边缘安全（EdgeSec）

用户指南

文档版本 06

发布日期 2024-05-24

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 开通边缘安全

前提条件

- 当前账号拥有BSS Administrator和EdgeSec_FullAccess权限。
- 需开通华为云的内容分发网络（Content Delivery Network，CDN）。

  说明

  边缘安全是基于内容分发网络（Content Delivery Network，CDN）站点提供的服务，您需要先开通CDN才可使用边缘安全。

规格限制

- 一个域名扩展包支持10个域名。
- 一个规则扩展包最多可添加10条IP黑白名单防护规则。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”。

步骤4 单击“购买”，进入“购买边缘安全”页面，设置您使用的产品参数。

- 套餐版本：支持企业版。
- 计费方式：
  - 流量：防护后的业务流量。

    说明

    按照每小时实际使用的流量进行计费，也可以购买流量包抵扣使用的流量。

    流量按阶梯价格计费，当月阶梯累积（以自然月为一个累积周期）。
- 域名扩展包：一个域名扩展包支持防护10个域名。
- 规则扩展包：一个规则扩展包包含10条IP黑白名单防护规则。

  如果当前版本的IP黑白名单防护规则数不能满足要求，您可以通过购买规则扩展包增加IP黑白名单防护规则数，以满足防护配置需求。

步骤5 选择“购买时长”。

说明

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤6 确认参数配置无误后，勾选“我已阅读并同意 **华为云边缘安全服务协议**”，并单击页面右下角的“立即购买”。

步骤7 确认订单详情无误后，单击“去支付”，完成购买操作。

----结束

2 站点加速

站点加速功能指导如下：

- 域名管理
- 统计分析
- 统计分析（新）
- 预热刷新
- 节点IP归属查询
- 域名证书管理
- 日志管理
- 资源包管理

3 安全防护

3.1 网站设置

3.1.1 添加防护网站

该章节指导您接入域名。

前提条件

已在“域名管理”中，添加了域名，域名管理请参见**域名管理**。

约束条件

- 仅支持在“域名管理”页面“业务类型”为“网站加速”的域名，业务类型说明请参见**CDN加速域名业务类型**。
- 同一防护域名不能重复添加。
- 仅支持添加20个域名。

规格限制

网站接入后，网站的文件上传请求限制为512MB。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在列表左上角，单击“添加防护网站”，参数说明如**表 添加防护网站参数说明**所示。

图 3-1 添加防护网站

表 3-1 添加防护网站参数说明

参数名称	参数说明
网站名称	网站的名称。命名规则如下： ● 不可重名。 ● 须以字母开头。 ● 长度不能超过128个字符。 ● 支持英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_:）。
防护域名	选择防护域名，仅支持选择在CDN服务中“域名管理”页面“业务类型”为“网站加速”的域名。
网站备注	网站补充信息。
策略配置	选择已创建的防护策略，默认为“系统自动生成策略”。

步骤6 单击“确定”，完成防护网站的添加。

----结束

3.1.2 查看基本信息

您可以通过边缘安全管理控制台，查看防护域名的策略名称、防护状态等信息。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 查看防护网站信息如**图3-2**所示，参数说明如**表 网站列表参数说明**所示。

图 3-2 网站列表

表 3-2 网站列表参数说明

参数名称	参数说明
域名	防护的域名。
近3天威胁	该域名3天内的防护情况。
工作模式	防护模式。单击▼，可以选择以下三种防护模式： ● “开启防护”：开启状态。 ● “暂停防护”：关闭状态。如果大量的正常业务被拦截，比如大量返回418返回码，可以将“工作模式”切换为“暂停防护”。该模式下，边缘安全对所有的流量请求只转发不检测。该模式存在风险，建议您优先选择**全局白名单（原误报屏蔽）规则**处理正常业务拦截问题。
调度状态	域名的调度状态。
防护策略	显示防护策略总数。单击数字可跳转到规则配置页面，配置具体的防护规则，具体的配置方法参见**配置防护规则**。
创建时间	添加该网站的时间。
操作	单击“删除”，可删除目标防护网站。

步骤6 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤7 查看防护网站的信息，如**图3-3**所示。

图 3-3 查看基本信息

- “告警页面”默认为“系统默认”的页面，您可以单击 ，在弹出的对话框中，配置“自定义”或者“重定向”页面。
- “流量标识”配置请参见**配置攻击惩罚的流量标识**。

----结束

3.1.3 切换工作模式

您可以切换防护状态。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

应用场景

- 开启防护：开启防护模式后，边缘安全会根据您配置的策略进行攻击检测。
- 暂停防护：如果大量的正常业务被拦截，比如大量返回418返回码，可以将“工作模式”切换为“暂停防护”。该模式下，边缘安全对所有的流量请求只转发不检测，日志也不会记录。该模式存在风险，建议您优先选择全局白名单规则处理正常业务拦截问题。

系统影响

切换为暂停模式后，EdgeSec只转发流程请求，网站安全可能存在风险，建议您优先选择**全局白名单（原误报屏蔽）规则**处理正常业务拦截问题。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上方的 ，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“工作模式”列，单击 ，选择工作模式。

图 3-4 切换工作模式

- 开启防护：开启防护模式后，边缘安全会根据您配置的策略进行攻击检测。
- 暂停防护：如果大量的正常业务被拦截，比如大量返回418返回码，可以将“工作模式”切换为“暂停防护”。该模式下，边缘安全对所有的流量请求只转发不检

测，日志也不会记录。该模式存在风险，建议您优先选择全局白名单规则处理正常业务拦截问题。

----结束

相关操作

- 处理误报事件

3.1.4 配置攻击惩罚的流量标识

边缘安全根据配置的流量标识识别客户端IP、Session或User标记，以分别实现IP、Cookie或Params恶意请求的攻击惩罚功能。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

约束条件

- 如果未配置IP标记，边缘安全默认通过客户端IP进行识别。
- 使用Cookie或Params恶意请求的攻击惩罚功能前，您需要分别配置对应域名的Session标记或User标记。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤6 在“流量标识”栏中，单击“IP标记”、“Session标记”或“User标记”后的 ，分别设置流量标记，相关参数说明如**表3-3**所示。

图 3-5 流量标识

表 3-3 流量标识参数说明

标识	说明	配置样例
IP标记	客户端最原始的IP地址的HTTP请求头字段。 该字段用于获取客户端的真实IP地址，可自定义字段名且支持配置多个字段（多个字段名以英文逗号隔开），配置后，EdgeSec优先从配置的字段中获取客户端真实IP（配置多个字段时，EdgeSec从左到右依次读取）。 **注意** • 不支持配置$remote_addr，EdgeSec默认以TCP连接IP作为客户端IP。 • 如果从自定义字段中未获取到客户端真实IP，EdgeSec将默认使用与CDN建立TCP连接的源IP地址作为客户端IP。	X-Forwarded-For
Session标记	用于Cookie恶意请求的攻击惩罚功能。在选择Cookie拦截的攻击惩罚功能前，必须配置该标识。	jssessionid
User标记	用于Params恶意请求的攻击惩罚功能。在选择Params拦截的攻击惩罚功能前，必须配置该标识。	name

步骤7 单击“确认”，完成标记信息配置。

----结束

相关操作

[配置攻击惩罚标准]

3.2 安全总览

在“安全总览”页面，您可以查看昨天、今天、3天、7天或者30天内所有防护网站或所有实例以及指定防护网站或实例的防护日志。包括各攻击类型统计次数、受攻击域名 Top10、攻击源IP Top10、受攻击URL Top10、攻击来源区域 Top10和业务异常监控 Top10等防护数据。

安全总览页面统计数据每分钟刷新一次。

前提条件

- 已添加了防护域名并已完成了域名接入，请参见[添加防护网站]。
- 已为防护域名添加了一个或者多个防护规则。

规格限制

在“安全总览”界面，最多可以查看30天的防护数据。

操作步骤

步骤1 登录管理控制台。

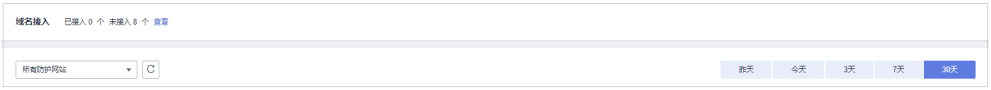
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在页面上方，设置要查询的域名、网站以及查询时间。

- “域名接入”：统计的是添加到边缘安全的防护域名的接入信息。单击“查看”跳转到“网站设置”界面，可以查看防护域名详细信息。
- 所有防护网站：默认统计的是该账号所有项目下添加到边缘安全的所有网站的相关数据。
- 查询时间：可选择昨天、今天、3天、7天、30天。

图 3-6 查询条件设置



步骤5 查看统计的总的请求次数、攻击次数以及各类型攻击的页面总数。

- “攻击次数”中统计的次数为网站被各类型攻击的总次数。
- 各攻击类型统计的次数为用户每次访问网站，在某个时间内被该类型攻击的页面总数。

图 3-7 防护统计数据

步骤6 数据展示。

图 3-8 安全统计

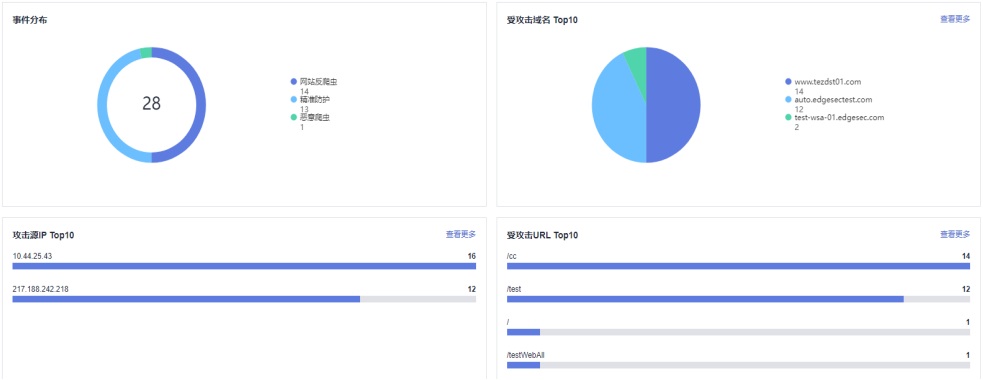


表 3-4 安全统计参数说明

参数名称	参数说明
事件分布	查看攻击事件类型。 单击“事件分布”中的任一个区域，可查看指定域名被攻击的类型、攻击的次数、以及攻击占比。
受攻击域名 Top10	受攻击统计次数Top 10的域名以及各域名受攻击的次数。 单击“查看更多”，可以跳转到“防护事件”页面，查看更多防护数据。
攻击源IP Top10	攻击次数Top 10的攻击源IP以及各源IP发起的攻击次数。 单击“查看更多”，可以跳转到“防护事件”页面，查看更多防护数据。
受攻击URL Top10	受攻击统计次数Top 10的URL以及各URL受攻击的次数。 单击“查看更多”，可以跳转到“防护事件”页面，查看更多防护数据。

----结束

3.3 管理防护事件

3.3.1 查看防护事件

您可以在防护事件中检索XSS攻击、SQL注入、CC防护、自定义精准防护等安全事件，快速定位攻击源或对攻击事件进行分析。

支持查看所有防护域名最近30天的防护事件数据。

须知

如果您将防护网站的“工作模式”切换为“暂停防护”模式，则该防护网站所有的流量请求只转发不检测，同时，日志也不会记录。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“防护事件”，进入“防护事件”页面。

步骤5 在网站下拉列表中选择待查看的防护网站，可查看“昨天”、“今天”、“3天”、“7天”、“30天”或者自定义时间范围内的防护日志。

- “防护事件趋势图”：展示所选网站在选择的时间段内的防护情况。
- “TOP10统计”：针对当前所选时间段的TOP10网站统计。

图 3-9 防护事件

步骤6 在“防护事件列表”中，查看防护详情。

- 根据筛选条件字段匹配值进行筛选，可设置多项匹配条件，单击“添加”后，匹配条件会展示在事件列表的上方，确认后单击“查询”，条件字段参数说明如**表3-5**所示。
- 单击  ，可选择防护事件列表展示的字段。
- 在目标事件的“操作”列单击“详情”，可查看目标域名攻击事件详情。

图 3-10 防护事件列表

表 3-5 条件字段参数说明

参数名称	参数说明
事件ID	标识该防护事件的ID。
事件类型	发生攻击的类型。 默认选择“全部”，查看所有攻击类型的日志信息，也可以根据需要，选择攻击类型查看攻击日志信息。
规则ID	内置Web基础防护规则ID。
防护动作	防护配置中设置的防护动作，包含：拦截、仅记录、人机验证等。
源IP	Web访问者的公网IP地址（攻击者IP地址）。 默认选择“全部”，查看所有的日志信息，也可以根据需要，选择或者自定义攻击者IP地址查看攻击日志信息。

参数名称	参数说明
URL	攻击的防护域名的URL。

表 3-6 防护事件列表参数说明

参数	说明	示例
时间	本次攻击发生的时间。	2023/03/04 13:20:04
源IP	Web访问者的公网IP地址（攻击者IP地址）。	-
防护域名	被攻击的防护域名。	www.example.com
地理位置	攻击者来源IP所在地区。	-
URL	攻击的防护域名的URL。	/admin
事件类型	发生攻击的类型。	精准防护
防护动作	防护配置中设置的防护动作，包含：拦截、仅记录、人机验证等。 **说明** 配置隐私屏蔽防护规则后，如果访问请求命中防护规则，则防护动作显示为“不匹配”。	拦截

----结束

3.3.2 处理误报事件

对于“防护事件”页面中的攻击事件，如果排查后您确认该攻击事件为误报事件，即未发现该攻击事件相关的恶意链接、字符等，则您可以通过设置URL和规则ID的忽略（Web基础防护规则）、删除或关闭对应的防护规则（自定义防护规则），屏蔽该攻击事件。将攻击事件处理为误报事件后，“防护事件”页面中将不再出现该攻击事件。

根据内置的Web基础防护规则和网站反爬虫的特征反爬虫，以及自定义防护规则（CC攻击防护规则、精准访问防护规则、黑白名单规则、地理位置访问控制规则等）检测到符合规则的恶意攻击时，会按照规则中的防护动作（仅记录、拦截等）在“防护事件”页面中记录检测到的攻击事件。

前提条件

事件详情列表中包含误报攻击事件。

约束条件

- 仅基于边缘安全内置的Web基础防护规则和网站反爬虫的特征反爬虫拦截或记录的攻击事情可以进行“误报处理”操作。
- 基于自定义规则（CC攻击防护规则、精准访问防护规则、黑白名单规则、地理位置访问控制规则等）拦截或记录的攻击事件，无法执行“误报处理”操作，如果

您确认该攻击事件为误报，可在自定义规则页面，将该攻击事件对应的防护规则删除或关闭。

- 同一个攻击事件不能重复进行误报处理，即如果该攻击事件已进行了误报处理，则不能再对该攻击事件进行误报处理。

使用场景

业务正常请求被拦截。例如，您在华为云ECS服务器上部署了一个Web应用，将该Web应用对应的公网域名接入边缘安全并开启Web基础防护后，该域名的请求流量命中了Web基础防护规则被边缘安全误拦截，导致通过域名访问网站显示异常，但直接通过IP访问网站正常。

系统影响

拦截事件处理为误报后，“防护事件”页面中将不再出现该事件。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“防护事件”，进入“防护事件”页面。

步骤5 在“防护事件列表”中，根据实际情况对防护事件进行处理。

- 确认事件为误报，在目标防护事件所在行的“操作”列，单击“事件处理 > 误报处理”，确认信息后单击“前去处理”，调整防护规则，防护配置请参见**配置防护策略**。

图 3-11 误报处理

表 3-7 误报处理参数说明

参数	参数说明	取值样例
防护方式	– 全部域名：默认防护当前策略下绑定的所有域名。 – 指定域名：选择策略绑定的防护域名或手动输入泛域名对应的单域名。	指定域名
防护域名	“防护方式”选择“指定域名”时，需要配置此参数。 需要手动输入当前策略下绑定的需要防护的泛域名对应的单域名，且需要输入完整的域名。 单击“添加”，支持配置多个域名。	www.example.com
条件列表	单击“添加”增加新的条件，一个防护规则至少包含一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。 条件设置参数说明如下： – 字段 – 子字段：当“字段”选择“Params”、“Cookie”或者“Header”时，请根据实际使用需求配置子字段。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。 – 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 – 内容：输入或者选择条件匹配的内容。	“路径”包含“/product”
不检测模块	– “所有检测模块”：通过边缘安全配置的其他所有的规则都不会生效，边缘安全将放行该域名下的所有请求流量。 – “Web基础防护模块”：选择此参数时，可根据选择的“不检测规则类型”，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。	Web基础防护模块

参数	参数说明	取值样例
不检测规则类型	“不检测模块”选择“Web基础防护模块”时，您可以选择以下方式进行配置： – 按类别：按攻击事件类别进行配置，如：XSS、SQL注入等。一个类别会包含一个或者多个规则id。 – 所有内置规则：**Web基础防护规则**里开启的所有防护规则。	按类别
不检测规则类别	当“不检测规则类型”选择“按类别”时，展示此参数。	SQL注入攻击
规则描述	可选参数，设置该规则的备注信息。	-
高级设置	如果您只想忽略来源于某攻击事件下指定字段的攻击，可在“高级设置”里选择指定字段进行配置，配置完成后，边缘安全将不再拦截指定字段的攻击事件。 在第一个下拉列表中选择目标字段。支持的字段有：Params、Cookie、Header、Body、Multipart。 – 当选择“Params”、“Cookie”或者“Header”字段时，可以配置“全部”或根据需求配置子字段。 – 当选择“Body”或“Multipart”字段时，可以配置“全部”。 – 当选择“Cookie”字段时，“防护域名”可以为空。 **说明** 当字段配置为“全部”时，配置完成后，边缘安全将不再拦截该字段的所有攻击事件。	Params 全部

- 将源IP添加到地址组。在目标防护事件所在行的“操作”列，单击“事件处理 > 添加到地址组”，添加成功后将根据该地址组所应用的防护策略进行拦截或放行。

  “添加方式”可选择已有地址组或者新建地址组。

图 3-12 添加至地址组

- 将源IP添加至对应防护域名下的黑白名单策略。在目标防护事件所在行的“操作”列，单击“事件处理 > 添加至黑白名单”，添加成功后该策略将始终对添加的攻击源IP进行拦截或放行。

图 3-13 添加至黑白名单

表 3-8 添加至黑白名单参数说明

参数	参数说明
添加方式	- 选择已有规则 - 新建规则
规则名称	- 添加方式选择“选择已有规则”时，在下拉框中选择规则名称 。 - 添加方式选择“新建规则”时，自定义黑白名单规则的名字。
IP/IP段或地址组	添加方式选择“新建规则”时，需要配置此参数。 支持添加黑白名单规则的方式，“IP/IP段”或“地址组”。
地址组名称	“IP/IP段或地址组”选择“地址组”时，需要配置此参数。 在下拉列表框中选择已添加的地址组。您也可以单击“添加地址组”创建新的地址组，详细操作请参见**添加黑白名单IP地址组**。
防护动作	- 拦截：IP地址或IP地址段设置的是黑名单且需要拦截，则选择“拦截”。 - 放行：IP地址或IP地址段设置的是白名单，则选择“放行”。 - 仅记录：需要观察的IP地址或IP地址段，可选择“仅记录”。
攻击惩罚	当“防护动作”设置为“拦截”时，您可以设置攻击惩罚标准。设置攻击惩罚后，当访问者的IP、Cookie或Params恶意请求被拦截时，边缘安全将根据惩罚标准设置的拦截时长来封禁访问者。
规则描述	可选参数，设置该规则的备注信息。

----结束

生效条件

设置误报处理后，1分钟左右生效，攻击事件详情列表中将不再出现此误报。您可以刷新浏览器缓存，重新访问设置了全局白名单规则的页面，验证是否配置成功。

相关操作

拦截事件处理为误报后，该误报事件对应的规则将添加到全局白名单规则列表中，您可以在“防护策略”界面的全局白名单页面查看、关闭、删除或修改该规则。有关配置全局白名单规则的详细操作，请参见**配置全局白名单（原误报屏蔽）规则**。

3.4 防护策略

3.4.1 新增防护策略

防护策略是多种防护规则的合集，用于配置和管理Web基础防护、黑白名单、精准访问防护等防护规则，一条防护策略可以适用于多个防护域名，但一个防护域名只能绑定一个防护策略。该任务指导您添加防护策略。

约束条件

- 一个防护域名只能绑定一个防护策略。
- 最多添加3000条防护策略。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“防护策略”，进入“防护策略”页面。

步骤5 在列表的左上角，单击“添加防护策略”。

图 3-14 添加防护策略

步骤6 在弹出的对话框中，输入策略名称，单击“确认”。

图 3-15 添加策略

步骤7 确认提示框中内容后，单击“确认”，添加的策略会展示在策略列表中。

步骤8 在目标策略所在行，单击策略名称，进入防护规则配置页面，参见配置防护规则为策略添加防护规则。

----结束

相关操作

- 若想修改策略名称，单击目标策略名称后的 ，在弹出的对话框中，重新输入新的策略名称即可。
- 若想删除添加的防护策略，在目标策略所在行的“操作”列，单击“删除”。

3.4.2 添加策略适用的防护域名

您可以通过边缘安全添加策略适用的防护域名。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“防护策略”，进入“防护策略”页面。

步骤5 在目标策略名称所在行的“操作”列，单击“添加防护域名”。

步骤6 选择适用于该策略的“防护域名”。

须知

- 一个防护域名有且只能配置一条防护策略。
- 一条防护策略可以适用于多个防护域名。
- 若想删除已绑定域名的防护策略，请先将此防护策略绑定的所有域名添加到其它防护策略，再在目标策略名称所在行的“操作”列中，单击“删除”。

步骤7 单击“确认”。

----结束

3.4.3 配置防护策略

3.4.3.1 配置引导

引擎检测机制

边缘安全服务内置的防护规则，可帮助您防范常见的Web应用攻击，包括XSS攻击、SQL注入、爬虫检测、Webshell检测等。同时，您也可以根据自己网站防护的需要，灵活配置防护规则，边缘安全根据您配置的防护规则更好的防护您的网站业务。边缘安全引擎内置防护规则的检测流程如图 引擎检测图所示，自定义规则的检测顺序如图3-17所示。

图 3-16 引擎检测图

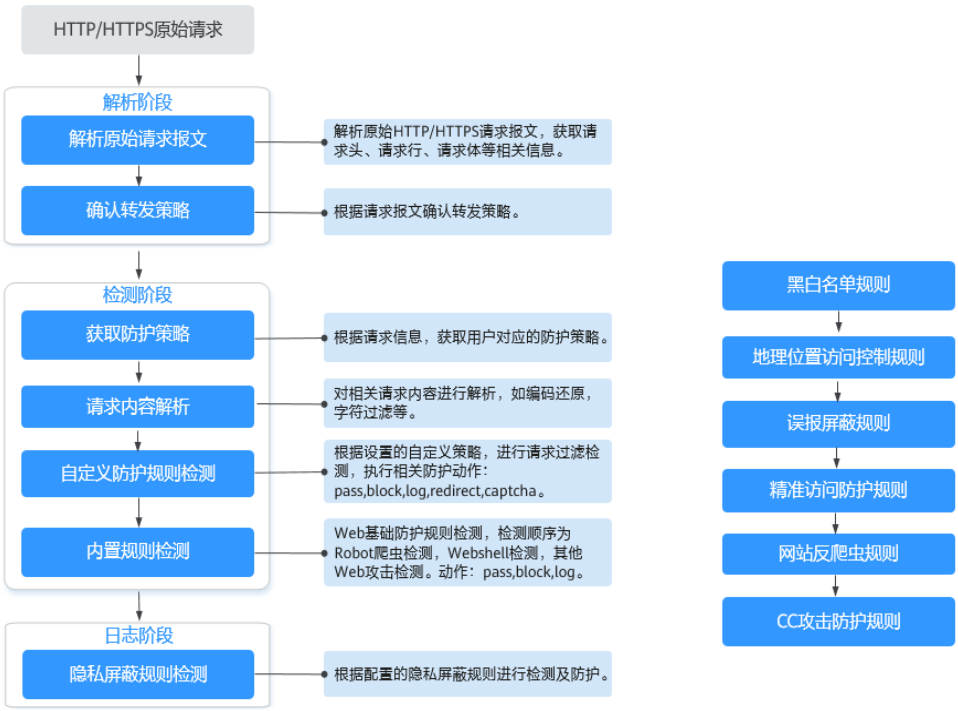
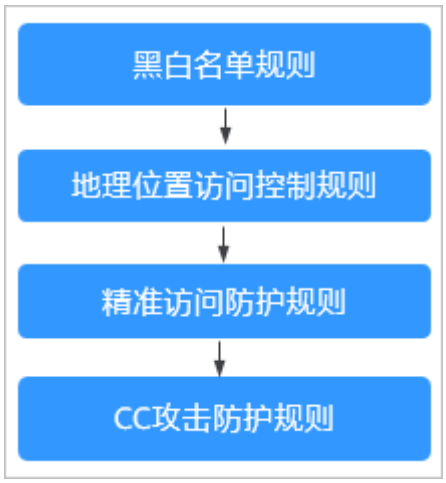


图 3-17 自定义防护规则的检测顺序



响应动作：

- pass：命中规则后无条件放行当前请求。
- block：命中规则后拦截当前请求。
- captcha：命中规则后执行人机验证动作。
- redirect：命中规则后通知客户端执行重定向动作。
- log：命中规则后仅记录攻击信息。
- mask：命中规则后对相关敏感信息进行脱敏处理。

防护规则配置方式

为了简化您的配置过程，边缘安全提供了自定义防护规则的配置方式。

此种方式适合域名业务较少或者域名业务适用的配置规则不相同的用户。

说明

域名添加后，边缘安全会自动为该域名绑定一个防护策略，为域名配置的防护规则默认也添加到绑定该域名的防护策略。如果以后有适用于该防护策略的域名，可直接通过该策略添加防护域名，具体的操作请参见**添加策略适用的防护域名**。

- 入口
  a. 在左侧导航栏选择“网站设置”，进入“网站设置”页面。
  b. 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

  图 3-18 网站列表

- 进入规则配置页面可配置的防护规则

表 3-9 可配置的防护规则

防护规则	说明	参考文档
Web基础防护规则	覆盖OWASP（Open Web Application Security Project，简称OWASP）TOP 10中常见安全威胁，通过预置丰富的信誉库，对恶意扫描器、IP、网马等威胁进行检测和拦截。	**配置Web基础防护规则防御常见Web攻击**
CC攻击防护规则	可以自定义CC防护规则，限制单个IP/Cookie/Referer访问者对您的网站上特定路径（URL）的访问频率，EdgeSec会根据您配置的规则，精准识别CC攻击以及有效缓解CC攻击。	**配置CC攻击防护规则防御CC攻击**
精准访问防护规则	精准访问防护策略可对HTTP首部、Cookie、访问URL、请求参数或者客户端IP进行条件组合，定制化防护策略，为您的网站带来更精准的防护。	**配置精准访问防护规则**
黑白名单规则	配置黑白名单规则，阻断、仅记录或放行指定IP的访问请求，即设置IP黑/白名单。	**配置IP黑白名单规则规则拦截/放行指定IP**

防护规则	说明	参考文档
攻击惩罚规则	当访问者的IP、Cookie或Params恶意请求被拦截时，您可以通过配置攻击惩罚，使边缘安全按配置的攻击惩罚时长来自动封禁访问者。	配置攻击惩罚标准
地理位置访问控制规则	针对指定国家、地区的来源IP自定义访问控制。	配置地理位置访问控制规则拦截/放行特定区域请求
网站反爬虫规则	动态分析网站业务模型，结合人机识别技术和数据风控手段，精准识别爬虫行为。	配置网站反爬虫防护规则防御爬虫攻击
全局白名单规则	针对特定请求忽略某些攻击检测规则，用于处理误报事件。	配置全局白名单规则忽略误报
隐私屏蔽规则	隐私信息屏蔽，避免用户的密码等信息出现在事件日志中。	配置隐私屏蔽规则

3.4.3.2 配置 Web 基础防护规则防御常见 Web 攻击

Web基础防护开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。您还可以根据实际使用需求，开启Webshell检测等Web基础防护。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

约束条件

- Web基础防护支持“拦截”和“仅记录”模式。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 当Web基础防护设置为“拦截”模式时，您可以**配置攻击惩罚标准**。配置攻击惩罚后，如果访问者的IP、Cookie或Params恶意请求被拦截时，边缘安全将根据攻击惩罚设置的拦截时长来封禁访问者。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

图 3-19 网站列表

步骤6 在“Web基础防护”配置框中，用户可根据自己的需要参照**表3-10**更改Web基础防护的“状态”和“模式”。

图 3-20 Web 基础防护配置框

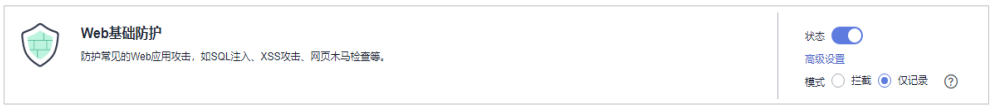


表 3-10 防护动作参数说明

参数	说明
状态	Web应用防护攻击的状态。 •  ：开启状态。 •  ：关闭状态。
模式	• 拦截：发现攻击行为后立即阻断并记录。 • 仅记录：发现攻击行为后只记录不阻断攻击。

步骤7 在“Web基础防护”配置框中，单击“高级设置”，进入“Web基础防护”界面。

步骤8 在“防护配置”页签，根据您的业务场景，开启合适的防护功能，检测项说明如**表3-12**所示。

图 3-21 Web 基础防护

须知

当“模式”设置为“拦截”时，您可以根据需要选择已配置的攻击惩罚。有关配置攻击惩罚的详细操作，请参见**配置攻击惩罚标准**。

1. 防护等级设置。

   在页面右上角，选择防护等级，Web基础防护设置了三种防护等级：“宽松”、“中等”、“严格”，默认情况下，选择“中等”。

表 3-11 防护等级说明

防护等级	说明
宽松	防护粒度较粗，只拦截攻击特征比较明显的请求。 当误报情况较多的场景下，建议选择“宽松”模式。
中等	默认为“中等”防护模式，满足大多数场景下的Web防护需求。
严格	防护粒度最精细，可以拦截具有复杂的绕过特征的攻击请求，例如jolokia网络攻击、探测CGI漏洞、探测Druid SQL注入攻击。 建议您等待业务运行一段时间后，根据防护效果配置全局白名单规则，再开启“严格”模式。

2. 防护检测类型设置。

须知

默认开启“常规检测”防护检测，用户可根据业务需要，参照表3-12开启其他需要防护的检测类型。

表 3-12 检测项说明

检测项	说明
常规检测	防护SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击。其中，SQL注入攻击主要基于语义进行检测。 **说明** 开启“常规检测”后，边缘安全将根据内置规则对常规检测项进行检测。
Webshell检测	防护通过上传接口植入网页木马。 **说明** 开启“Webshell检测”后，边缘安全将对通过上传接口植入的网页木马进行检测。

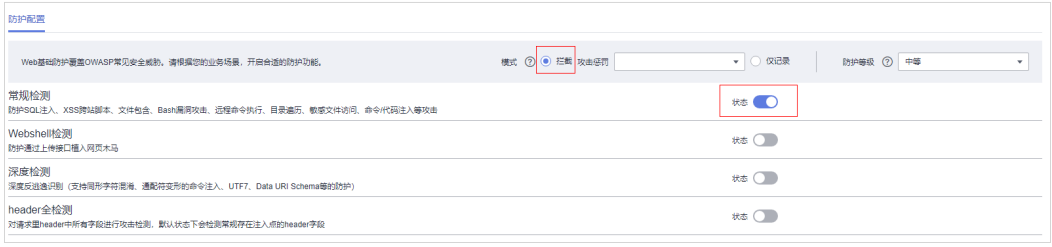
----结束

配置示例-拦截 SQL 注入攻击

假如防护域名“www.example.com”已接入边缘安全，您可以参照以下操作步骤验证是否拦截SQL注入攻击。

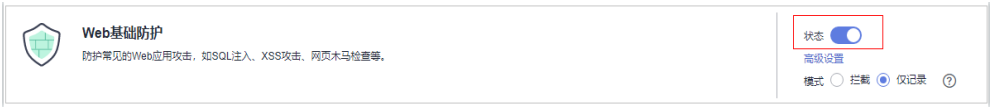
步骤1 开启Web基础防护的“常规检测”，并将防护模式设置为“拦截”。

图 3-22 开启“常规检测”



步骤2 开启Web基础防护。

图 3-23 开启 Web 基础防护



步骤3 清理浏览器缓存，在浏览器中输入模拟SQL注入攻击（例如，http://www.example.com?id=' or 1=1）。

此时访问请求被拦截，拦截页面示例如**图6 拦截攻击请求**所示。

图 3-24 拦截攻击请求

步骤4 返回边缘安全管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

----结束

3.4.3.3 配置 CC 攻击防护规则防御 CC 攻击

CC攻击防护规则支持通过限制单个IP/Cookie/Referer访问者对防护网站上源端的访问频率，同时支持策略限速（同一策略下对应的所有域名请求次数合并限速）、域名限速（每个域名单独统计总请求次数）和URL限速（每个URL请求单独统计请求次数），精准识别CC攻击以及有效缓解CC攻击；当您配置完CC攻击防护规则并开启CC攻击防护后（即“CC攻击防护”配置框的“状态”为  ），才能根据您配置的CC攻击防护规则进行防护。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

约束条件

- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- CC攻击防护规则可以添加引用表，引用表防护规则对所有防护域名都生效，即所有防护域名都可以使用CC攻击防护规则的引用表。
- CC攻击防护规则支持“人机验证”、“阻断”等防护动作，您可以根据使用需求设置对应的防护动作。例如，通过配置CC攻击防护规则实现以下功能：根据Cookie标识的用户字段（例如name），当边缘安全识别到同一name值的用户在60秒内访问您域名下的URL（例如，/admin*）页面超过10次时，封禁该用户访问目标网址600秒。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

图 3-25 网站列表

步骤6 在“CC攻击防护”配置框中，用户可根据自己的需要更改“状态”，单击“自定义CC攻击防护规则”，进入CC防护规则配置页面。

图 3-26 CC 防护规则配置框

步骤7 在“CC攻击防护”规则配置页面左上角，单击“添加规则”。

步骤8 在弹出的对话框中，根据表3-13配置CC防护规则。

表 3-13 CC 防护规则参数说明

参数	参数说明	取值样例
规则名称	自定义规则名称。	test
规则描述	可选参数，设置该规则的备注信息。	--

参数	参数说明	取值样例
限速模式	• “源限速”：对源端限速，如某IP（或用户）的访问频率超过限速频率，就会对该IP（或用户）的访问限速。 “IP限速”：根据IP区分单个Web访问者。	--
限速条件	单击“添加”增加新的条件，至少配置一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。 • 字段：路径、IP、Cookie、Header、Params、返回码(HTTP Code)。 • 子字段：当“字段”选择“Cookie”、“Header”、“Params”时，请根据实际需求配置子字段。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。 • 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 **说明** 当“逻辑”关系选择“包含任意一个”、“不包含所有”、“等于任意一个”、“不等于所有”、“前缀为任意一个”、“前缀不为所有”、“后缀为任意一个”或者“后缀不为所有”时，需要选择引用表，创建引用表的详细操作请参见**创建引用表对防护指标进行批量配置**。 • 内容：输入或者选择条件匹配的内容。	“路径”包含“/admin/”
限速频率	单个Web访问者在限速周期内可以正常访问的次数，如果超过该访问次数，边缘安全将根据配置的“防护动作”来处理。	10次/60秒
防护动作	当访问的请求频率超过“限速频率”时，可设置以下防护动作： • 人机验证：表示超过“限速频率”后弹出验证码，进行人机验证，完成验证后，请求将不受访问限制。人机验证目前支持英文。 • 阻断：表示超过“限速频率”将直接阻断。 • 仅记录：表示超过“限速频率”将只记录不阻断。	阻断
阻断时长	当“防护动作”选择“阻断”时，可设置阻断后恢复正常访问页面的时间。	600秒

参数	参数说明	取值样例
阻断页面	当“防护动作”选择“阻断”时，需要设置，即当访问超过限速频率时，返回的错误页面。 • 当选择“默认设置”时，返回的错误页面为系统默认的阻断页面。 • 当选择“自定义”，返回错误信息由用户自定义。	自定义
页面类型	当“阻断页面”选择“自定义”时，可选择阻断页面的类型“application/json”、“text/html”或者“text/xml”。	text/html
页面内容	当“阻断页面”选择“自定义”时，可设置自定义返回的内容。	不同页面类型对应的页面内容样式： • text/html：<html><body>Forbidden</body></html> • application/json：{"msg": "Forbidden"} • text/xml：<?xml version="1.0" encoding="utf-8"?><error><msg>Forbidden</msg></error>

步骤9 单击“确认”，添加的CC攻击防护规则展示在CC规则列表中。

- 规则添加成功后，默认的“规则状态”为“已开启”，若您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 若需要修改添加的CC攻击防护规则时，可单击待修改的CC攻击防护规则所在行的“修改”，修改CC攻击防护规则。
- 若需要删除用户自行添加的CC攻击防护规则时，可单击待删除的CC攻击防护规则所在行的“删除”，删除CC攻击防护规则。

----结束

配置示例-人机验证

假如防护域名“www.example.com”已接入边缘安全，您可以参照以下操作步骤验证人机验证防护效果。

步骤1 添加防护动作为“人机验证”CC防护规则。

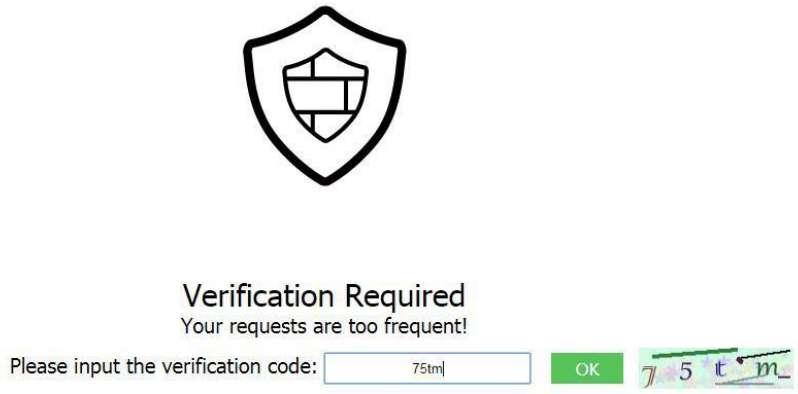
图 3-27 添加“人机验证”防护规则

步骤2 开启CC攻击防护。

图 3-28 CC 防护规则配置框

步骤3 清理浏览器缓存，在浏览器中访问“http://www.example.com/admin/”页面。

当您在60秒内访问页面10次，在第11次访问该页面时，页面弹出验证码。此时，您需要输入验证码才能继续访问。



步骤4 返回边缘安全管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

----结束

3.4.3.4 配置精准访问防护规则

精准访问防护策略可对HTTP首部、Cookie、访问URL、请求参数或者客户端IP进行条件组合，定制化防护策略，为您的网站带来更精准的防护。

精准访问防护规则允许您设置访问防护规则，对常见的HTTP字段（如IP、路径、Referer、User Agent、Params等）进行条件组合，用来筛选访问请求，并对命中条件的请求设置仅记录、放行或阻断操作。

精准访问防护规则可以添加引用表，引用表防护规则对所有防护域名都生效，即所有防护域名都可以使用精准防护规则的引用表。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

约束条件

- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 当精准访问防护规则的“防护动作”设置为“阻断”时，您可以**配置攻击惩罚标准**。配置攻击惩罚后，如果访问者的IP、Cookie或Params恶意请求被拦截时，边缘安全将根据攻击惩罚设置的拦截时长来封禁访问者。

应用场景

精准访问防护支持业务场景定制化的防护策略，可用于盗链防护、网站管理后台保护等场景。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

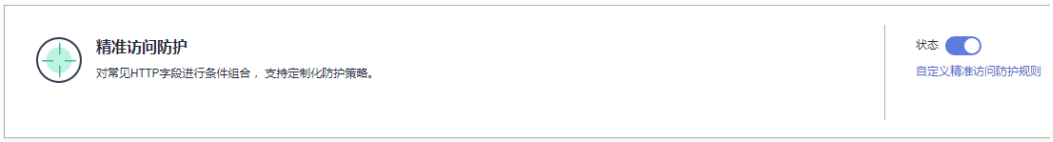
步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

图 3-29 网站列表

步骤6 在“精准访问防护”配置框中，用户可根据自己的需要更改“状态”，单击“自定义精准访问防护规则”，进入精准访问防护规则配置页面。

图 3-30 精准访问防护配置框



步骤7 在“精准访问防护配置”页面，设置“检测模式”，如图3-31所示。

精准访问防护规则提供了两种检测模式：

- 短路检测：当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。
- 全检测：当用户的请求符合精准防护中的拦截条件时，不会立即拦截，它会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。

图 3-31 检测模式

步骤8 在“精准访问防护配置”页面左上角，单击“添加规则”。

步骤9 在弹出的对话框中，根据表3-14和表 条件列表配置添加精准访问防护规则。

以图3-32的配置为例，其含义为：当用户访问目标域名下包含“/admin”的URL地址时，边缘安全将阻断该用户访问目标URL地址。

须知

如果不确定配置的精准访问防护规则是否会误拦截正常的访问请求，您可以先将精准访问防护规则的“防护动作”设置为“仅记录”，在“防护事件”页面查看防护事件，确认不会误拦截正常的访问请求后，再将该精准访问防护规则的“防护动作”设置为“阻断”。

图 3-32 添加精准访问防护规则

表 3-14 规则参数说明

参数	参数说明	取值样例
条件列表	单击“添加”增加新的条件，一个防护规则至少包含一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。 条件设置参数说明如下： ● 字段 ● 子字段：当字段选择“IP”、“Params”、“Cookie”或者“Header”时，请根据实际使用需求配置子字段。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。 ● 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 **说明** – 选择“包含任意一个”、“不包含所有”、“等于任意一个”、“不等于所有”、“前缀为任意一个”、“前缀不为所有”、“后缀为任意一个”或者“后缀不为所有”时，“内容”需要选择引用表名称，创建引用表的详细操作请参见**创建引用表对防护指标进行批量配置**。 – “不包含所有”、“不等于所有”、“前缀不为所有”、“后缀不为所有”是指当访问请求中字段不包含、不等于、前/后缀不为引用表中设置的任何一个值时，将进行防护动作（阻断、放行或仅记录）。例如，设置“路径”字段的逻辑为“不包含所有”，选择了“test”引用表，如果“test”引用表中设置的值为test1、test2和test3，则当访问请求的路径不包含test1、test2或test3时，将进行防护动作。 ● 内容：输入或者选择条件匹配的内容。 **说明** 具体的配置请参见**表3-15**。	● “路径”包含“/admin/” ● “User Agent”前缀不为“mozilla/5.0” ● “IP”等于“192.168.2.3” ● “Cookie[key1]”前缀不为“jsessionid”
防护动作	可选择“阻断”、“放行”、“仅记录”或“JS挑战”（返回JS代码）。	“阻断”
攻击惩罚	当“防护动作”设置为“阻断”时，您可以设置攻击惩罚标准。设置攻击惩罚后，当访问者的IP、Cookie或Params恶意请求被拦截时，边缘安全将根据惩罚标准设置的拦截时长来封禁访问者。	长时间IP拦截

参数	参数说明	取值样例
优先级	设置该条件规则检测的顺序值。如果您设置了多条规则，则多条规则间有先后匹配顺序，即访问请求将根据您设定的精准访问控制规则优先级依次进行匹配，优先级较小的精准访问控制规则优先匹配。 您可以通过优先级功能对所有精准访问控制规则进行排序，以获得最优的防护效果。 **须知** 如果多条精准访问控制规则的优先级取值相同，则根据添加防护规则的先后顺序进行排序匹配。	5
生效时间	用户可以选择“立即生效”或者自定义设置生效时间段。 自定义设置的时间只能为将来的某一时间段。	“立即生效”

表 3-15 条件列表配置

字段	子字段	逻辑	内容（举例）
路径：设置的防护路径，不包含域名，仅支持精准匹配（需要防护的路径需要与此处填写的路径完全相等。例如，需要防护的路径为“/admin”，该规则必须填写为“/admin”）	--	在“逻辑”下拉列表框中选择逻辑关系。	*/buy/phone/* **须知** 路径设置为“/”时，表示防护网站所有路径。
User Agent：设置为需要防护的扫描器的用户代理。	--		*Mozilla/5.0 (Windows NT 6.1)*
IP：设置为需要防护的访问者IP地址。	• 客户端IP • X-Forwarded-For		XXX.XXX.1.1
Params：设置为需要防护的请求参数。	--		201901150929
Cookie：根据Cookie区分的Web访问者。	• 所有字段 • 任意子字段 • 自定义		jsessionid

字段	子字段	逻辑	内容（举例）
Referer：设置为需要防护的自定义请求访问的来源。 例如：防护路径设置为“/admin/xxx”，若用户不希望访问者从“www.test.com”访问该页面，则“Referer”对应的“内容”设置为“http://www.test.com”。	--		http://www.test.com
Header：设置为需要防护的自定义HTTP首部。	• 所有字段 • 任意子字段 • 自定义		*text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8*
Method：需要防护的自定义请求的方法。	--		GET、POST、PUT、DELETE、PATCH
Request Line：需要防护的自定义请求行的长度。	--		50
Request：需要防护的自定义请求的长度。包含请求头、请求行、请求体。	--		--
Protocol：需要防护的请求的协议。	--		http
Request Body：请求的消息体。	--		--

步骤10 单击“确认”，添加的精准访问防护规则展示在精准访问防护规则列表中。

- 若需要修改添加的精准访问防护规则时，可单击待修改的精准访问防护规则所在行的“修改”，修改精准访问防护规则。
- 若需要删除添加的精准访问防护规则时，可单击待删除的精准访问防护规则所在行的“删除”，删除精准访问防护规则。

----结束

防护效果

假如已添加域名“www.example.com”，且配置了如图3-32所示的精准访问防护规则。可参照以下步骤验证防护效果：

步骤1 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。

- 不能正常访问，参照章节**添加防护网站**重新完成域名接入。
- 能正常访问，执行**2**。

步骤2 清理浏览器缓存，在浏览器中访问“http://www.example.com/admin”页面或者包含/admin的任意页面，正常情况下，边缘安全会阻断满足条件的访问请求，返回拦截页面。

----结束

配置示例-单独放行指定 IP 的访问

配置两条精准访问防护规则，一条拦截所有的请求，如图3-33所示，一条单独放行指定IP的访问，如图3-34所示。

图 3-33 阻断所有的请求

图 3-34 放行指定 IP

配置示例-仅允许某一地区来源 IP 访问请求

假如防护域名“www.example.com”已接入边缘安全，当您只允许某一地区的IP可以访问防护域名，例如，只允许来源“新加坡”地区的IP可以访问防护域名，请参照以下步骤处理。

步骤1 添加一条精准访问防护规则，字段为“地理位置”，设置“新加坡”地区“放行”的防护动作。

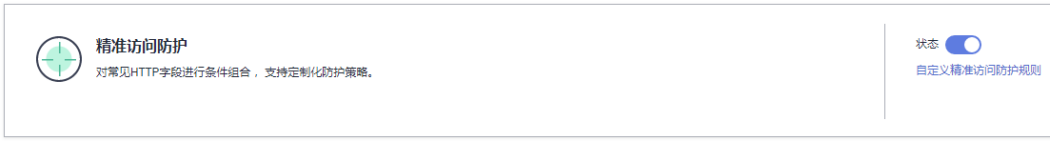
图 3-35 添加放行的防护动作

步骤2 配置一条拦截所有的请求的精准访问防护规则。

图 3-36 拦截所有访问请求

步骤3 开启精准访问防护规则。

图 3-37 精准访问防护配置框



步骤4 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

当非“新加坡”地区的源IP访问页面时，边缘安全将拦截该访问请求，拦截页面示例如**图 拦截攻击请求**所示。

图 3-38 拦截攻击请求

步骤5 返回边缘安全管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看到非“新加坡”地区的源IP都被拦截。

----结束

3.4.3.5 创建引用表对防护指标进行批量配置

该章节指导您创建引用表，即可对路径、User Agent、IP、Params、Cookie、Referer、Header这些单一类型的防护指标进行批量配置，引用表能够被CC攻击防护规则和精准访问防护中的规则所引用。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

约束条件

最多创建100条引用表。

应用场景

CC攻击防护规则和精准访问防护规则批量配置防护字段时，可以使用引用表。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

图 3-39 网站列表

步骤6 在“CC攻击防护”或者“精准访问防护”配置框中，单击“自定义CC攻击防护规则”或者“自定义精准访问防护规则”，进入规则配置页面。

步骤7 在列表左上角，单击“引用表管理”。

步骤8 在“引用表管理”界面，单击“添加引用表”。

步骤9 在弹出的“添加引用表”对话框中，添加引用表，参数说明如**表3-16**所示。

图 3-40 添加引用表

表 3-16 添加引用表参数说明

参数名称	参数说明	取值样例
名称	用户自定义引用表的名字。	test

参数名称	参数说明	取值样例
类型	• 路径：设置的防护路径，不包含域名。 • User Agent：设置为需要防护的扫描器的用户代理。 • IP：设置为需要防护的访问者IP地址。 • Params：设置为需要防护的请求参数。 • Cookie：根据Cookie区分的Web访问者。 • Referer：设置为需要防护的自定义请求访问的来源。例如：防护路径设置为“/admin/xxx”，若用户不希望访问者从“www.test.com”访问该页面，则“Referer”对应的“值”设置为“http://www.test.com”。 • Header：设置为需要防护的自定义HTTP首部。	路径
值	对应“类型”的取值，该值不支持通配符。 **说明** 可单击“添加”设置多个值。	/buy/phone/

步骤10 单击“确认”，添加的引用表展示在引用表列表。

----结束

相关操作

- 若需要修改创建的引用表，可单击待修改的引用表所在行的“修改”，修改引用表。
- 若需要删除创建的引用表，可单击待删除的引用表所在行的“删除”，删除引用表。

3.4.3.6 配置 IP 黑白名单规则规则拦截/放行指定 IP

IP地址默认全部放行，您可以通过配置黑白名单规则，阻断、仅记录或放行指定IP地址/IP地址段的访问请求。配置黑白名单规则时，边缘安全支持单个添加或通过引用地址组批量导入黑白名单IP地址/IP地址段。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

约束条件

- 边缘安全支持批量导入黑白名单，如果您需要配置多个IP/IP地址段规则，请添加地址组，详细操作请参见**添加黑白名单IP地址组**。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 边缘安全黑白名单规则不支持配置0.0.0.0/0 IP地址段，且白名单规则优先级高于黑名单规则。如果您需要放行某个网段指定的IP并拦截某个网段其他所有IP，请先添加黑名单规则，拦截将该网段的所有IP，然后添加白名单规则，放行指定IP。
- 当黑白名单规则的“防护动作”设置为“拦截”时，您可以**配置攻击惩罚标准**。配置攻击惩罚后，如果访问者的IP、Cookie或Params恶意请求被拦截时，边缘安全将根据攻击惩罚设置的拦截时长来封禁访问者。

注意事项

- 如果您在边缘安全和**内容分发网络（CDN）服务**中同时配置了IP黑白名单，则IP黑白名单规则的执行顺序为“CDN->边缘安全”。
- 如果您当前版本的IP黑白名单防护规则条数不能满足要求时，您可以通过购买规则扩展包（一个规则扩展包包含10条IP黑白名单防护规则）增加IP黑白名单防护规则条数，以满足的防护配置需求。

系统影响

将IP或IP地址段配置为黑名单/白名单后，来自该IP或IP地址段的访问，边缘安全将不会做任何检测，直接拦截（黑名单）/放行（白名单）。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

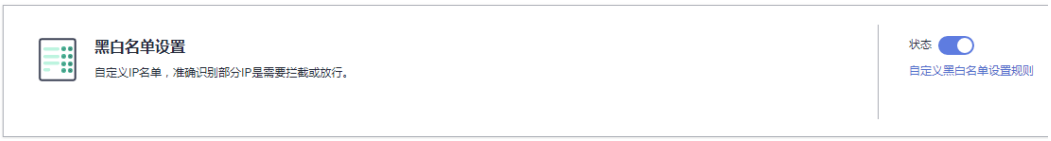
步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

图 3-41 网站列表

步骤6 在“黑白名单设置”配置框中，用户可根据自己的需要更改“状态”，单击“自定义黑白名单设置规则”，进入黑白名单设置规则页面。

图 3-42 黑白名单配置框



步骤7 在“黑白名单”页面左上角，单击“添加规则”。

步骤8 在弹出的对话框中，添加黑白名单规则，如图 添加黑白名单规则所示，参数说明如表3-17所示。

说明

- 将IP配置为仅记录后，来自该IP的访问，边缘安全将根据防护规则进行检测并记录该IP的防护事件数据。
- 其他的IP将根据配置的防护规则进行检测。

图 3-43 添加黑白名单规则

表 3-17 黑白名单参数说明

参数	参数说明	取值样例
规则名称	用户自定义黑白名单规则的名字。	EdgeSectest
IP/IP段或地址组	支持添加黑白名单规则的方式，“IP/IP段”或“地址组”。	IP/IP段

参数	参数说明	取值样例
IP/IP段	当“IP/IP段或地址组” 选择“IP/IP段”时需要设置该参数。 支持IP地址或IP地址段。 • IP地址：添加黑名单或者白名单的IP地址。 • IP地址段：IP地址与子网掩码。	XXX.XXX.2.3
选择地址组	当“IP/IP段或地址组” 选择“地址组”时需要设置该参数，在下拉列表框中选择已添加的地址组。您也可以单击“添加地址组”创建新的地址组，详细操作请参见**添加黑白名单IP地址组**。	-
防护动作	• 拦截：IP地址或IP地址段设置的是黑名单且需要拦截，则选择“拦截”。 • 放行：IP地址或IP地址段设置的是白名单，则选择“放行”。 • 仅记录：需要观察的IP地址或IP地址段，可选择“仅记录”。	拦截
攻击惩罚	当“防护动作”设置为“拦截”时，您可以设置攻击惩罚标准。设置攻击惩罚后，当访问者的IP、Cookie或Params恶意请求被拦截时，边缘安全将根据惩罚标准设置的拦截时长来封禁访问者。	长时间IP拦截
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 输入完成后，单击“确认”，添加的黑白名单展示在黑白名单规则列表中。

- 规则添加成功后，默认的“规则状态”为“已开启”，若您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 若需要修改添加的黑白名单规则时，可单击待修改的黑白名单IP规则所在行的“修改”，修改黑白名单规则。
- 若需要删除添加的黑白名单规则时，可单击待删除的黑白名单IP规则所在行的“删除”，删除黑白名单规则。

----结束

配置示例-放行指定 IP

假如防护域名“www.example.com”已接入边缘安全，您可以参照以下操作步骤验证放行指定IP防护效果。

步骤1 添加以下2条黑白名单规则，拦截所有来源IP。

图 3-44 拦截 1.0.0.0/1 IP 地址段

图 3-45 拦截 128.0.0.0/1 IP 地址段

您也可以通过添加一条精准访问防护规则，拦截所有访问请求，如图3-46所示。

图 3-46 拦截所有访问请求

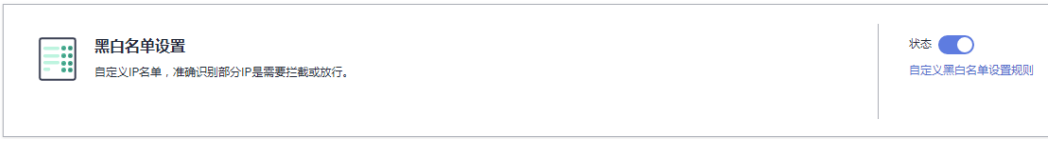
有关配置精准访问防护规则的详细介绍，请参见**配置精准访问防护规则**。

步骤2 参照图3-47示例添加黑白名单规则，放行指定IP，例如，XXX.XXX.2.3。

图 3-47 放行指定 IP

步骤3 开启黑白名单防护规则。

图 3-48 黑白名单配置框



步骤4 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

当访问者的源IP不属于步骤2中设置的放行IP地址时，将拦截该访问请求，拦截页面示例如图3-49所示。

图 3-49 拦截攻击请求

步骤5 返回边缘安全管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

----结束

3.4.3.7 配置攻击惩罚标准

当访问者的IP、Cookie或Params恶意请求被拦截时，您可以通过配置攻击惩罚，使边缘安全按配置的攻击惩罚时长来自动封禁访问者。例如，访问者的源IP（192.168.1.1）为恶意请求，如果您配置了IP攻击惩罚拦截时长为500秒，该攻击惩罚生效后，则该IP被拦截时，边缘安全将封禁该IP，时长为500秒。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

约束条件

- Web基础防护、精准访问防护和黑白名单设置支持攻击惩罚功能，当攻击惩罚标准配置完成后，您还需要在Web基础防护、精准访问防护或黑白名单规则中选择攻击惩罚，该功能才能生效。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 在配置Cookie或Params恶意请求的攻击惩罚标准前，您需要在域名详情页面设置对应的流量标识。相关操作请参见**配置攻击惩罚的流量标识**。

规格限制

- 支持设置6种拦截类型，每个拦截类型只能设置一条攻击惩罚标准。
- 最大拦截时长为30分钟。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

图 3-50 网站列表

步骤6 在“攻击惩罚”配置框中，用户可根据自己的需要更改“状态”，单击“自定义攻击惩罚标准”，进入攻击惩罚标准页面。

图 3-51 攻击惩罚配置框

步骤7 在攻击惩罚标准的列表左上角，单击“添加攻击惩罚”。

步骤8 在弹出的对话框中，添加攻击惩罚标准，参数说明如表3-18所示。

图 3-52 添加攻击惩罚

表 3-18 攻击惩罚参数说明

参数	参数说明	取值样例
拦截类型	支持以下拦截方式： • 长时间IP拦截 • 短时间IP拦截 • 长时间Cookie拦截 • 短时间Cookie拦截 • 长时间Params拦截 • 短时间Params拦截	长时间IP拦截
拦截时长（秒）	拦截时长需要设置为整数，且设置范围为： • 300<长时间拦截时长≤1800 • 短时间拦截时长≤300	500

参数	参数说明	取值样例
规则描述	可选参数，设置该规则的备注信息。	-

步骤9 输入完成后，单击“确认”，添加的攻击惩罚标准展示在列表中。

----结束

相关操作

- 若需要修改添加的攻击惩罚标准，可单击待修改的攻击惩罚标准所在行的“修改”，修改该标准的拦截时长。
- 若需要删除添加的攻击惩罚标准，可单击待删除的攻击惩罚标准所在行的“删除”，删除该标准。

配置示例-Cookie 拦截攻击惩罚

假如防护域名“www.example.com”已接入边缘安全，访问者IP XXX.XXX.248.195为恶意请求，而您需要对来自该IP地址Cookie标记为jsessionid的访问请求封禁10分钟。您可以参照以下操作步骤验证封禁效果。

步骤1 在“网站设置”页面，单击“www.example.com”，进入域名基本信息页面。

步骤2 配置防护域名的Cookie流量标识，即“Session标记”。

图 3-53 流量标识

步骤3 添加一条拦截时长为600秒的“长时间Cookie拦截”的攻击惩罚标准。

图 3-54 添加 Cookie 拦截攻击惩罚

步骤4 开启攻击惩罚。

图 3-55 攻击惩罚配置框

步骤5 添加一条黑白名单规则，拦截XXX.XXX.248.195，且“攻击惩罚”选择“长时间Cookie拦截”。

图 3-56 选择攻击惩罚规则

步骤6 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

当XXX.XXX.248.195源IP访问页面时，会被边缘安全拦截。当检测到来自该源IP的Cookie标记为jsessionid访问请求时，将封禁该访问请求，时长为10分钟。

图 3-57 拦截攻击请求

步骤7 返回边缘安全管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

----结束

3.4.3.8 配置地理位置访问控制规则拦截/放行特定区域请求

您可以通过配置地理位置访问控制规则。可针对指定国家、地区的来源IP自定义访问控制。

如果您仅允许某一地区的来源IP访问防护网站，请参见**配置示例-仅允许某一地区来源IP访问请求**进行配置。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

约束条件

- 同一个地区只能配置到一条地理位置访问控制规则中。例如，如果某个地理位置访问控制规则已设置了“新加坡”地区，那么“新加坡”地区不能再添加到其他地理位置访问控制规则。
- 添加或修改防护规则后，规则生效需要几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。

注意事项

如果您在边缘安全和内容分发网络（CDN）服务中同时配置了区域访问控制，则区域访问控制规则的执行顺序为“CDN->边缘安全”。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

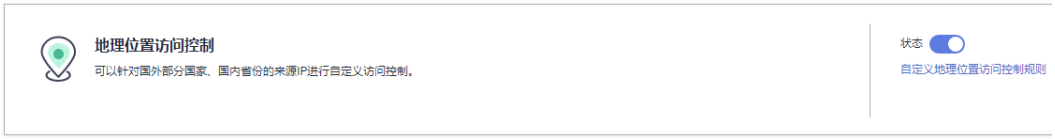
步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

图 3-58 网站列表

步骤6 在“地理位置访问控制”配置框中，用户可根据自己的需要更改“状态”，单击“自定义地理位置访问控制规则”，进入“地理位置访问控制”页面。

图 3-59 地理位置访问控制配置框



步骤7 在“地理位置访问控制”页面左上角，单击“添加规则”。

步骤8 在弹出的对话框中，添加地理位置访问控制规则，如**图3-60**所示，根据**表3-19**配置参数。

图 3-60 添加地理位置访问控制规则

表 3-19 添加地理位置访问控制规则参数说明

参数	参数说明	取值样例
规则名称	用户自定义地理位置控制规则的名字。	-
规则描述	可选参数，设置该规则的备注信息。	-
地理位置	IP访问的地理范围。	-
防护动作	可以根据需要选择“拦截”、“放行”或者“仅记录”。	“拦截”

步骤9 单击“确认”，添加的地理位置访问控制规则展示在地理位置访问控制规则列表中。

- 若需要修改添加的地理位置访问控制规则时，可单击待修改的地理位置访问控制规则所在行的“修改”，修改地理位置访问控制规则。

- 若需要删除添加的地理位置访问控制规则时，可单击待删除的地理位置访问控制规则所在行的“删除”，删除地理位置访问控制规则。

----结束

配置示例-仅允许某一地区来源 IP 访问请求

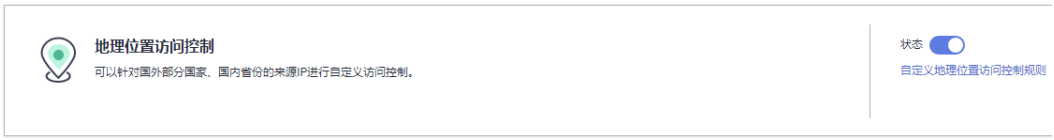
假如防护域名“www.example.com”已接入边缘安全，当您只允许某一地区的IP可以访问防护域名，例如，只允许来源“新加坡”地区的IP可以访问防护域名，请参照以下步骤处理。

步骤1 添加一条地理位置访问控制规则，添加“新加坡”地区的“放行”防护动作。

图 3-61 添加“放行”防护动作

步骤2 开启地理位置访问控制。

图 3-62 地理位置访问控制配置框



步骤3 配置一条精准访问防护规则，拦截所有的请求。

图 3-63 拦截所有访问请求

有关配置精准访问防护规则的详细介绍，请参见**配置精准访问防护规则**。

步骤4 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

当非“新加坡”地区的源IP访问页面时，将拦截该访问请求，拦截页面示例如**图3-64**所示。

图 3-64 拦截攻击请求

步骤5 返回边缘安全管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看到非“上海”地区的源IP都被拦截。

----结束

防护效果

假如已添加域名“www.example.com”。可参照以下步骤验证防护效果：

步骤1 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。

- 不能正常访问，参照章节**添加防护网站**重新完成域名接入。
- 能正常访问，执行**2**。

步骤2 参照**操作步骤**，将您的客户端IP来源地配置为拦截。

步骤3 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面，正常情况下，会阻断该来源地IP的访问请求，返回拦截页面。

----结束

3.4.3.9 配置网站反爬虫防护规则防御爬虫攻击

您可以通过配置网站反爬虫防护规则，防护搜索引擎、扫描器、脚本工具、其它爬虫等爬虫，以及自定义JS脚本反爬虫防护规则。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

约束条件

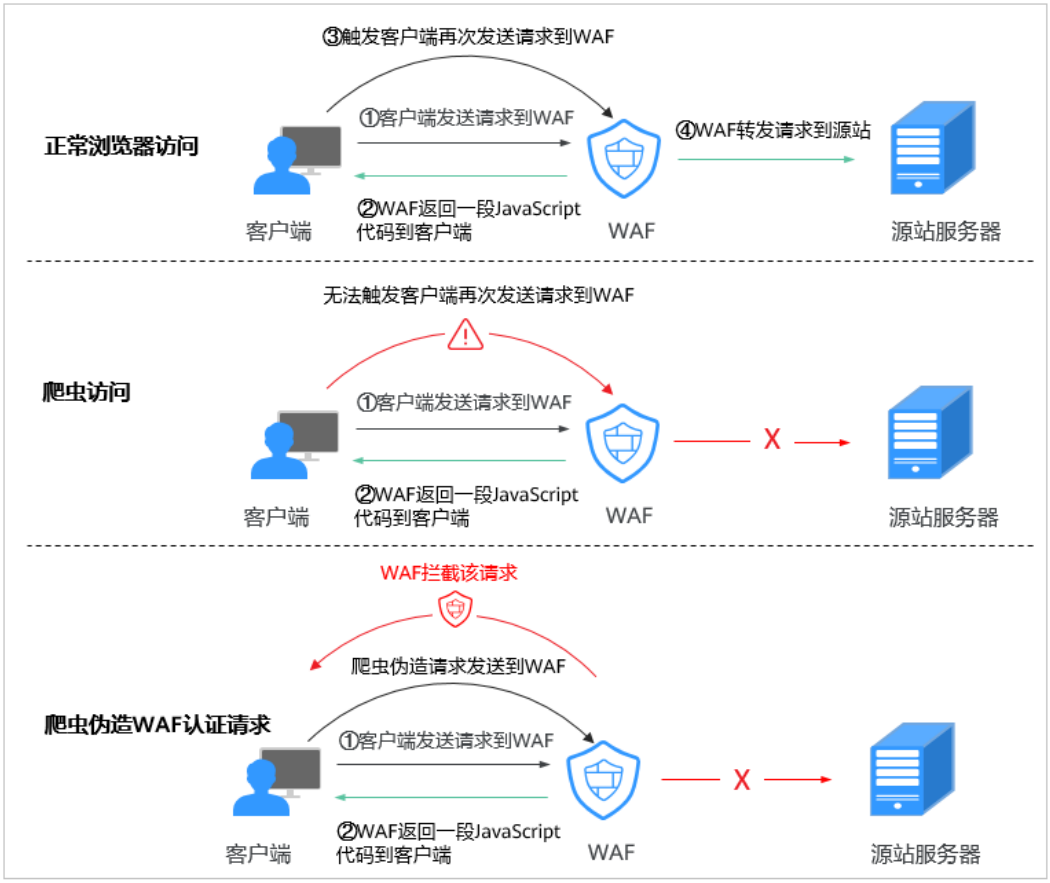
- 本功能依赖浏览器的Cookie机制、JavaScript解析能力，如果客户端浏览器不支持Cookie，此功能无法使用。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 如果您的业务接入了CDN服务，请谨慎使用此功能。

  由于CDN缓存机制的影响，网站反爬虫特性将无法达到预期效果，并且有可能造成页面访问异常。

JS 脚本反爬虫检测机制

JS脚本检测流程如**图3-65**所示，其中，①和②称为“js挑战”，③称为“js验证”。

图 3-65 JS 脚本检测流程说明



开启JS脚本反爬虫后，当客户端发送请求时，会返回一段JavaScript代码到客户端。

- 如果客户端是正常浏览器访问，就可以触发这段JavaScript代码再发送一次请求，即边缘安全完成js验证，并将该请求转发给源站。
- 如果客户端是爬虫访问，就无法触发这段JavaScript代码再发送一次请求，即边缘安全无法完成js验证。
- 如果客户端爬虫伪造了认证请求，发送到边缘安全时，会拦截该请求，js验证失败。

通过统计“js挑战”和“js验证”，就可以汇总出JS脚本反爬虫防御的请求次数。例如，图3-66中JS脚本反爬虫共记录了18次事件，其中，“js挑战”（EdgeSec返回JS代码）为16次，“js验证”（EdgeSec完成JS验证）为2次，“其他”（即爬虫伪造EdgeSec认证请求）为0次。

图 3-66 JS 脚本反爬虫防护数据

须知

“js挑战”和“js验证”的防护动作为仅记录，EdgeSec不支持配置“js挑战”和“js验证”的防护动作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

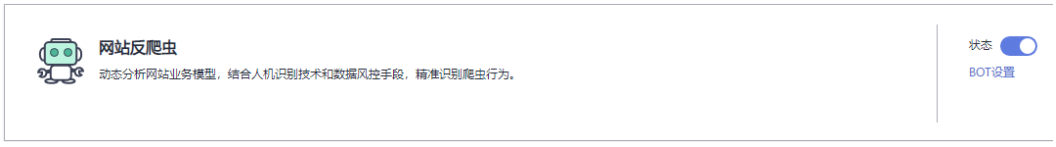
步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

图 3-67 网站列表

步骤6 在“网站反爬虫”配置框中，用户可根据自己的需要参照图3-68更改网站反爬虫的“状态”，单击“BOT设置”，进入网站反爬虫规则配置页面。

图 3-68 网站反爬虫配置框



步骤7 在“特征反爬虫”页签，根据您的业务场景，开启合适的防护功能，如图3-69所示，检测项说明如表3-20所示。

特征反爬虫规则提供了两种防护动作：

- 拦截
  发现攻击行为后立即阻断并记录。
- 仅记录
  默认防护动作，发现攻击行为后只记录不阻断攻击。

默认开启“扫描器”防护检测，用户可根据业务需要，配置防护动作并开启其他需要防护的检测类型。

图 3-69 特征反爬虫防护

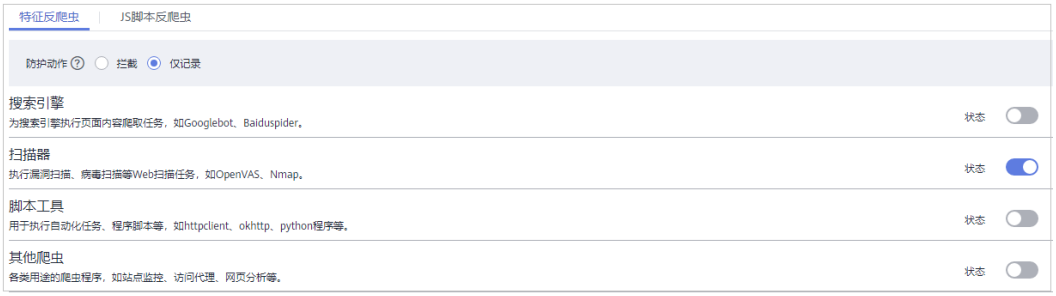


表 3-20 特征反爬虫检测项说明

检测项	说明	功能说明
搜索引擎	搜索引擎执行页面内容爬取任务，如Googlebot、Baiduspider。	开启后，EdgeSec将检测并阻断搜索引擎爬虫。 **说明** 如果不开启“搜索引擎”，EdgeSec针对谷歌和百度爬虫不会拦截，如果您希望拦截百度爬虫的POST请求，可参照**配置示例-搜索引擎**进行配置。
扫描器	执行漏洞扫描、病毒扫描等Web扫描任务，如OpenVAS、Nmap。	开启后，EdgeSec将检测并阻断扫描器爬虫。
脚本工具	用于执行自动化任务、程序脚本等，如httpclient、okhttp、python程序等。	开启后，EdgeSec将检测并阻断执行自动化任务、程序脚本等。 **说明** 如果您的应用程序中使用了httpclient、okhttp、python程序等脚本工具，建议您关闭“脚本工具”，否则，EdgeSec会将使用了httpclient、okhttp、python程序等脚本工具当成恶意爬虫，拦截该应用程序。

检测项	说明	功能说明
其他爬虫	各类用途的爬虫程序，如站点监控、访问代理、网页分析等。 **说明** “访问代理”是指当网站接入EdgeSec后，为避免爬虫被EdgeSec拦截，爬虫者使用大量IP代理实现爬虫的一种技术手段。	开启后，EdgeSec将检测并阻断各类用途的爬虫程序。

步骤8 选择“JS脚本反爬虫”页签，用户可根据业务需求更改JS脚本反爬虫的“状态”和“防护模式”。

默认关闭JS脚本反爬虫，单击  ，在弹出的“警告”提示框中，单击“确定”，开启JS脚本反爬虫  。

须知

- JS脚本反爬虫依赖浏览器的Cookie机制、JavaScript解析能力，如果客户端浏览器不支持Cookie，此功能无法使用，开启后会造成永远无法访问源站。
- 如果您的业务接入了CDN服务，请谨慎使用JS脚本反爬虫。

  由于CDN缓存机制的影响，JS脚本反爬虫特性将无法达到预期效果，并且有可能造成页面访问异常。

步骤9 根据业务配置JS脚本反爬虫规则，相关参数说明如表3-21所示。

JS脚本反爬虫规则提供了“防护所有请求”和“防护指定请求”两种防护动作。

- 除了指定请求规则以外，防护其他所有请求

  “防护模式”选择“防护所有请求”，单击“添加排除请求规则”，配置排除请求规则后，单击“确认”。

图 3-70 添加排除防护路径

- 只防护指定请求时

  “防护模式”选择“防护指定请求”，单击“添加请求规则”，配置请求规则后，单击“确认”。

图 3-71 添加请求规则

表 3-21 JS 脚本反爬虫参数说明

参数	参数说明	示例
规则名称	自定义规则名称。	EdgeSec
规则描述	可选参数，设置该规则的备注信息。	-
生效时间	立即生效。	立即生效
条件列表	条件设置参数说明如下： • 字段：在下拉列表中选择需要防护的字段，当前仅支持“路径”、“User Agent”。 • 子字段 • 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 **说明** 选择“包含任意一个”、“不包含所有”、“等于任意一个”、“不等于所有”、“前缀为任意一个”、“前缀不为所有”、“后缀为任意一个”或者“后缀不为所有”时，“内容”需要选择引用表名称，创建引用表的详细操作请参见**创建引用表**。 • 内容：输入或者选择条件匹配的内容。	“路径”包含“/admin/”
优先级	设置该条件规则检测的顺序值。如果您设置了多条规则，则多条规则间有先后匹配顺序，即访问请求将根据您设定的优先级依次进行匹配，优先级较小的规则优先匹配。	5

----结束

相关操作

- 若需要修改添加的JS脚本反爬虫规则，可单击待修改的路径规则所在行的“修改”，修改该规则。
- 若需要删除添加的JS脚本反爬虫规则时，可单击待删除的路径规则所在行的“删除”，删除该规则。

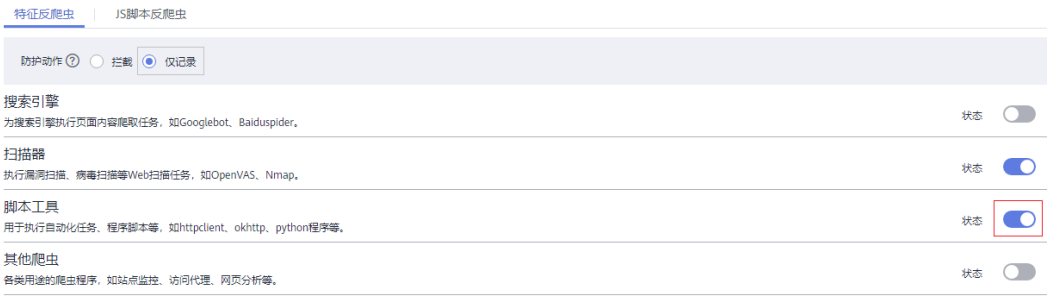
配置示例-仅记录脚本工具爬虫

假如防护域名“www.example.com”已接入EdgeSec，您可以参照以下操作步骤验证反爬虫防护效果。

步骤1 执行JS脚本工具，爬取网页内容。

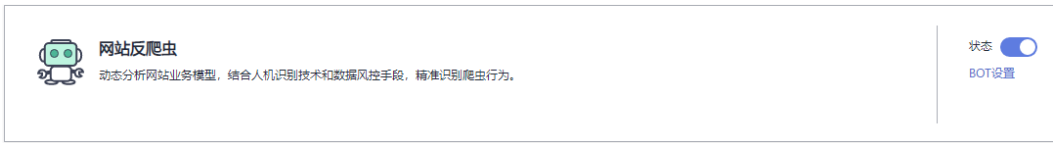
步骤2 在“特征反爬虫”页签，开启“脚本工具”，“防护动作”设置为“仅记录”（EdgeSec检测为攻击行为后，只记录不阻断）。

图 3-72 开启“脚本工具”



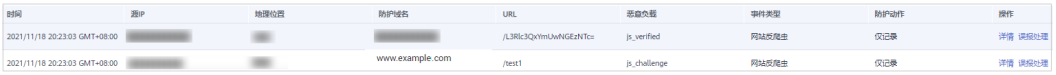
步骤3 开启网站反爬虫。

图 3-73 网站反爬虫配置框



步骤4 在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

图 3-74 查看防护事件-脚本爬虫



----结束

配置示例-搜索引擎

放行百度或者谷歌的搜索引擎，同时拦截百度的POST请求。

步骤1 参照**步骤6**将“搜索引擎”设置为放行，即将“搜索引擎”的“状态”设置为 。

步骤2 参照**配置精准访问防护规则**配置如**图3-75**的规则。

图 3-75 拦截 POST 请求

----结束

3.4.3.10 配置全局白名单规则忽略误报

当EdgeSec根据您配置的Web基础防护规则或自定义规则检测到符合规则的恶意攻击时，会按照规则中的防护动作对攻击事件进行处理。

对于误报情况，您可以添加白名单对误报进行忽略，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。

- “不检测模块”选择“所有检测模块”时：通过EdgeSec配置的其他所有的规则都不会生效，EdgeSec将放行该域名下的所有请求流量。
- “不检测模块”选择“Web基础防护模块”时：可根据选择的“不检测规则类型”，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

约束条件

- 当“不检测模块”配置为“所有检测模块”时，通过EdgeSec配置的其他所有的规则都不会生效，EdgeSec将放行该域名下的所有请求流量。
- 当“不检测模块”配置为“Web基础防护模块”时，仅对EdgeSec预置的Web基础防护规则和网站反爬虫的“特征反爬虫”拦截或记录的攻击事件可以配置全局白名单规则，防护规则相关说明如下：
  - Web基础防护规则

    防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击，以及Webshell检测、深度反逃逸检测等Web基础防护。
  - 网站反爬虫的“特征反爬虫”规则

    可防护搜索引擎、扫描器、脚本工具、其它爬虫等爬虫。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 您可以通过**处理误报事件**来配置全局白名单规则，处理误报事件后，您可以在全局白名单规则列表中查看该误报事件对应的全局白名单规则。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

图 3-76 网站列表

步骤6 在“全局白名单”配置框中，用户可根据自己的需要更改“状态”，单击“自定义全局白名单规则”，进入规则配置页面。

图 3-77 全局白名单配置框

步骤7 在“全局白名单”规则配置页面左上角，单击“添加规则”。

步骤8 添加全局白名单规则，参数说明如表3-22所示。

图 3-78 添加全局白名单规则

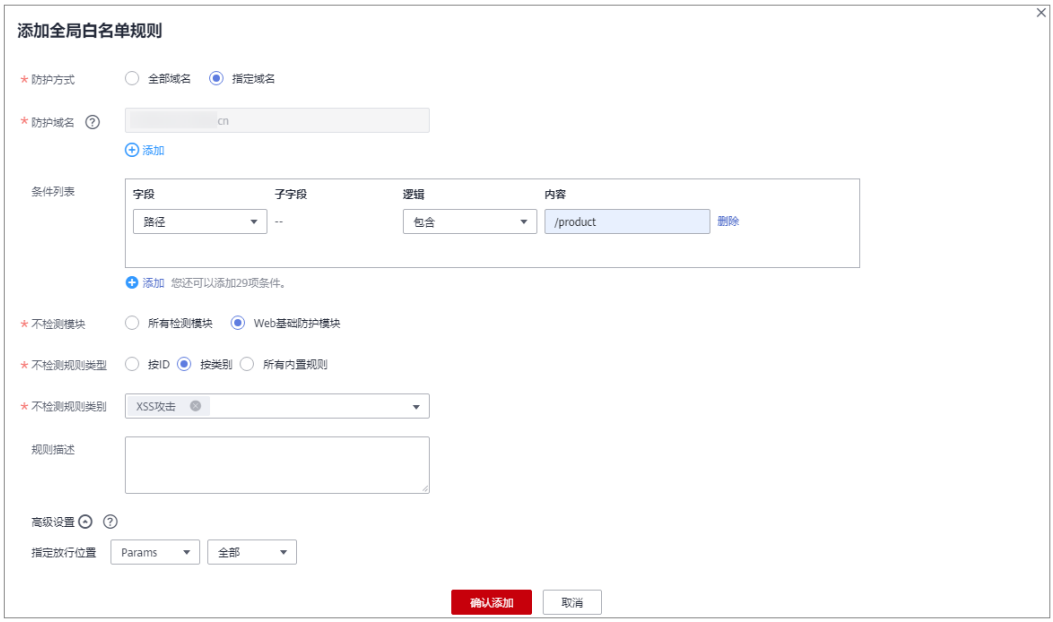


表 3-22 参数说明

参数	参数说明	取值样例
防护方式	• “全部域名”：默认防护当前策略下绑定的所有域名。 • “指定域名”：配置当前策略下需要防护的是泛域名对应的单域名。	指定域名
防护域名	“防护方式”选择“指定域名”时，需要配置此参数。 需要手动输入当前策略下绑定的需要防护的泛域名对应的单域名，且需要输入完整的域名。	www.example.com

参数	参数说明	取值样例
条件列表	单击“添加”增加新的条件，一个防护规则至少包含一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。 条件设置参数说明如下： ● 字段 ● 子字段：当字段选择“Params”、“Cookie”或者“Header”时，请根据实际使用需求配置子字段。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。 ● 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 ● 内容：输入或者选择条件匹配的内容。	“路径”包含“/product”
不检测模块	● “所有检测模块”：通过EdgeSec配置的其他所有的规则都不会生效，EdgeSec将放行该域名下的所有请求流量。 ● “Web基础防护模块”：选择此参数时，可根据选择的“不检测规则类型”，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。	Web基础防护模块
不检测规则类型	“不检测模块”选择“Web基础防护模块”时，您可以选择以下三种方式进行配置： ● 按类别：按攻击事件类别进行配置，如：XSS、SQL注入等。一个类别会包含一个或者多个规则id。 ● 所有内置规则：**Web基础防护规则**里开启的所有防护规则。	按类别
不检测规则类别	当“不检测规则类型”选择“按类别”时，需要配置此参数。 在下拉框中选择事件类别。 EdgeSec支持的防护事件类别有：XSS攻击、网站木马、其他类型攻击、SQL注入攻击、恶意爬虫、远程文件包含、本地文件包含、命令注入攻击。	SQL注入攻击
规则描述	可选参数，设置该规则的备注信息。	不拦截SQL注入攻击

参数	参数说明	取值样例
高级设置	如果您只想忽略来源于某攻击事件下指定字段的攻击，可在“高级设置”里选择指定字段进行配置，配置完成后，EdgeSec将不再拦截指定字段的攻击事件。 在左边第一个下拉列表中选择目标字段。支持的字段有：Params、Cookie、Header、Body、Multipart。 ● 当选择“Params”、“Cookie”或者“Header”字段时，可以配置“全部”或根据需求配置子字段。 ● 当选择“Body”或“Multipart”字段时，可以配置“全部”。 ● 当选择“Cookie”字段时，“防护域名”和“路径”可以为空。 **说明** 当字段配置为“全部”时，配置完成后，EdgeSec将不再拦截该字段的所有攻击事件。	Params 全部

步骤9 单击“确认添加”。

----结束

相关操作

- 若需要修改添加的全局白名单规则时，可单击待修改的全局白名单规则所在行的“修改”，修改全局白名单规则。
- 若需要删除添加的**全局白名单**规则时，可单击待删除的全局白名单规则所在行的“删除”，删除全局白名单规则。

3.4.3.11 配置隐私屏蔽规则

您可以通过EdgeSec配置隐私屏蔽规则。隐私信息屏蔽，避免用户的密码等信息出现在事件日志中。

前提条件

已添加防护网站，详情操作请参见**添加防护网站** 。

约束条件

添加或修改防护规则后，规则生效需要几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。

系统影响

配置隐私屏蔽规则后，防护事件中将屏蔽敏感数据，防止用户隐私泄露。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

图 3-79 网站列表

步骤6 在“隐私屏蔽”配置框中，用户可根据自己的需要更改“状态”，单击“自定义隐私屏蔽规则”，进入隐私屏蔽规则配置页面。

图 3-80 隐私设置配置框

步骤7 在“隐私屏蔽”规则配置页面左上角，单击“添加规则”。

步骤8 添加隐私屏蔽规则，根据表3-23配置参数。

图 3-81 添加隐私屏蔽规则

表 3-23 添加隐私屏蔽规则参数说明

参数	参数说明	取值样例
路径	完整的URL链接，不包含域名。 ● 前缀匹配：以*结尾代表以该路径为前缀。例如，需要防护的路径为“/admin/test.php”或“/adminabc”，则路径可以填写为“/admin*”。 ● 精准匹配：需要防护的路径需要与此处填写的路径完全相等。例如，需要防护的路径为“/admin”，该规则必须填写为“/admin”。 **说明** ● 该路径不支持正则，仅支持前缀匹配和精准匹配的逻辑。 ● 路径里不能含有连续的多条斜线的配置，如“///admin”，访问时，引擎会将“///”转为“/”。	/admin/login.php 例如：需要防护的URL为“http://www.example.com/admin/login.php”，则“路径”设置为“/admin/login.php”。
屏蔽字段	设置为屏蔽的字段。 ● Params：请求参数。 ● Cookie：根据Cookie区分的Web访问者。 ● Header：自定义HTTP首部。 ● Form：表单参数。	● “屏蔽字段”为“Params”时，屏蔽字段名请根据实际使用需求设置，如果设置为“id”，设置后，与“id”匹配的内容将被屏蔽。 ● “屏蔽字段”为“Cookie”时，屏蔽字段名请根据实际使用需求设置，如果设置为“name”，设置后，与“name”匹配的内容将被屏蔽。
屏蔽字段名	根据“屏蔽字段”设置字段名，被屏蔽的字段将不会出现在日志中。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。	
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 单击“确认”，添加的隐私屏蔽规则展示在隐私屏蔽规则列表中。

----结束

相关操作

- 若需要修改添加的隐私屏蔽规则时，可单击待修改的隐私屏蔽规则所在行的“修改”，修改隐私屏蔽规则。
- 若需要删除添加的隐私屏蔽规则时，可单击待删除的隐私屏蔽规则所在行的“删除”，删除隐私屏蔽规则。

配置示例-屏蔽 Cookie 字段

假如防护域名“www.example.com”已接入EdgeSec，您可以参照以下操作步骤验证屏蔽Cookie字段名“jsessionid”防护效果。

步骤1 添加一条隐私屏蔽规则。

图 3-82 添加“jsessionid”字段名隐私屏蔽规则

步骤2 开启隐私屏蔽。

图 3-83 隐私设置配置框

步骤3 在左侧导航树中，单击“防护事件”，进入“防护事件”页面。

步骤4 在目标防护事件所在行的“操作”列中，单击“详情”，查看事件详细信息。

该防护事件的Cookie字段名“jsessionid”信息被屏蔽。

图 3-84 查看防护事件-隐私屏蔽

----结束

3.5 地址组管理

3.5.1 添加黑白名单 IP 地址组

IP地址组集中管理IP地址或网段，被黑白名单规则引用时可以批量设置IP/IP地址段。

约束条件

- 添加IP地址组时，请确保IP/IP地址段未添加到其他IP地址组，重复添加同一IP/IP地址段会导致添加IP地址组失败。

规格限制

- 每个用户可以拥有50个地址组。1个地址组可以添加200个IP地址/IP地址段。
- 添加地址组前，请确保当前版本有剩余的IP黑白名单规则配额。

  说明

  - 您可以参见**配置IP黑白名单规则规则拦截/放行指定IP**，查看当前IP黑白名单规则配额。
  - 如果您当前版本的IP黑白名单防护规则条数不能满足要求时，您可以通过购买规则扩展包或升级版本增加IP黑白名单防护规则条数，以满足的防护配置需求。一个规则扩展包包含10条IP黑白名单防护规则。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“地址组管理”，进入“地址组管理”页面。

步骤5 在“我的地址组”列表左上方，单击“添加地址组”。

步骤6 在弹出的“添加地址组”对话框中，输入“地址组名称”和“IP/IP段”，如图 添加地址组所示。

图 3-85 添加地址组

说明

- 多个IP地址/IP地址段以英文逗号分隔，输入时不支持换行。
- 支持配置200个IP地址/IP地址段。

步骤7 单击“确认”， 地址组创建成功。

----结束

3.5.2 修改或删除黑白名单 IP 地址组

您可以通过修改或删除IP地址，管理IP地址组信息。

前提条件

已成功创建地址组。

约束条件

- 修改IP地址组时，请确保IP地址组中的IP/IP地址段未添加到其他IP地址组，重复添加同一IP/IP地址段会导致添加IP地址组失败。
- 如果地址组已被黑白名单规则引用，删除地址组前需要解除该地址组与黑白名单规则的绑定关系。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“地址组管理”，进入“地址组管理”页面。

步骤5 在地址组列表中，查看地址组信息。

表 3-24 参数说明

参数名称	参数说明
地址组名称	用户自定义的地址组名称。
IP/IP段	地址组添加的IP地址/IP地址段。
应用规则	引用地址组的防护规则。
备注	地址组补充信息。

步骤6 修改或删除IP地址组。

- 修改地址组

  在目标地址组所在行的“操作”列中，单击“修改”，在弹出的“修改地址组”对话框中，修改地址组名称或IP地址/IP地址段后，单击“确认”。

- 删除地址组

  在目标地址组所在行的“操作”列中，单击“删除”，在弹出的提示框中，单击“确认”。

----结束

3.6 DDoS 攻击监控

业务接入后，您可以查看DDoS攻击防护信息，了解当前业务的安全状态。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 边缘安全”。

步骤3 在左侧导航栏选择“安全防护”，进入“安全防护”的“安全总览”页面。

步骤4 在左侧导航栏选择“DDoS攻击监控”，进入“概览”页面。

步骤5 在页面上方，查看DDoS攻击防护日志，参数说明如表 DDoS攻击参数说明所示。

表 3-25 DDoS 攻击参数说明

参数	说明
攻击流量带宽峰值	租户指定时间段内受到攻击的最大流量带宽值。

说明

在防护日志页面的流量或报文的图表中，不同的查询时间间隔对应的展示粒度不同，具体如下：

- 查询时间≤3天：展示粒度为1分钟。
- 3天＜查询时间≤30天：展示粒度为1小时。

----结束

4 权限管理

4.1 创建用户组并授权使用 EdgeSec

如果您需要对您所拥有的边缘安全（Edge Security，EdgeSec）进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用EdgeSec资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将EdgeSec资源委托给更专业、高效的其他华为账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用EdgeSec服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图 给用户授权服务权限流程**所示。

前提条件

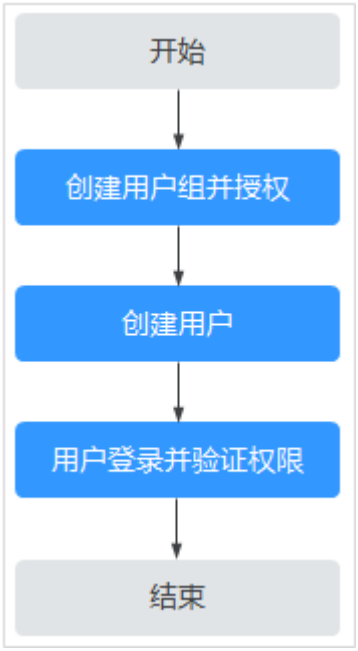
给用户组授权之前，请您了解用户组可以添加的EdgeSec权限，并结合实际需求进行选择，EdgeSec支持的系统权限如**表 EdgeSec系统角色**所示。

表 4-1 EdgeSec 系统角色

系统角色/策略名称	描述	类别	依赖关系
EdgeSec FullAccess	边缘安全服务所有权限	系统策略	无。
EdgeSec ReadOnlyAccess	边缘安全服务只读权限	系统策略	

示例流程

图 4-1 给用户授权服务权限流程



1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予边缘安全权限“EdgeSec FullAccess”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限
   新创建的用户登录控制台，切换至授权区域，验证权限：
   在“服务列表”中选择除边缘拿全外（假设当前策略仅包含“EdgeSec FullAccess”）的任一服务，若提示权限不足，表示“EdgeSec FullAccess”已生效。

5 云审计服务支持的关键操作

5.1 云审计服务支持的 EdgeSec 操作列表

云审计服务（Cloud Trace Service，CTS）记录了边缘安全相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务用户指南》。

云审计服务支持的EdgeSec操作列表如**表 云审计服务支持的EdgeSec操作列表**所示。

表 5-1 云审计服务支持的 EdgeSec 操作列表

操作名称	资源类型	事件名称
添加cdn域名调度任务	cdnDomainScheduleTask	addCdnDomainScheduleTask
用户添加防护的域名	bsgDomainName	addBsgDomainName
用户删除防护的域名信息	bsgDomainName	deleteBsgDomainName
用户修改防护的域名信息	bsgDomainName	updateBsgDomainName
用户开通服务	serviceInfo	addServiceInfo
用户退订服务	serviceInfo	deleteServiceInfo
添加ddos防护域名	ddosDomainNames	addEdgeDDosDomainNames
删除ddos防护域名	ddosDomainNames	deleteEdgeDDosDomainNames
更新ddos防护域名	ddosDomainNames	updateEdgeDDosDomainNames
创建脚本反爬虫规则	EdgeSecAntiCrawlerRule	createEdgeSecAntiCrawlerRule
删除脚本反爬虫规则	EdgeSecAntiCrawlerRule	deleteEdgeSecAntiCrawlerRule

操作名称	资源类型	事件名称
修改脚本反爬虫防护模式	EdgeSecAntiCrawlerRule	switchEdgeSecAntiCrawlerRule
更新脚本反爬虫规则	EdgeSecAntiCrawlerRule	updateEdgeSecAntiCrawlerRule
创建cc规则	EdgeSecCcRule	createEdgeSecCcRule
删除cc规则	EdgeSecCcRule	deleteEdgeSecCcRule
更新cc规则	EdgeSecCcRule	updateEdgeSecCcRule
创建证书	EdgeSecCertificate	createEdgeSecCertificate
删除证书	EdgeSecCertificate	deleteEdgeSecCertificate
更新证书	EdgeSecCertificate	updateEdgeSecCertificate
创建精准防护规则	EdgeSecCustomRule	createEdgeSecCustomRule
删除精准防护规则	EdgeSecCustomRule	deleteEdgeSecCustomRule
更新精准防护规则	EdgeSecCustomRule	updateEdgeSecCustomRule
创建防护域名	EdgeSecDomain	createEdgeSecDomain
删除防护域名	EdgeSecDomain	deleteEdgeSecDomain
更新防护域名	EdgeSecDomain	updateEdgeSecDomain
创建地理位置规则	EdgeSecGeoIpRule	createEdgeSecGeoIpRule
删除地理位置规则	EdgeSecGeoIpRule	deleteEdgeSecGeoIpRule
更新地理位置规则	EdgeSecGeoIpRule	updateEdgeSecGeoIpRule
创建误报屏蔽规则	EdgeSecIgnoreRule	createEdgeSecIgnoreRule
删除误报屏蔽规则	EdgeSecIgnoreRule	deleteEdgeSecIgnoreRule
重置误报屏蔽规则	EdgeSecIgnoreRule	recountEdgeSecIgnoreRule
更新误报屏蔽规则	EdgeSecIgnoreRule	updateEdgeSecIgnoreRule
创建IP地址组	EdgeSecIpGroup	CreateEdgeSecIpGroup
删除IP地址组	EdgeSecIpGroup	DeleteEdgeSecIpGroup
更新IP地址组	EdgeSecIpGroup	UpdateEdgeSecIpGroup
更新防护策略的域名	EdgeSecPolicy	applyEdgeSecPolicy

操作名称	资源类型	事件名称
创建防护策略	EdgeSecPolicy	createEdgeSecPolicy
删除防护策略	EdgeSecPolicy	deleteEdgeSecPolicy
更新防护策略	EdgeSecPolicy	updateEdgeSecPolicy
创建隐私屏蔽规则	EdgeSecPrivacyMaskRule	createEdgeSecPrivacyMaskRule
删除隐私屏蔽规则	EdgeSecPrivacyMaskRule	deleteEdgeSecPrivacyMaskRule
更新隐私屏蔽规则	EdgeSecPrivacyMaskRule	updateEdgeSecPrivacyMaskRule
创建攻击惩罚规则	EdgeSecPunishmentRule	createEdgeSecPunishmentRule
删除攻击惩罚规则	EdgeSecPunishmentRule	deleteEdgeSecPunishmentRule
更新攻击惩罚规则	EdgeSecPunishmentRule	updateEdgeSecPunishmentRule
创建引用表	EdgeSecValueList	createEdgeSecValueList
删除引用表	EdgeSecValueList	deleteEdgeSecValueList
更新引用表	EdgeSecValueList	updateEdgeSecValueList
创建IP黑白名单规则	EdgeSecWhiteBlackIpRule	createEdgeSecWhiteBlackIpRule
删除IP黑白名单规则	EdgeSecWhiteBlackIpRule	deleteEdgeSecWhiteBlackIpRule
更新IP黑白名单规则	EdgeSecWhiteBlackIpRule	updateEdgeSecWhiteBlackIpRule

5.2 查看云审计日志

开启了云审计服务后，系统开始记录EdgeSec资源的操作。云审计服务管理控制台保存最近7天的操作记录。

查看审计日志的详细操作请参见**查看审计事件**。

6 监控

6.1 EdgeSec 监控指标说明

功能说明

本节定义了边缘安全上报云监控服务的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控服务提供管理控制台或API接口来检索边缘安全产生的监控指标和告警信息。

命名空间

SYS.EdgeSec

说明

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务，也能够互不干扰。

监控指标

表 6-1 EdgeSec 支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
requests	请求量	该指标用于统计测量对象近5分钟内EdgeSec返回的请求量的总数。 单位：次 采集方式：统计防护域名请求量的总数	≥0 次 值类型：Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
EdgeSec_http_2xx	EdgeSec返回码（2XX）	该指标用于统计测量对象近5分钟内EdgeSec返回的2XX状态码的数量。 单位：次 采集方式：统计EdgeSec引擎返回的2XX系列状态响应码的数量	≥0 次 值类型：Float	防护域名	5分钟
EdgeSec_http_3xx	EdgeSec返回码（3XX）	该指标用于统计测量对象近5分钟内EdgeSec返回的3XX状态码的数量。 单位：次 采集方式：统计EdgeSec引擎返回的3XX系列状态响应码的数量	≥0 次 值类型：Float	防护域名	5分钟
EdgeSec_http_4xx	EdgeSec返回码（4XX）	该指标用于统计测量对象近5分钟内EdgeSec返回的4XX状态码的数量。 单位：次 采集方式：统计EdgeSec引擎返回的4XX系列状态响应码的数量	≥0 次 值类型：Float	防护域名	5分钟
EdgeSec_http_5xx	EdgeSec返回码（5XX）	该指标用于统计测量对象近5分钟内EdgeSec返回的5XX状态码的数量。 单位：次 采集方式：统计EdgeSec引擎返回的5XX系列状态响应码的数量	≥0 次 值类型：Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
EdgeSec_fused_counts	EdgeSec熔断量	该指标用于统计测量对象近5分钟内被EdgeSec熔断保护的请求数量。 单位：次 采集方式：统计防护域名被熔断保护的请求数量	≥0 次 值类型：Float	防护域名	5分钟
inbound_traffic	入网总流量	该指标用于统计测量对象近5分钟内总入带宽的大小。 单位：Mbit 采集方式：统计近5分钟内总入带宽的大小	≥0 Mbit 值类型：Float	防护域名	5分钟
outbound_traffic	出网总流量	该指标用于统计测量对象近5分钟内总出带宽的大小。 单位：Mbit 采集方式：统计近5分钟内总出带宽的大小	≥0 Mbit 值类型：Float	防护域名	5分钟
EdgeSec_process_time_0	EdgeSec处理时延-区间[0-10ms)	该指标用于统计测量对象近5分钟内EdgeSec处理时延在区间[0-10ms)内的总数量 单位：次 采集方式：统计近5分钟内EdgeSec处理时延在区间[0-10ms)内的总数量	≥0 次 值类型：Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
EdgeSec_process_time_10	EdgeSec处理时延-区间[10-20ms)	该指标用于统计测量对象近5分钟内EdgeSec处理时延在区间[10-20ms)内的总数量 单位：次 采集方式：统计近5分钟内EdgeSec处理时延在区间[10-20ms)内的总数量	≥0 次 值类型：Float	防护域名	5分钟
EdgeSec_process_time_20	EdgeSec处理时延-区间[20-50ms)	该指标用于统计测量对象近5分钟内EdgeSec处理时延在区间[20-50ms)内的总数量 单位：次 采集方式：统计近5分钟内EdgeSec处理时延在区间[20-50ms)内的总数量	≥0 次 值类型：Float	防护域名	5分钟
EdgeSec_process_time_50	EdgeSec处理时延-区间[50-100ms)	该指标用于统计测量对象近5分钟内EdgeSec处理时延在区间[50-100ms)内的总数量 单位：次 采集方式：统计近5分钟内EdgeSec处理时延在区间[50-100ms)内的总数量	≥0 次 值类型：Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
EdgeSec_process_time_100	EdgeSec处理时延-区间[100-1000ms)	该指标用于统计测量对象近5分钟内EdgeSec处理时延在区间[100-1000ms)内的总数量 单位：次 采集方式：统计近5分钟内EdgeSec处理时延在区间[100-1000ms)内的总数量	≥0 次 值类型：Float	防护域名	5分钟
EdgeSec_process_time_1000	EdgeSec处理时延-区间[1000+ms)	该指标用于统计测量对象近5分钟内EdgeSec处理时延在区间[1000+ms)内的总数量 单位：次 采集方式：统计近5分钟内EdgeSec处理时延在区间[1000+ms)内的总数量	≥0 次 值类型：Float	防护域名	5分钟
qps_peak	QPS峰值	该指标用于统计近5分钟内防护域名的QPS峰值 单位：次 采集方式：统计近5分钟内防护域名的QPS峰值	≥0 次 值类型：Float	防护域名	5分钟
qps_mean	QPS均值	该指标用于统计近5分钟内防护域名的QPS均值 单位：次 采集方式：统计近5分钟内防护域名的QPS均值	≥0 次 值类型：Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
EdgeSec_http_0	无返回的EdgeSec状态码	该指标用于统计测量对象近5分钟内EdgeSec无返回的状态响应码的数量 单位：次 采集方式：统计近5分钟内EdgeSec无返回的状态响应码的数量	≥0 次 值类型：Float	防护域名	5分钟
upstream_code_2xx	业务返回码（2XX）	该指标用于统计测量对象近5分钟内业务返回的2XX系列状态响应码的数量 单位：次 采集方式：统计近5分钟内业务返回的2XX系列状态响应码的数量	≥0 次 值类型：Float	防护域名	5分钟
upstream_code_3xx	业务返回码（3XX）	该指标用于统计测量对象近5分钟内业务返回的3XX系列状态响应码的数量 单位：次 采集方式：统计近5分钟内业务返回的3XX系列状态响应码的数量	≥0 次 值类型：Float	防护域名	5分钟
upstream_code_4xx	业务返回码（4XX）	该指标用于统计测量对象近5分钟内业务返回的4XX系列状态响应码的数量 单位：次 采集方式：统计近5分钟内业务返回的4XX系列状态响应码的数量	≥0 次 值类型：Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
upstream_code_5xx	业务返回码（5XX）	该指标用于统计近5分钟内业务返回的5XX系列状态响应码的数量 单位：次 采集方式：统计近5分钟内业务返回的5XX系列状态响应码的数量	≥0 次 值类型：Float	防护域名	5分钟
upstream_code_0	无返回的业务状态码	该指标用于统计测量对象近5分钟内业务无返回的状态响应码的数量 单位：次 采集方式：统计近5分钟内业务无返回的状态响应码的数量	≥0 次 值类型：Float	防护域名	5分钟
inbound_traffic_peak	入网流量的峰值	该指标用于统计近5分钟内防护域名入网流量的峰值 单位：Mbit/s 采集方式：统计近5分钟内防护域名入网流量的峰值	≥0 Mbit/s 值类型：Float	防护域名	5分钟
inbound_traffic_mean	入网流量的均值	该指标用于统计近5分钟内防护域名入网流量的均值 单位：Mbit/s 采集方式：统计近5分钟内防护域名入网流量的均值	≥0 Mbit/s 值类型：Float	防护域名	5分钟
outbound_traffic_peak	出网流量的峰值	该指标用于统计近5分钟内防护域名出网流量的峰值 单位：Mbit/s 采集方式：统计近5分钟内防护域名出网流量的峰值	≥0 Mbit/s 值类型：Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
outbound_traffic_mean	出网流量的均值	该指标用于统计近5分钟内防护域名出网流量的均值 单位：Mbit/s 采集方式：统计近5分钟内防护域名出网流量的均值	≥0 Mbit/s 值类型：Float	防护域名	5分钟
attacks	攻击总次数	该指标用于统计近5分钟内防护域名攻击请求量的总数 单位：次 采集方式：统计近5分钟内防护域名攻击请求量的总数	≥0 次 值类型：Float	防护域名	5分钟
crawlers	爬虫攻击次数	该指标用于统计近5分钟内防护域名爬虫攻击请求量的总数 单位：次 采集方式：统计近5分钟内防护域名爬虫攻击请求量的总数	≥0 次 值类型：Float	防护域名	5分钟
base_protection_counts	web基础防护次数	该指标用于统计近5分钟内由Web基础防护规则防护的攻击数量 单位：次 采集方式：统计近5分钟内由Web基础防护规则防护的攻击数量	≥0 次 值类型：Float	防护域名	5分钟
precise_protection_counts	精准防护次数	该指标用于统计近5分钟内由精准防护规则防护的攻击数量 单位：次 采集方式：统计近5分钟内由精准防护规则防护的攻击数量	≥0 次 值类型：Float	防护域名	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
cc_protection_counts	cc防护次数	该指标用于统计近5分钟内由CC防护规则防护的攻击数量。 单位：次 采集方式：统计近5分钟内由CC防护规则防护的攻击数量。	≥0 次 值类型：Float	防护域名	5分钟

维度

Key	Value
instance_id	EdgeSec独享引擎实例ID
EdgeSec_instance_id	EdgeSec防护网站ID

监控指标原始数据格式样例

```
[
  {
    "metric": {
      // 命名空间
      "namespace": "SYS.EdgeSec",
      "dimensions": [
        {
          // 维度名称，例如防护网站
          "name": "EdgeSec_instance_id",
          // 该维度下的监控对象ID，例如防护网站ID
          "value": "082db2f542e0438aa520035b3e99cd99"
        }
      ],
      // 指标ID
      "metric_name": "EdgeSec_http_2xx"
    },
    // 生存时间，指标预定义
    "ttl": 172800,
    // 指标值
    "value": 0.0,
    // 指标单位
    "unit": "Count",
    // 指标值类型
    "type": "float",
    // 指标采集时间
    "collect_time": 1637677359778
  }
]
```

6.2 设置监控告警规则

通过设置EdgeSec告警规则，用户可自定义监控目标与通知策略，设置告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助您及时了解EdgeSec防护状况，从而起到预警作用。

前提条件

防护域名已接入EdgeSec。

操作步骤

步骤1 单击页面左上方的 ☰，选择“管理与监管 > 云监控服务 CES”。

步骤2 在左侧导航树栏，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤3 在页面右上方，单击“创建告警规则”，进入“创建告警规则”界面。

步骤4 根据界面提示配置参数，关键参数如下，更多参数信息请参见**创建告警规则和通知**：

- 告警类型：指标
- 资源类型：边缘安全
- 维度：边缘DDoS

图 6-1 EdgeSec 监控告警规则

步骤5 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

6.3 查看监控指标

您可以通过管理控制台，查看EdgeSec的相关指标，及时了解EdgeSec防护状况，并通过指标设置防护策略。

前提条件

EdgeSec已对接云监控，即已在云监控页面设置监控告警规则。有关设置监控告警规则的详细操作，请参见**设置监控告警规则**。

操作步骤

步骤1 单击页面左上方的 ☰，选择“管理与监管 > 云监控服务 CES”。

步骤2 在左侧导航树栏，选择“云服务监控 > 边缘安全”，进入“云服务监控”页面。

步骤3 在目标EdgeSec实例所在行的“操作”列中，单击“查看监控指标”，查看对象的指标详情。

----结束

7 修订记录

发布日期	修改记录
2024-05-24	第六次正式发布。 优化： 全文架构调整，分为“站点加速”和“安全防护”章节。
2024-01-25	第五次正式发布。 新增： **配置精准访问防护规则**章节中，仅允许某一地区来源IP访问请求的配置示例 优化： ● **DDoS攻击监控**章节中，参数名称及说明。 ● **设置监控告警规则**章节中，配置步骤及参数。 删除： **开通边缘安全**章节中，区域参数。
2023-12-05	第四次正式发布。 删除： ● DDoS防护中概览页章节。 ● 管理全量日志章节中，DDoS日志字段。
2023-10-31	第三次正式发布。 优化： **开通边缘安全**。
2023-08-08	第二次正式发布。 新增： ● 管理边缘安全和管理边缘DDoS中增加企业项目信息。 ● 管理全量日志。 ● 管理项目和企业。
2023-03-30	第一次正式发布。