包含以上任意缓存头部，则按照平台自定义配置的缓存时间缓存。

不缓存策略

如果在 EdgeOne 规则引擎或全局站点设置内，配置缓存规则为不缓存，则该文件无论源站是否带有 `Cache-Control` 及其他缓存头部，均不缓存文件。

自定义缓存时间



自定义缓存时间可以帮助您按照自定义配置的时间来缓存文件，支持开启/关闭强制缓存：

- 开启强制缓存：默认开启，无论源站是否携带有 `Cache-Control` 及其他缓存头部，均无视对应头部配置，按照 EdgeOne 平台内配置的自定义缓存时间缓存该文件。
- 关闭强制缓存：关闭强制缓存后，如果源站的 HTTP 响应头中携带有以下任意的不缓存响应头时，文件将不会缓存：
  - `Cache-Control:private`
  - `Cache-Control:no-store`
  - `Cache-Control:no-cache`
  - `Cache-Control:max-age=0`

如果不包含以上的任意 HTTP 响应头，则文件将按照 EdgeOne 平台内配置的自定义缓存时间缓存该文件。

了解更多

- 如何配置节点缓存规则
- 如何清除节点内缓存文件
- 如何提前将热点文件缓存至节点中

查询字符串

最近更新时间：2023-02-08 16:46:06

功能简介

通过调整资源 URL 中的查询字符串，优化节点缓存，提升请求资源的加载速度。

查询字符串如何影响节点缓存?

查询字符串是请求 URL 中 `?` 之后的字符串（包含一个或多个参数，用 `&` 分隔），例如 `https://www.example.com/images/example.jpg?color=blue&size=large` 中的 `color=blue&size=large` 。

节点响应请求资源时，默认按照完整的请求 URL 作为缓存标识去匹配缓存资源，例如：请求 `https://www.example.com/images/example.jpg?time=1` 和 `https://www.example.com/images/example.jpg?time=2` ，即使两个请求 URL 的路径相同，但因为后面携带的查询字符串不同，导致节点会缓存两次 `example.jpg` 图片，请求分别匹配两份节点缓存，如果资源不在节点上，会回源请求，增加回源量。

如果 `example.jpg` 不会因为查询字符串参数而异，即 `time` 参数不同时 `example.jpg` 都是同一张图片，则可忽略请求 URL 中的全部查询字符串来匹配节点缓存，将两个请求收敛和统一，匹配一份节点缓存即可：请求 `https://www.example.com/images/example.jpg?time=1` 和 `https://www.example.com/images/example.jpg?time=2` 均匹配 `https://www.example.com/images/example.jpg` 这份缓存资源。

请您确认业务资源 URL 中的查询字符串对资源的影响，并通过**查询字符串**功能优化缓存。

操作步骤

站点全局配置

1. 登录 边缘安全加速平台控制台 ，在左侧菜单栏中，单击**站点加速 > 缓存配置**。
2. 在缓存配置页面，选择所需站点，单击查询字符串模块的**设置**，选择保留/忽略参数的模式。

模式说明：

- 全部保留（默认配置）：保留完整的查询字符串，查询字符串一旦有变化，则为不同请求 URL。

  > **说明**
  >
  > 什么情况下会被识别为不同查询字符串?
  > - 任一参数内容不同，例如： ?sign=x;time=y 和 ?sign=z;time=y。
  > - 参数内容均相同，但相对顺序不同，例如：?sign=x;time=y 和 ?time=y;sign=x。
  > - 参数内容均相同，但大小写不同，例如：?sign=A 和 ?sign=a。若希望此场景下被视为是同样的查询字符串，请启用 忽略大小写 配置功能。

- 全部忽略：忽略整个查询字符串。
- 保留指定参数：仅保留查询字符串中指定的参数。
  - 仅可指定参数名，不同参数名之间用“;”隔开，例如：sign;time。
  - 至多可输入10个参数。
- 忽略指定参数：仅忽略查询字符串中指定的参数。
  - 仅可指定参数名，不同参数名之间用“;”隔开，例如：sign;time。
  - 至多可输入10个参数。

差异化配置

如需针对子域名，URL Path 或文件后缀等单独配置与站点全局配置不同的规则，请前往规则引擎配置。

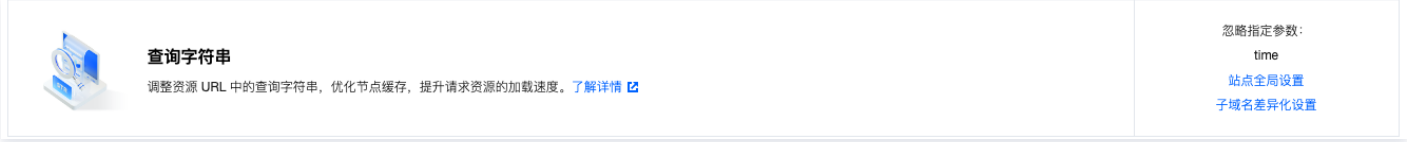
1. 在左侧菜单栏中，单击**规则引擎**。
2. 创建规则的详细使用说明请参见 规则引擎 。

注意事项

1. 此功能不会影响回源请求 URL，仅会变更请求在节点中的缓存标识，回源请求 URL 和客户端发起的原始请求 URL 保持一致。
2. 如果请求 URL 的查询字符串中不同参数之间用的是非 `&` 字符分隔的，则无法被正常识别。

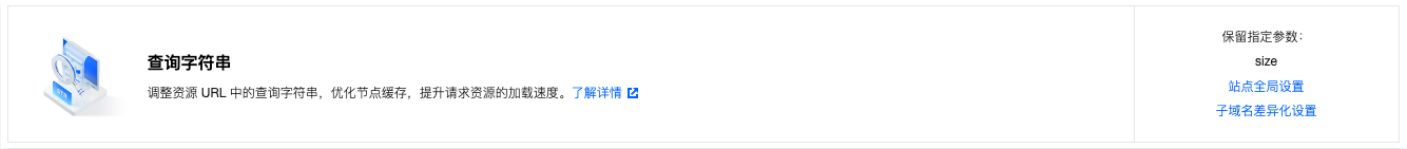
配置示例

1. 站点 example.com 请求资源不会根据查询字符串 `time` 参数而异，则需要忽略 `time` 参数，配置如下：



则请求：`https://www.example.com/images/example.jpg?time=1` 与 `https://www.example.com/images/example.jpg?time=1` 匹配缓存时会忽略 `time` 参数，均匹配 `https://www.example.com/images/example.jpg` 这份缓存资源。

2. 站点 example.com 请求资源会根据查询字符串 `size` 参数而异，即不同 `size` 参数值资源内容不同，其他参数则不影响资源，则需要仅保留 `size` 参数，配置如下：



则请求：`https://www.example.com/images/example.jpg?size=small&color=blue` 与 `https://www.example.com/images/example.jpg?size=1arge&color=blue` 匹配缓存时会仅保留 `size` 参数，则两个请求分别匹配 `https://www.example.com/images/example.jpg?size=small` 和 `https://www.example.com/images/example.jpg?size=large` 两份缓存资源。

忽略大小写

最近更新时间：2023-02-08 16:46:07

功能简介

通过忽略或不忽略客户端请求 URL 中英文字母的大小写，优化节点缓存，提升请求资源的加载速度。

大小写如何影响节点缓存?

节点响应请求资源时，默认按照完整的请求 URL 作为缓存标识去匹配缓存资源，遵循原请求 URL 中英文字母的大小写，即使 URL 内容一样，大小写不同，则会被分别匹配不同的节点缓存，例如：请求 URL 中英文字母的大小写例如：
`https://www.example.com/images/demo.JPG`与`https://www.example.com/images/demo.jpg` 会被识别为不同的资源请求，如果资源不在节点上，会回源请求，增加回源量。

如果 `demo.jpg` 不会因为大小写而异，即大小写不同时 `demo.jpg` 都是同一张图片，则可忽略大小写，将两个请求收敛和统一，匹配一份节点缓存即可。例如：请求 `https://www.example.com/images/demo.jpg` 和 `https://www.example.com/images/demo.JPG` 均匹配 `https://www.example.com/images/demo.jpg` 这份缓存资源。

请您确认业务资源 URL 中的大小写对资源的影响，并通过**忽略大小写**功能优化缓存。

操作步骤

站点全局配置

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点加速 > 缓存配置**。
2. 在缓存配置页面，选择所需站点，单击忽略大小写模块的“开关”，开启或关闭忽略大小写功能。

参数说明：

- 关闭状态（默认配置）：遵循请求 URL 中英文字母的大小写，即使 URL 内容一致，但大小写不同，则是不同的资源。
- 开启状态：忽略请求 URL 中英文字母的大小写，当 URL 内容一致，即使大小写不同，也认为是相同的资源。

差异化配置

如需针对子域名，URL Path 或文件后缀等单独配置与站点全局配置不同的规则，请前往规则引擎配置。

1. 在左侧菜单栏中，单击**规则引擎**。
2. 创建规则的详细使用说明请参见 规则引擎 。

注意事项

此功能不会影响回源请求 URL，仅会变更请求在节点中的缓存标识，回源请求 URL 和客户端发起的原始请求 URL 保持一致。

自定义 Cache Key

最近更新时间：2022-11-25 17:48:05

功能简介

支持通过调整资源 URL 中的查询字符串和配置忽略大小写，拼接 HTTP 标头等，自定义调整资源 Cache Key，优化节点缓存，根据不同场景响应对应的资源，提升请求资源的加载速度。

什么是 Cache Key?

Cache Key 是节点缓存资源的唯一标识。节点响应请求资源时，默认按照完整的请求 URL 作为 Cache Key（缓存标识）去匹配缓存资源，例如：请求 `https://www.example.com/images/example.jpg?key1=value1` 与 `https://www.example.com/images/example.jpg?key2=value2` 对应两个不同的节点 Cache Key，因为其查询字符串不同。

适用场景

客户端请求的资源与 URL 查询字符串，URL 字符大小写，HTTP 头部或请求协议有关，需要自定义配置资源在节点的缓存标识，实现客户端根据不同的请求行为适配到相应的节点缓存。

操作步骤

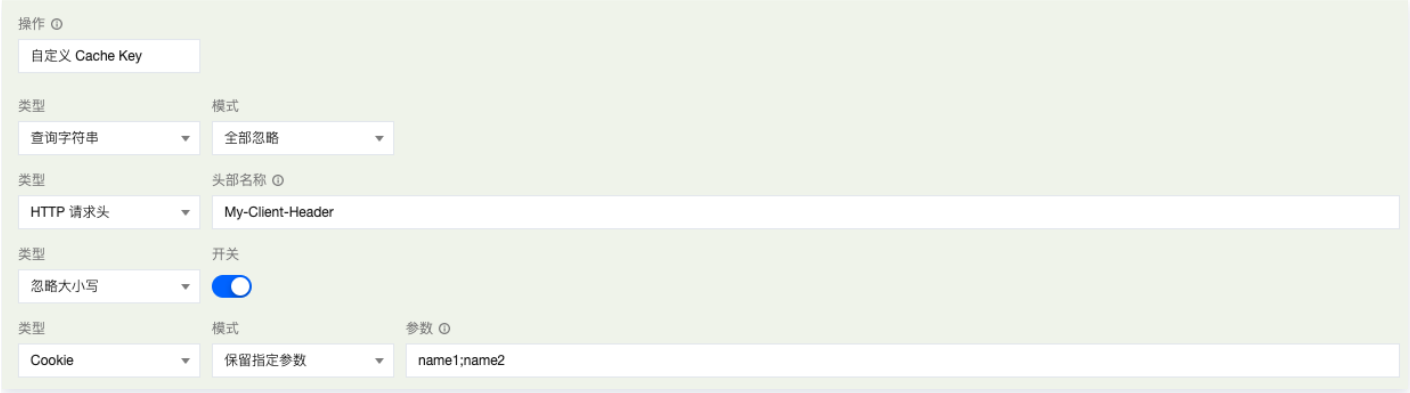
1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**规则引擎**。
2. 在规则引擎页面，选择所需站点，可按需配置自定义 Cache Key 规则。如何使用规则引擎，请参见 规则引擎 。

   配置项说明：

配置项	说明
查询字符串	调整 URL 中的查询字符串后生成 Cache Key，默认保留原请求的全部查询参数。具体说明可参见 查询字符串 。
忽略大小写	是否忽略 URL 中英文字母的大小写，即使 URL(s) 内容一致 。具体说明可参见 忽略大小写 。
HTTP 请求头	资源会根据某些客户端 HTTP 请求头而异，指定 HTTP 请求头拼接在 URL 后方生成 Cache Key 。只需输入 HTTP 请求头名称。 ○ 自定义头部：例如 `X-Client-Header`。 ○ 预设头部：支持根据客户端 `User-Agent` 和 IP 信息聚合的客户端信息头部，满足根据不同设备或浏览器类型缓存的需求。 　○ 客户端设备类型：`EO-Client-Device`。取值：`Mobile`，`Desktop`，`SmartTV`，`Tablet` 或 `Others`。 　○ 客户端操作系统：`EO-Client-OS`。取值：Android，`iOS`，`Windows`，`MacOS`，`Linux` 或 `Others`。 　○ 客户端浏览器类型：`EO-Client-Browser`。取值：`Chrome`，`Safari`，`Firefox`，`IE` 或 `Others`。 　○ 客户端 IP 所在地理位置：`EO-Client-IPCountry`。取值：两位字母国家/地区代码（ISO 3166-1 alpha-2 codes）。
Cookie	调整 Cookie 参数，将调整后的 Cookie 拼接在 URL 后方生成 Cache Key 。
请求协议	是否根据不同请求协议（HTTP/HTTPS）区分缓存，默认不区分。

配置示例

若域名 `www.example.com` 的自定义 Cache Key 配置如下：



Cache Key 由 URL+My-Client-Header+Cookie 组成：不区分请求协议（默认），忽略全部查询字符串，忽略 URL 大小写，拼接My-Client-Header和保留指定参数后的 Cookie。

则客户端请求 A

URL： `https://www.example.com/path/demo.jpg?key1=value1&key2=value2` 。

HTTP 请求头：含 `My-Client-Header:fruit` 。

Cookie：name1=yummy;name2=tasty;name3=strawberry。

与客户端请求 B

URL： `http://www.example.com/path/demo.JPG?key1=value1&key2=value2&key3=value3` 。

HTTP 请求头：含 `My-Client-Header:fruit` 。

Cookie：name1=yummy;name2=tasty;name3=blueberry。

与客户端请求 C

URL： `http://www.example.com/path/demo.JPG?key1=value1&key2=value2&key3=value3&key4=value4` 。

HTTP 请求头：含 `My-Client-Header:sea` 。

Cookie：name1=yummy;name2=tasty;name3=fish。

A 和 B 请求将会命中同一份缓存资源，C 命中另一份缓存资源。

节点缓存 TTL

最近更新时间：2022-12-23 10:59:47

功能简介

调整资源在节点中缓存的时间长短，优化节点缓存，提升请求资源的加载速度，及时淘汰旧资源。

说明

- EdgeOne 会根据节点缓存 TTL 中配置的缓存过期时间，判断节点缓存的资源是否过期。
- 若客户端访问的资源在节点的缓存未过期，节点直接将缓存返回给客户端。
- 若客户端访问的资源在节点未缓存该资源或缓存已过期，则节点会回源站获取最新资源并缓存到节点，同时返回给客户端。
- 若源站资源更新后，需要立刻更新节点的缓存，可使用 清除缓存 功能主动清除节点未过期的旧缓存，保证后续请求可以获取到源站最新的资源。

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**站点加速 > 缓存配置**。
2. 在缓存配置页面，选择所需站点，单击节点缓存 TTL 模块的**设置**。

配置项说明：

- 遵循源站 Cache-Control 头：

配置项	源站无 Cache-Control 头时	详情
遵循源站 Cache-Control 头（默认配置）	默认缓存策略（默认配置）	详情请参见 对应表格
	不缓存	-
	自定义时间	-

遵循默认缓存策略：

分类	缓存
源站含 Last-Modified 头	缓存时间=（当前时间 - last_modified）* 0.1。计算结果在10秒~3600秒及之间的，取计算结果时间；小于10秒的，按照10秒处理；大于3600秒的，按照3600秒处理
源站不含 Last-Modified 头	依据文件后缀缓存 ○ 动态文件后缀：php、aspx、asp、jsp、do、dwr、cgi、fcgi、action、ashx、axd、json，不缓存。 ○ 静态文件后缀：以下列举的文件后缀缓存2小时，未匹配以下文件后缀的则不缓存。 ○ 图片：jpg、png、jpeg、webp、gif、heif、heic、kpg、ico。 ○ 网页：mp4、mp3、m3u8、ts、m4a、avi、m4s、ogg。 ○ 网页：html、js、css。 ○ zip、7z、tar、br、gz、rar、bz2。 ○ 文档：doc、docx、xls、xlsx、pdf、ppt、pptx。 ○ 应用程序：apk、exe、bin。 ○ 其它：vsv、iso、jar、swf、chunk、atlas。

- 不缓存：不在节点缓存资源。

- 自定义时间：自定义资源缓存时长，默认开启“强制缓存”。

> **说明**
> - 开启“强制缓存”时，节点缓存 TTL 按照配置的自定义时间，即使源站的 `Cache-Control` 为 `no-cache/no-store/private` 等不缓存头
> - 关闭“强制缓存”时，当源站的 `Cache-Control` 为 `no-cache/no-store/private` 等不缓存头，即使配置了自定义时间，节点仍不缓存资源，优先遵循源站的不缓存头
> - 关闭“强制缓存”需前往 规则引擎 自定义配置节点缓存 TTL 规则。为了保证缓存效果，建议您保持开启“强制缓存”。

3. 如需针对某个子域名或请求 URL等更细请求维度设置区别于站点全局的配置，请前往 规则引擎 创建自定义规则。

附：整体节点缓存行为如下：


源站返回响应头部
默认遵循源站 Cache Control 头
源站含 Cache-Control 头
否
默认缓存策略
是
遵循源站 Cache-Control 头
调整节点缓存 TTL 配置
设置自定义时间
否
设置为"不缓存"
不缓存
是
开启"强制缓存"
否
源站 CC：private/no-store/no-cache
是
是
遵循自定义时间
不缓存
否

缓存预刷新

最近更新时间：2023-02-08 16:46:07

功能简介

在缓存资源过期之前就回源验证缓存资源是否有效，不用等到过期后再验证，提升站点加速性能，更快响应请求。

操作步骤

站点全局配置

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点加速** > **缓存配置**。
2.在缓存配置页面，选择所需站点，找到**缓存预刷新**配置卡片，默认为开启状态。

配置项	说明
配置状态	默认开启。
预刷新时间	占节点缓存 TTL 的百分比，输入1-99整数。默认90%。 假设节点缓存 TTL 已设置为10秒： 若资源有效，则将其节点缓存 TTL 重置为10秒。 若资源已失效，则从源站获取最新的有效资源至节点，并将其节点缓存 TTL 重置为10秒。

差异化配置

如需针对子域名，URL Path 或文件后缀等单独配置与站点全局配置不同的规则，请前往规则引擎配置。

1. 在左侧菜单栏中，单击**规则引擎**。
2. 创建规则的详细使用说明请参见 规则引擎 。

配置示例

希望提升 example.com 的节点响应速度，节点缓存 TTL 已设置为10秒，缓存预刷新设置为60%，配置如下：

则：不用等到10秒后缓存过期，在第6-10秒缓存未过期时就异步回源验证缓存资源是否有效。

- 若资源有效，则将其节点缓存 TTL 重置为10秒。
- 若资源已失效，则从源站获取最新的有效资源至节点，并将其节点缓存 TTL 重置为10秒。

浏览器缓存 TTL

最近更新时间：2022-07-29 17:45:35

功能简介

通过调整资源在浏览器缓存的时间长短，优化浏览器缓存，提升请求资源的加载速度。

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**站点加速 > 缓存配置**。
2. 在缓存配置页面，选择所需站点，单击浏览器缓存 TTL 模块的**设置**。

3. 在浏览器缓存 TTL 弹窗中，选择所需模式，单击**保存**。

参数说明：

- 遵循源站（默认配置）：遵循源站的 Cache-Control 头部或 Last-Modified 头部。
- 不缓存：不在浏览器缓存资源。
- 自定义时间：自定义资源缓存时长。

附：整体缓存策略内容如下：


源站返回响应头部
EdgeOne 默认“遵循源站”
源站含 Cache-Control 头部
否
浏览器是否支持启发式缓存
否
遵循浏览器的缓存策略，例如：不缓存
是
启发式缓存
含 Last-Modified: Mtime 头部
否
缓存时间：600 s
是
Mtime 是否是未来时间
否
缓存时间：（当前时间 - Mtime）* 0.1
是
缓存时间：600 s
是
遵循源站 Cache-Control 头部
调整 EdgeOne 配置
EdgeOne浏览器缓存TTL为自定义时间
否
EdgeOne 浏览器缓存 TTL 为“不缓存”
不缓存
是
遵循 EdgeOne 浏览器缓存 TTL 自定义时间

状态码缓存 TTL

最近更新时间：2022-11-25 17:52:09

功能简介

配置源站响应状态码在节点的缓存时间，由节点直接响应非2xx异常状态码，减轻源站压力。

目前支持以下状态码：

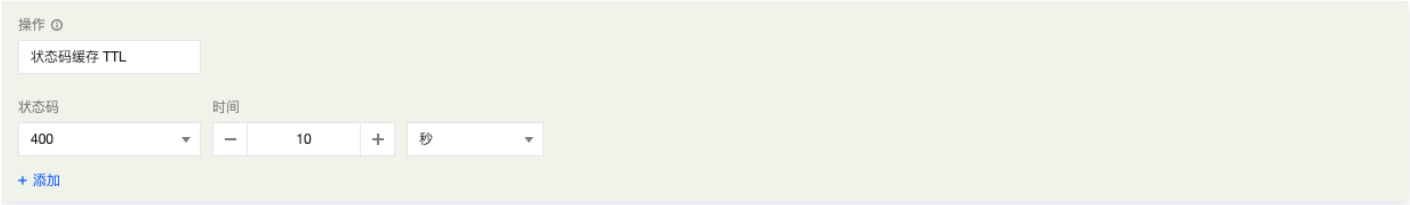
- 4xx：400、401、403、404、405、407、414。
- 5xx：500、501、502、503、504、509、514。

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**规则引擎**。
2. 在规则引擎页面，选择所需站点，可按需配置状态码缓存 TTL 规则。如何使用规则引擎，请参见 规则引擎 。

配置示例

当请求的资源获取失败，源站响应404状态码时，希望节点缓存404状态码，且后续10秒内的请求直接由节点响应，而不是全部透传回源站，以减轻源站压力，可配置：



离线缓存

最近更新时间：2023-02-08 16:46:07

功能简介

启用离线缓存后，当您的源站故障，即无法正常回源拉取资源时，可使用节点中已缓存的资源（即使资源已过期），直到源站恢复。

- 若节点有缓存，则返回缓存内容。即使命中的内容已过期，仍响应已过期的内容，直到源站恢复，可正常回源。
- 若节点无缓存，则正常返回源站故障的报错信息。

操作步骤

站点全局配置

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点加速** > **缓存配置**。
2. 在缓存配置页面，选择所需站点，单击离线缓存模块的“开关”，开启或关闭离线缓存功能。

- 开启状态（默认配置）：启用离线缓存。
- 关闭状态：停用离线缓存。

差异化配置

如需针对子域名，URL Path 或文件后缀等单独配置与站点全局配置不同的规则，请前往规则引擎配置。

1. 在左侧菜单栏中，单击**规则引擎**。
2. 创建规则的详细使用说明请参见 规则引擎 。

文件优化
智能压缩

最近更新时间：2022-12-14 09:30:34

功能简介

节点对资源进行 Gzip 或 Brotli 压缩，减小传输文件大小，提升请求资源的加载速度。

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**站点加速 > 文件优化**。
2. 在文件优化页面，选择所需站点，单击智能压缩模块的“开关”，开启或关闭智能压缩功能。

参数说明：

- 开启状态（默认）：启用智能压缩。
- 关闭状态：不支持智能压缩。

注意事项

1. 智能压缩支持的文件大小范围：256B - 30MB。
2. 智能压缩为同步压缩，在回源获取文件同时压缩文件，首次请求压缩文件时节点可直接响应压缩后的文件。
3. 智能压缩默认根据 Content-Type 压缩，支持以下类型：

```
text/html
text/xml
text/plain
text/css
text/javascript
application/json
application/javascript
application/x-javascript
application/rss+xml
application/xmltext
image/svg+xml
image/tiff
text/richtext
text/x-script
text/x-component
text/x-java-source
text/x-markdown
text/js
image/x-icon
image/vnd.microsoft.icon
application/x-perl
application/x-httpd-cgi
application/xml
application/xml+rss
application/vnd.api+json
application/x-protobuf
multipart/bag
```

```
multipart/mixed
application/xhtml+xml
font/ttf
font/otf
font/x-woff
application/vnd.ms-fontobject
application/ttf
application/x-ttf
application/otf
application/x-otf
application/truetype
application/opentype
application/x-opentype
application/font-woff
application/eot
application/font
application/font-sfnt
application/wasm
application/javascript-binast
application/manifest+json
application/ld+json
```

4. 同时开启 Gzip 压缩和 Brotli 压缩，且客户端请求头 Accept-Encoding 同时携带 br 和 gzip 时：
   - 若节点同时有 br 和 gzip 压缩的缓存内容，则优先响应 Brotli 压缩。
   - 若节点仅有 br 压缩的缓存内容，则优先响应 Brotli 压缩。
   - 若节点仅有 gzip 压缩的缓存内容，则优先响应 Gzip 压缩。
5. 仅开启 Brotli 压缩时，若请求压缩头为 gzip，则压缩不会生效，将返回原始资源；仅开启 Gzip 压缩时，若请求压缩头为 br，则压缩不会生效，将返回原始资源。
6. 若源站开启了压缩功能，且服务端携带响应头：Content-Encoding，则智能压缩功能将不再生效。

请求示例

- 未开启智能压缩
  首次请求 gzip 压缩文件，未命中节点缓存，回源获取原文件并缓存至节点，EdgeOne 响应原文件：

```
> GET / HTTP/1.1
> Host:
> User-Agent:
> Accept: */*
> Accept-Encoding:gzip
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Server: nginx/1.6.2
< Date: Thu, 08 Dec 2022 02:35:35 GMT
< Content-Type: text/html
< ETag: "6225cf25-269"
< X-Test-Header: test-tengine
< test: test
< Last-Modified: Mon, 07 Mar 2022 09:23:49 GMT
< Cache-Control: max-age=120
< Content-Length: 617
< Accept-Ranges: bytes
< Connection: keep-alive
< EO-LOG-UUID: 11326208985179133709
< EO-Cache-Status: MISS
```

- 开启智能压缩
  - 首次请求 gzip 压缩文件，未命中节点缓存，回源获取文件，节点同步压缩并缓存压缩后的文件，EdgeOne 响应压缩文件：
    智能压缩支持 chunk 流式压缩，若请求未命中节点缓存，回源获取文件后会以 chunk 的方式响应。

```
> GET / HTTP/1.1
> Host:
> User-Agent:
> Accept: */*
> Accept-Encoding:gzip
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Server: nginx/1.6.2
< Date: Thu, 08 Dec 2022 02:45:20 GMT
< Content-Type: text/html
< ETag: "6225cf25-269"
< X-Test-Header: test-tengine
< test: test
< Accept-Ranges: bytes
< Last-Modified: Mon, 07 Mar 2022 09:23:49 GMT
< Content-Encoding: gzip
< Cache-Control: max-age=120
< Transfer-Encoding: chunked
< Connection: keep-alive
< EO-LOG-UUID: 14760569083123482079
< EO-Cache-Status: MISS
```

- 再次请求，命中节点 gzip 压缩文件的缓存，节点直接响应压缩文件。

```
> GET / HTTP/1.1
> Host:
> User-Agent:
> Accept: */*
> Accept-Encoding:gzip
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Etag: "6225cf25-269"
< Server: nginx/1.6.2
< Date: Thu, 08 Dec 2022 02:45:20 GMT
< Content-Type: text/html
< X-Test-Header: test-tengine
< test: test
< Accept-Ranges: bytes
< Last-Modified: Mon, 07 Mar 2022 09:23:49 GMT
< Content-Encoding: gzip
< Cache-Control: max-age=120
< Content-Length: 384
< Connection: keep-alive
< EO-LOG-UUID: 12884259569631389017
< EO-Cache-Status: HIT
```

媒体处理
图片缩放

最近更新时间：2023-01-06 14:45:29

功能简介

支持按需调整图片大小和转换图片格式。由节点直接处理、缓存和响应缩放的图片。

使用场景

- 将同一图片缩放成不同尺寸，响应客户端请求，源站仅需存储原图，减少源站的图片管理成本。
- 在不影响肉眼感官体验的情况下动态压缩图片，提升页面加载速度，优化图片加速性能。

配置指南

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点加速 > 媒体处理**。
2. 在媒体处理页面，单击**图片缩放**的“开关”开启，即可开始使用。

3. 您需通过在客户端请求 URL 后拼接 `eo-img` 相关参数传递图片缩放需求，例如 `https://www.example.com/foo.png?eo-img.resize=w/100` 。

参数说明如下：

能力	参数名	参数值（type/pixel）	说明
重置大小	eo-img.resize	w/100	指定宽度，高度自适应
		h/100	指定高度，宽度自适应
		w/100/h/100	指定宽高
		l/100	指定长边，短边自适应
		s/100	指定短边，长边自适应
格式转换	eo-img.format	webp, heif, avif, guetzli, tpg, svg, jpg2000, jpg-xr 选其一	将原图转换为指定格式

注意事项

1. 处理的原图不可超过20MB，若超过则无法处理，维持原图。
2. 一条请求 URL 中，`eo-img.resize` 和 `eo-img.format` 参数可单独存在，也可同时存在，如 `eo-img.resize=w/100&eo-img.format=webp` ，即重置大小又转换格式。
3. 一条请求 URL 中，同一参数不可重复出现，如 `eo-img.resize=w/100&eo-img.resize=w/200` 或 `eo-img.resize=w/100&eo-img.format=webp&eo-img.resize=w/200` 是不合法传参，视为无效参数，维持原图。
4. 宽/高和长/短参数不可混用，如 `w/300/s/200` 是不合法的传参，视为无效参数，维持原图。
5. 其他错误传参，如 `eo-img.resize=w=100` 等格式不正确或拼写错误等，均视为无效参数，维持原图。
6. 若关闭了**图片缩放**功能，则 `eo-img` 相关参数被视为普通查询字符串，无图片缩放处理。

计费说明

此功能为收费功能，将根据图片缩放请求数计费，详见 计费说明 。

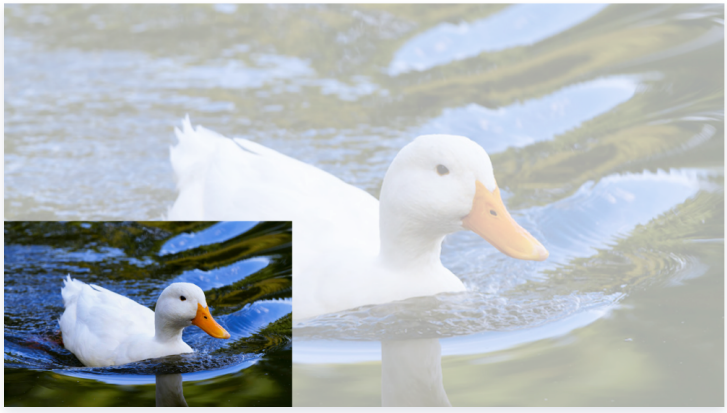
> **说明**
> 此功能正在限时免费，请关注后续计费通知。

配置示例

处理的原图为 500*280，500 KB，处理示例如下：

1. 指定宽度为200px，高度自适应。

   请求 url： http://www.example.com/foo.png?eo-img.resize=w/200 。



2. 指定高度为200px，宽度自适应。

   请求 url： http://www.example.com/foo.png?eo-img.resize=h/200 。

3. 指定宽度为300px，高度为200px。

   请求 url： http://www.example.com/foo.png?eo-img.resize=w/300/h/200 。

> **注意**
> 同时指定宽高，会按照指定的值缩放，不再保持原图长宽比。

4. 指定长边为400px，短边自适应。

请求 url： http://www.example.com/foo.png?eo-img.resize=l/400 。

5. 指定短边为200px，长边自适应。

请求 url： http://www.example.com/foo.png?eo-img.resize=l/200 。

6. 指定图片转换格式为 webp。

请求 url： http://www.example.com/foo.png?eo-img.format=webp 。

输出图片格式：webp。

7. 指定宽度为200px，高度自适应，并转换格式为 webp。

请求 url： http://www.example.com/foo.png?eo-img.resize=w/200&eo-img.format=webp 。

清除缓存

最近更新时间：2023-01-16 11:55:10

功能简介

清除缓存，即清除节点中已缓存的资源。清除后，用户访问资源时，将回源获取最新的资源进行响应。

> **注意**
> 清除缓存后，因节点上无该资源的缓存，只能回源获取，短时间内会增加回源请求量，减弱加速效果。如果清除的缓存资源较多，产生较多回源请求，源站会有一定压力。

适用场景

发布新资源

业务源站更新了资源，需清除节点上已缓存的旧资源，避免用户仍请求到旧资源。清空全网缓存后，用户可请求到最新的资源。

清理违规资源

如果业务站点上存在违规资源，需要及时整改并清理。由于节点上可能仍缓存着这些违规资源，需要清除节点上已缓存的违规资源。

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，选择所需站点，单击**站点加速 > 清除缓存**。
2. 在清除缓存页面，选择需清除的资源类型，输入对应的资源内容，单击**确定清除**。

支持类型	详情
URL	匹配 Url(s) 的节点缓存资源，例如 `https://www.example.com/path/foo.jpg` 。
前缀	匹配前缀路径的节点缓存资源，例如 `https://www.example.com/path` 。
Hostname	匹配 Hostname(s) 的节点缓存资源，例如 `www.example.com` 。 注意：不支持提交 `http://*.test.com/` 格式的 URL，即域名中不能包含*，需要写明对应的子域名。
Cache-Tag	匹配 HTTP 应答包中 `Cache-Tag` 响应头的标签值（tags）清除缓存，例如 `Cache-Tag: tag1,tag2,tag3` 。 ○ 仅适用企业版套餐。 ○ EdgeOne 支持识别源站响应头 `Cache-Tag` ，请添加 tag(s) 至此头部： 　○ 头部大小最大为 6KB。 　○ 多个 tag 用“,”分隔，单个 tag 不超过128字符，tag 个数上限为1,000。 　○ tag 忽略大小写，即 Tag1 和 tag1 会识别为相同的 tag。
全部缓存	站点在节点的全部缓存资源。 注意：若当前站点（example.com）下接入了泛域名，例如 *.foo.example.com，则该泛域名无法生效，需单独提交其各个具体子域名的清除缓存任务。

3. 切换至**历史记录** Tab 页，可查看指定时间段和清除类型的历史记录。

注意事项

内容规范

请您先关注确认提交的内容是否符合规范：

- 请避免提交已关闭/被锁定/未接入当前账号的站点内容。
- 若您选择了上传文件的提交方式，需确保文件格式为 txt，大小不超过10M。

提交限额

- 不同计费套餐有不同限额，详见 计费概述 。
- 若您选择了上传文件的提交方式，无单次限额，会直接在单日限额中扣除提交的个数。

预热缓存

最近更新时间：2023-01-16 11:55:11

功能简介

预热 URL 即将匹配 Url(s) 的资源提前从源站缓存至节点，当用户请求资源时，直接从节点响应，强加速效果，缓解源站压力。

> **注意**
> - 预热资源时会模拟请求，回源拉取对应资源，若提交的预热任务较多，则会产生较多回源请求，源站带宽增大。
> - 若预热的资源与节点缓存有冲突，即若节点已缓存同名资源，且尚未过期，则仍有效，不会被预热的资源覆盖。如同名资源有变动，您可在预热前先清除对应的节点缓存。
> - 资源默认预热至边缘节点，所产生的边缘层流量会作为正常的计费流量。

适用场景

发布安装包

正式对外发布新版本安装包或升级包前，将安装包资源预热至节点。正式发布后，用户请求下载这些安装包时，可直接从节点获取安装包资源，提升下载速度的同时降低了源站压力。

举办运营活动

正式举办运营活动前，将活动页面涉及到的静态资源（例如，网页图片）预热至节点。活动正式开始后，用户请求中的这些静态资源均由节点直接响应，加速页面访问速度，提升用户体验。

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，选择所需站点，单击**站点加速 > 预热缓存**。
2. 在预热缓存页面，输入或上传 URL，单击**确定预热**。
3. 切换至**历史记录** Tab 页，可查看指定时间段的历史记录。

注意事项

内容规范

请您先关注确认提交的内容是否符合规范：

- 请避免提交已关闭/被锁定/未接入当前账号的站点内容。
- 不支持提交 `http://*.test.com/` 格式的 URL，即域名中不能包含 `*`，需要写明对应的子域名。
- 若您选择了上传文件的提交方式，需确保文件格式为 txt，大小不超过10M。

提交限额

- 不同计费套餐有不同限额，详见 计费概述 。
- 若您选择了上传文件的提交方式，无单次限额，会直接在单日限额中扣除提交的个数。

HTTPS

最近更新时间：2023-02-24 16:20:46

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点加速** > **HTTPS**。
2. 在 HTTPS 配置页面，选择所需站点，可为站点加速提供如下一系列 HTTPS 配置选项：

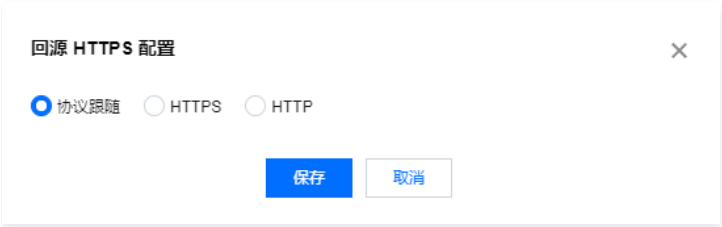
强制 HTTPS

在强制 HTTPS 模块中，单击  强制将所有边缘 HTTP 请求通过301/302重定向至 HTTPS。默认不开启。

> **说明**
> 开启后全部请求走 HTTPS，请确认提供服务的子域名的证书已部署到 EdgeOne。

回源 HTTPS

在回源 HTTPS 模块中，单击**编辑**，选择回源的加密模式，即回源采用的协议，单击**保存**。



参数说明：

- 协议跟随（默认）：跟随请求协议，请求协议用的是 HTTP，则回源也采用 HTTP。
- HTTP：回源请求一律采用 HTTP 协议。
- HTTPS：回源请求一律采用 HTTPS 协议。

HTTP Strict Transport Security (HSTS)

1. 在 HSTS 模块中，单击**启用 HSTS**，配置相关参数，单击**确定**。

参数说明：

- 配置状态：默认关闭，使用 HSTS 功能时，需要开启。
- 缓存时间： HSTS 头部的过期时间，单位为秒，可配置范围为1-31536000秒。该时间内浏览器会始终以 HTTPS 发起请求。
- 包含子域名：开启时，当前域名及其子域名均会开启 HSTS。
- 预加载：开启时，允许浏览器自动预加载 HSTS 配置，以避免首次 HTTP 请求的潜在攻击风险。域名需提前加入浏览器 HSTS Preload List 才能生效。

2. 配置 HSTS 后，EdgeOne 加速节点响应增加 `Strict-Transport-Security` 头部，强制客户端（浏览器等）使用 HTTPS 与边缘节点创建链接，全局加密网站。

- HSTS 头部格式

```
Strict-Transport-Security: max-age=expireTime [; includeSubDomains] [; preload]
```

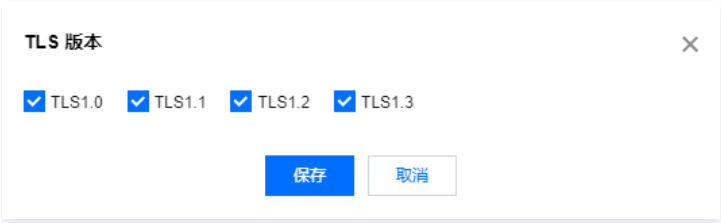
- 字段说明
  - max-age：HSTS 头部的过期时间，单位为秒。该时间内浏览器会始终以 HTTPS 发起请求。
  - includeSubDomains：可选字段，开启时，当前域名及其子域名均会开启 HSTS。
  - preload：可选字段，开启时，允许浏览器自动预加载 HSTS 配置，以避免首次 HTTP 请求的潜在攻击风险。域名需提前加入浏览器 HSTS Preload List 才能生效。

> **说明**
> - 开启 HSTS 前，请确保域名证书已部署，HTTPS 请求可正常响应。
> - 启用 HSTS 时建议您同步启用 强制 HTTPS，否则当请求为 HTTP 时，浏览器将不执行 HSTS 配置。
> - max-age 可配置范围为1-31536000秒。

TLS 版本

在 TLS 版本模块中，单击**编辑**，选择所需版本，单击**保存**。

> **说明**
> 仅允许开启的 TLS 版本的 HTTPS 链接，可选择的 TLS 版本为1.0-1.3，只可开启连续或单个版本号。



OCSP 装订

在 OCSP 装订模块中，TLS 握手时发送事先缓存的 OCSP 响应以提高握手效率。单击 开启后，加速节点会缓存 OCSP 响应以供客户端验证，客户端无需向数字证书认证机构（CA）发送查询请求，从而提高 TLS 握手效率。

网络优化
HTTP/2

最近更新时间：2023-02-08 16:46:08

功能简介

支持 HTTP/2 (HTTP 2.0) 请求，加速站点、提升 Web 性能。

什么是 HTTP/2?

HTTP/2（即 HTTP 2.0，超文本传输协议第2版），是 HTTP 协议的第二个主要版本，能有效减少网络延迟，提高站点页面加载速度。

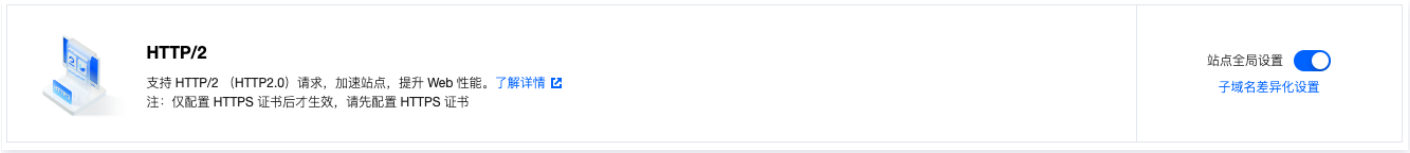
前提条件

仅配置 HTTPS 证书后才生效，请先配置 HTTPS 证书。

操作步骤

站点全局配置

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点加速** > **网络优化**。
2. 在网络优化页面，选择所需站点，单击 HTTP/2 模块的“开关”，开启或关闭 HTTP/2 功能。



- 开启状态（默认）：使用 HTTP/2 加速站点。
- 关闭状态：不支持使用 HTTP/2 加速站点。

差异化配置

如需针对子域名单独配置与站点全局配置不同的规则，请前往规则引擎配置。

1. 在左侧菜单栏中，单击**规则引擎**。
2. 创建规则的详细使用说明请参见 规则引擎 。

注意事项

1. 若客户端不支持 HTTP/2，则使用 HTTP 1.x。
2. 此处仅支持访问请求，不支持 HTTP/2 回源。若需配置 HTTP/2 回源，请前往 规则引擎 。

HTTP/3 (QUIC)

最近更新时间：2023-02-08 16:46:08

功能简介

支持 HTTP/3 (QUIC) 请求，使用 HTTP/3 (QUIC) 加速站点请求，提升数据传输效率及安全性。

什么是 QUIC？

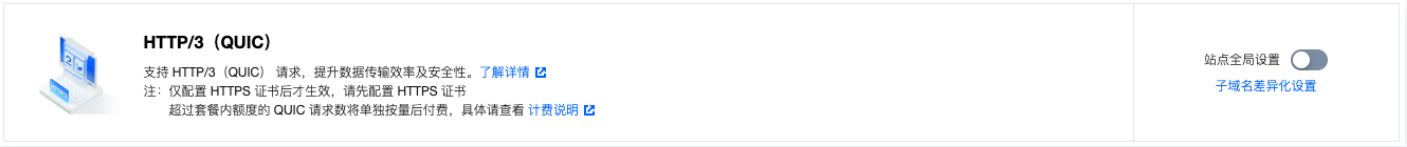
QUIC（Quick UDP Internet Connections）是一个通用的网络协议，提供几乎等同于 TCP 连接的可靠性，但大大减少传输和连接时的延时，避免网络拥塞，同时能够保障网络安全性。

EdgeOne 当前支持的 QUIC 版本有：h3-29、h3-Q050、h3-Q046、h3-Q043、Q046、Q043。

操作步骤

站点全局配置

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点加速** > **网络优化**。
2. 在网络优化页面，选择所需站点，单击 HTTP/3 (QUIC) 模块的“开关”，开启或关闭 HTTP/3 (QUIC) 功能。



- 关闭状态（默认）：不支持 HTTP/3 (QUIC) 请求。
- 开启状态：支持 HTTP/3 (QUIC) 请求，使用 HTTP/3 (QUIC) 加速站点请求。

> **注意**
> - 仅配置 HTTPS 证书后才生效，请先配置 HTTPS 证书。
> - 超出套餐内额度的 HTTP/3 (QUIC) 请求数将单独按量后付费。

差异化配置

如需针对子域名单独配置与站点全局配置不同的规则，请前往规则引擎配置。

1. 在左侧菜单栏中，单击**规则引擎**。
2. 创建规则的详细使用说明请参见 规则引擎 。

注意事项

1. 若同时开启 HTTP/2 和 HTTP/3 (QUIC)，则根据实际客户端请求使用 HTTP/2 或 HTTP/3 (QUIC)。
2. 此处仅支持请求访问，不支持 HTTP/3 (QUIC) 回源。

IPv6 访问

最近更新时间：2023-03-22 14:53:07

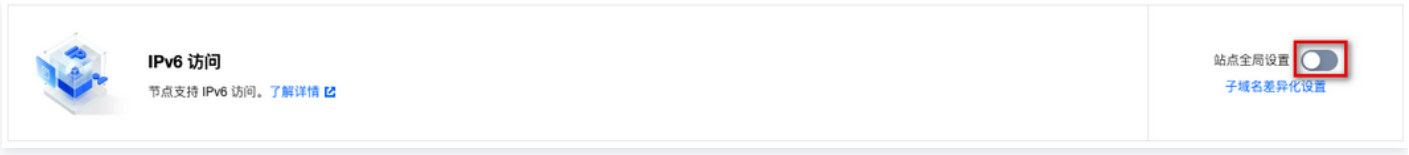
功能简介

一键开启 IPv6 访问，支持 IPv6 客户端以 IPv6 协议访问节点。

操作步骤

站点全局配置

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点加速** > **网络优化**。
2.在网络优化页面，选择所需站点，单击 IPv6 访问模块的“开关”，开启或关闭 IPv6 访问功能。



差异化配置

如需针对不同请求单独配置与站点全局配置不同的规则，请前往**规则引擎**配置，规则引擎内的规则优先级将高于站点全局配置生效。

1. 在左侧菜单栏中，单击**规则引擎**。
2. 单击**创建规则**，在创建规则页内，可根据需求自定义调整规则匹配方式及操作。创建规则的详细使用说明请参见：规则引擎 。

最大上传大小

最近更新时间：2023-03-13 11:05:39

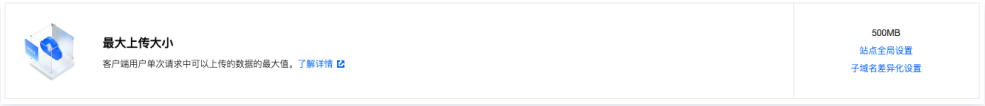
功能简介

最大上传大小即客户端用户单次请求中可以上传的数据的最大值。通过限制最大上传大小，可在一定程度上提升数据传输速率，优化网络传输。

操作步骤

站点全局配置

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点加速** > **网络优化**。
2. 在网络优化页面，选择所需站点，单击最大上传大小模块的**设置**。



3. 在最大上传大小弹窗中，选择是否开启大小限制，并输入上限值，单击**保存**。

配置项说明：

- 大小限制：默认开启；企业版套餐下，支持关闭大小限制，即支持任意大小的上传数据（平台为流式传输）。
- 上限值：当开启大小限制时，支持设置1-500MB 的上传数据值。默认为500 MB。

差异化配置

如需针对子域名，URL Path 或文件后缀等单独配置与站点全局配置不同的规则，请前往规则引擎配置。

1. 在左侧菜单栏中，单击**规则引擎**。
2. 创建规则的详细使用说明请参见 规则引擎 。

注意事项

此处的配置会优先于源站的配置生效。

WebSocket

最近更新时间：2023-02-08 16:46:08

功能简介

支持 WebSocket 协议，使用 WebSocket 协议使得服务端可主动向客户端推送数据。

什么是 WebSocket？

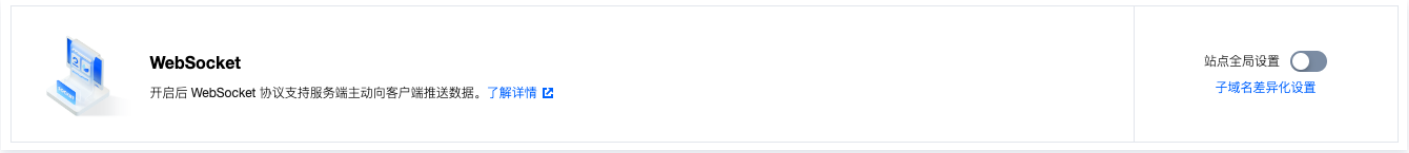
WebSocket 协议是基于 TCP 的一种持久化协议，它实现了客户端与服务器全双工（full-duplex）通信，允许服务器主动发送信息给客户端。在 Websocket 协议之前，实现客户端和服务端双工通讯的 Web App 需要通过不断发送 HTTP 请求呼叫来进行询问，这导致了服务成本增加和效率低下的问题。

由于具有全双工通信的优势，WebSocket 广泛应用于社交订阅、协同办公、行情播报、互动直播、在线教育、物联网等场景，能更好地节省服务器资源和带宽，并且能够更实时地进行通讯。

操作步骤

站点全局配置

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点加速** > **网络优化**。
2. 在网络优化页面，选择所需站点，单击 WebSocket 模块的“开关”，开启或关闭 WebSocket 功能。



- 关闭状态（默认）：不支持WebSocket 协议。
- 开启状态：支持 WebSocket 协议。

3. 在 WebSocket 最大连接时长窗口中，调整最大时长，单击**保存**。

> **说明**
> - 最大连接时长：超时时间之内若没有数据收发，连接将被断开。
> - 不同套餐支持的最大连接时长如下所示：
>   - 企业版：300秒。
>   - 标准版：120秒。

差异化配置

如需针对子域名单独配置与站点全局配置不同的规则，请前往规则引擎配置。

1. 在左侧菜单栏中，单击**规则引擎**。
2. 创建规则的详细使用说明请参见 规则引擎 。

真实客户端 IP 头部

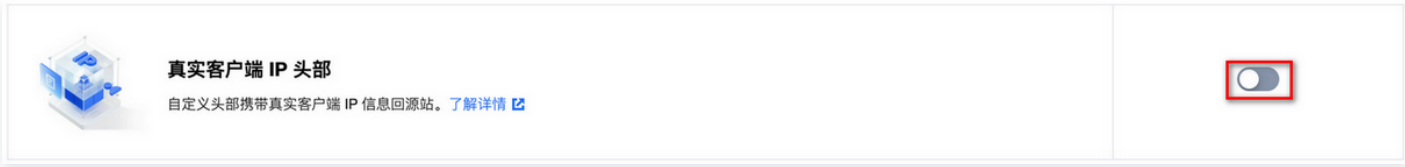
最近更新时间：2022-11-25 17:53:43

功能简介

支持自定义回源 HTTP 请求头部，携带真实客户端 IP 信息回源。

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**站点加速** > **网络优化**。
2. 在网络优化页面，选择所需站点，单击，开启“真实客户端 IP 头部”功能。



3. 在弹窗中，自定义设置该头部的名称，例如 Tencent-Client-IP，单击**保存**。

客户端 IP 地理位置

最近更新时间：2022-11-25 17:53:48

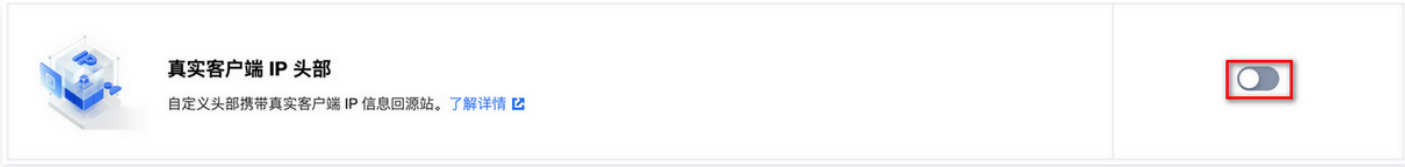
功能简介

自定义头部携带客户端 IP 地理位置信息回源站。

> **说明**
> - 国家/地区维度，值采用两位字母国家/地区代码：ISO 3166-1 alpha-2 codes。
> - 暂不支持 IPv6。

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**站点加速** > **网络优化**。
2. 在网络优化页面，选择所需站点，单击，开启“客户端 IP 地理位置”功能。



3. 在弹窗中，可自定义设置该头部的名称，或直接使用默认名称 EO-Client-IPCountry，单击**保存**。

gRPC

最近更新时间：2023-01-06 16:34:12

功能简介

EdgeOne 开启 gRPC 协议，可以同时支持 HTTP/HTTPS/gRPC 协议，根据用户请求协议自动适配，即请求 HTTP，则使用 HTTP 协议；请求 gRPC，则使用 gRPC 协议。

什么是 gRPC？

gRPC (gRPC Remote Procedure Calls) 是 Google 发起的一个开源远程过程调用（Remote procedure call）系统。该系统基于 HTTP/2 标准设计，具备诸如双向流、流控、头部压缩、单 TCP 连接上的多复用请求等特性。

前提条件

gRPC 是基于全链路 HTTP/2实现的，即请求和回源均需要开启 HTTP/2，详情请参见 HTTP/2 。

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**站点加速 > 网络优化**。
2.在网络优化页面，选择所需站点，单击 gRPC 模块的“开关”，开启或关闭 gRPC 功能。

参数说明：

- 关闭状态（默认）：不支持 gRPC 协议。
- 开启状态：支持 gRPC 协议。目前只支持 Simple RPC、Server-side streaming RPC 两种模式。

URL 重写
访问 URL 重定向

最近更新时间：2022-11-08 17:43:39

功能简介

节点通过响应特定状态码将客户端请求 URL 重定向到目标 URL。

适用场景

将您业务场景中原先需要源站生成并返回的 URL 重定向，改为直接由 EdgeOne 边缘节点构造并且返回，减少回源的网络延时和源站生成 URL 重定向的负载，提升客户端访问性能。

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**规则引擎**。
2. 在规则引擎页面，选择所需站点，可按需配置访问 URL 重定向规则。如何使用规则引擎，请参见 规则引擎 。

配置项说明：

配置项	说明
目标 URL	希望重定向的目标 URL，例如：https://www.example.com/images/foo.jpg 或 https://www.example.com/foo/bar
携带查询参数	是否携带原查询参数至目标 URL ，默认会携带
状态码	选择重定向的响应状态码： ○ 302（默认） ○ 301 ○ 303 ○ 307

配置示例

若请求 URL `https://www.example.com/path/foo.html` 的访问 URL 重定向配置如下：

则客户端请求：`https://www.example.com/path/foo.html?key1=value1` ，则节点响应 301 重定向 `https://www.example.com/newpath/bar.html` 。

回源 URL 重写

最近更新时间：2022-11-08 17:43:47

功能简介

将节点收到的用户请求 URL，按照指定规则，在节点向源站发起请求时重写到源站上的目标 URL，不影响节点的缓存标识（Cache Key）。

适用场景

若客户端访问的 URL 已经对外发布，不宜更改，而业务源站出于某些原因变更了源站上的 URL 路径；或者为了搜索引擎优化（SEO），客户端访问的 URL 和源站 URL 的路径并不一致。在这些情况下，通过设置回源 URL 重写规则，节点可以在不改变客户端访问 URL 的情况下，把回源的 URL 重写为源站上资源对应的实际 URL。

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**规则引擎**。
2. 在规则引擎页面，选择所需站点，可按需配置访问 URL 重定向规则。如何使用规则引擎，请参见 规则引擎 。

配置项说明：

类型	说明
增加路径前缀	增加指定路径前缀至请求 URL Path，例如请求 URL是 `http://www.example.com/path0/index.html` ，增加的路径前缀为/prefix，则重写后的 URL 是 `http://www.example.com/prefix/path0/index.html` 。
移除路径前缀	移除请求 URL 的指定路径前缀内，例如请求 URL是 `http://www.example.com/path0/path1/index.html` ，指定移除的路径前缀是/path0，则重写后的 URL 是 `http://www.example.com/path1/index.html` 。
替换完整路径	替换完整的请求 URL Path，例如请求 URL是 `http://www.example.com/path0/index.html` ，替换完整路径为/new/page.html，则重写后的 URL 是 `http://www.example.com/new/page.html` 。

配置示例

若请求 URL `https://www.example.com/path0/path1/foo.html` 的访问 URL 重定向配置如下：

则客户端请求： `https://www.example.com/path0/path1/foo.html?key1=value1` 回源会被重写为 `https://www.example.com/path1/foo.html?key1=value1` 获取请求资源。若回源时还需忽略 key1=value1 查询字符串，请使用 回源请求参数设置 操作。

修改头部
修改 HTTP 节点响应头

最近更新时间：2023-01-04 14:41:23

功能简介

支持自定义变更/增加/删除 HTTP 响应头（从节点响应客户端用户时的 HTTP 响应头），不会影响节点缓存。

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**规则引擎**。
2. 在规则引擎页面，选择所需站点，可按需配置修改 HTTP 节点响应头规则。如何使用规则引擎，请参见 规则引擎 。

   配置项说明：

类型	说明
设置	变更指定头部参数的取值为设置后的值，且头部唯一。注意：若指定头部不存在，则会增加该头部。
增加	增加指定的头部。注意：若头部已存在，则会覆盖原有头部且唯一。
删除	删除指定的头部。

注意事项

- 自定义头部参数格式要求如下：
  - 参数名：1 - 100个字符，由数字0 - 9、字符a - z、A - Z，及特殊符 `-` 组成。
  - 参数值：1 - 1000个字符，不支持中文。
- 一个修改 HTTP 请求头操作中，可添加多条不同类型操作，最多30条，执行顺序为从上至下。
- 部分标准头部不支持修改，清单如下：

```
Accept-Ranges
Age
Allow
Authentication-Info
Cache-Control
Connection
Content-Encoding
Content-Length
Content-Location
Content-MD5
Content-Range
Content-Type
Date
Error
ETag
Expires
If-Modified-Since
Last-Modified
Meter
Proxy-Authenticate
Retry-After
Set-Cookie
Transfer-Encoding
```

```
Vary
WWW-Authenticate
```

配置示例

Access-Control-Allow-Origin

用于解决资源的跨域权限问题，实现跨域访问。

- 头部名称：Access-Control-Allow-Origin。
- 头部值：支持输入“*”，或多个域名 / IP / 域名与 IP 混填（必须包含 `http://` 或 `https://`，例如：`http://test.com,http://1.1.1.1`，逗号隔开，最多可输入1000字符）。
- 不同值示例说明：

头部值	说明
*	全匹配：响应添加头部：`Access-Control-Allow-Origin:*`，允许被所有域请求。
`http://cloud.tencent.com, https://cloud.tencent.com,http://www.b.com`	固定匹配： ○ 来源 `https://cloud.tencent.com`，命中列表，则响应添加头部：`Access-Control-Allow-Origin: https://cloud.tencent.com`。 ○ 来源为 `https://www.qq.com`，未命中列表，则不会响应跨域头部。
`https://*.tencent.com`	二级泛域名匹配： ○ 来源 `https://cloud.tencent.com`，命中列表，则响应添加头部：`Access-Control-Allow-Origin: https://cloud.tencent.com`。 ○ 来源为 https://cloud.qq.com，未命中列表，则不会响应跨域头部。
`https://cloud.tencent.com:8080`	端口匹配： ○ 来源为 `https://cloud.tencent.com:8080`，命中列表，则响应添加头部：`Access-Control-Allow-Origin:https://cloud.tencent.com:8080`。 ○ 来源为 `https://cloud.tencent.com`，未命中列表，则不会响应跨域头部。 注意：不支持任意端口匹配，若存在特殊端口，则必须在头部值中指定该端口。

Access-Control-Allow-Methods

设置跨域允许的 HTTP 请求方法。

- 头部名称：Access-Control-Allow-Methods。
- 头部值：可同时设置多个，例如 POST,GET,POTIONS。

Access-Control-Max-Age

指定预检请求的结果在多少秒内有效。

> **说明**
>
> 非简单的跨域请求，在正式通信之前，需要增加一次 HTTP 查询请求，称为“预请求”，用来查明这个跨域请求是不是安全可以接受的，如下请求会被视为非简单的跨域请求：
> 以 GET、HEAD 或者 POST 以外的方式发起，或者使用 POST，但是请求数据类型为 application / x-www-form-urlencoded、multipart / form-data、text / plain 以外的数据类型，如 application / xml 或者 text / xml。

- 头部名称：Access-Control-Max-Age。
- 头部值：输入秒数，例如1728000。

Content-Language

指定访问页面所使用的语言。

- 头部名称：Content-Language。

- 头部值：例如 zh-CN 或 en-US。

Content-Disposition

用来激活浏览器的下载，同时可以设置默认的下载的文件名。

服务端向客户端浏览器发送文件时，如果是浏览器支持的文件类型，如 TXT、JPG 等类型，会默认直接使用浏览器打开，如果需要提示用户保存，则可以通过配置 Content-Disposition 字段覆盖浏览器默认行为。

- 头部名称：Content-Disposition。
- 头部值：常见配置示例如： `attachment;filename=FileName.txt` 。

修改 HTTP 回源请求头

最近更新时间：2023-01-04 15:24:16

功能简介

支持自定义变更/增加/删除 HTTP 请求头（从节点向源站请求回源时的 HTTP 请求头）。

> **说明**
> EdgeOne 默认支持携带 X-Forwarded-For 和 X-Forwarded-Proto 回源，您无需再配置。

操作指南

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**规则引擎**。
2. 在规则引擎页面，选择所需站点，可按需配置修改 HTTP 请求头规则。如何使用规则引擎，请参见 规则引擎 。

配置项说明：

类型	说明
设置	变更指定头部参数的取值为设置后的值，且头部唯一。注意：若指定头部不存在，则会增加该头部。
增加	增加指定的头部。注意：若头部已存在，则会覆盖原有头部且唯一。
删除	删除指定的头部

头部类型说明：

头部类型	说明
自定义	自定义头部。 ○ 名称：1 - 100个字符，由数字0 - 9、字符a - z、A - Z，及特殊符 - 组成。 ○ 值：1 - 1000个字符，不支持中文。
预设头部	根据客户端 `User-Agent` 信息聚合的客户端信息头部： ○ 客户端设备类型：EO-Client-Device 。 取值：Mobile ， Desktop ， SmartTV ， Tablet 或 Others 。 ○ 客户端操作系统：EO-Client-OS 。 取值：Android ， iOS ， Windows ， MacOS ， Linux 或 Others 。 ○ 客户端浏览器类型：EO-Client-Browser 。 取值：Chrome ， Safari ， Firefox ， IE 或 Others 。

注意事项

- 一个修改 HTTP 请求头操作中，可添加多条不同类型操作，最多30条，执行顺序为从上至下。
- 部分标准头部不支持修改，清单如下：

Accept	Accept-Charset	Accept-Encoding	Accept-Language
Accept-Ranges	Age	Authorization	Cache-Control
chunked	close	Connection	Content-Encoding

Content-Length	Content-Range	Content-Type	Cookie
Date	Etag	Expect	Expires
From-Tencent-Lego-Cluster	From-Tencent-Lego-Cluster-Client-Info	From-Tencent-Lego-Cluster-Edge-Server-Info	From-Tencent-Lego-Dsa
From-Tencent-Lego-Dsa-Client-Info	From-Tencent-Lego-Dsa-Edge-Server-Info	From-Tencent-Lego-Overload	Host
identity	If-Match	If-Modified-Since	If-None-Match
If-Range	keep-alive	Last-Modified	Location
multirange	normal	Pragma	Proxy-Authorization
Proxy-Connection	Range	Referer	Server
Server-Timing	Set-Cookie	Transfer-Encoding	upgrade
Upgrade	Upgrade-Insecure-Requests	User-Agent	Via
X-Cache-Lookup	X-Forwarded-For	X-Last-Update-Info	x-redirect-to-self
X-Via	-	-	-

自定义错误页面

最近更新时间：2022-11-25 17:54:17

功能简介

当源站响应指定错误状态码时，返回302状态码跳转到对应的自定义页面。

> **说明**
> 此功能为回源错误状态码的重定向，不支持 IP 黑白名单，Token 鉴权等访问控制产生的状态码重定向。

操作步骤

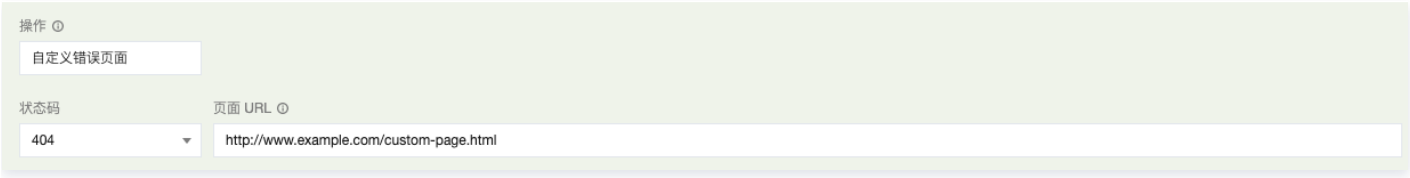
1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**规则引擎**。
2. 在规则引擎页面，选择所需站点，可按需配置自定义错误页面规则。如何使用规则引擎，请参见 规则引擎 。

配置项说明：

配置项	说明
状态码	指定源站响应的错误状态码： ○ 4XX：400, 403, 404, 405, 414, 416, 451 ○ 5XX：500, 501, 502, 503, 504
页面地址	指定错误页面地址，例如：http://www.example.com/custom-page.html

配置示例

当请求的源站响应为 404 Not Found 时，跳转到一个自定义错误页面，配置如下：

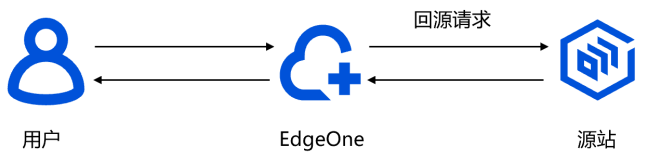


请求与响应行为
EdgeOne 默认 HTTP 回源请求头

最近更新时间：2023-03-03 10:13:27

概述

默认情况下， EdgeOne 在回源请求时，将透传客户端的所有请求头部，同时携带由 EdgeOne 自定义的默认请求头部回源。如果您还需要对回源的 HTTP 头部进行增删改配置，可参见 修改 HTTP 回源请求头 。



默认 HTTP 回源请求头介绍

以下为 EdgeOne 在回源时，默认增加的 HTTP 请求头及含义。

EO-Client-IP

EO-Client-IP 记录了与 EdgeOne 建立连接的客户端请求 IP 地址。如果该请求未经过任何代理服务器，则该头部 IP 即为真实客户端 IP 地址，如果请求经过代理服务器，则该头部 IP 值指代理服务器的 IP 地址。

X-Forwarded-For

X-Forwarded-For 用于记录代理服务器和真实客户端 IP 地址。当用户请求经过多跳到达 EdgeOne 边缘节点中时，可通过该头部来查看真实的客户端 IP 地址以及到达 EdgeOne 边缘节点的前序代理服务器地址。该头部取值如下：

- 如果发送到 EdgeOne 的请求中携带有 X-Forwarded-For 头部，该头部已记录了最原始的访问客户端 IP 地址，则 EdgeOne 会将到达 EdgeOne 边缘节点的前序代理服务器 IP 地址追加到头部值。假设与 EdgeOne 边缘节点建连的前序代理服务器 IP 地址为 10.1.1.1 ，且请求时携带 X-Forwarded-For: 192.168.1.1（原始客户端 IP） ，则回源请求头取值为 X-Forwarded-For: 192.168.1.1.10,10.1.1.1 。
- 如果发送到 EdgeOne 边缘节点的请求中没有 X-Forwarded-For 头部，则 EdgeOne 将在回源请求时，增加 X-Forwarded-For 头部，该头部取值为与 EdgeOne 边缘节点建连的前序代理服务器 IP 地址，取值与 EO-Client-IP 头部相同。

更多详情请参见 X-Forwarded-For 。

X-Forwarded-Proto

X-Forwarded-Proto 用于记录客户端的请求协议，取值为当前客户端发起请求所使用的 HTTP 协议，头部取值有：

- X-Forwarded-Proto：http
- X-Forwarded-Proto：https
- X-Forwarded-Proto：quic

更多详情请参见 X-Forwarded-Proto 。

CDN-Loop

CDN-Loop 用于记录当前请求经过 EdgeOne 边缘加速节点的次数，主要用于平台防止请求环路。当客户端请求每重复经过 1 次 EdgeOne 的边缘节点时， CDN-Loop 的次数则加1，并标记到请求头中，当请求头的 Loops 数值达到 ⩾ 16时，则节点将拒绝请求并响应423状态码。

该头部格式示例： CDN-Loop: TencentEdgeOne; loops=3 。

EO-LOG-UUID

EO-LOG-UUID 代表了当前请求的唯一标识符，该头部主要用于当出现访问异常时，通过该头部值匹配用户请求的全链路日志来定位问题。

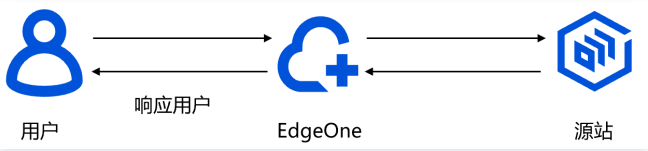
该头部格式示例： EO-LOG-UUID: 4105283880544427145 。

EdgeOne 默认 HTTP 响应头

最近更新时间：2023-03-03 10:13:27

概述

默认情况下， EdgeOne 会透传源站的响应头部给客户端，除非客户有自定义 HTTP 头部增删改配置。如下将介绍由 EdgeOne 定义的响应头部，这些头部会默认响应给客户端。



默认 HTTP 响应头介绍

以下为 EdgeOne 在响应客户端请求时默认携带的 HTTP 响应头介绍。

EO-Cache-Status

`EO-Cache-Status` 用于标识当前客户端发起的请求是否命中缓存的状态标识，该请求头有两种响应状态：

- `EO-Cache-Status：HIT` ：表示请求资源在 EdgeOne 节点命中缓存资源，直接由节点响应用户请求。
- `EO-Cache-Status：MISS` ：表示请求资源在 EdgeOne 节点未命中缓存资源，需要回源站获取资源。

Server

用于标识服务器名称。头部值取决于 Web Server 是基于什么服务搭建的。默认情况下，如果源站的 HTTP 响应头中包含该头部，则透传该头部至客户端，如果源站没有响应该头部，则 EdgeOne 节点将新增该头部，取值 `Server：TencentEdgeOne` 。更多详情请参见 Server 。

腾讯云常见的源站类型响应 Server 值如下：

- 源站为腾讯云 COS 时： `Server: tencent-cos` 。
- 源站为腾讯云 CVM 时： `Server: nginx` 、 `Server: Apache` 、 `Server: tomcat` 、 `Server: Microsoft-IIS` 。
- 源站为腾讯云 CLB 时： `Server: openresty` 。

Date

`Date` 用于标识 EdgeOne 节点最近一次回源更新文件的时间。默认情况下，如果源站 HTTP 响应头包含该头部，则透传该头部至客户端，如果源站没有响应该头部，则 EdgeOne 节点将新增该头部，取值为节点服务器当前时间。更多详情请参见 Date 。

例如：EdgeOne 请求回源，源站响应 `Date: Sat, 07 Jan 2023 14:15:52 GMT` ，若资源在 CDN 设置缓存1小时，则客户端在1小时内访问该资源，获取到的 Date 头部取值均为： `Date: Sat, 07 Jan 2023 14:15:52 GMT`

Connection

用于标识客户端和服务器通信时对于长链接如何进行处理。 默认情况下，如果源站 HTTP 响应头中包含该头部，则透传该头部至客户端，如果源站没有响应该头部，EdgeOne 将根据以下情况，新增该头部：

- 如果当前请求使用 HTTP/2 或者 QUIC 则不添加此头部。
- 如果当前请求使用 HTTP1.0 且没有开启 keepalive，则该头部设置为： `Connection:close` 。
- 源站响应头中不包含 `content-length` 且与 `transfer-encoding` 头部，则该头部设置为： `Connection:close` 。
- 其他情况下，该头部设置为 `Connection:keepalive` 。

更多详情请参见 Connection 。

Alt-Svc

`Alt-Svc` 全称为“Alternative-Service”，该头部列举了当前站点备选的访问方式列表。一般用于在提供 QUIC 等新访问协议支持的同时，实现向下兼容。若域名开启 HTTP/3（QUIC）访问，则 EdgeOne 会默认在 HTTP 响应头中增加该头部。更多详情请参见 Alt-Svc 。

EO-LOG-UUID

EO-LOG-UUID 代表了当前请求的唯一标识符，该头部主要用于当出现访问异常时，通过该头部值匹配用户请求的全链路日志来定位问题。

该头部举例如下：`EO-LOG-UUID: 4105283880544427145`。

源站配置

源站组
源站组列表

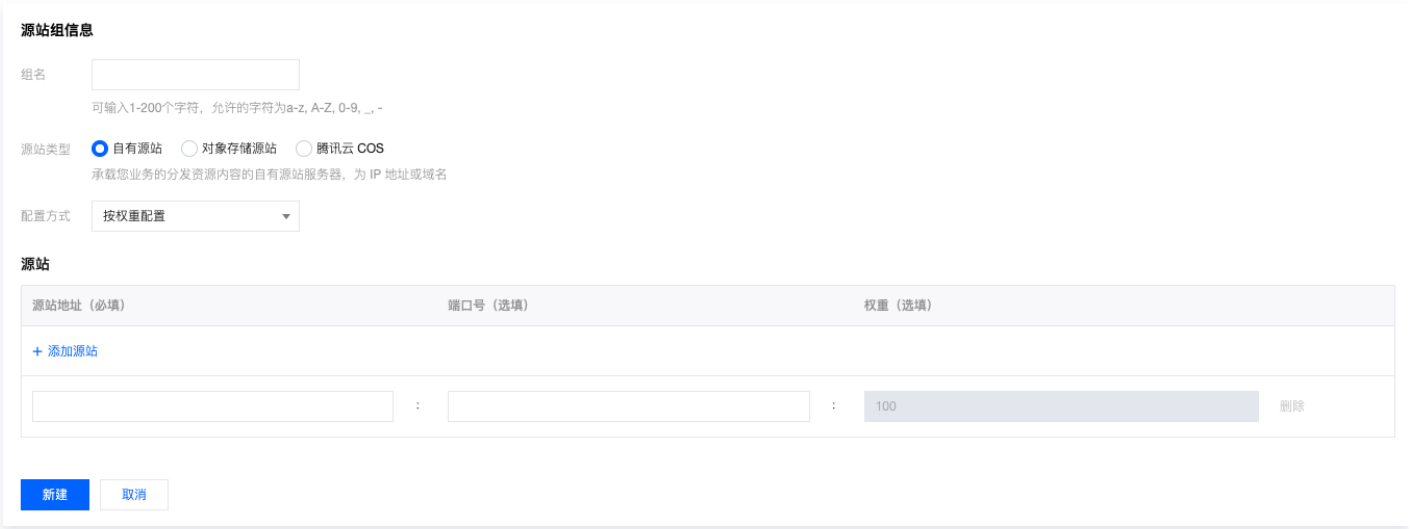
最近更新时间：2022-11-08 17:47:23

功能简介

以源站组的方式管理业务源站。此处配置的源站组可于 负载均衡 和 四层代理 功能中按需引用。

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**源站配置** > **源站组**。
2. 在源站组页面，选择所需站点，单击**新建源站点**。
3.在新建源站点页面，配置相关参数，单击**新建**。



参数说明：

- 组名：源站组名称描述，不同源站组需要设置不同的组名。可输入1-200个字符，允许的字符为 `1a-z, A-Z, 0-9, _, -` 。
- 源站类型：自有源站，对象存储源站或腾讯云 COS。
  - 自有源站：自有源站：承载您业务的分发资源内容的自有源站服务器，为 IP 地址或域名。
  - 对象存储源站：云存储服务厂商的对象存储源站，为一个 Bucket 地址，可开启私有访问，目前仅支持 Amazon Web Services S3。
  - 腾讯云 COS：选择当前账号下腾讯云对象存储（COS）中的一个存储桶作为源站。
- 配置方式：若选择了“自有源站”类型，则可选：
  - 按权重配置：分权重回源。

    说明
    - 只有一个源站地址时，权重默认为100，不可调整。
    - 自定义权重支持 1- 99。
  - 按区域配置：按照客户端 IP 所在区域回源。

    说明
    - 全部地区为默认全局规则，不可删除。
    - 若多条规则中有区域重复，上方的优先级更高。
  - 按 HTTP 协议配置：按照客户端请求 HTTP 协议回源。

    说明

    HTTPS 和 HTTP 至少各配一个源站地址。

自有源站配置约束

- 单个源站组中至多可添加100个源站地址，IPv4 和 IPv6 源站不可混填。

> **注意**
> 目前仅部分节点支持 IPv6 回源。

- 端口号：可配置端口，支持 1 - 65535。
- 若一个源站组被 负载均衡 引用，则：
  - 若代理模式选择“仅 DNS”：源站地址不可配置端口；IP 和域名形式源站不可混填。
- 若一个源站组被 四层代理 引用，则：
  - 所有源站地址必须配置端口。
  - 不支持“按区域配置”和“按 HTTP 协议配置”模式。
  - 若需配置域名形式源站，只能配置1个域名源站，不可与 IP 源站混填。
  - 四层代理暂不支持 IPv6 回源，不可配置 IPv6 源站。

源站健康检查

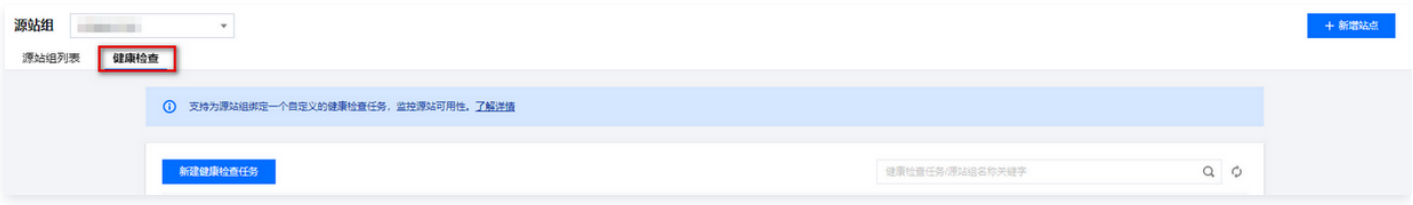
最近更新时间：2022-10-12 16:18:55

功能简介

源站健康检查支持为源站组绑定一个自定义的健康检查任务，监控源站可用性，正常回源被判定为“健康”的源站组，屏蔽被判定为“不健康”的源站组。

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**源站配置 > 源站组**，切换顶部 Tab 到**健康检查**。



2. 在健康检查页面，选择所需站点，创建或编辑源站健康检查任务。
   - 创建源站健康检查任务：单击**新建健康检查任务**，填写相关参数，单击**确认创建**即可。

参数名称		参数详情	备注
选择源站组		选择需要配置自定义源站健康检查的源站组。	○ 请选择正在 域名服务 中使用的源站组，即已绑定 负载均衡 任务的源站组。 ○ 若不同源站组在 域名服务 中绑定了同一个域名，则必须绑定同一个健康检查任务。 ○ 暂不支持 四层代理 的源站健康检查。
配置健康检查任务	任务名称	健康检查任务的名称。	-
	URL	健康检查的请求 URL，路径默认为/。	-
	HTTP Method	HTTP 请求方法。	-
	检查频率	每隔多久发起一次健康检查任务。	较高频率可能会更及时发现源站故障，但同时会增加源站负载。
	超时时间	单次检查允许的回源超时时间，大于则被判定为“不健康”。	-
	HTTP 状态码	选择可通过健康检查，即被判定为“健康”的 HTTP 状态码，除此之外的状态码则被判定为“不健康”。	-
	重试次数	允许失败（被判定“不健康”）后重试的次数，大于则直接被判定为“不健康”。	-
	健康判定	源站组整体被判定为“健康”时，其中至少被判定为“健康”的源站地址个数。	健康判定是源站组维度，一个源站组中可能有多个源站地址。
	健康阈值	当源站组连续几次检查为健康时，源站组被判定为“健康”，恢复为可用状态。	-
	遵循重定向	是否启用遵循301/302重定向。启用后，301/302默认为“健康”的 HTTP 状态码，默认跳转3次。	-

	自定义请求头	发起健康检查时，携带自定义请求头回源。	-

- 编辑源站健康检查任务：单击目标任务操作列的**编辑**，修改相关参数，单击**确认保存**即可。

注意事项

1. 若一个源站组同时用于多个负载均衡任务，则其可能在不同负载均衡任务中被判定为不同的健康状态，例如：在负载均衡任务 A 中是“健康”的，在负载均衡任务 B 中是“不健康”的。EdgeOne 此时会在控制台展示并通过站内信/邮件/短信等通知您该源站组在负载均衡任务 B 中被判定为“不健康”，请您关注并确认。
2. 若源站健康检查任务无任何绑定的源站组，或绑定的源站组不再用于负载均衡任务，则源站健康检查会暂停，不再运行。

负载均衡

最近更新时间：2022-12-02 16:31:55

功能简介

动态优化回源，智能分配流量，有效规避故障源站，减少源站服务器过载，保障整体服务可用性。

> **说明**
> 目前支持基于不同地域和权重的负载均衡。

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**源站配置** > **负载均衡**。
2. 在负载均衡页面，选择所需站点，单击**新建负载均衡任务**。
3. 在新建负载均衡页面，配置相关参数，单击**提交任务**。

参数说明：

- Hostname：站点加速域名，也是默认回源时访问的源站地址下具体的站点域名，即回源 Host。

  > **注意**
  > - 绑定自有源站时，若您需要设置回源 Host 与加速域名不同，可使用 Host Header 重写 功能，重写 Host 至实际回源 Host。
  > - 若 Hostname 与 域名服务 里的已有记录冲突，则负载均衡里的配置优先级更高，将覆盖 域名服务 里的记录。

- 代理模式：
  - 代理加速：EdgeOne 将根据站点套餐类型，为该主机记录（子域名）自动下发安全/加速配置。
- 源站：
  - 主备回源：最多可配置两个源站组，按优先级顺次回源 。当且仅当优先级为1的源站组故障不可用时，转移至优先级为2的源站组（即主源站和备用源站的概念）。
  - 高级回源配置：支持按照匹配 URL 路径配置负载均衡源站。

    > **注意**
    > - 代理加速模式最多可配置2个源站组：按优先级顺次回源 – 当且仅当优先级为1的源站组故障不可用时，会转移至优先级为2的源站组，即主源站和备用源站的概念。
    > - 私有对象存储源站组暂不可作为优先级为 2 的源站组（备用源站组）。

4. 在负载均衡页面，可查看已创建的任务，每个负载均衡任务都有一个对应的部署状态。
   - 部署中：当前负载均衡任务正在部署中，不可删除，请等待完成部署。
   - 运行中：当前负载均衡任务正在现网生效中，不可删除，如需删除，请先停用。
   - 已停用：当前负载均衡任务已停用。

常见问题

为什么在配置源站时，有些源站组置灰不可选？

- 已到达可配置的源站组数量：
  - 最多可配置2个源站组。
- 置灰的源站组为开启了私有访问的对象存储源站：
  - 私有对象存储源站组暂不可作为优先级为 2 的源站组（备用源站组）。

Host Header 重写

最近更新时间：2022-10-12 16:19:03

功能简介

重写 Host 头字段。若您的回源 Host 与 负载均衡 任务中接入的加速域名不同，可使用此功能重写 Host 至实际回源 Host。

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**源站配置** > **规则引擎**。
2. 在规则引擎页面，选择所需站点，单击+可按需配置 Host Header 重写规则。
3. 在规则引擎页面，匹配类型 **Host**，操作选择 **Host Header 重写**，并按需配置其他参数，单击**保存发布**或**仅保存**。

> **说明**
> 目前支持的匹配类型为 Host。

分片回源

最近更新时间：2022-10-12 16:19:06

功能简介

开启后支持分片回源，有助于减少大文件回源消耗，缩短响应时间。

为什么分片回源可以提升大文件分发效率?

节点在缓存资源时，为提高缓存效率，会将资源文件分片缓存（所有分片在节点的缓存时间相同，遵循节点缓存过期 TTL 配置），同时支持 Range 请求。若客户端请求时携带 HTTP 头部 `Range: bytes = 0-999` ，则只返回文件的前1000个字节，并非整个文件。

开启分片回源后，若客户端请求的并非整个文件，仅部分文件，且该部分文件在节点的缓存已过期，需回源获取最新的资源。节点会根据客户端请求分片回源，即仅回源拉取客户端需要的部分文件缓存至节点，同时返回给用户。有效减少回源消耗，提升了整体响应速度。

若未开启分片回源，客户端请求的是部分文件，节点回源时遵循客户端 range 范围回源拉取，也只会拉取请求的部分文件并缓存至节点，同时返回给客户端请求的部分文件，但是可能在性能上无法达到最优化。在大文件场景下，建议打开分片回源。

适用场景

若您的业务资源都是静态大文件，且源站已支持 Range 请求，或源站为腾讯云 COS 源站且**未使用**数据处理类功能（例如：图片处理），建议开启分片回源，提升分发效率和响应速度。

注意事项

- 业务源站需同步支持 Range 请求，否则可能会导致回源失败。
- 若请求资源都是静态小文件，或业务源站为腾讯云 COS 源站且已使用数据处理类功能（例如：图片处理），不建议开启分片回源，开启后会影响回源。

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**源站配置** > **规则引擎**。
2. 在规则引擎页面，选择所需站点，单击  可按需配置分片回源规则。
3. 在规则引擎页面，操作选择**分片回源**，并按需配置其他参数，单击**保存发布**或**仅保存**。

> **注意**
> 目前支持的匹配类型为 Host，URL Path 和文件后缀。

HTTP/2 回源

最近更新时间：2022-10-12 16:19:10

功能简介

支持以 HTTP/2 协议请求回源。

什么是 HTTP/2?

HTTP/2（即 HTTP 2.0，超文本传输协议第2版），是 HTTP 协议的第二个主要版本，能有效减少网络延迟，提高站点页面加载速度。

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**源站配置** > **规则引擎**。
2. 在规则引擎页面，选择所需站点，单击 + 可按需配置 HTTP/2 回源规则。

> **注意**
> 目前仅支持匹配条件为 Host 时配置 HTTP/2 回源。

参数说明：

开关	说明
开启	支持以 HTTP/2 协议请求回源注意：仅源站服务器支持 HTTPS 协议回源才生效
关闭	不支持以 HTTP/2 协议请求回源

回源跟随重定向

最近更新时间：2022-11-08 17:51:05

功能简介

请求回源时跟随源站服务器的302/301重定向，可指定最大重定向次数（默认为3次，支持设置1-5次）。

适用场景

节点默认不缓存301/302状态码，当源站返回301/302请求后，节点默认会将响应返回给客户端，由客户端重定向到对应的资源进行访问。

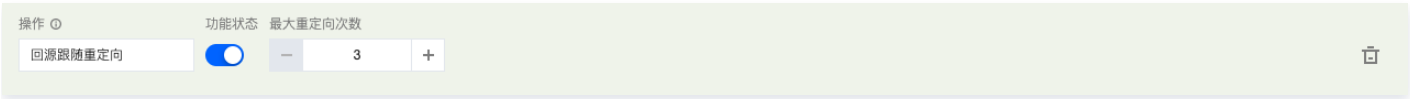
通过开启回源跟随重定向，从节点回源时遇到301/302会主动跟随重定向（不超过设置的最大重定向次数），若获取了所需资源，则响应客户端实际资源，客户端无需再重定向。

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**规则引擎**。
2. 在规则引擎页面，选择所需站点，可按需配置回源跟随重定向规则。如何使用规则引擎，请参见 规则引擎 。

配置示例

若 Host `www.example.com` 的回源跟随重定向配置如下：



则用户 A 请求：`http://www.example.com/a` ，在节点未命中缓存，则节点回源获取所需资源。若源站返回的 HTTP Response 状态码为302，指向重定向地址为 `http://www.example.com/b` ，则：

1. 节点直接向重定向指向的地址 `http://www.example.com/b` 发起请求。
2. 重定向3次内若获取到所需资源，见3；重定向3次内若未获取到所需资源，见4。
3. 缓存资源至节点，并返回给用户 A；此时用户 B 也向 `http://www.example.com/a` 发起请求，则会在节点直接命中并返回给用户 B 。
4. 直接返回301/302给用户，由客户端继续重定向。

回源请求参数设置

最近更新时间：2022-11-28 09:15:01

功能简介

自定义设置回源请求时，是否包含请求中原有的查询字符串和 Cookie。默认情况下，回源时会保留请求中原有的全部查询字符串和 Cookie。此配置不影响节点缓存行为。

适用场景

1. 业务源站会根据不同查询字符串或 Cookie 信息做精细化管理，返回不同的资源。
2. 原请求含节点鉴权相关查询字符串，为保障成功回源获取资源，回源时需忽略该鉴权参数。

操作步骤

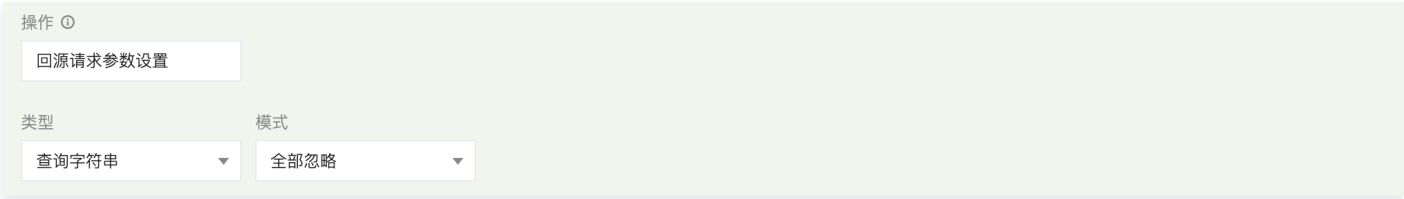
1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**规则引擎**。
2. 在规则引擎页面，选择所需站点，可按需配置回源请求参数设置规则。如何使用规则引擎，请参见 规则引擎 。

   配置项说明：

配置项	说明
查询字符串	调整 URL 中的查询字符串，默认保留原请求的全部查询参数。
Cookie	调整 Cookie 参数，默认保留原请求的全部 Cookie 参数。

配置示例

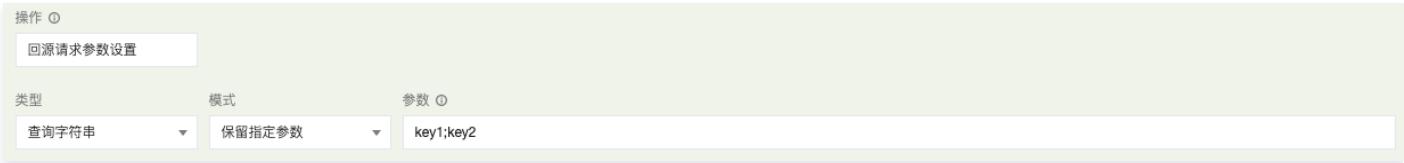
- 若原请求的查询字符串为节点鉴权相关参数，请求回源时需忽略该鉴权参数，则可配置如下：



  客户端请求 URL：`http://www.example.com/path/demo.jpg?abc=18867530-chgdksbvhjsbvdjhsbvfj12`（`abc` 为鉴权参数）。

  回源请求 URL：`http://www.example.com/path/demo.jpg` 。

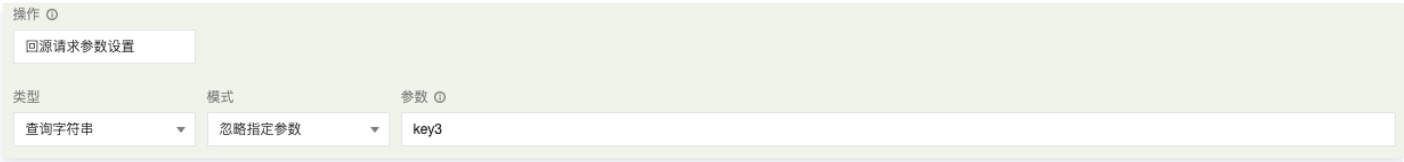
- 若源站仅需要 `key1` 和 `key2` 查询参数，回源时可仅保留这两个参数，其余参数都忽略，可配置如下：



  客户端请求 URL：`http://www.example.com/path/demo.jpg?key1=a&key2=b&key3=c&key4=d` 和 `http://www.example.com/path/demo.jpg?key1=a&key2=b&key3=c&key4=d&key5=e` 。

  回源请求 URL：`http://www.example.com/path/demo.jpg?key1=a&key2=b` 。

- 若源站不需要 `key3` 查询参数，回源时可忽略此参数，保留其余有用的参数，可配置如下：



客户端请求 URL：`http://www.example.com/path/demo.jpg?key1=a&key2=b&key3=c&key4=d` 。

回源请求 URL：`http://www.example.com/path/demo.jpg?key1=a&key2=b&key4=d` 。

规则引擎

概览

最近更新时间：2022-12-02 16:20:58

功能简介

规则引擎旨在通过丰富的规则语言，支持按需自定义处理特定类型请求的配置规则。在规则引擎创建的自定义策略将覆盖边缘服务器的默认行为。

适用场景

- 站点加速处的站点级配置无法覆盖全部业务情况，不同子域名，路径或文件后缀等不同条件下有差异化配置，需针对特定请求自定义功能配置。
- 当前业务除了需要缓存，HTTPS 等基础配置，还需要自定义 Cache Key， URL 重写和修改 HTTP 头部等其他加速功能

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**规则引擎**。
2. 在规则引擎页面，选择所需站点，单击**添加规则**。
3. 在添加规则窗口中，配置相关参数，需提交规则：
   - 仅保存：仅保存规则内容，不下发配置至现网生效。
   - 保存并发布：保存并下发规则内容至现网生效。

关键术语

定义	说明
规则	规则包含特定类型的请求以及应用于它们的一系列操作。 包括： • 一组条件表达式，用于定义识别请求的逻辑。 • 一组匹配条件，定义用于识别请求的标准。 • 定义CDN 将如何处理上述请求的一组功能。
条件表达式	用于定义识别请求的逻辑，支持以下类别： • IF 注：IF 语句可以嵌套在一层 IF 语句下，即执行内嵌 IF 语句之前必须先满足最外层 IF 语句。 • ELSE IF • ELSE
匹配条件	用于定义识别请求的标准，包括： • 匹配类型 • 运算符 • 值
And/Or	逻辑与/逻辑或，可连接多个匹配条件。
操作	命中的请求执行的一系列功能配置。

优先级

范围	说明
规则引擎 vs 站点加速	规则引擎优先级更高，是最终生效的配置。
规则引擎单条规则中	受相对顺序影响，从上至下执行，下方优先级更高，是最终生效的配置。
规则引擎中的多条规则	受相对顺序影响，从上至下执行，下方优先级更高，是最终生效的配置。

	提示：确定规则放置位置时，可将具有通用性或粗粒度的规则放在上方位置作为默认配置，针对特定请求或细粒度的规则放在下方位置。

注意事项

部分操作不受相对顺序的影响，具体说明如下：

- Token 鉴权

  Token 鉴权 不管出现在哪个位置，永远是最先执行的。例如，现有请求同时命中了2条规则，Token 鉴权操作在下方的规则中，则 Token 鉴权会最先执行，鉴权通过才继续执行剩下的内容。

匹配条件

最近更新时间：2022-11-28 15:26:59

说明

匹配条件用于定义识别请求的标准，包括：

- 匹配类型
- 运算符
- 值

匹配类型

类型	说明	值（示例）
HOST	请求 Host	www.example.com
URL Path	请求 URL 路径	/example/foo/bar
URL Full	请求 URL 完整内容	https://www.example.com/foo
查询字符串	请求 URL 中的查询字符串	参数名：key 参数值：value
文件后缀	请求内容的文件后缀（文件扩展名）	jpg png css
文件名称	请求内容的文件名称	foo.txt
HTTP 请求头	HTTP 请求头部	头部名称：name 头部值：value
客户端国家/地区	客户端 IP 所在国家/地区	美国
全部	站点任意请求	-

运算符

类型	说明
等于	请求等于任一指定值（对应匹配类型的值）
不等于	请求不等于任一指定值（对应匹配类型的值）
存在	任一指定值出现在请求中（请求 HTTP 头部名称或查询参数的参数名称）
不存在	任一指定值不出现在请求中（请求 HTTP 头部名称或查询参数的参数名称）
正则匹配	支持 Google RE2 正则表达式匹配

值

所选匹配类型的内容。

通配符

部分匹配类型支持输入包含通配符的内容：

类型	说明	值（示例）
*	匹配0或多个字符	URL Path 的值为 `/foo/*/bar` ，则 `/foo/example/bar` 和 `/foo/demo/bar` 都是有效值

忽略大小写

部分匹配类型的值支持调整大小写敏感：默认均为大小写敏感，即大写与小写视为不同值。若开启”忽略大小写“开关，则大写与小写视为同一值。

操作

最近更新时间：2023-02-13 11:39:48

说明

操作为命中的请求执行的一系列功能配置，支持以下类型：

操作	说明
访问控制	Token 鉴权
	视频拖拽
缓存配置	节点缓存 TTL
	浏览器缓存 TTL
	离线缓存
	状态码缓存 TTL
	自定义 Cache Key
	缓存预刷新
网络优化	HTTP/2
	HTTP/3 (QUIC)
	WebSocket
	最大上传大小
	真实客户端 IP 头部
	客户端 IP 地理位置
URL 重写	访问 URL 重定向
	回源 URL 重写
回源优化	智能加速
	HTTP/2 回源
	分片回源
	回源跟随重定向
	回源请求参数设置
	Host Header 重写

HTTPS 配置	强制 HTTPS
	回源 HTTPS
	HSTS 配置
	TLS 版本
	OCSP 装订
修改 HTTP 头	修改 HTTP 回源请求头
	修改 HTTP 节点响应头
高级配置	自定义错误页面

规则管理

最近更新时间：2022-11-08 17:42:32

控制台支持了一系列图标和按钮来管理规则，例如调整规则的上下顺序，复制规则和启用/关闭规则等，详细说明如下。

图标/按钮	描述
	拖拽规则以调整其上下顺序。
	置顶规则，即将规则放置最上方。
	置底规则，即将规则放置最下方。
	编辑所选模块。
	复制规则：创建一条与所复制规则内容相同的新规则。
	删除所选模块。
	根据规则名称或注释关键词搜索规则，快速定位。
	规则状态： • 启用：发布至现网生效。 • 关闭：未发布至现网生效，仅保存规则内容。
	仅保存规则内容，不发布现网生效
	保存并启用规则，发布至现网生效
	若您的单条规则内容较复杂，含多个 IF 条件表达式，则可通过给 IF 添加相关注释。注释内容将自动生成对应的规则导航，展示在规内容右侧，方便您后续通过注释内容关键词快速查看和定位规则内容。