百度智能云

WAF 文档

目录

目录 2
产品描述 4
介绍 4
核心概念 4
功能 4
优势 5
应用场景 6
产品定价 6
操作指南 7
接入管理 7
CDN-WAF-概述 7
BLB-WAF概述 9
SAAS-WAF概述 11
配置自定义TLS 13
开启IPv6防护 14
WAF回源及回源保护 14
安全运营 16
查看数据报表 16
攻击日志 16
访问概览 18
防护配置 20
防护配置概述 20
基础Web防护引擎 23
CC防护配置 27
自定义访问控制策略 28
访问频率限制 30
防篡改功能设置 32
IP黑白名单 34
BOT 功能设置 35
自定义拦截页面 42
日志投递 44
信息泄露防护 45
Web 应用集成SDK 46
报警设置 49
API参考 52
概述 52
使用须知 53
API服务域名 54
调用规范 54
错误返回 55

WAF数据报表相关接口 57
BLB-WAF-API 61
CDN-WAF-API 74
附录 82
更新历史 85
常见问题 85
Web攻击分类说明 85
如何获取近6个月攻击拦截日志 86
告警无法关闭 86
服务等级协议 SLA 86
应用防火墙服务等级协议 SLA 86

产品描述

介绍

什么是 Web 应用防火墙

Web应用防火墙（Web Application Firewall，简称WAF）是百度智能云面向用户提供的Web安全防护产品，能够有效防护各种Web攻击，协助用户定制访问规则，提升网站等业务的安全。独创的全新WAF技术架构体系，能够将WAF实例灵活部署在各个Web业务入口，避免了传统云WAF架构下黑客绕过代理直攻源站的尴尬。云端安全大数据能力的集成也让WAF能更有效更快捷的帮助客户提升网站安全性与可用性。

如果要使用Web应用防火墙（WAF）防护您的Web业务，您必须先将Web业务接入WAF。百度WEB应用防火墙支持云原生WAF和SAAS WAF两种接入方式，您可以根据Web业务的部署特征，选择合适的接入方式。

下方表格通过实现原理、推荐场景、接入对象和接入方式的对比，介绍云原生WAF和SAAS WAF接入。

类型	云原生BLB WAF接入	SAAS WAF或云防护接入
实现原理	WAF应用防火墙 通过和百度云负载均衡服务（Baidu Load Balance，简称 BLB）进行联动，对 BLB 监听上的 HTTP/HTTPS 流量进行分析识别，对攻击流量拦截，实现对网站应用的安全防护。 该过程中，WAF不参与流量转发，避免因额外引入一层转发而带来各种兼容性和稳定性问题。	通过添加域名，通过 DNS 解析，将域名解析到百度云 WAF 服务提供的 CNAME 地址上，从而实现访问流量先经过 WAF 节点安全防护再回源站的业务模式。百度云 WAF 在其中对 HTTP/HTTPS 流量进行攻击识别和过滤，将正常流量回源到源站，保护源站的安全。
推荐场景	业务服务器部署在百度云，Web业务已启用百度云负载均衡服务 BLB，建议您选择该接入方式。	业务服务器部署在百度云或非百度云，可选择SAAS WAF或云防护接入方式。
接入对象	部署在BLB的实例上的所有域域名	Web 业务域名
接入方式	在BLB控制台，为实例或域名开启WAF防护。 详细接入操作：BLB-WAF概述	1.接入域名并完成监听配置、转发配置 2.修改域名的DNS解析记录 3.配置防护策略 详细接入操作：SAAS-WAF概述（云防护同SAAS-WAF操作）

核心概念

WAF

Web应用防火墙（Web Application Firewall），简称WAF。

Web攻击

针对Web应用发起的攻击，包括但不限于以下攻击类型：SQL注入、XSS跨站、Webshell上传、命令注入、非法HTTP协议请求、非授权文件访问等。

功能

主要功能

功能	简介
Web攻击防护	基于各种安全AI分析能力，快速精准有效的防御常见Web攻击，如SQL注入、非授权访问、XSS跨站脚本、CSRF跨站请求伪造，Webshell、木马等等
0day漏洞虚拟补丁	百度安全工程师实时监控互联网各种安全讯息，对于高危0day漏洞防，会第一时间更新防御策略，为客户打上虚拟补丁，大大降低客户被攻击的影响，为企业争取漏洞修复时间
网页防篡改	用户可设置将核心网页内容缓存云端，实现网页替身效果，防止网页篡改给企业带来负面影响
CC攻击防护	智能CC防护，针对业务真实流量的学习、分析和监控，智能化的生成针对性防御策略，高效缓解CC攻击问题
BOT识别	基于AI智能评估的BOT机器人识别功能，协助企业规避恶意BOT行为，降低业务风险
支持旁路观察模式	设置旁路观察模式，对于攻击只记录不阻断，客户方便评估总定义等多种规则在实际业务中的工作情况
精准的访问控制	用户可以对多种HTTP字段进行组合匹配形成自己业务等定制规则，支持简单的逻辑语法

优势

多种接入防护方式

支持云原生 WAF 和 SAAS WAF 两种模式，供客户按需使用。可以根据自己需求将 WAF 实例部署到您的云上IT网络架构中去的。

- 云原生 WAF：一键绑定百度云负载均衡的 HTTP/HTTPS 监听，实现精准域名 web 流量检测和威胁清洗。
- SAAS WAF：通过 CNAME 的方式接入，隐藏用户真实源站，返回干净业务流量，能够覆盖百度云上和云下的各种场景。

AI 安全规则引擎准确有效

- 全面覆盖 OWASP Top10 Web 攻击类型，对于 SQL 注入、非授权访问、XSS 跨站脚本、CSRF 跨站请求伪造、命令行注入等攻击，有很好的防御效果。同时引入百度 AI 规则引擎，对于请求能够联系上下文、交叉分析验证、行为分析，对于 0day 攻击及其它新型未知攻击有着较好的防御效果。
- 基于云上业务实时流量学习业务的真实特征，生成个性化防护策略，减少误报，提供更精确的防护，从而大大提升运营效率。
- 防护体系源于百度内部的安全经验共享，这些经验通过百度云 WAF 为企业持续保驾护航，规则策略准确有效，防护效果好。

事件可追溯

- 完整的记录攻击事件的各种信息元素，方便企业对其进行二次分析和了解攻击详情。

BOT 流量管理

- 支持客户对访问者启用指纹技术，为每一位访问者建立唯一身份标识，进行持续观测。
- 基于百度的爬虫风险评分机制，通过流量画像匹配行为模型及行为标签，对所有流量进行爬虫风险高效评估。评估结果以 Riskscore 的形式附在请求中，辅助业务做决策。
- 提供 IP 情报等多种威胁情报，掌握第一手威胁信息。
- 提供多种灵活的业务场景定义防护策略。 提供已知、未知和自定义类型 BOT 详细报表和统计，快速定位和防御恶意 BOT，保护网站业务安全。

同时支持 IPv4、IPv6 安全防护

完全兼容 IPv4 和 IPv6 访问，稳定迅捷。

应用场景

应用场景

Web 应用防火墙被广泛应用于金融、电商、o2o、互联网+、游戏、政府、保险、政府等各类网站的Web应用安全防护。

政务网站保护

- 精准有效防御各种常见 Web 攻击，安全无忧。
- 支持网页防篡改，避免网站内容被篡改，造成不良影响。
- 一键接入，使用简单，配置轻松。

电商网站保护

- 精准有效防御各种常见 Web 攻击，安全无忧。
- 支持BOT分析识别，搭配AI安全分析技术，可智能识别各种机器人行为，保障业务安全。
- 支持CC攻击，有效阻断 CC 攻击请求，保障网站可用性。

金融、保险网站保护

- 精准有效防御各种常见 Web 攻击，安全无忧。
- 支持CC攻击，有效阻断 CC 攻击请求，保障网站可用性。
- 0day攻击防护，针对被披露的系统软件的最新漏洞，提供快速防御和快速止血的规则策略。

数据防泄漏

- 防数据泄漏，避免因黑客的注入攻击，导致核心数据被窃取。
- 0day攻击防护，针对被披露的系统软件的最新漏洞，提供快速防御和快速止血的规则策略。

产品定价

计费概述

百度智能云Web应用防火墙目前支持 预付费方式 和 后付费方式。具体价格请参考：WAF价格详情。

套餐规格

WAF按套餐规格计费，目前出售套餐版本，包括如下参数：

分类	类别	云原生WAF-基础版	SAAS WAF-高级版	SAAS WAF-企业版
接入管理	主域名	1	1	1
	子域名	1，可扩展到100	1，可扩展到100	5，可扩展到100
	泛域名	不支持	支持	支持
	业务协议	HTTP/HTTPS	HTTP/HTTPS	HTTP/HTTPS/WebSocket
	IP 地址	客户EIP	共享EIP组	共享EIP组，可独享
	接入端口	80、443	80、443	80、443、支持非标端口定制
业务峰值	带宽峰值	客户EIP的带宽大小	10Mb~50Mb可选	100Mb~1Gb可选
	QPS峰值	BLB QPS峰值	100~500QPS可选	1000~10000QPS可选
	超量后付	不支持	支持，创建资源时需开启	支持，创建资源时需开启
基础安全防护	Web 防护引擎	支持	支持	支持
	0day 虚拟补丁	支持	支持	支持
	自定义防护规则	20，可扩展到100	20，可扩展到100	20，可扩展到100
	CC智能防护	不支持	支持	支持
	IP 地域封禁	不支持	支持	支持
	网页防篡改	不支持	支持	支持
日志服务	日志投递	不支持	支持	支持
BOT管理	BOT威胁评估	不支持	不支持	支持
	IP威胁情报	不支持	不支持	支持
	设备威胁情报	不支持	不支持	支持
	设备指纹追踪	不支持	不支持	支持
服务支持	1对1售前服务	不支持	不支持	支持
	7*24工单售后	支持	支持	支持

余额不足提醒和欠费处理

- 到期说明：当您购买的防护服务到期，为用户保留7天Web应用防火墙配置，7天内续费则继续防护，7天后，Web应用防火墙配置释放，服务不可用。
- 扣费周期：以用户购买当日起，按月/年售卖。
- 购买前需保证账户无欠款。

操作指南

接入管理

CDN-WAF-概述

应用防火墙WAF负责为CDN提供应用安全防护功能，有效防御SQL注入、XSS跨站脚本、后门上传、非授权访问等各种常见Web攻击。用户需要为创建的WAF实例添加CDN中的域名，WAF才能为您的域名提供web防护。

创建 CDN WAF实例

1. 登录百度智能云控制台。
2. 登录成功后，选择“产品服务>应用防火墙 WAF”，进入WAF 列表页。

3. 点击『购买WAF实例』按键，选择配置信息：

参数	说明
地域	全局
支持根域名数	每个WAF实例保护一个主域名
支持子域名数	套餐默认包括对10个子域名进行保护；根据业务需要，您也可以额外购买更多子域名进行防护。
支持协议	套餐包括两种协议类型，http和https
Web安全防护	WAF服务能够自动更新攻击漏洞，包括各种常见Web攻击、0day攻击规则。
自定义访问规则	通过自定义规则实现对您自己的业务控制和过滤，当前支持对http请求的“来源IP”、“URL地址”、“Referer”字段、“User-Agent”字段等内容的匹配处理。套餐默认支持最大20条自定义规则；如果您需要定制更多自定义规则，请在控制台额外购买。

4. 选择购买时长和WAF实例个数，点击『下一步』，确认购买信息并支付。

5. 支付完成后，成功创建WAF实例，返回列表页查看。

关联CDN实例

1. 进入CDN WAF 列表页，在一个WAF实例的操作列点击『配置』按键。

2. 填写需要防护的”根域名”、”子域名”，并选择绑定的域名。

   只能绑定在百度智能云CDN域名列表里存在的主域名，仅支持HTTP/HTTPS 协议，如没有符合条件的域名，请前往控制台购买或重新配置。

3. 开启Web防护，选择防护策略等级。

   - 默认开启中级策略集，越严格安全防护效果越好。高级策略集，表示开启严格的防护策略，但可能出现误拦截情况；中级表示具备中和低两种策略集；低级表示防护策略宽松。
   - 每种防护策略都具备『拦截』和『观察』功能，拦截模式发现攻击请求立即阻断；观察模式发现攻击请求立即记录但不拦截。

4. （可选）开启自定义访问控制，点击『添加』按键，通过自定义规则实现对您自己的业务控制和过滤。

参数	说明
名称	自定义访问控制规则名称
匹配项	http请求的“来源IP”、“URL地址”、“Referer”字段、“User-Agent”字段等内容的匹配处理。
匹配模式	选择匹配模式：前缀、包含或后缀。
匹配字符串	输入需要访问控制的字符串。
执行动作	将字符串列为黑名单或白名单
模式	拦截：发现攻击请求立即阻断；观察：发现攻击立即记录但不拦截。

5. 点击『确认生效』，完成绑定BLB操作。

CDN实例绑定WAF

1. 在控制台选择**内容分发网络CDN**进入产品页面，左侧导航栏点击**域名管理**，进入CDN域名管理列表页。

2. 点击需要添加WAF防护的域名，进入域名详情页，在左侧导航栏中点击**安全配置**，进入WAF配置页面。

3. 点击WAF配置旁边的按钮，进入WAF配置修改界面，在弹窗中选择**开启**，开启WAF防护功能。

   WAF配置默认关闭，只有用户选择开启后才能使用。

4. 在WAF实例列表中，选择需要绑定的WAF实例，最后点击保存，完成CDN实例绑定WAF的操作，如果您还没有购买WAF实例，则根据提示，进行购买CDN WAF实例的操作。

> 注意： 主域名状态解释：当主域名列表显示未配置，则表示主域名未配置；显示bfgdu.com表示主域名不一致；发生两种情况都需要您完成配置后，才能使用WAF功能。 域名配置上线为20个，如超出配合需要删除暂时不可用的域名。

5. （可选）点击弹窗中的**管理我的WAF实例**，跳转到CDN WAF列表页面，用户可以在此对WAF实例进行管理、配置。

BLB-WAF概述

BLB负责对HTTP和HTTPS协议请求的解析和转发，应用防火墙WAF负责在中间提供安全防护功能。需要将创建的WAF实例与同区域BLB实例上的HTTP／HTTPS业务绑定，WAF才能对HTTP／HTTPS业务提供Web防护。

> **注意：**
>
> 用户在配置BLB WAF时一定要确保购买的BLB和WAF是同一地域。

创建BLB WAF实例

1. 登录百度智能云控制台。
2. 登录成功后，选择“产品服务>应用防火墙服务 WAF”，进入BLB WAF 列表页。
3. 点击『购买WAF实例』按键，选择配置信息：

参数	说明
地域	目前，支持华北－北京、华南－广州、香港、华东－苏州，金融华东－上海、华北－保定、 华中－武汉
支持根域名数	每个WAF实例保护一个主域名(每个WAF实例只可以绑定一个BLB实例)
支持子域名数	套餐默认包括对10个子域名进行保护；根据业务需要，您也可以额外购买更多子域名进行防护。
支持协议	套餐包括两种协议类型，http和https
Web安全防护	WAF服务能够自动更新攻击漏洞，包括各种常见Web攻击、0day攻击规则。
自定义访问规则	通过自定义规则实现对您自己的业务控制和过滤，当前支持对http请求的“来源IP”、“URL地址”、“Referer”字段、“User-Agent”字段等内容的匹配处理。套餐默认支持最大20条自定义规则；如果您需要定制更多自定义规则，请在控制台额外购买。

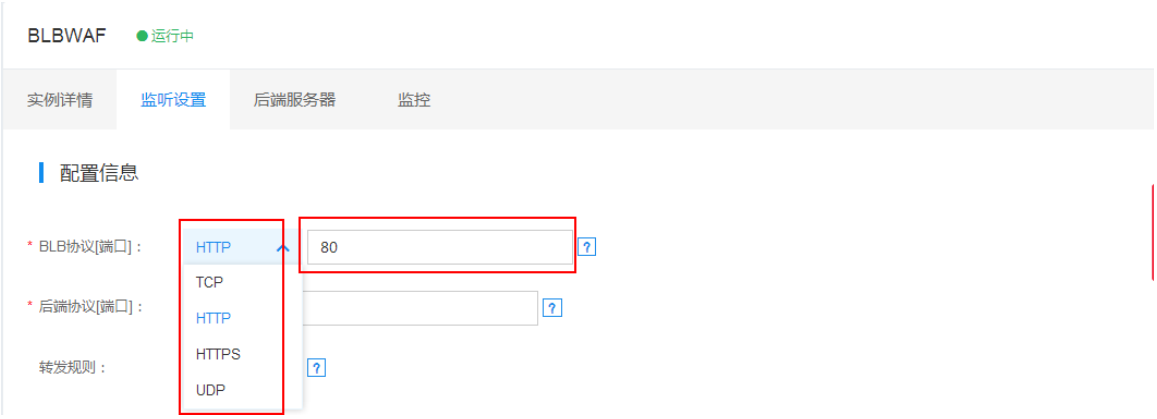
4. 选择购买时长和WAF实例个数，点击『下一步』，确认购买信息并支付。
5. 支付完成后，成功创建WAF实例，返回列表页查看。

配置BLB

配置BLB监听

1. 选择“产品服务>负载均衡BLB”，进入实例列表页面。
2. 选择需要配置监听的BLB实例，然后在**前端协议/端口**或**后端协议/端口**栏中，点击**配置**，进入监听设置详情页面进行配置。

3. 配置信息填写



参数|

说明 ----|---- BLB协议【端口】|根据用户实际业务对外服务的协议和端口，选择协议类型为http/https并填写端口。 后端协议【端口】|根据用户实际业务对外服务的协议和端口，选择协议类型为http/https并填写端口。

4. 其余功能默认既可以，最后点击**确定**，完成BLB监听的设置。

BLB添加后端服务器

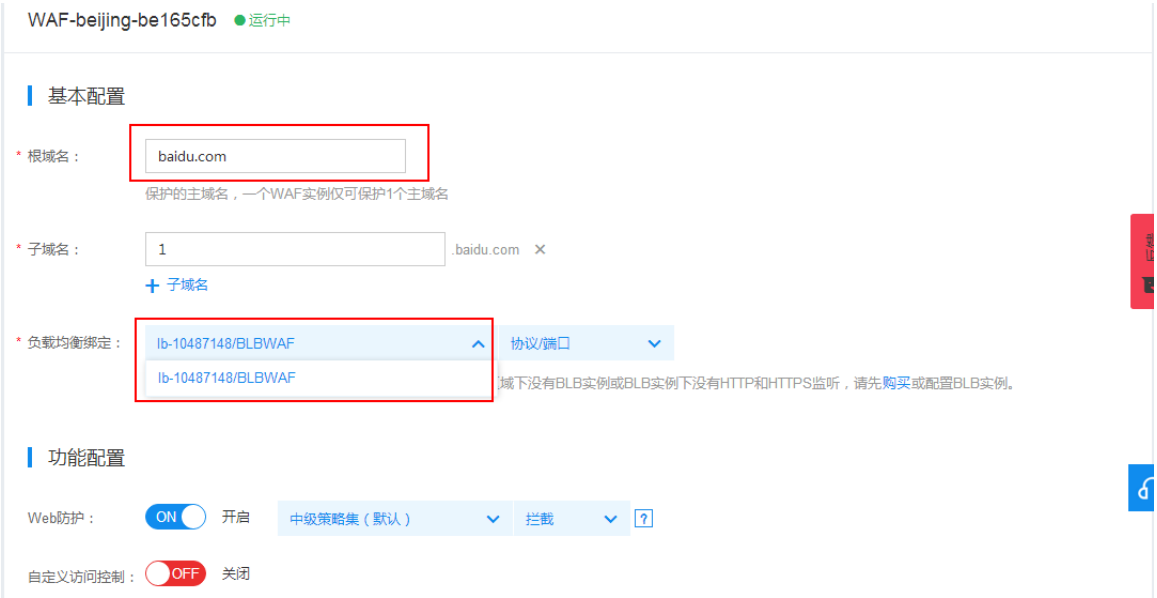
1. 选择“产品服务>负载均衡BLB”，进入实例列表页面。
2. 选择需要配置监听的BLB实例，然后在**后端服务器**栏中，点击**配置**，进入后端服务器页面。
3. 点击**添加后端服务器**，弹出的菜单栏中，选择需要配置的服务器BCC实例，点击**下一步**，然后设置服务器权重值，最后点击确认。完成BLB添加后端服务器的操作。

配置 WAF

完成WAF的实例购买后，需要对其进行配置，才能够实现WAF的防护能力，配置步骤如下：

1. 选择“产品服务>应用防火墙服务 WAF”，进入BLB WAF 列表页，点击**主域名**栏下的**配置**，进入配置详情页面。
2. 基本配置填写，填写需要防护的”根域名”、”子域名”，并选择绑定的负载均衡BLB实例。

   只能绑定与WAF实例所在同一区域的BLB实例，仅支持HTTP/HTTPS 协议，如没有符合条件的BLB实例，请前往控制台购买或重新配置BLB实例。



3. 开启Web防护，选择防护策略等级。
   - 默认开启中级策略集，越严格安全防护效果越好。高级策略集，表示开启严格的防护策略，但可能出现误拦截情况；中级表示具备中和低两种策略集；低级表示防护策略宽松。
   - 每种防护策略都具备『拦截』和『观察』功能，拦截模式发现攻击请求立即阻断；观察模式发现攻击请求立即记录但

不拦截。

4. （可选）开启自定义访问控制，点击『添加』按键，通过自定义规则实现对您自己的业务控制和过滤。

参数	说明
名称	自定义访问控制规则名称
匹配项	http请求的“来源IP”、“URL地址”、“Referer”字段、“User-Agent”字段等内容的匹配处理。
匹配模式	选择匹配模式：前缀、包含或后缀。
匹配字符串	输入需要访问控制的字符串。
执行动作	将字符串列为黑名单或白名单
模式	拦截：发现攻击请求立即阻断；观察：发现攻击立即记录但不拦截。

5. 点击『确认生效』，完成绑定BLB操作。

重新绑定EIP

为了实现BLB的WAF防护功能，需要将EIP从云服务器BCC上解绑，然后绑定到对应的BLB上。具体步骤如下所示：

> **注意：** 此步骤中需要解绑EIP，会造成业务的中断，请合理安排此操作时间，降低对线上业务的影响。

从BCC上解绑EIP

1. 选择“产品服务>云服务器BCC”，进入BCC实例列表页。
2. 点击需要解绑EIP的实例名称，进入该实例的实例详情页面。
3. 在**配置信息**内容中，点击解绑EIP，在弹出的菜单栏中，选择**确认**，完成EIP从BCC上的解绑操作。

将EIP绑定到BLB

1. 选择“产品服务>负载均衡BLB”，进入BLB实例列表页。
2. 选择需要绑定EIP的BLB实例，点击**公网IP/带宽**栏中对应的网络符号，进入EIP绑定页面。

3. 从EIP列表中，选择刚从BCC解绑的EIP，然后点击**确定**，完成将EIP绑定到BLB上的绑定操作。

SAAS-WAF概述

Web应用防火墙（WAF）的 SAAS 服务版本为客户的混合云场景业务、云下业务提供应用安全防护功能，能够有效防御SQL注入、XSS跨站脚本、后门上传、非授权访问等各种常见Web攻击。用户需要在WAF实例中添加回源信息、并且完成域名的 CNAME 解析，WAF才能为您的域名提供web防护。

> **注意：**
>
> 用户在完成 SAAS WAF 的转发配置后，先在本地绑定HOST的方式验证转发设置已经配置成功，再切换 CNAME 解析。

创建SAAS WAF实例

1. 登录百度智能云控制台。
2. 登录成功后，选择“产品服务>Web应用防火墙 WAF”，进入WAF的控制台。
3. 左侧菜单中，选择 资源管理-资源列表，点击“购买WAF实例”按键，进入资源创建页面。
4. SAAS WAF 配置说明：

参数	说明
地域	目前仅支持华北－北京，因为是 SAAS 服务模式，其他 Region 也可使用
支持根域名数	每个WAF实例保护一个主域名
支持子域名数	不同的套餐默认包含不等数量的子域名进行保护；根据业务需要，您也可以额外购买更多子域名进行防护
自定义规则数	不同的套餐默认包含一定数量的自定义规则；根据业务需要，您也可以额外购买更多自定义规则
网页防篡改	支持对页面进行静态缓存的方式，对网页进行防篡改保护
BOT防护	支持 BOT 识别管理功能
业务保底	支持 QPS、流量、带宽的业务保底计费模式。超量弹性开关开启时，遇到超出保底的情况，会对超量部分收取费用。超量弹性开关关闭时，遇到超出保底的情况，会对业务进行流量压制。

5. 选择购买时长和WAF实例个数，点击『下一步』，确认购买信息并支付。
6. 支付完成后，成功创建WAF实例，返回资源列表页查看。

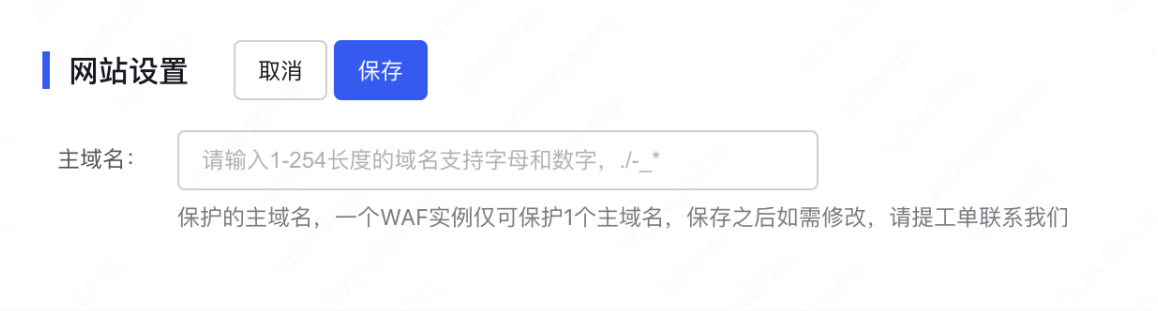
接入设置

在完成资源创建后，可以在资源的操作区域找到『接入设置』按钮，点击进入接入设置。

主域名设置

设置资源要保护的主域名，并进行保存。

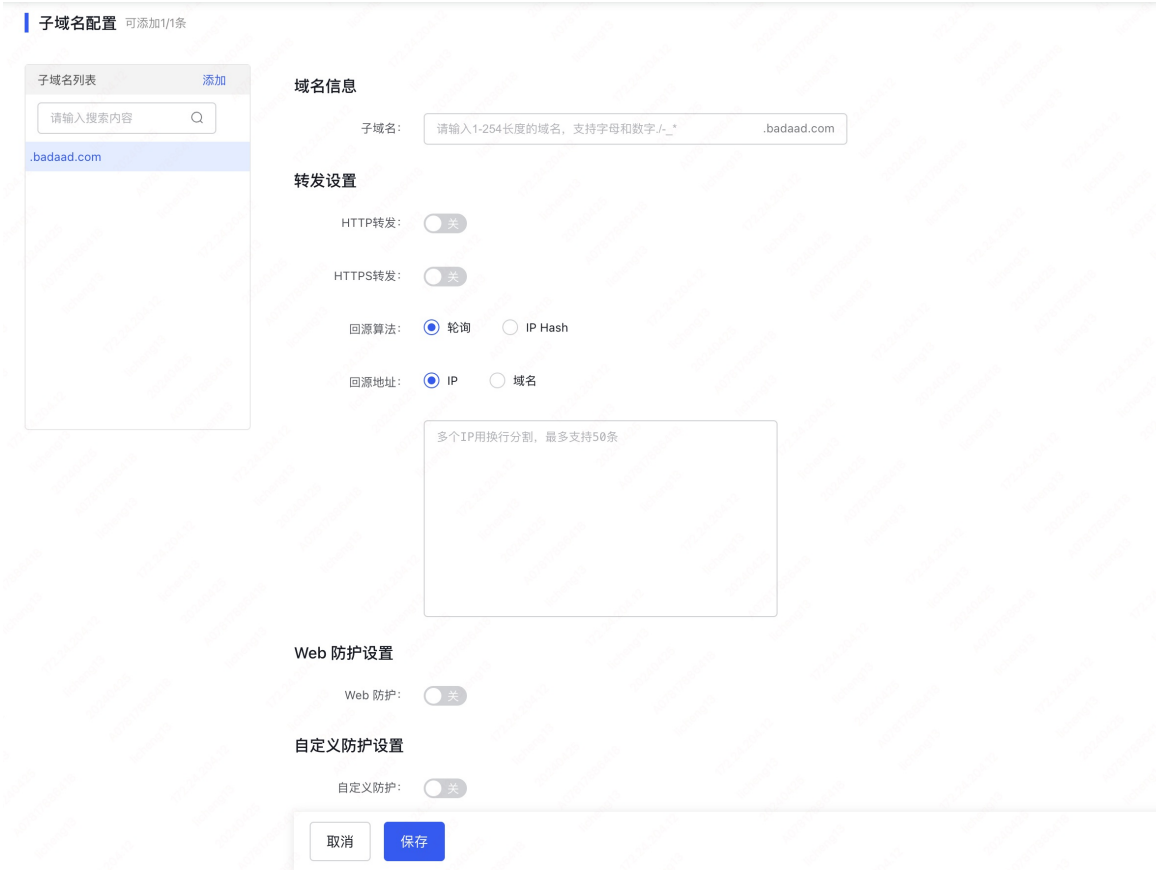
> **注意：**
>
> 考虑到主域名修改，可能对业务造成中断影响，如需修改，请提交工单联系售后进行修改。



子域名设置

完成主域名设置后，即可对其子域名进行设置。

- 转发协议支持 HTTP 或 HTTPS，其中 HTTP 转发的前端端口固定为80，HTTPS 转发的前端端口固定为 443。
- 前端协议为 HTTP 时，回源协议也需要为 HTTP。前端协议为 HTTPS 时，回源协议可以为 HTTP 或 HTTPS。支持 HTTPS 强制转化，即对浏览器发出的 HTTP 请求强制转换成 HTTPS 请求。
- 回源算法 支持 轮询 和 IP HASH。
- 回源地址 IP 或 域名。
- Web 防护和自定义防护开关，当开关开启后，需装载已设置好的防护模板。



配置自定义TLS

如果已通过SAAS WAF 接入Web应用防火墙防护的域名使用的是HTTPS协议传输数据，WAF支持对该网站域名自定义TLS协议版本，拦截不在指定范围内的TLS协议版本的访问流量。

前提条件

- 域名已通过SAAS WAF接入完成网站接入。
- 网站域名使用的是HTTPS协议且已上传了HTTPS证书。

操作步骤

1. 登录Web应用防火墙控制台，确认域名对应的接入模式为SAAS WAF接入
2. 在左侧导航栏，选择**资源管理** > **接入配置**，定位到需要配置TLS的域名
3. 在**子域名转发配置**，开启Https协议转发，找到**【TLS协议版本】**，只有使用了HTTPS协议的网站域名需要配置TLS。如果网站域名使用的是HTTP协议或者使用HTTPS协议但是未上传HTTPS证书，转发配置不显示TLS协议版本配置。

开启IPv6防护

开启IPv6防护

IPv6防护为网站防御IPv6环境下发起的攻击，帮助源站实现IPv6协议请求的安全防护。本文介绍如何开启IPv6防护。

开启IPv6安全防护功能后，WAF的CNAME地址将实现双路解析。解析规则如下：

- IPv4客户端发起的解析请求将解析到一个IPv4地址的防护集群。
- IPv6客户端发起的解析请求将解析到一个IPv6地址的防护集群。

双路解析实现了对IPv4和IPv6流量的威胁检测与防御，并将安全的访问流量转发至源站服务器。

前提条件

1.已开通WAF 实例

2.已使用SAAS WAF 接入模式完成域名接入配置

操作步骤

1. 登录Web应用防火墙控制台
2. 在左侧导航栏，选择进【资源管理】 > 【接入配置】 >【子域名配置】
3. 在域名列表中，定位到要操作的域名，打开IPv6开关

WAF回源及回源保护

当客户域名接入WAF后，客户流量包用尽，服务异常或者其他特殊需求需要临时回源的场景，开启WAF回源操作和回源保护，避免线上故障。

一键回源

前提条件

1.已开通WAF服务且进行防护域名接入配置

2.SAAS WAF版本

操作说明

一键回源：

进入【资源列表】，选择【操作】，对已经接入WAF的域名可勾选域名进行一键回源操作。

回源操作验证：回源过程中，将进行安全短信验证，避免误操作导致业务未进入WAF安全防护造成损失。

回源状态说明：

接入状态	说明
WAF未设置	客户业务未进行WAF接入配置
DNS未设置	客户业务进行WAF接入配置，但是Cname未验证通过
DNS生效中	客户进行WAF接入配置，有多个子域名，部分子域名DNS还在生效中
未全部接入	客户存在多个域名，部分子域名未进行接入配置
已接入	接入配置的域名，WAF DNS 全部生效
DNS回源中	客户对已接入域名进行回源操作且DNS生效中
DNS已回源	客户对已接入域名进行回源操作，DNS 回源已生效

切回WAF

当回源的域名完成紧急情况排查，可对其进行切回WAF操作，原有配置保持一致。

1.进入左侧导航览【资源管理】>资源列表操作

2.选择切换WAF

3.进行回源操作的域名可进行切回WAF操作

回源保护

当客户流量包用尽，服务异常或者有特殊需求需要临时回源的场景，网站的业务流量流回源站不经过WAF防护，源站IP泄露，攻击者会绕过WAF直接攻击源站。您可以开启回源保护，回源到本地指定IP地址，流量不经过WAF服务器，客户可在本机调试，避免源站IP泄漏。

前提条件：

业务域名已进行回源操作

操作：

1.进入【资源列表】>【接入配置】

2.进入【子域名】>【转发配置】

3.开启【回源保护】

安全运营

查看数据报表

攻击日志

攻击日志

攻击日志为客户防护业务接入WAF后，会对其攻击日志进行采集，您可以通过攻击日志对防护对象的日志数据进行查询与下载分析，并基于查询与分析结果生成统计图表、创建告警等。

前提条件

1.已开通WAF服务

2.已经将Web业务域名进行WAF的防护配置

操作步骤

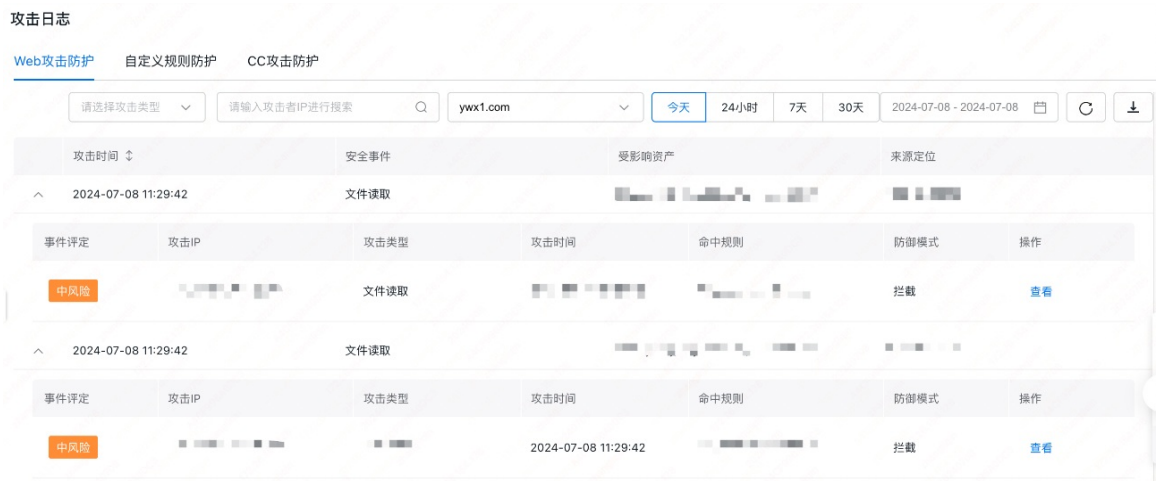
1. 登录Web应用防火墙 控制台。
2. 在左侧导航栏，选择**安全运营 > 攻击日志**。
3. 在攻击日志页面上方，选择要查询日志的防护对象。
4. 支持Web攻击防护、自定义规则防护、CC攻击防护查询

攻击检索条件

下表描述了高级搜索支持设置的搜索条件。

搜索条件	说明
选择攻击类型	支持SQL注入、文件上传、代码执行、文件读取、敏感信息探测、权限绕过、IP黑白名单等类型日志检索
攻击IP	支持通过攻击者IP进行检索
攻击域名	支持通过对攻击的域名进行检索
攻击时间	支持通过不同时间维度进行检索
下载日志	支持下载筛选日志结果

攻击结果分析



攻击类型	攻击结果
Web攻击防护	对攻击时间、攻击IP、攻击类型、受影响资产、来源评定、命中时间、防御模式等进行详细攻击日志查询
自定义防护规则	对攻击时间、攻击IP、攻击类型、受影响资产、来源评定、命中时间、防御模式等进行详细攻击日志查询
CC攻击	被攻击站点URL、攻击源IP、攻击起止、攻击详情进行分析
事件评定	根据命中不同风险等级防护规则，进行事件评定中风险、高风险、低风险等
攻击详情	对攻击行为进行详细定位分析，攻击时间、攻击类型、命中规则等

访问概览

访问概览

接入WAF防护后，您可以通过访问概览界面，查询带宽、流量、请求数、QPS详情数据，了解近期Web业务的服务状态。

前提条件

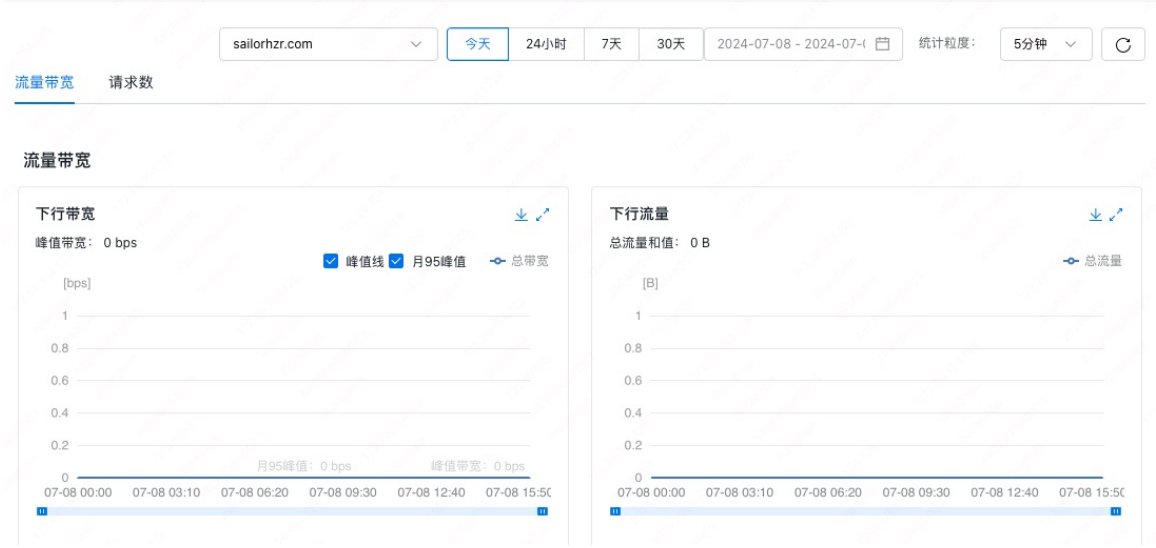
1.已开通WAF服务。

2.已经将Web业务添加为WAF的防护对象。

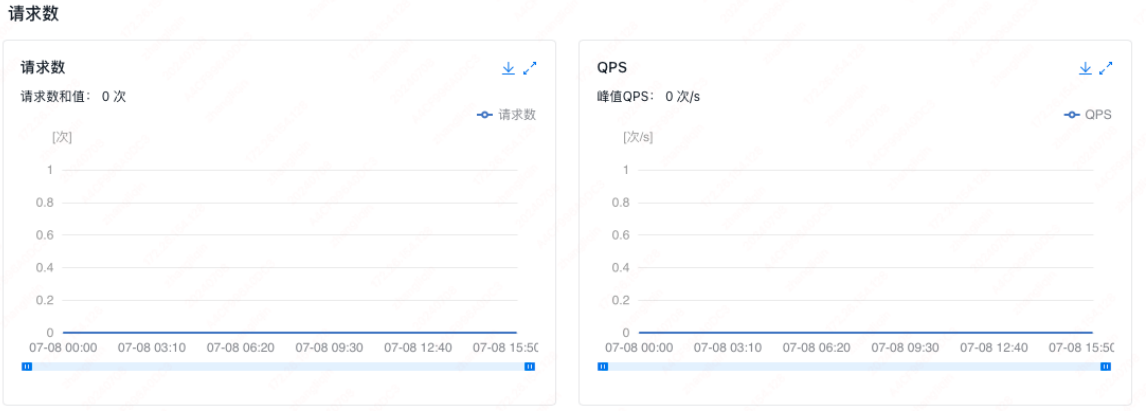
操作说明

您可以通过时间筛选条件和粒度统计，查看指定筛选条件下的访问概览。

1.流量带宽



2.请求数



3.详细操作说明

数据类型	说明	支持的操作
下行带宽	通过折线图，展示在指定时间范围内，防护对象公网下行带宽（单位：bps）变化趋势。	• 将光标放置在折线图上的某一点，可以查看该时刻的具体数据。 • 查看下行带宽峰值线。 • 查看峰值带宽。 • 下载相关带宽数据（格式：xls）。 • 对横坐标进行缩放。
上行带宽	通过折线图，展示在指定时间范围内，防护对象公网上行带宽（单位：bps）变化趋势。	• 将光标放置在折线图上的某一点，可以查看该时刻的具体数据。 • 查看峰值带宽。 • 下载相关带宽数据（格式：xls）。 • 对横坐标进行缩放。
下行流量	通过折线图，展示在指定时间范围内，防护对象公网下行流量（单位：B）变化趋势。	• 将光标放置在折线图上的某一点，可以查看该时刻的具体数据。 • 查看总流量和值。 • 下载相关流量数据（格式：xls）。 • 对横坐标进行缩放。
上行流量	通过折线图，展示在指定时间范围内，防护对象公网上行流量（单位：B）变化趋势。	• 将光标放置在折线图上的某一点，可以查看该时刻的具体数据。 • 查看总流量和值。 • 下载相关流量数据（格式：xls）。 • 对横坐标进行缩放。
请求数	通过折线图，展示在指定时间范围内，防护对象收到请求次数的变化趋势。	• 将光标放置在折线图上的某一点，可以查看该时刻的具体数据。 • 下载请求数相关数据（格式：xls）。 • 查看请求数和值。 • 对横坐标进行缩放。
QPS	通过折线图，展示在指定时间范围内，防护对象收到的请求QPS的变化趋势。	• 将光标放置在折线图上的某一点，可以查看该时刻的具体数据。 • 下载请求数相关数据（格式：xls）。 • 查看峰值QPS。 • 对横坐标进行缩放。

防护配置

防护配置概述

概述

本文介绍了Web应用防火墙（Web Application Firewall，简称WAF）服务防护配置的相关术语、配置流程、防护模块概览及典型配置案例。

防护配置流程

Web业务接入WAF防护后，您可以参照以下步骤，为Web业务配置 防护规则 。不同接入方式下的防护配置流程略有差异。

步骤	云原生BLB WAF 接入	SAAS WAF接入
1. 添加防护域名	完成云原生接入的BLB实例，可绑定相关实例域名进行WAF转发配置	在Web应用防火墙控制台添加防护主子域名进行WAF转发配置
2. 定义防护规则模板	您可以在防护规则中配置不同的防护规则，然后将规则模板应用到指定的防护域名。 可以定义多套规则模板，为不同防护域名应用不同的防护规则。	您可以在防护规则中配置不同的防护规则，可以将规则模板应用到指定的防护域名。 可以定义多套规则模板，为不同防护域名应用不同的防护规则。
3. 管理防护规则	您可以在不同防护模块下的规则模板中管理具体的防护规则， 规则模板中发生的规则变动将直接应用到该规则模板的生效域名。不同规则模板支持的规则操作不完全相同。	您可以在不同防护模块下的规则模板中管理具体的防护规则， 规则模板中发生的规则变动将直接应用到该规则模板的生效域名。不同规则模板支持的规则操作不完全相同。

防护规则概览

下表描述了WAF支持的所有防护模块，以及不同防护模块的默认配置。

防护规则	说明	默认规则模板	配置建议
基础Web防护引擎	基于百度云安全AI分析能力，快速精准有效的防御常见Web攻击，如SQL注入、非授权访问、XSS跨站脚本、CSRF跨站请求伪造，Webshell、木马等等	内置一套默认规则（包含百度多年WAF的基础防护规则集）。**重要：**新接入WAF防护的域名开启Web防护默认受到基础防护规则的防护，基础防护规则会自动拦截攻击请求。	建议开启基础防护配置。业务接入WAF防护一段时间后，如果您发现基础防护规则集存在误拦截，可以通过设置白名单规则，屏蔽产生误拦截的基础防护规则。
CC防护	基于内置的通用CC防护算法，缓解产品规格内的高频请求（HTTP Flood）攻击。您也可以通过访问频率限制进行更加灵活的自定义CC防护	内置一套默认规则（包含百度多年WAF的基础防护规则集）	如需启用自定义规则，在对应防护模版开启相关规则。
IP白名单	白名单模块允许您根据业务场景，自定义放行具有指定特征的请求，使请求不经过全部或特定防护模块的检测		如需启用自定义规则，在对应防护模版开启相关规则。
IP黑名单	IP黑名单模块允许您根据业务场景，自定义拦截来自特定IP地址IPV4或地址段的请求。		如需启用自定义规则，在对应防护模版开启相关规则。
自定义访问控制策略	自定义规则模块允许您基于自定义的HTTP请求特征或特征组合，对符合条件的请求执行拦截、记录日志等处置。		如需启用自定义规则，在对应防护模版开启相关规则。
区域黑白名单	一键封禁来自特定区域的客户端IP，支持海外和国内地区		如需启用自定义规则，在对应防护模版开启相关规则。
访问频率限制	设置单一IP访问次数进行检测拦截封禁		如需启用自定义规则，在对应防护模版开启相关规则。
网页防篡改	提供对页面进行强制缓存功能，从而防止黑客对网页进行篡改。帮助您锁定需要保护的网站页面，被锁定的页面在收到请求时，返回已设置的缓存页面。		如需启用自定义规则，在对应防护模版开启相关规则。
Bot管理-基础防护规则	支持基础情报策略和多条复合策略配置	仅企业版支持	如需启用自定义规则，在对应防护模版开启相关规则。
源站健康检查	设置源站响应超时、检查间隔、异常报警阈值、业务恢复判断阈值		如需启用自定义规则，在对应防护模版开启相关规则。

泛域名防护配置说明

当实例中存在泛域名解析配置且准备开启自定义防护设置时，需要注意以下事项：

1、当存在泛域名配置时，如果存在同级精准域名的解析配置，且未开启自定义防护，该精准域名也会匹配泛域名的自定义防护模板。即同级别的精准域名均保持自定义防护设置开启且配置相应防护模板。

2、如不需要任何防护，则在Web防护规则列表，如下图所示，将所有防护能力关闭即可。

基础Web防护引擎

基础Web防护引擎基于百度云安全AI分析能力，快速精准有效的防御常见Web攻击，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，对漏洞攻击、网页木马等威胁进行检测和拦截。 如SQL注入、非授权访问、目录遍历（路径绕过）、XSS跨站脚本、CSRF跨站请求伪造，Webshell、木马等。

支持的解码

基础防护规则支持7种不同格式的解码，包括：

- JSON、XML、Multipart等数据格式的解析，用以提升检测的准确率。

支持内置检测模块

防护策略： Web防护配置按照防护严格程度，Web基础防护设置了三种防护等级：“低级策略集”、“中级策略级”、“高级策略集”，默认情况下，选择“中级策略集”。

1.中级策略集（默认）：默认选用该策略，默认为“中等”防护模式，满足大多数场景下的Web防护需求。

2.低级策略集（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。

3.高级策略集（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“高级策略集”模式，使WAF能有效防护更多攻击。
> 您也可以根据业务需要，配置自定义规则，策略集越严格安全防护效果越好，但业务实现不规范时可能有误拦截；

规则动作

Web防护当请求命中该规则时，支持2种规则动作：

1.拦截：表示拦截命中规则的请求，发现攻击请求立即阻断，并向发起请求的客户端返回拦截响应页面。说明WAF默认使用统一的拦截响应页面，您可以通过自定义响应功能，自定义拦截响应页面。

2.观察：表示发现攻击只记录不拦截。您可以通过WAF 攻击日志，查询命中当前规则的请求，分析规则的防护效果（例如，是否有误拦截等）。观察模式方便您试运行首次配置的规则，待确认规则没有产生误拦截后，再将规则设置为拦截模式。

支持的规则模板

模块	SaaS WAF 高级版	SaaS WAF 企业版	云原生WAF
默认内置规则组	支持	支持	支持
自定义规则组	支持	支持	不支持

前提条件

- 已开通Web应用防火墙服务
- 已将Web业务进行WAF接入配置

创建Web基础防护规则模板

1. 登录Web应用防火墙

2. 在左侧导航栏，选择**防护配置** > **Web基础防护**

3. 在规则模板列表页，单击**规则模板**

配置项	说明
模板信息	模板名称：请输入1~40位字符，支持中文，英文及数字，符号仅限/_- 接入类型：支持 SaaSWAF及云原生WAF 两种形式 网站不在百度云，希望接入WAF 防护，推荐部署SaaS WAF应用防火墙 网站在百度云上，但没有解析到七层负载均衡（BLB），推荐部署SaaS WAF应用防火墙 网站在百度云上，且业务流量解析七层负载均衡（BLB），推荐部署云原生BLB WAF应用防火墙
规则引擎	**1.处置动作：**选择当请求命中该规则时，要执行的防护动作。可选项： **拦截：**表示拦截命中规则的请求，并向发起请求的客户端返回拦截响应页面。说明WAF默认使用统一的拦截响应页面，您可以通过自定义响应功能，自定义拦截响应页面。 **观察：**表示不拦截命中规则的请求，只通过日志记录请求命中了规则。您可以通过WAF日志，查询命中当前规则的请求，分析规则的防护效果（例如，是否有误拦截等）。观察模式方便您试运行首次配置的规则，待确认规则没有产生误拦截后，再将规则设置为拦截模式。 **2.规则组类型**：配置Web核心防护规则关联的规则组类型并选择相应的规则组。可选项： **默认：**选择该项后，关联**默认规则组**，支持**宽松规则组**、**中等规则组**（默认）和**严格规则组**。 **自定义：**选择该项后，需在下拉列表中选择相应的规则组。关于新建规则组的具体操作，请参见创建自定义规则组。
防护站点	可以选择不同接入类型下不同实例的防护站点，进行防护配置

成功创建规则模板后，您可以在规则列表执行如下操作： 查看模板关联的站点的数量。通过模板开关，开启或关闭模板。编辑或删除规则模板。

4.您也可以在Web基础防护列表区域，单击规则组管理，查看规则组与规则模板的关联关系。

创建自定义规则组

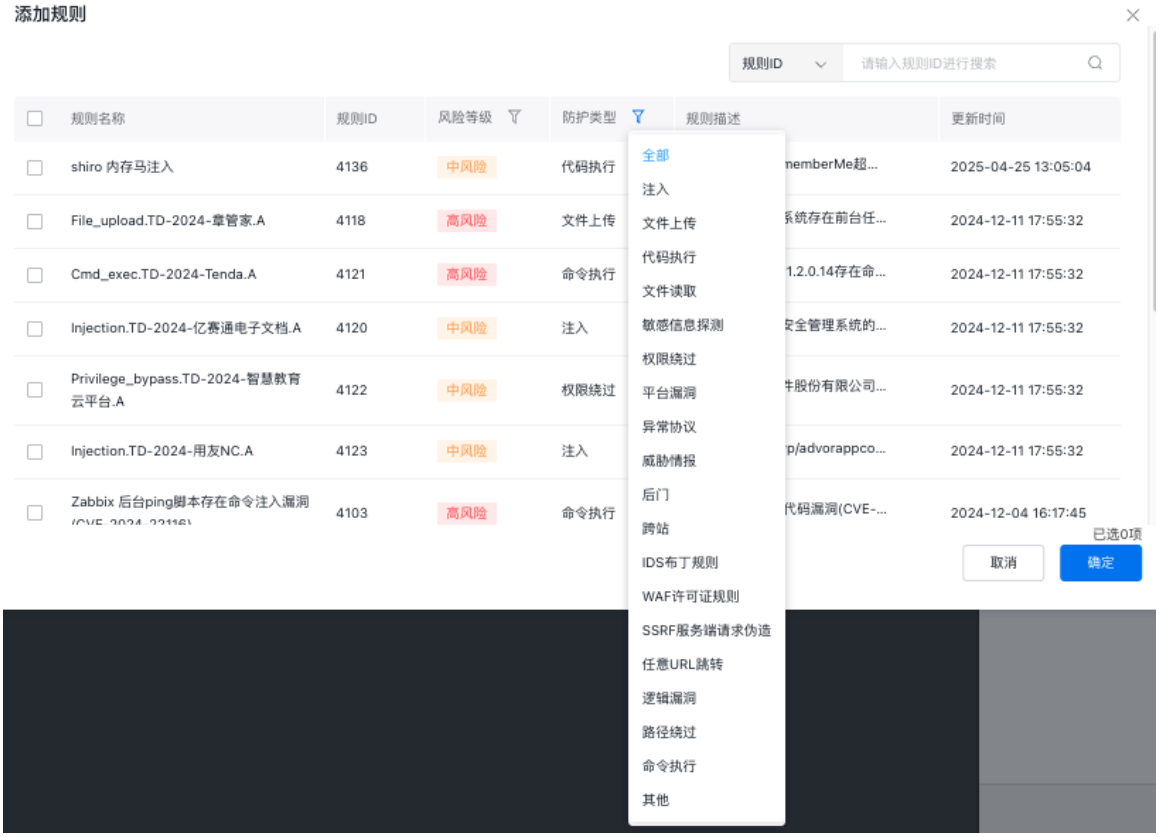
自定义规则组可以从零创建，也可以在默认规则组的基础上创建。

1. 登录Web应用防火墙 控制台
2. 在左侧导航栏，选择**防护配置>Web基础防护**

3. 在**Web基础防护**，规则列表区域，单击**规则组管理**

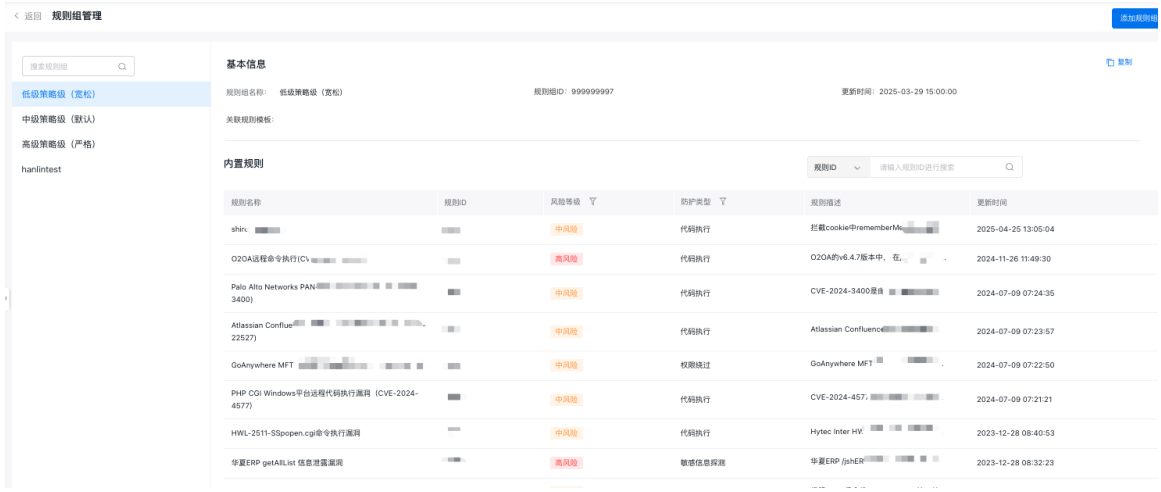
4. 在规则组管理页面，单击添加规则组

配置项	说明
规则组名称	请输入1~40位字符，支持中文，英文及数字，符号仅限/_-
规则组模板	**复用内置规则组**：关联默认规则组，支持宽松规则组、中等规则组（默认）和严格规则组。 **从零开始创建规则组**：添加规则，将从规则库中自定义选择对应的规则，通过输入**规则名称、规则ID，设置危险等级、防护类型**，筛选并选中规则库的防护规则，单击添加；或单击全部添加规则列表的规则默认按照更新时间倒序排列。
自动更新	官方默认规则组中新增或移除的规则（例如0day应急规则或不再适用的规则）将自动同步到当前自定义规则组。



5. 完成添加后，如果您需要删除已添加的防护规则，可在规则列表，通过输入规则名称、规则ID，设置危险等级、防护类型，筛选并选中防护规则，取消勾选移除。

6. 编辑、复制或删除规则组。



- 复制后的规则组默认命名为“原规则组名称-copy”。复制后的规则组无关联防护对象。
- 已关联防护模板的规则组不允许被删除。如果您需要删除该规则组，请先删除与Web核心防护规则的关联关系。

CC防护配置

概述

接入Web应用防火墙（Web Application Firewall，简称WAF）后，您可以设置CC防护规则，基于内置的通用CC防护算法，缓解产品规格内的高频请求（HTTP Flood）攻击进行拦截，并返回403拦截提示页面。您也可以通过访问频率限制进行更加灵活的自定义CC防护。

前提条件

已开通Web应用防火墙服务 已将Web业务进行WAF接入配置

防护状态

宽松模式：出现高频请求次数较高，如需减少误拦截，可选用该策略。

严格模式：出现高频请求阈值较低，如需提高攻击检测命中率，可选用该策略。

超级严格模式：出现高频请求阈值次数偏低，如需攻击检测命中率高，可选用该策略

操作步骤

1. 登录Web应用防火墙
2. 在左侧导航栏，选择**配置中心** > **Web防护规则**
3. 创建Web防护规则，填写规则基本信息
4. 开启CC防护，选择防护状态

自定义访问控制策略

接入Web应用防火墙后，您可以自定义访问控制策略规则，满足客户多样的防护需求。 根据客户端IP、请求URL及常见的请求头字段定义请求特征匹配条件，对命中匹配条件的请求执行相应处置。

例如，您可以使用自定义规则拦截访问指定URI的请求、对包含指定User-Agent内容的请求进行校验等。

前提条件

已开通Web应用防火墙服务

已将Web业务进行WAF接入配置

操作步骤

1. 登录Web应用防火墙
2. 在左侧导航栏，选择**配置中心** > **Web防护规则**。

3. 创建Web防护规则，填写规则基本信息

4.在**自定义访问控制策略**，点击开启并**添加策略**

策略 字段	说明
模式	匹配
策略	URI Get param Cookie Referer User-Agent Method 支持以上策略前缀、后缀、包含、不包含、等于、不等于匹配
阻断类型	**拦截**：表示拦截命中规则的请求，发现攻击请求立即阻断，并向发起请求的客户端返回拦截响应页面。 **观察**：表示发现攻击只记录不拦截。您可以通过WAF 攻击日志，查询命中当前规则的请求，分析规则的防护效果（例如，是否有误拦截等）。观察模式方便您试运行首次配置的规则，待确认规则没有产生误拦截后，再将规则设置为拦截模式。 **拦截并追加封禁**：表示拦截命中规则的请求，发现攻击请求立即阻断，并向发起请求的客户端返回拦截响应页面，同时对发起的请求ip进行封禁。

访问频率限制

接入Web应用防火墙（Web Application Firewall，简称WAF）后，在自定义访问控制策略基础上，定义访问频率检测条件，对访问频率异常的统计对象执行相应处置。

例如： 如果同一个IP或会话在短时间内频繁命中匹配条件，您可以通过启用频率控制，在一段时间内拦截该IP或会话的请求。当WAF与访问者之间并无代理设备时，通过源IP来检测攻击行为较为精确，建议直接使用IP限速的方式进行访问频率限制。

注意事项

已开通Web应用防火墙服务

已将Web业务进行WAF接入配置

操作步骤

1. 登录Web应用防火墙
2. 在左侧导航栏，选择配置中心 > Web防护规则。
3. 创建Web防护规则，填写规则基本信息

4.添加访问频率限制防护策略

策略字段	说明
策略名称	自定义规范策略名称，1~40位字符，支持中文，英文及数字，符号仅限/_-
URI	输入需要检测访问频率限制的URI
匹配类型	完全匹配、前缀匹配
检测时长	输入2-10800整数
单一IP访问次数	输入2-5000整数 对输入的URI识别到对应的IP，检测访问次数
阻断类型	封禁：表示封禁命中规则的请求，发现攻击请求立即阻断，同时对发起的请求ip进行封禁。

防篡改功能设置

Web应用防火墙（WAF）服务，提供对页面进行强制缓存功能，从而防止黑客对网页进行篡改。

防篡改功能

登录 WAF 服务控制台，点击左侧『配置中心-防篡改规则』，找到已设置的主域名，点击『设置』对防篡改功能进行设置。

防篡改设置

根据页面内容，可以对要强制缓存的页面，进行相关设置。

URL支持通配符，例如：

1)对img.yoursite.com进行特定设置，需增加URL:img.yoursite.com/

2)对www.yoursite.com/news/进行特定设置，需增加URL: www.yoursite.com/news/

3)对www.yoursite.com所有html页面进行特定设置，需增加URL:www.yoursite.com/.html

4)对www.yoursite.com所有html页面进行特定设置，需增加URL:www.yoursite.com//damin/*.html

IP黑白名单

接入Web应用防火墙（Web Application Firewall，简称WAF）后，您可以设置IP黑白名单，满足精细维度的应用防护需求。

IP地址默认全部放行，您可以通过配置黑白名单规则，阻断或放行指定IP地址/IP地址段的访问请求，白名单规则优先级高于黑名单规则。配置黑白名单规则时，WAF支持单个添加黑白名单IP地址/IP地址段。

前提条件

已开通Web应用防火墙服务

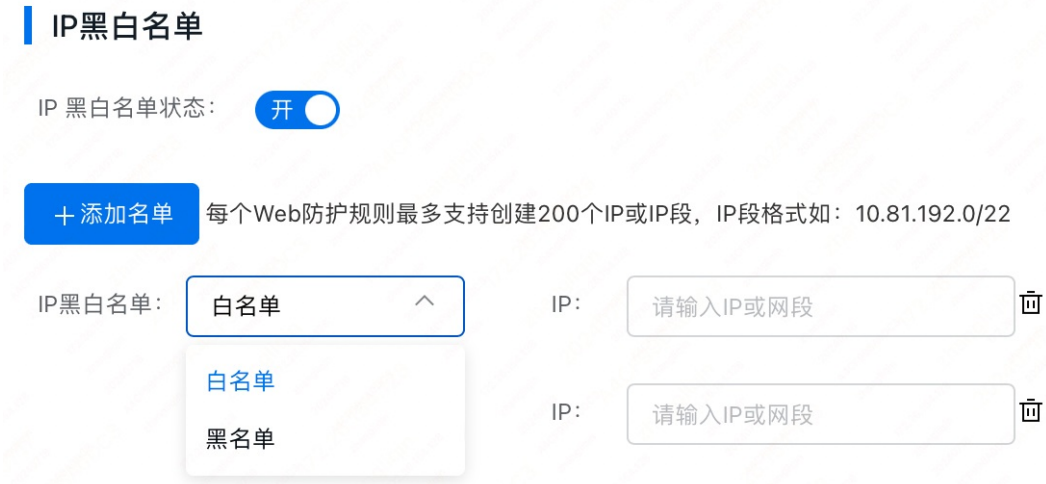
已将Web业务进行WAF接入配置

操作步骤

1. 登录Web应用防火墙
2. 在左侧导航栏，选择配置中心 > Web防护规则。
3. 创建Web防护规则，填写规则基本信息

4.添加IP黑白名单设置

每个Web防护规则最多支持创建200个IP或IP段，IP段格式如：10.81.192.0/22



IP白名单：通过设置白名单规则，默认放行具有指定特征的请求，使请求不经过全部或自定义防护模块（例如基础防护规则、IP黑名单、自定义规则、扫描防护等）的检测本文介绍如何创建白名单规则模板并添加白名单规则。

IP黑名单：通过设置IP黑名单规则，拦截来自特定IP地址或地址段的请求。

BOT 功能设置

如果您的业务存在因自动化工具（例如脚本、模拟器等）造成网站数据被爬取、业务作弊或欺诈、撞库或垃圾注册、恶意秒杀或薅羊毛、短信接口滥刷等情况，您可以开通Web 应用防火墙 WAF（Web Application Firewall）SAAS WAF 企业版，制定有针对性的Bot防护策略，缓解核心数据资产泄露和业务营销活动风险，降低服务器带宽费用和负载。

功能介绍

Bot规则为您提供如下功能，尽可能的帮助您快速识别机器流量，防御爬虫风险，避免您的业务数据被爬取。

风险识别：

Web应用防火墙（WAF）配备了内建的手机号信誉数据库，旨在防范垃圾账号注册、营销活动作弊等行为。WAF可以根据配置，在HTTP请求中检测手机号或其Sha1加密信息，并将其与信誉库进行对比。如果发现与异常行为相关的标签，WAF将采取相

应的措施，例如启动滑块验证、观察、拦截等处置动作

Bot行为识别：

AI智能防护：基于百度搜索等全系场景多年防爬规则应用，对访问流量进行分析和自动学习，生成针对性的防护规则或黑名单。

自定义限速：支持IP和会话自定义限速，可自定义访问频率限制条件，有针对性地对访问频率过高的爬虫请求进行过滤，有效缓解Bot攻击。

自定义Bot策略：

支持自定义多种复杂策略配置，包括 IP地域情报库、IP动态情报库、设备情报库、Referer、Cookie、User Agent、IP等多种条件Bot策略配置，对多个用户有多次恶意爬取行为的攻击源IP进行处置。

Bot特征识别：

支持JavaScript校验和动态令牌挑战。JavaScript校验在用户提交表单之前，对输入的数据进行格式检查、范围验证等，从而确保数据的准确性和合法性。这有助于减少服务器端的处理负担，提高应用程序的响应速度和用户体验。动态令牌挑战通过定期更换令牌或要求用户输入一次性令牌来增强系统的安全性。

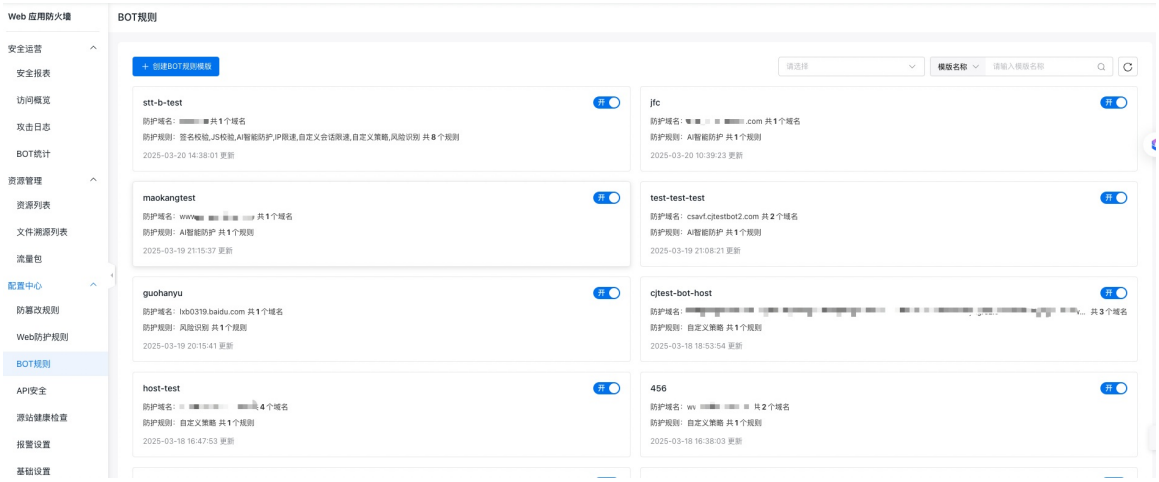
前提介绍

- 在Web应用防火墙控制台，购买Saas WAF企业版
- 已在接入配置页面完成Web业务接入

Bot规则配置

1.创建Bot规则模板

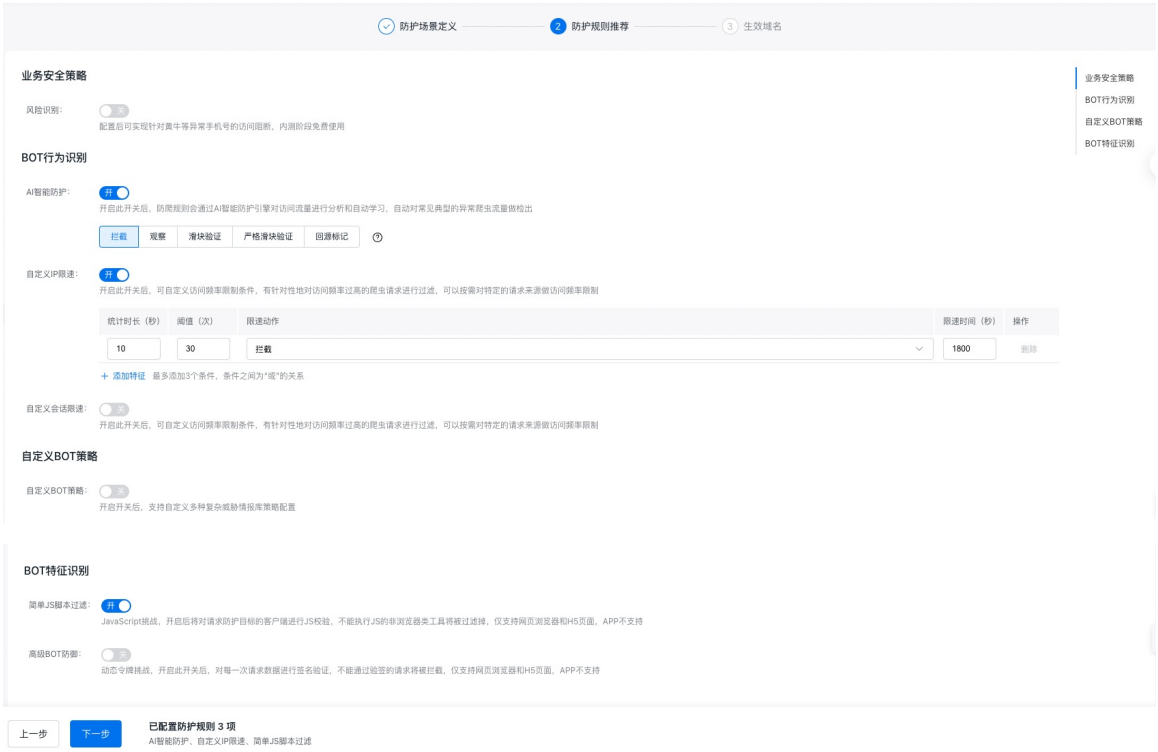
在Web应用防火墙控制台左侧导航栏，【配置中心】-【Bot规则】-【创建Bot规则模板】 每个域名支持配置多个多个模板



2.防护场景定义

配置项	说明
模板名称	1~40位字符，支持中文，英文及数字，符号仅限/_-，不能为空
Web SDK集成	采用基于JavaScript的Web SDK，提升Web浏览器场景下的防护效果，避免部分不兼容问题。开启该功能后，WAF将自动在防护对象的HTML页面中引用SDK。采集相关的浏览器信息、特定攻防探针、操作行为等（不涉及个人敏感信息）后，WAF将根据获取的信息请求风险识别和拦截。 **手动集成（默认）**：适合于无法满足自动集成的场景，或当前站点与组件产生冲突的情况，手动集成必须满足以下条件： 1.所有依赖配置了防护场景的 API 接口所在的页面，都必须接入特定组件 2.在页面使用组件功能之前，必须先完成组件script代码的注入 **自动集成**：可在配置网页防爬场景化的防护场景定义时，选择自动集成，此时网站HTML页面由WAF接管，WAF会在页面请求响应时，向页面注入组件script标签，客户网页无需进行代码改造即可完成部署，同时享受线上组件的热更新。 更多配置信息，请参见Web应用集成SDK
防护目标特征	添加目标流量的HTTP请求字段及其规则，即访问该防护目标时，HTTP请求报文中生成的有关该防护业务场景的字段内容。最多可以添加5个条件特征，且各条件之间为与关系。

3.配置相关Bot防护能力



配置项	说明
业务安全	风险识别：启用规则后，配置后可实现针对黄牛等异常手机号的访问阻断。 **1、账号提取：**最多添加5个条件，条件之间为“或”关系 账号类型- 手机号，手机号 sha1，默认填写手机号 账号位置：Cookie名称、Query参数、Body参数，默认填写Cookie名称 2、风险标签：最多添加5个条件，条件之间为“或”关系 **诈骗风险**：疑似历史上存在欺诈行为，默认高风险，可选中高、低风险 **机器注册**：疑似使用非法工具进行用户注册，用于后续的营销活动等。默认高风险，可选中高、低风险 **营销作弊：**疑似使用非法工具参与营销活动，如批量注册领取优惠券等。默认高风险，可选中高、低风险。 **风险账号：**疑似使用非法工具参与抢票或其他秒杀类活动。默认高风险，可选中高、低风险
Bot行为识别	**AI智能防护**：勾选AI智能防护后，需要设置识别的Bot行为为观察、滑块或回源标记。如果设置为回源标记，您还需要设置回源时标记的Header名称、Header内容。 勾选后策略将生效，防爬规则会通过AI智能防护引擎对访问流量进行分析和自动学习，自动对常见典型的异常爬虫流量做检出。 **自定义限速**：开启此开关后，可自定义访问频率限制条件，有针对性地对访问频率过高的爬虫请求进行过滤，可以按需对特定的请求来源做访问频率限制。 **IP限速：**（默认）在统计时长（秒）内，来自同一IP地址的访问次数超过指定阈值（次）时，在限速时间（秒）内，对来自该IP的访问请求执行观察、滑块或拦截的限速动作。最多可以设置3个限制规则，且规则之间为或关系。 **自定义会话限速**：在统计时长（秒）内，对指定的会话类型的访问次数超过指定阈值（次）时，在限速时间（秒）内，对该会话的请求执行观察、滑块或拦截的限速动作。最多可以设置3个限制规则，且规则之间为或关系。会话类型支持自定义header、自定义参数、自定义cookie、Session。
Bot特征识别	**简单脚本过滤（JavaScript校验）：**开启规则后，对访问防爬防护目标的客户端进行JS校验，过滤不支持JS校验的来自非浏览器类工具的流量，阻断简单脚本类攻击。 **高级Bot防御（动态令牌挑战）：**开启规则后，对每一次请求数据进行签名验证，不能通过验签的请求将被拦截。可选项： 签名验证异常（必选）：指未携带签名或者签名非法时，请求将被拦截。 签名时间戳异常：指签名时间戳异常时，请求将被拦截。 WebDriver攻击：指遭遇WebDriver攻击时，请求将被拦截。
处置动作	选择当请求命中该规则时，要执行的防护动作。可选项： **拦截：**表示拦截命中规则的请求，并向发起请求的客户端返回拦截响应页面。说明WAF默认使用统一的拦截响应页面，您可以通过自定义响应功能，自定义拦截响应页面。 **观察：**表示不拦截命中规则的请求，只通过日志记录请求命中了规则。您可以通过WAF日志，查询命中当前规则的请求，分析规则的防护效果（例如，是否有误拦截等）。观察模式方便您试运行首次配置的规则，待确认规则没有产生误拦截后，再将规则设置为拦截模式。 **滑块：**表示WAF向客户端返回滑动验证页面。如果客户端成功执行滑动验证，则WAF在一段时间（默认30分钟）内放行该客户端的所有请求（不需要重复验证），否则拦截请求。 **严格滑块：**表示WAF向客户端返回滑动验证页面。如果客户端成功执行滑动验证，则WAF放行本次请求，否则拦截请求。严格滑块验证模式下，客户端的每次请求都需要验证。 **回源标记：**用户可以自定义Header及内容，WAF不会直接处理，而是会通过新增Header的方式将命中信息返回给源站，用户可以与后端风控系统结合做业务侧处理。

自定义Bot策略

支持自定义多种复杂BOT高级防护策略配置，包括 IP地域情报库、IP动态情报库、IDC设备情报库、Referer、Cookie、User Agent、IP等多种复杂条件Bot策略配置，多个用户有多次恶意爬取行为的攻击源IP进行处置。

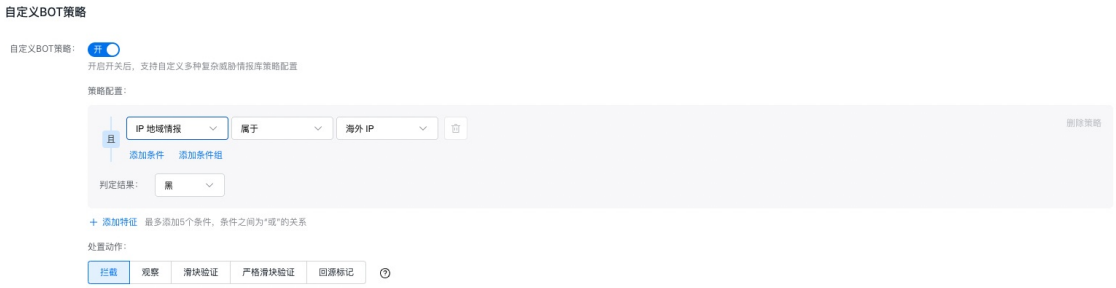
- 情报策略：情报策略支持『IP情报』和『设备情报』。

> IP情报：包括 IP地域情报库 和 IP动态情报库。
> 1）IP地域情报包括：海外IP情报、IDC IP情报、基站IP情报。

> 2）IP动态情报包括：高危IP情报、爬虫IP情报、NAT出口IP情报。
> 3）**当同个域名配置多个自定义策略特征时，优先首次配置策略生效。**

> 设备情报：用户唯一设备指纹，持续维护跟踪。

多条基础策略的组合，支持语法，支持与或，支持条件嵌套。



匹配条件	说明	逻辑符
P地域及静态情报库	收录一段时间内在百度云上对多个用户不同地域多次恶意爬取行为的攻击源IP，并对其执行观察、拦截、滑块、严格滑块或回源标记处置。 海外IP：来自海外攻击源IP 基站IP：来自基站攻击源IP IDC内IP：来自IDC内部攻击源IP	属于、不属于
IP动态情报库	**公共出口 IP：**这些 IP 普遍有较多的正常用户共享的出口，如小区运营商、办公网络、活跃基站等共享 NAT 或代理的出口。这些 IP 建议站长做一定的多维度策略，防止对正常用户的打扰。 **搜索引擎：**搜索引擎的请求来源。如果客户是希望各搜索引擎来抓取的场景，建议针对此情报命中的请求加白。 **高危 IP：**根据历史行为存在高安全风险的IP地址，这些IP地址可能与恶意活动、网络攻击、钓鱼网站或其他不安全的行为有关。多数场景下这些请求来源的流量可以直接做处置	属于、不属于
设备情报	对不同时间段的新旧的设备进行异常行为，对其执行观察、拦截、滑块、严格滑块或回源标记处置。包括： 1小时以内的新设备 1天以上的旧设备 7天以上的旧设备	属于、不属于
IP	请求的来源IP，即发起请求的客户端的IP地址。 匹配内容填写要求如下： 支持使用IPv4地址（例如，1.XX.XX.1）、IPv6地址（例如，2001:db8:ffff:ffff:ffff:ffff:ffff:ffff）。 支持使用IP网段格式（例如，1.XX.XX.1/16）。	属于、不属于； 等于、不等于； 包含、不包含； 前缀匹配、后缀匹配
		等于、不等于； 包含、

Referer	请求的来源网址，即该请求从哪个页面跳转产生。	不包含；前缀匹配、后缀匹配
User-Agent	发起请求的客户端的浏览器标识、渲染引擎标识和版本信息等浏览器相关信息。	同上
Cookie	请求中的Cookie信息。	同上
Get Patam	在编程和软件开发中获取所需参数的过程或操作	同上
处置动作	选择当请求命中该规则时，要执行的防护动作。可选项： **拦截**：表示拦截命中规则的请求，并向发起请求的客户端返回拦截响应页面。说明WAF默认使用统一的拦截响应页面，您可以通过自定义响应功能，自定义拦截响应页面。 **观察**：表示不拦截命中规则的请求，只通过日志记录请求命中了规则。您可以通过WAF日志，查询命中当前规则的请求，分析规则的防护效果（例如，是否有误拦截等）。观察模式方便您试运行首次配置的规则，待确认规则没有产生误拦截后，再将规则设置为拦截模式。 **滑块**：表示WAF向客户端返回滑动验证页面。如果客户端成功执行滑动验证，则WAF在一段时间（默认30分钟）内放行该客户端的所有请求（不需要重复验证），否则拦截请求。 **严格滑块**：表示WAF向客户端返回滑动验证页面。如果客户端成功执行滑动验证，则WAF放行本次请求，否则拦截请求。严格滑块验证模式下，客户端的每次请求都需要验证。 **回源标记**：用户可以自定义Header及内容，WAF不会直接处理，而是会通过新增Header的方式将命中信息返回给源站，用户可以与后端风控系统结合做业务侧处理。	/

4.查看Bot统计报表

Bot统计报表

1、防护总览 通过折线图，展示在指定时间范围内，Bot管理防护策略中已配置的【规则动作】和【规则命中】情况。

> 单击具体的规则动作或规则，显示或隐藏该折线图。将光标放置在折线图上的某一点，可以查看该时刻的具体数据。纵轴为次，横轴为时间可拖动缩放时间线。
>
> **规则动作包括**：请求次数、拦截、观察、滑块、严格滑块、回源标记
>
> **命中规则包括**：自定义Bot策略、业务安全、AI智能防护、IP限速、会话限速

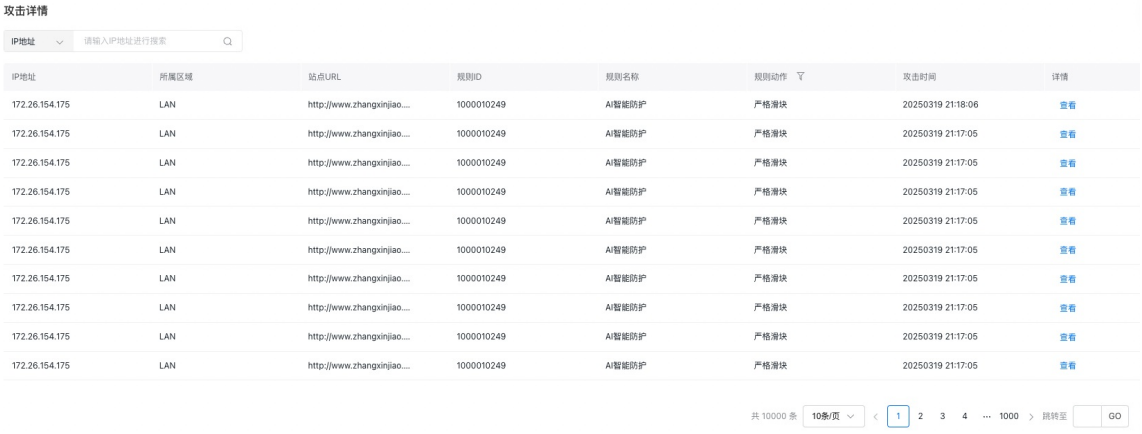
2、规则命中统计

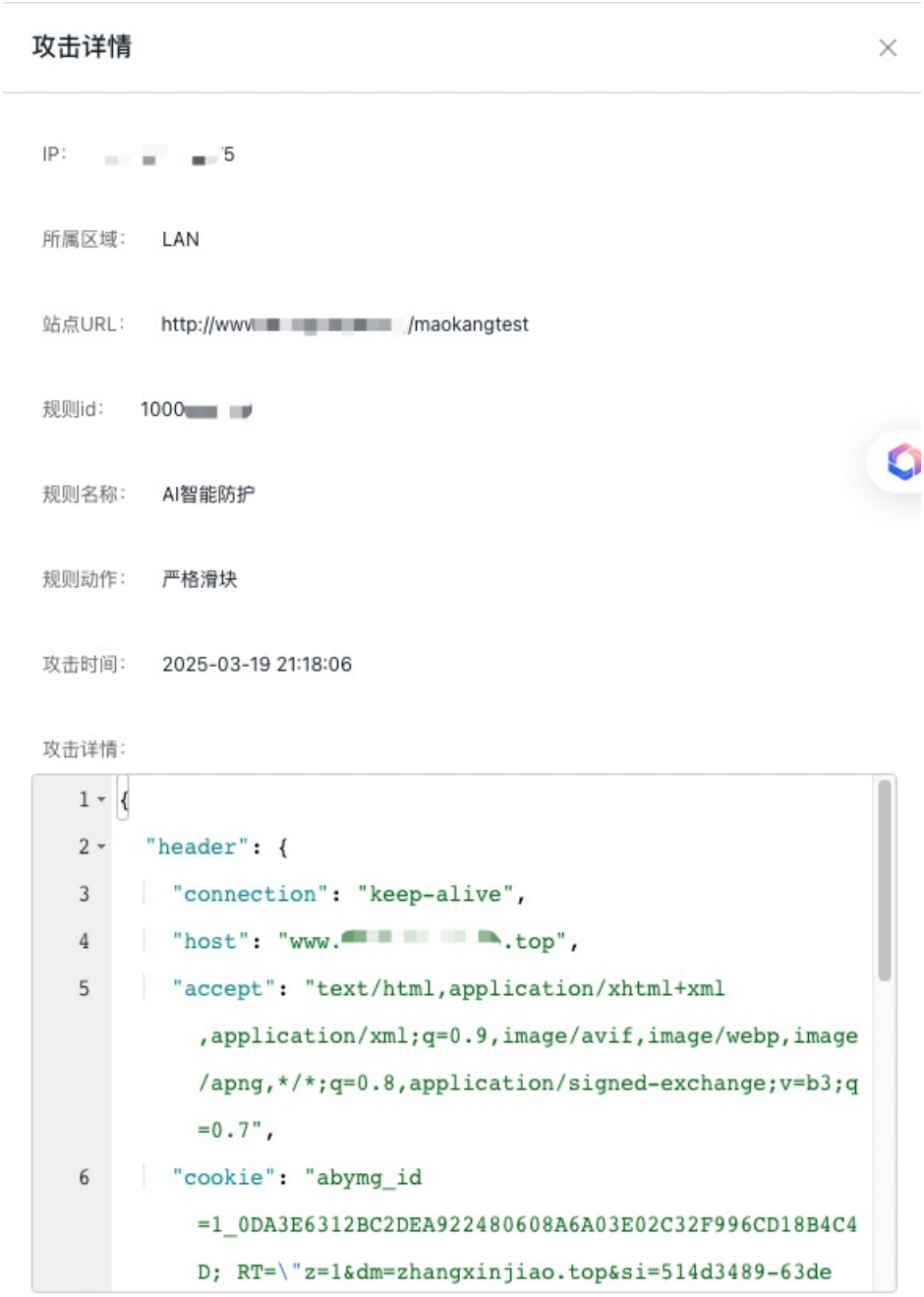
通过列表，展示已配置的防护规则的规则ID、防护域名、包含观察模式的命中次数情况。 列表每页最多展示5条，超过翻页显示。

通过切换tap展示被拦截、滑块、严格滑块、回源标的Top 10攻击源IP及其攻击次数。

3、攻击详情

通过列表，展示在指定时间范围内（时间同Bot报表顶部时间保持一致），命中Bot管理防护规则的IP情况，包括攻击IP、IP所属区域、URL、规则ID、规则名称、规则动作等信息。





自定义拦截页面

接入Web应用防火墙（Web Application Firewall，简称WAF）后，您可以自定义客户端请求被WAF拦截时返回给客户端的拦截页面的样式和内容，包括状态码、响应头、HTML返回页面。

前提条件

已开通Web应用防火墙服务 已将Web业务进行WAF接入配置

操作步骤

如果未设置自定义拦截页面，WAF拦截客户端请求时，默认向客户端返回统一的拦截页面。

您可以通过设置自定义拦截响应的内容，包括响应头字段Response Headers、HTML返回页面等。

1. 登录Web应用防火墙
2. 在左侧导航栏，选择**配置中心** > **基础配置**
3. **自定义拦截页面**-**设置**填写配置信息

自定义拦截页面

状态码

状态码: 403

自定义Header

Header名 Header值

AS-123_2d header

+添加

HTML返回页面

默认HTML页面生成

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <title>{:{response_code}:}</title>
    <script>
        (function (doc, win) {
            var dummy = doc.createElement('_').style;
            dummy.width = '1vw';
            if (dummy.width) {
                return;
            }
            var docEl = doc.documentElement,
                resizeEvt = 'orientationchange' in win ?
                  'orientationchange' : 'resize',
                recalc = function () {
                    var clientWidth = docEl.clientWidth;
                    if (!clientWidth) {
                        return;
                    }
                    docEl.style.fontSize = (clientWidth / 20)
                      + 'px';
                };
            recalc();
            win.addEventListener(resizeEvt, recalc, false);
        })(document, window);
    </script>
    <style>
        * {
```

页面关键字说明：响应码：{:{response_code}:} 拦截类型：:{action_type}:} 规则ID：:{rule_id}:}

对不起，由于您的访问存在安全风险，已经被拦截，错误状态码：[redacted]

拦截类型：[redacted] 规则ID：[redacted]

误报反馈 官网访问

配置项	说明
状态码	客户端请求被WAF拦截时，WAF返回给客户端的HTTP状态码。WAF的默认拦截状态码为403
自定义header	设置客户端请求被WAF拦截时，WAF返回给客户端的响应包含的头字段。 每个头字段包含header名和header 值。最多支持添加五个header字段。 **header名**：请求 uuid，请求客户端 IP，X-Frame-Options、X-Content-Type-Options、Content-Security-Policy、自定义字段 **header值**：最长100个字符
HTML返回页面	设置自定义拦截页面的源代码。配置要求如下： 支持使用HTML格式 您可以通过自定义header，指定响应体的格式 代码字符长度不超过4000 误报反馈：https://cloud.baidu.com/survey/connect-us.html 返回官网：https://cloud.baidu.com/product/waf.html

【确定保存】后，所有实例的拦截页面将被替换为您在自定义拦截页面中设置的内容。
如果要恢复默认拦截页面，请在HTML返回页面中设置默认HTML页面生成，

日志投递

概述

当您有日志等保合规需求，开启日志投递服务后，WAF产生的所有访问日志（含攻击日志）数据将推送投递到 BLS（日志服务），产生费用将由BLS收取，计费参照对应服务计费规则BLS计费详情

前提条件

1.已开通SaaS WAF服务

2.已经将Web业务添加为WAF的防护对象

操作步骤

1.登陆Web应用防火墙控制台。在左侧导航栏，选择配置中心>日志投递服务。

2.在BLS服务界面创建投递路径，完成投递路径的相关配置，单击保存即可生效。

配置项	说明
选择实例	为日志投递任务选择日志来源，所选实例的全部访问日志都将被投递到指定路径。
投递的服务	支持投递者BLS
投递路径	如果预先没有创建投递路径，请在对应服务界面创建路径后再选择投递路径。保存后创建任务名称：WAF*yyyymmdd*'投递服务'_'当日该投递服务创建任务数' eg：WAF_20240624_BLS_02 保存后创建路径：投递多个实例，则在对应服务Bucket下，创建多个命名为【waf-实例id+时间年月日时分】的日志路径 例如：waf-e23457-2024080916.zip
投递间隔时间	默认60分钟，不可更改。 用户创建任务后，创建开始60分钟内存储日志，60分钟后正式投递
压缩类型	BLS：默认JSON
投递授权	保存任务后，您将自动授权WAF，将日志投递到对应存储服务Bucket或日志集，并创建带有WAF标识路径

3.在投递任务列表中，找到创建的投递任务，日志投递服务默认为开启状态，关闭目标任务的日志投递服务，则停止日志投递。

5.单击删除即可删除投递任务。

6.单击编辑，可以编辑投递任务配置。

7.设置完成后，如需查看日志，可以通过BLS平台操作您投递的日志，实现数据的获取与分析。

说明：日志投递功能仅适用于开启日志投递任务后新生成的日志。

信息泄露防护

概述

接入Web应用防火墙（Web Application Firewall，简称WAF）后，您可以通过设置信息泄露防护规则，可以通过设置信息泄露防护规则，使得网站过滤服务器返回内容（例如异常页面、关键字）中的敏感信息（包含身份证号、电话号码、银行卡号、敏感词汇），脱敏展示敏感信息或返回默认异常响应页面。

前提条件

1.已开通Web应用防火墙SaaS WAF服务

2.已将Web业务进行WAF接入配置

操作步骤

1.登录Web应用防火墙

2.在左侧导航栏，选择配置中心 > Web防护规则。

3.创建Web防护规则，填写规则基本信息

4.在信息泄露防护模块，添加策略 您可以指定检测响应码、敏感信息、敏感关键字分类下的一种或多种类型。 如果选中并且，则可以进一步指定要检测的URL，即只在指定的页面中检测敏感信息。

配置项	说明
策略名称	1~40位字符，支持中文，英文及数字，符号仅限/_-
匹配条件	定义要在请求响应中检测的敏感信息类型，可选值： **响应码**：400、401、402、403、404、500、501、502、503、504、405~499、505~599，避免响应页面暴露泄漏数据 **敏感信息**：下拉框选择身份证、银行卡、电话号码。重要防敏感信息泄露功能目前仅支持处理中华人民共和国境内使用的数据格式（例如身份证号、电话号码、银行卡号），暂不支持处理中国境外的身份证号、电话号码、银行卡号等数据格式。 **敏感关键字**：支持自定义敏感关键字，1-40个字符
阻断类型	定义在请求响应中检测到敏感信息后执行的操作： 1.匹配条件为**响应码**时，支持以下匹配动作： **观察**：表示不拦截命中规则的请求，只通过日志记录请求命中了规则。 **拦截**：表示拦截命中规则的请求，并向发起请求的客户端返回该模版生效的自定义拦截响应页面。 2.匹配条件为**敏感信息/敏感关键字**时，支持以下匹配动作： **打码**：表示不拦截命中规则的请求，只将敏感信息中部分内容替换成星号（*）显示。 **观察**：表示不拦截命中规则的请求，只通过日志记录请求命中了规则。

Web 应用集成SDK

Web 应用集成SDK

您必须在应用中集成JSSDK，才能配置网页防爬场景化规则。本文介绍了如何为Web应用集成WAF防护JSSDK（以下简称JSSDK）。

组件

Web JSSDK集成包括JavaScript挑战、异步接口响应两个组件。

JavaScript挑战组件

JavaScript挑战组件是JavaScript挑战能力的Web集成模块。当在控制台配置开启了网页防爬场景化的JavaScript挑战能力之后，WAF会对访问了该配置路径的流量发起JavaScript挑战，若客户端未通过挑战，则不会返回真实页面，会对拒绝的请求并返

回JavaScript挑战验证页。

JavaScript挑战组件会在客户端页面的域名下植入cookie，以帮助客户端完成JavaScript挑战，站长可以通过自动集成或者手动集成的情况下接入该组件，在自动集成的情况下，WAF会为站点所有页面在最前方注入该组件，而在手动集成的情况下，客户需要手动将该组件写在页面最前方位置。

在客户端中，若发起的页面请求，WAF会返回一个可以执行JavaScript代码中间页，并在中间页中加载并执行该组件种下cookie，之后刷新页面。若客户端发起的是异步请求，WAF会在该异步请求所在页面的最前方注入并执行该组件，以种下cookie。 JavaScript挑战植入的cookie是有有效期的，在页面集成该组件的情况下，定期刷新这个cookie，以保证cookie在有限期内。

异步接口响应组件

在防爬场景化配置页面中，可以配置对指定条件下的接口开启了动态签名功能，以及滑块验证码功能，这两个功能需要通过自动或者手动方式集成异步接口响应组件来完成。 异步响应组件包含两个能力，客户端签名能力和验证码弹出能力，自动集成了异步响应组件之后，组件将接管Web应用的异步请求，在请求发起与请求响应时，完成指定挑战任务（动态签名挑战与验证码挑战），待客户端完成挑战任务之后，客户端才会执行后续动作。

异步接口响应组件自动集成工作原理：

1、Hook异步API：在自动集成异步接口响应组件的情况下，组件会全局重写XMLHttpRequest（xhr）、Fetch两个异步请求的Web API，在API接口请求对象上额外封装一层代码，通常情况不会影响原始对象的各种特性。

2、动态签名注入：对通过XMLHttpRequest、Fetch这两个Web API发起的所有异步接口的请求URL中添加一个query参数作为动态签名。

3、验证码挑战：当异步请求响应式，组件会通过Hook先判断当前response是否为WAF发起的验证码挑战标识，若response为验证码挑战标识，页面会弹出验证码进行验证码挑战，待客户端完成挑战后，携带验证码Token对请求进行重试，若response并非为WAF返回的验证码挑战标识，组件不会执行任何动作，将结果传递给站点本身的JS代码执行。

> 说明：异步接口响应组件Hook功能只会对XMLHttpRequest和fetch发起的异步请求添加动态签名挑战与验证码挑战，对于SSE（Server-Sent Events）、Form表单提交、Image、script标签发起的请求，不会自动完成异步接口响应组件的挑战。

自动集成异步接口响应组件时：

会自动进行XMLHttpRequest和fetch的hook，此时hook可能会产生兼容性冲突问题（详情见下文兼容性说明章节），若无法处理产生的冲突，则可以选择使用手动集成的形式，手动集成形式不会对XMLHttpRequest和fetch进行hook，站长需要通过异步接口响应组件提供的JSAPI，在防护场景的API接口上手动进行动态签名注入和验证码挑战。

手动集成异步接口响应组件时：

- 对于动态签名能力，需要确保配置并开启了动态签名场景化保护的接口一定要携带上动态签名，否则WAF将会拒绝访问
- 对于滑块验证码能力，需要确保配置并开启了异常流量处置的场景化保护接口在被WAF返回验证码挑战标识之后，若要对接口进行重试，必须携带上验证码验证通过之后的token，否则waf会再次返回验证码挑战标识

部署方式

1、自动集成

可在配置网页防爬场景化的防护场景定义时，选择自动集成，此时网站HTML页面由WAF接管，WAF会在页面请求响应时，向页面注入组件script标签，客户网页无需进行代码改造即可完成部署，同时享受线上组件的热更新。

2、手动集成 适合于无法满足自动集成的场景，或者当前站点与组件产生冲突的情况，手动集成必须满足以下条件

- 所有依赖配置了防护场景的 API 接口所在的页面，都必须接入特定组件
- 在页面使用组件功能之前，必须先完成组件script代码的注入

JavaScript挑战组件

```
<script>window.__noxlmd = 1</script>
<script src="https//sec-captcha-waf.cdn.bcebos.com/static/wb/1.0/nox_20241230.js"></script>
```

异步接口响应组件

```
<script src="https//sec-captcha-waf.cdn.bcebos.com/static/wb/1.0/tox_20241230.js"></script>
```

如内容安全策略csp不允许从sec-captcha-waf.cdn.bcebos.com加载资源，可将组件资源下载至服务本地进行本地化部署

3、JSAPI

在手动集成了异步接口响应组件之后，可通过一下JSAPI生成动态签名和验证码挑战。

动态签名生成：

1、通过Tox.getToken获取动态签名，若网络波动导致异步接口响应组件加载失败，可以使用错误码 499 作为降级签名

```
var toxToken = typeof Tox !== 'undefined' ? Tox.getToken() : '499';
```

2、将toxToken添加到防护场景的API接口的URL Query参数中，query的key为tox_token，value为toxToken，如下

```
/path/to/request?query1=value1&tox_token={toxToken}
```

验证码挑战：

1、通过 Tox.isCaptchaResponse 先判断当前response是否为WAF发起的验证码挑战标识。

```
// 传入响应状态码status、响应类型content-type、响应体body
const isWafCaptchaFlag = Tox.isCaptchaResponse(status, contentType, responseBody);
```

2、然后通过 Tox.getCaptchaToken 发起验证码挑战，并通过回调获取验证码通过之后的token。

```
// 传入响应体body、回调函数callback
Tox.getCaptchaToken(responseBody, function (captchaToken) {
    // 处理captchaToken
});
```

3. 将captchaToken添加到防护场景的API接口的URL Query参数中，query的key为svcp_stk，value为captchaToken，如下：

```
/path/to/request?query1=value1&svcp_stk={captchaToken}
```

常见问题

兼容性说明 1.浏览器环境兼容性：兼容IE10内核以上各类浏览器与客户端容器。

2.兼容性依赖：客户端需要支持cookie功能。容器或请求本身不支持cookie，则JavaScript挑战组件功能会被影响。

3.Hook兼容。

> 第三方组件冲突：异步接口响应组件会对所有异步请求的query中添加参数，这会与不支持多余query参数的第三方组件产生冲突
>
> 非标异步请求冲突：异步接口响应组件在添加query参数过程中，会按照标准对请求的URL进行解析并编码，若服务器接口

> 解析URL的方式不标准，则会产生冲突
>
> 关于Hook兼容冲突问题，可通过手动接入的形式避免冲突的产生。

组件副作用说明

性能增加

> 1、自动集成情况下，会在页面head标签中注入组件script，若网络波动导致组件加载过慢，会导致页面出现白屏。
>
> 2、自动集成情况下，异步接口响应组件会为页面接口无差别添加动态签名tox_token，这会消耗部分计算资源

报警设置

****Web 应用防火墙支持常见事件的报警。

网站接入Web应用防火墙（Web Application Firewall，简称WAF）后，您可以通过报警设置，使WAF在网站请求流量中检测到攻击事件、异常流量时向您发送告警通知，帮助您及时掌握业务的安全状态。本文介绍如何设置报警。

前提条件

- 已将网站接入WAF防护。

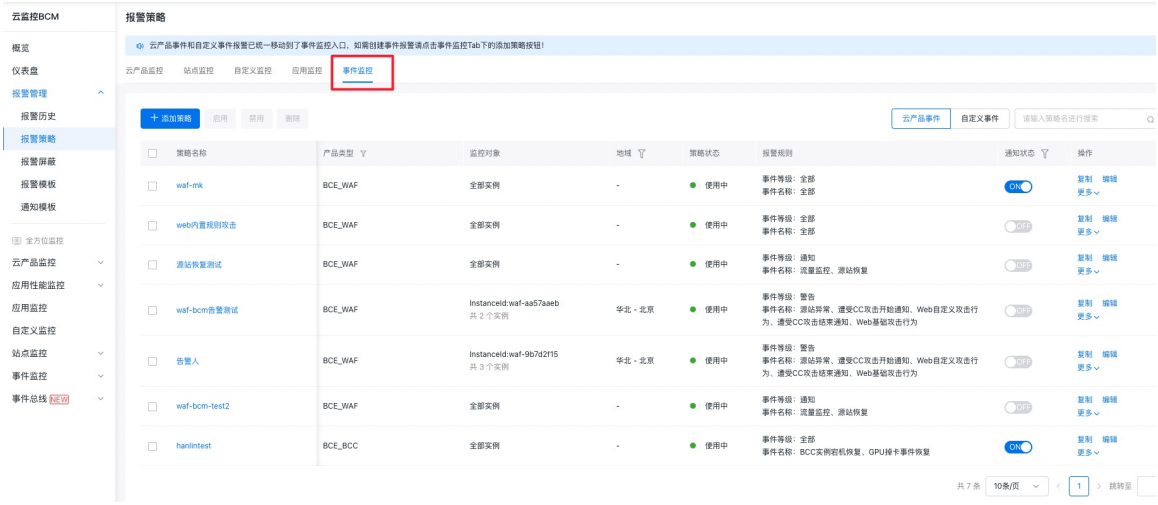
操作步骤

1. 登录Web应用防火墙（WAF）控制台。
2. 在左侧导航栏，选择**配置中心 > 告警设置**
3. 在**报警设置**页面，根据事件类型，进入BCM云监控通知配置。

> 注意： 如需要修改或者关闭WAF旧版本默认告警，需进入云监控配置告警后，才可以在报警列表开启或者关闭告警，避免因为频繁告警造成干扰

4.进入**云监控通知（BCM）**配置

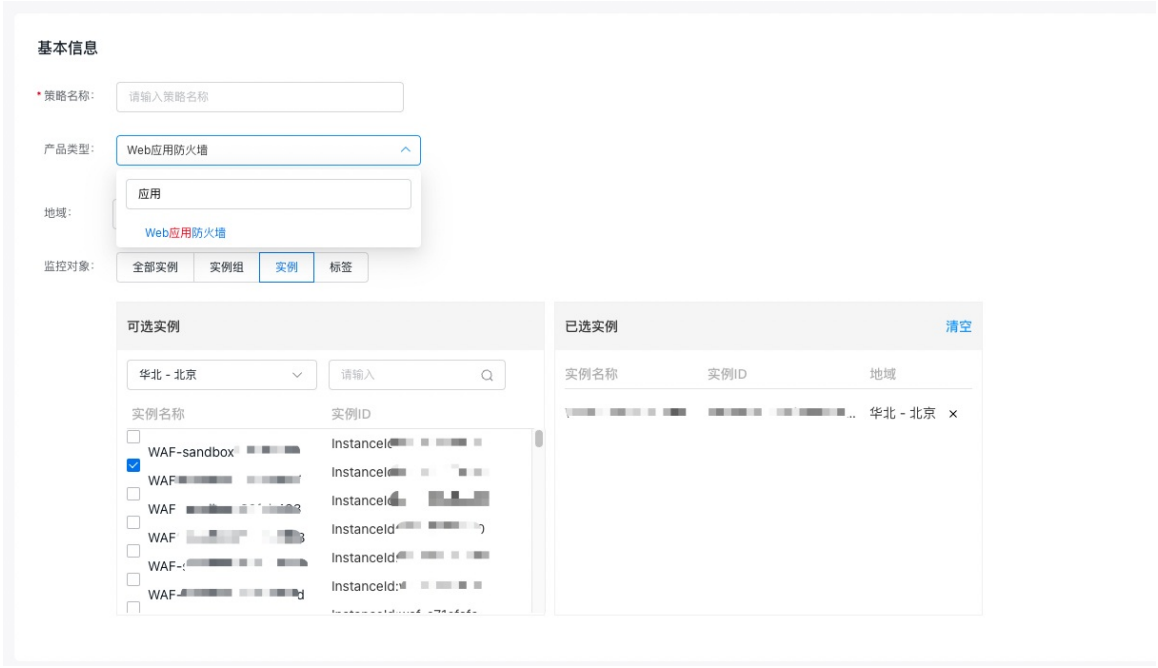
点击【报警管理】，进入【事件告警】tab，【添加策略】



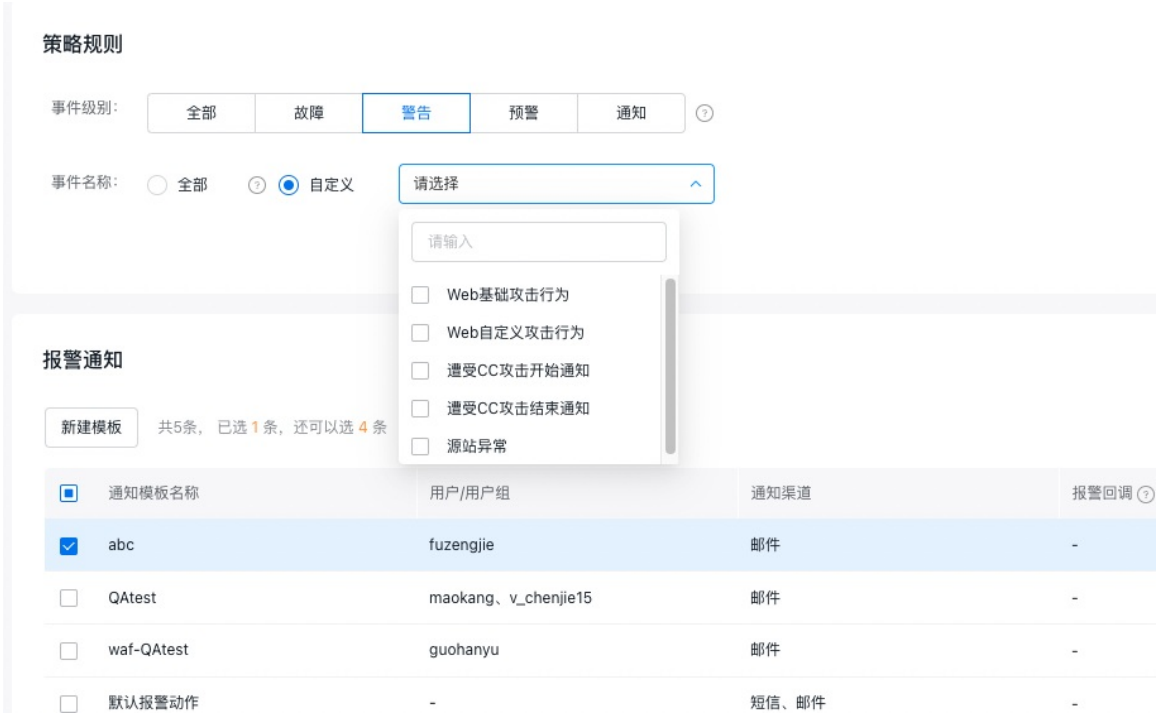
报警列表： 在报警策略列表，可对报警通知进行开启和关闭、启用、禁用操作（**首次需进行报警配置后，可在列表进行告警开关闭**）

报警配置：

进入报警策略页面，添加策略，搜索【Web应用防火墙】，选择对应的实例或全部实例，配置对应的告警策略

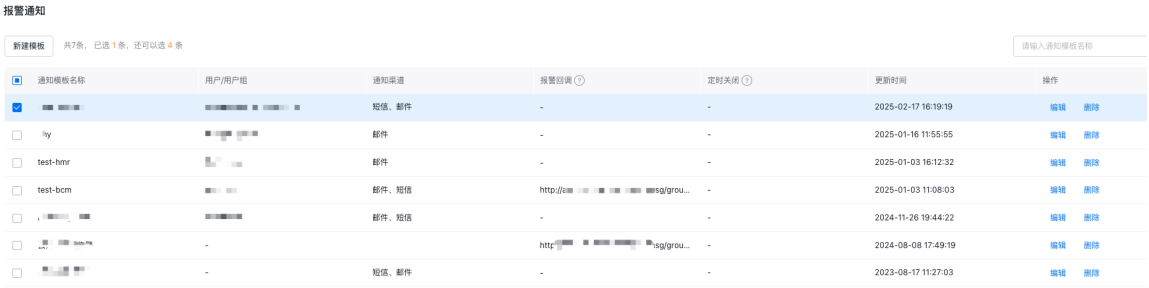


可以自定义选择攻击事件进行告警配置：

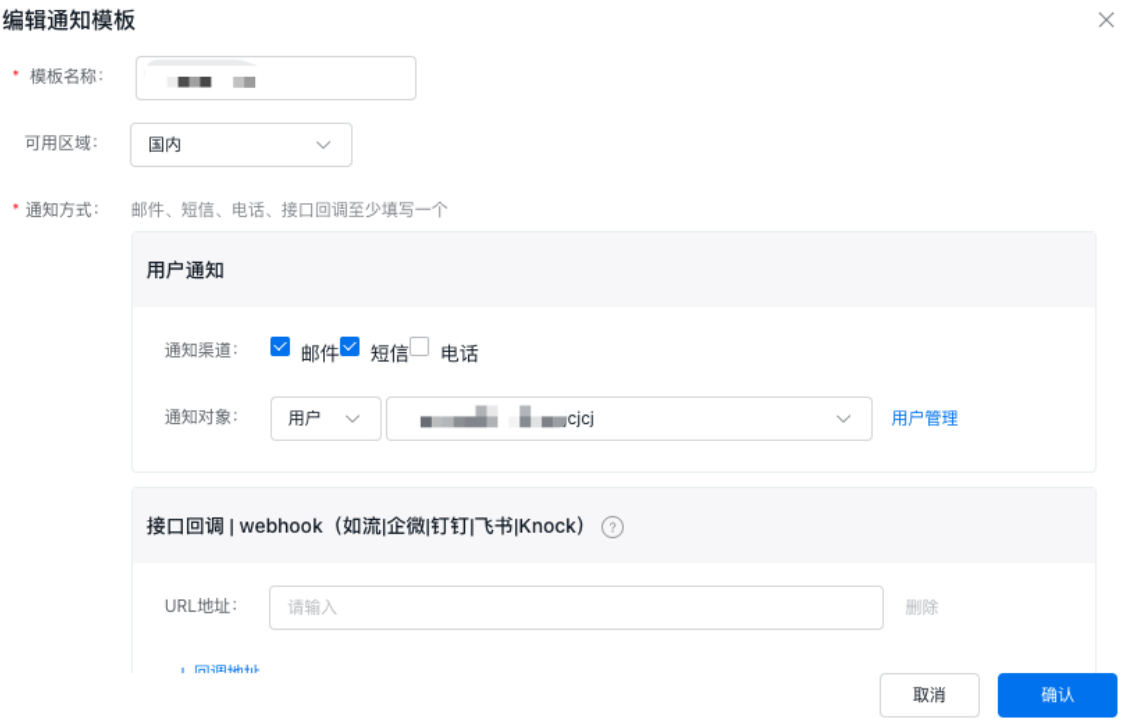


报警通知：

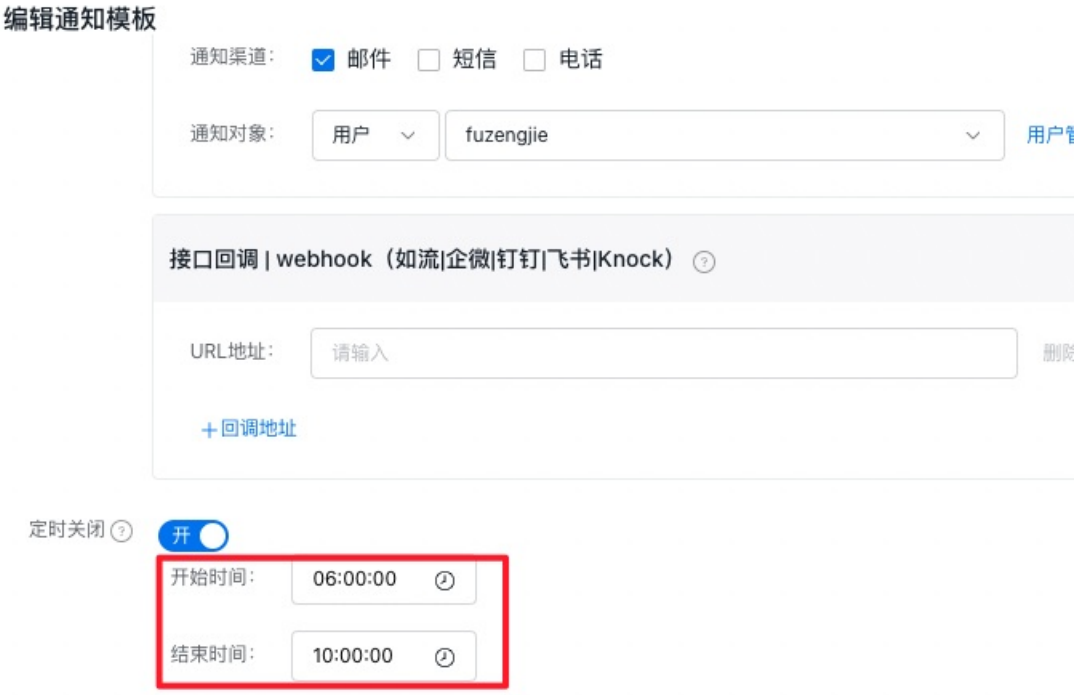
选择对应报警通知模版，支持短信、邮件、电话通知，并自定义通知用户



接口回调支持webhook（如流|企微|钉钉|飞书|Knock） 等。



也可以设置定时关闭报警： 可以自定义配置不接收报警通知时间段，报警通知关闭时将不发送报警通知，但在报警历史里会显示报警内容



报警设置类型说明

当前报警类型支持安全事件和业务监控

安全事件：

安全事件	报警说明
Web基础攻击行为	基于大量的突发流量型Web攻击拦截事件告警，告警后可在攻击日志查看攻击时间、拦截和请求次数，攻击流量分析。
CC攻击行为	检测到存在CC攻击恶意消耗计算资源业务响应慢，进行拦截事件告警，告警后可在攻击日志查看攻击时间、拦截和请求次数，攻击流量分析。
Web自定义攻击行为	基于大量的突发访问自定义Web防护规则或BOT攻击拦截事件告警，告警后可在攻击日志查看攻击时间、拦截和请求次数，攻击流量分析。

业务监控：

业务监控	报警说明
源站异常	基于异常业务流量统计数据支持，您可依赖产品提供的异常业务流量统计数据指标，结合自己的异常业务需求，配置定制的异常业务监控告警事件，并可自定义配置事件的通知方式和通知对象。
源站恢复	检测到源站在访问超时或者错误之后恢复正常。
流量监测	基于业务流量的监控提前预警，避免流量耗尽影响站点服务，您可根据产品提供的业务流量统计数据指标，结合自己的业务需求，配置定制的业务监控告警事件，并可自定义配置事件的通知方式和通知对象。

API参考

概述

API 概述

欢迎使用百度智能云的应用防火墙服务（WAF，Web Application Firewall Service，以下简称 WAF）。 WAF 遵循依据百度智能云

的 API 设计规范，对外提供 Restful API。您可以通过 API 实现对WAF 产品的管理使用。

如果您是初次调用百度智能云产品的API，可以观看API入门视频指南，快速掌握调用API的方法。

接口类型

接口类型	接口描述
BLB-WAF-API	BLB-WAF相关的接口，包括WAF实例查询，可绑定的blb查询，绑定、解绑blb，可配置的子域名查询，下发、查询WAF配置等。
CDN-WAF-API	CDN-WAF相关的接口，包括WAF实例查询，可绑定的blb查询，绑定、解绑blb，可配置的子域名查询，下发、查询WAF配置等。
WAF数据报表接口	WAF的报表类接口，包括WAF实例的详情查询，攻击事件详情查询，攻击事件数量趋势查询等。

使用须知

了解以下内容可以帮助您更好地使用API操作WAF服务：

- 签名认证
- 幂等性
- 时间与日期
- 排版约定

签名认证

WAF API会对每个访问的请求进行身份认证，以保障用户的安全。安全认证采用Access Key与请求签名机制。Access Key由Access Key ID和Secret Access Key组成，均为字符串，由百度智能云官方颁发给用户。其中Access Key ID用于标识用户身份，Access Key Secret 是用于加密签名字符串和服务器端验证签名字符串的密钥，必须严格保密。

签名字符串格式

```
bce-auth-v{version}/{accessKeyId}/{timestamp}/{expireTime}/{signedHeaders}/{signature}
```

签名申请步骤

关于AK/SK的获取，请参看获取AK/SK

签名生成算法

有关签名生成算法的具体介绍，请参看鉴权认证机制

幂等性

当调用创建接口时如果遇到了请求超时或服务器内部错误，用户可能会尝试重发请求，这时用户通过clientToken参数避免创建出比预期要多的资源，即保证请求的幂等性。

幂等性基于clientToken，clientToken是一个长度不超过64位的ASCII字符串，通常放在query string里，如`<http://bss.bj.baidubce.com/open-api/v2/wafStatistics/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20。>`

如果用户使用同一个clientToken值调用创建接口，则服务端会返回相同的请求结果。因此用户在遇到错误进行重试的时候，可以通过提供相同的clientToken值，来确保只创建一个资源；如果用户提供了一个已经使用过的clientToken，但其他请求参数（包括queryString和requestBody）不同甚至url Path不同，则会返回IdempotentParameterMismatch的错误代码。

clientToken的有效期为24小时，以服务端最后一次收到该clientToken为准。也就是说，如果客户端不断发送同一个

clientToken，那么该clientToken将长期有效。

时间与日期

日期与时间的表示有多种方式。为统一起见，除非是约定俗成或者有相应规范的，凡需要日期时间表示的地方一律采用UTC时间，遵循ISO 8601，并做以下约束：

- 表示日期一律采用YYYY-MM-DD方式，例如2014-06-01表示2014年6月1日
- 表示时间一律采用hh:mm:ss方式，并在最后加一个大写字母Z表示UTC时间。例如23:00:10Z表示UTC时间23点0分10秒。
- 凡涉及日期和时间合并表示时，在两者中间加大写字母T，例如2014-06-01T23:00:10Z表示UTC时间2014年6月1日23点0分10秒。

排版约定

排版格式	含义
< >	变量
[ ]	可选项
{ }	必选项
|	互斥关系
等宽字体 Courier New	屏幕输出

API服务域名

WAF API的服务域名为：

Region	Endpoint	Protocol
全局	bss.bj.baidubce.com	HTTP and HTTPS
北京	bss.bj.baidubce.com	HTTP and HTTPS
广州	bss.gz.baidubce.com	HTTP and HTTPS
苏州	bss.su.baidubce.com	HTTP and HTTPS
上海	bss.fsh.baidubce.com	HTTP and HTTPS
武汉	bss.fwh.baidubce.com	HTTP and HTTPS
保定	bss.bd.baidubce.com	HTTP and HTTPS

说明：WAF API支持HTTP和HTTPS两种调用方式。为了提升数据的安全性，建议通过HTTPS调用。

调用规范

数据交换格式为JSON，所有request/response body内容均采用UTF-8编码。URL参数中所使用的IP均使用点分十进制表示。

请求参数

请求参数包括如下4种：

参数类型	说明
URI	通常用于指明操作实体,如:PUT /v1/schedule/{scheduleId}
Query参数	URL中携带的请求参数
HEADER	通过HTTP头域传入,如:x-bce-date
RequestBody	通过JSON格式组织的请求数据体

API版本号

参数	类型	参数位置	描述	是否必须
version	String	Url参数	当前API版本为2	是

返回值说明

返回值分为两种形式：

返回内容	说明
HTTP STATUS CODE	如200,400,403,404等
ResponseBody	JSON格式组织的响应数据体

公共头

公共请求头

下表列出了所有waf API所携带的公共头域。HTTP协议的标准头域不在此处列出

头域（HEADER）	是否必须	说明
Authorization	是	包含Access Key与请求签名
Content-Type	是	application/json; charset=utf-8
x-bce-date	否	表示日期的字符串，符合BCE API规范
Host	是	表示请求API的域名

公共响应头

下表列出了所有Waf API的公共响应头域。HTTP协议的标准响应头域不在此处列出

头域（HEADER）	说明
Content-Type	只支持JSON格式，application/json; charset=utf-8
x-bce-request-id	Waf后端生成，并自动设置到响应头域中

错误返回

请求发生错误时通过respone body返回详细错误信息，遵循如下格式：

参数名	类型	说明
code	String	错误码
message	String	错误描述
requestId	String	本次请求的requestId

示例：

```
 {
   "requestId" : "ae2225f7-1c2e-427a-a1ad-5413b762957d",
   "code" : "NoSuchKey",
   "message" : "The resource you requested does not exist"
}
```

错误码分百度智能云公共错误码和WAF服务特有错误码两类，具体错误码如下：

BCE公共错误码

错误返回码	错误消息	状态码	说明
AccessDenied	Access denied.	403Forbidden	无权限访问对应的资源。
InappropriateJSON	The JSON you provided was well-formed and valid, but not appropriate forthis operation.	400 Bad Request	请求中的JSON格式正确，但语义上不符合要求。如缺少某个必需项，或值类型不匹配等。出于兼容性考虑，对于所有无法识别的项应直接忽略，不应该返回这个错误。
InternalError	We encountered an internal error Please try again.	500 Internal Server Error	所有未定义的其他错误。在有明确对应的其他类型的错误时（包括通用的和服务自定义的）不应该使用。
InvalidAccessKeyId	The Access Key ID you provided doesnot exist in our records.	403Forbidden	Access Key ID不存在。
InvalidHTTPAuthHeader	The Access Key ID you provided does notexist in our records.	400 BadRequest	Authorization头域格式错误。
InvalidHTTPRequest	There was an error in the body of your HTTP request.	400 Bad Request	HTTP body格式错误。例如不符合指定的Encoding等。
InvalidURI	Could not parse the specified URI.	400 Bad Request	URI形式不正确。例如一些服务定义的关键词不匹配等。对于ID不匹配的问题，应定义更加具体的错误码，如NoSuchKey。
MalformedJSON	The JSON you provided was not well-formed.	400 BadRequest	JSON格式不合法。
InvalidVersion	The API version specified was invalid.	404 NotFound	URI的版本号不合法。
OptInRequired	A subscription for the service is required.	403Forbidden	没有开通对应的服务。
PreconditionFailed	The specified If-Match header doesn’tmatch the ETag header.	412PreconditionFailed	详见Etag。
RequestExpired	Request has expired. Timestamp date is <Data>.	400 BadRequest	请求超时。要改成x-bce-date。若请求中只有Date，需将Date转成datetime。
IdempotentParameterMismatch	The request uses the same client token asa previous, but non-identical request.	403Forbidden	clientToken对应的API参数不一样。
	The request signature we calculated does not match	400	

SignatureDoesNotMatch	the signature you provided. Check yourSecret Access Key and signing method. Consultthe service documentation for details.	Bad Request	Authorization头域中附带的签名和服务端验证不一致。

Waf业务错误码

错误码	错误描述	HTTP状态码	语义
ReadWafDenied	No read waf permission	403	无waf读服务权限
OperateWafDenied	No operate waf permission	403	无操作waf权限
WafAdminDenied	No waf admin permission	403	无waf管理权限
UnsupportedWAFOperation	The status of specified waf does not support this operation	400	waf实例的状态不支持操作
WafInterfaceError	The interface not supporte this kind of waf type	400	调用的接口不支持传入的waf实例类型
WafBindNotFound	The specified waf bind does not exist	404	要绑定的blb未找到
WafUnBindNotFound	The specified waf unbind does not exist	404	要解除绑定的blb未找到
WafBindRepeatError	The specified waf bind is repetition	400	waf已经绑定过blb了并且没解绑
InvalidParameter	Invalid Parameters	400	接口传入的参数不符合要求

WAF数据报表相关接口

WAF查询实例详情

接口描述

查询waf的实例详情，包括waf实例的状态，waf到期时间，以及配置的规则数量，近日web防护和自定义规则拦截的攻击事件的统计。

- 注意需要指定waf标志符才能正常调用。

请求结构

```
GET /v{version}/wafStatistics/{waf_id}?clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
waf_id	String	是	URL参数	waf标志符
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
payType	String	支付方式
wafName	String	waf名称
status	String	waf实例状态:可以是available/paused/pausing/updating/deleting/deleted
endTime	String	到期时间
rule	Object	已经配置的访问规则和剩余可配置的规则
webAttack	Object	web攻击事件近日统计
customAttack	Object	自定义规则攻击事件近日统计

请求示例

```
 GET /v2/wafStatistics/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

返回示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
    "payType": "prepay|postpay",         //支付方式
    "wafName": "WAFNAME",                 //WAF NAME
    "status": "STATUS",                   //WAF实例状态:available/paused/pausing/updating/deleting/deleted
    "endTime": "2017-03-14 16:40:43",    //到期时间：本地时间
    "rule": {
        "used": COUNT,                  //已配置的访问规则，INT型
        "use": INIT,                   //剩余可配置的访问规则，INT型
    },
    "webAttack": {
        "today": COUNT,                 //今天受web攻击次数，INT型
        "lastWeek": INIT,              //最近七天受web攻击次数，INT型
    },
    "customAttack":  {
        "today": COUNT,                 //已今天受到自定义规则次数，INT型
        "lastWeek": INIT,              //最近其他受到自定义攻击次数，INT型
    },
}
```

WAF查询攻击事件详情

接口描述

查询一段时间内攻击事件的详情列表。需要指定攻击事件的类型，必须是全部事件、web攻击事件、自定义规则阻拦事件的一种。需要指定开始时间和结束时间，用时间戳表示。

请求结构

```
GET /v{version}/wafEvent/{waf_id}?type={type}&beginTime={time}&endTime={time}&pageNo={pageno}&pageSize={pagesize}&clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
waf_id	String	是	URL参数	waf标志符
type	String	是	QUERY 参数	取值 all、webAttack、customAttack 分别表示全部事件、web攻击事件、自定义规则阻拦事件
beginTime	TIMESTAMP	是	QUERY 参数	时间戳：选择事件开始时间段
endTime	TIMESTAMP	是	QUERY 参数	时间戳：选择事件结束时间段
pageNo	Int	是	QUERY 参数	显示攻击事件列表页号
pageSize	Int	是	QUERY 参数	每页条数
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
data	List<AttackEvent>	waf拦截的攻击事件的列表
total	Int	攻击事件的数量

请求示例

```
GET /v2/wafEvent/waf-3a4b5c?type=webAttack&beginTime=1546963200&endTime=1547625600&pageSize=10&pageNo=1&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

返回示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
   "data": [
      {
         "time": "2017-03-14 19:49:53",          //发生事件,本地时间
         "bcc": ["instance_id1", "instance_id2"],  //受影响资产
         "ip": "ip",                            //攻击者IP
         "addr": "美国",                         //攻击值地址
         "userAgent": "baidu spider",            //攻击者伪装
         "url": "URL",                          //攻击者URL
         "ruleId": "zdy_id",                    //当用户设置自定义后这里为用户自定义规则名字
         "ruleName": "sql-0001",                //防御模式
         "ruleInfo": "SQL注入",                  //安全事件
         "type": "deny|log",                    //匹配模式
         "body": "body",                        //匹配内容
      },
      {...},
   ]
  "total": 1000,                                //总数
}
```

WAF查询一段时间攻击事件的趋势

接口描述

查询24小时内攻击事件发生次数的趋势图，需要指定攻击事件类型，必须是全部事件、web攻击事件、自定义规则阻拦事件的一种。需要指定时间段的结束时刻，用时间戳表示。

请求结构

```
 GET /v{version}/wafCount/{waf_id}?time={time}&type={type}&clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
time	TIMESTAMP	是	QUERY参数	时间戳：选择事件结束时间段
type	String	是	QUERY 参数	取值 all、webAttack、customAttack 分别表示全部事件、web攻击事件、自定义规则阻拦事件
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
total	List<PeriodAttackCount>	一段时间内的每小时的攻击次数的数组

请求示例

```
 GET /v2/wafCount/waf-3a4b5c?
time=1546963200&type=webAttack&pageSize=10&pageNo=1&clientToken=be31b98c-5e41-4838-9830-
9be700de5a20 HTTP/1.1
HOST bss.{region}.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

返回示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
   "total":[
      {
         "time":00,
         "total":10
      },
      {
         "time":"12",
         "total":"20"
      },
   ]
}
```

BLB-WAF-API

wafBlbRegionOverview

接口描述

用于查询用户在某个区域购买的 BLB WAF 实例列表清单，需要指定pageNo、pageSize用来做分页查询。

请求结构

```
GET /v{version}/wafBlbRegionOverview?pageNo=1&pageSize=10&clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域。

参数名称	类型	是否必需	描述
region	region	是	详见Region

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
pageNo	Int	是	Query参数	waf列表页号码
PageSize	Int	是	Query参数	waf列表页展示的数量
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码 。

返回头域

除公共头域外，无其他特殊头域。

返回参数

参数名称	类型	描述
wafList	List<WafResourceInstanceModel>	BLB-WAF实例的列表
totalCount	Int	用户在某个区的WAF实例的数量

请求示例

```
GET /v2/wafBlbRegionOverview?pageNo=1&pageSize=10&clientToken=be31b98c-5e41-4838-9830-9be700de5a20
HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

返回示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
   "wafList": [
      {
         "region": "bj",               //WAF实例资源所在地域,gz:广州|bj:北京|su:苏州|hkg:香港|fsh:上海|fwh:武汉|bd:保定
         "wafName": "NAME",            //WAF实例的名称
         "wafId": "WAFID",             //WAF实例的ID
         "status": "available",        //WAF实例的状态,见InstanceStatus
         "blbName": "BLBNAME",         //绑定的BLB实例的名称
         "blbId": "BLBID",             //绑定的BLB实例的ID
         "blbListenerId": "BLID",      //BLB监听ID
         "blbListenerPort": "8003",    //BLB监听端口
         "blbListenerProtocol": "HTTP", //BLB监听协议
         "autoRenew": "true",          //是否自动续费，true:是|false:否
         "domain": "demo.com",         //绑定的主域名
         "productType": "postpay",     //计费方式，postpy:后付费|prepay:预付费
         "expireTime": "2022-06-06T06:10:00Z"，//服务过期时间
         "subDomainConfig": {
            "customSwitch": "0",       //子域名自定义防护开关,0:关闭|1:开启
            "subDomain": "test",       //子域名
            "webSwitch": "0",          //子域名web防护开关,0:关闭|1:开启
         },
         "ipCustomSwitch": "0",        //BLB EIP自定义防护开关,0:关闭|1:开启
         "ipWebSwitch": "0",           //BLB EIP web防护开关,0:关闭|1:开启
         "webSwitch": "0",             //子域名web防护开关,0:关闭|1:开启。只要有任意一个子域名为开启状态，该字段即
标记为开启
         "customSwitch": "0",          //子域名自定义防护开关,0:关闭|1:开启。只要有任意一个子域名为开启状态，该字
段即标记为开启
         "webDomainCloseN": 0,         //关闭web防护的子域名数量
         "webDomainOpenN": 8,          //开启web防护的子域名数量
         "customDomainCloseN": 1,      //关闭自定义防护子域名数量
         "customDomainOpenN": 7,       //开启自定义防护域名数量
      },
      {...},
   ],
   "totalCount": 100                   //总条目数
}
```

wafBlbAllOverview

描述

用于查询用户在所有区域购买的BLB WAF 实例列表清单，需要指定pageNo、pageSize用来做分页查询。

请求结构

```
 GET /v{version}/wafBlbAllOverview?pageNo=1&pageSize=10&clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域。

参数名称	类型	是否必需	描述
region	region	是	详见Region

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
pageNo	Int	是	Query参数	waf列表页号码
PageSize	Int	是	Query参数	waf列表页展示的数量
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码 。

返回头域

除公共头域外，无其他特殊头域。

返回参数

参数名称	类型	描述
wafList	List<WafResourceInstanceModel>	BLB-WAF实例的列表
totalCount	Int	用户在某个区的WAF实例的数量

请求示例

```
 GET /v2/wafBlbRegionOverview?pageNo=1&pageSize=10&clientToken=be31b98c-5e41-4838-9830-9be700de5a20
HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

返回示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
   "wafList": [
      {
         "region": "bj",               //WAF实例资源所在地域,gz:广州|bj:北京|su:苏州|hkg:香港|fsh:上海|fwh:武汉|bd:保定
         "wafName": "NAME",            //WAF实例的名称
         "wafId": "WAFID",             //WAF实例的ID
         "status": "STATUS",           //WAF实例的状态，见附录InstanceStatus
         "blbName": "BLBNAME",         //绑定的BLB实例的名称
         "blbId": "BLBID",             //绑定的BLB实例的ID
         "blbListenerId": "BLID",      //BLB监听ID
         "blbListenerPort": "8003",    //BLB监听端口
         "blbListenerProtocol": "HTTP", //BLB监听协议
         "autoRenew": "true",          //是否自动续费，true:是|false:否
         "domain": "demo.com",         //绑定的主域名
         "productType": "postpay",     //计费方式，postpy:后付费|prepay:预付费
         "expireTime": "2022-06-06T06:10:00Z"，//服务过期时间
         "subDomainConfig": {
            "customSwitch": "0",       //子域名自定义防护开关,0:关闭|1:开启
            "subDomain": "test",       //子域名
            "webSwitch": "0",          //子域名web防护开关,0:关闭|1:开启
         },
         "ipCustomSwitch": "0",        //BLB EIP自定义防护开关,0:关闭|1:开启
         "ipWebSwitch": "0",           //BLB EIP web防护开关,0:关闭|1:开启
         "webSwitch": "0",             //子域名web防护开关,0:关闭|1:开启。只要有任意一个子域名为开启状态，该字段即
标记为开启
         "customSwitch": "0",          //子域名自定义防护开关,0:关闭|1:开启。只要有任意一个子域名为开启状态，该字
段即标记为开启
         "webDomainCloseN": 0,         //关闭web防护的子域名数量
         "webDomainOpenN": 8,          //开启web防护的子域名数量
         "customDomainCloseN": 1,      //关闭自定义防护子域名数量
         "customDomainOpenN": 7,       //开启自定义防护域名数量
      },
      {...},
   ],
   "totalCount": 100                   //总条目数
}
```

wafBlb

描述

查询用户名下可用于绑定某个 WAF 实例的所有blb实例，以及blb实例下可绑定的协议和端口。需要指定waf的标志符。

请求结构

```
 GET /v{version}/wafBlb/{waf_id}?clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域。

参数名称	类型	是否必需	描述
region	region	是	详见Region

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
waf_id	String	是	URL参数	waf标志符
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码 。

返回头域

除公共头域外，无其他特殊头域。

返回参数

参数名称	类型	描述
blbList	List<BlbInstance>	用户拥有的blb实例的配置详情列表

请求示例

```
 GET /v2/wafBlb/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
Server: nginx
{
  "blbList": [
     {
        "blbId": "BLBID",              //BLB ID
        "blongId": "BLBLONGID",         //BLB 长ID
        "blbName": "NAME",              //BLB NAME
        "listenerList": [
           {
              "listenerId": "396920",   //listener监听ID
              "protocol": "HTTP",      //listener协议,HTTP|HTTPS
              "port": "80",           //listener端口,1-65535
              "rsList" [
                  "xxxxxx-xxxxxx-xxxxxx-xxxx",             //BLB绑定的BCC
                    ]

           },
           {
             ...
           },
        ],
        "bccList": ["instance-1","instance-2"], //BLB绑定的BCC
     },
     {...},
  ]
}
```

wafBind

描述

将一个 WAF实例绑定到目标BLB实例的监听上，需要指定waf标志符、blb的标志符以及blb绑定协议和监听端口。

请求结构

```
 PUT /v{version}/wafBind/{waf_id}?clientToken={clientToken}  HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
{
   "blbId": "BLBID",                 //BLB 标志符
   "listener": {
      "protocol": "HTTP|HTTPS",      //listener协议,HTTP|HTTPS,需要注意大小写
      "port": "80",                 //listener端口,1-65535
   }
   bindEip: "0|1"                    //是否绑定eip,1:是|0:否
}
```

请求头域

除公共头域外，无其他特殊头域。

参数名称	类型	是否必需	描述
region	region	是	详见Region

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
waf_id	String	是	URL参数	waf标志符
blbId	String	是	Request Body参数	要绑定的blb标志符
listener	Object	是	Request Body参数	blb监听的 协议和端口
bindEip	int	是	Request Body参数	是否绑定 EIP
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码 。

返回头域

除公共头域外，无其他特殊头域。

返回参数

无特殊返回参数。

请求示例

```
 PUT /v2/wafBind/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
{
    "blbId": "lb-ecfca910"
    "listener": {
        "protocol": "HTTP",
        "port": 80,
    }
    bindEip:1
}
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
```

wafUnbind

接口描述

将一个 WAF实例从BLB实例的监听上解除绑定，需要指定waf标志符、blb的标志符以及blb绑定协议和监听端口。

请求结构

```
 PUT /v{version}/wafUnbind/{waf_id}?clientToken={clientToken} HTTP/1.1
Host: bss.{region}.baidubce.com
Authorization: authorization string
{
    "blbId": "BLBID",                    //BLB ID
    "listener": {
        "protocol": "HTTP|HTTPS",          //listener协议:HTTP|HTTPS,需要注意大小写
        "port": "80",                    //listener端口，int型: 1-65535
    }
    bindEip: "0|1"                       //是否绑定eip,1:是|0:否
}
```

请求头域

除公共头域外，无其他特殊头域。

参数名称	类型	是否必需	描述
region	region	是	详见Region

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
waf_id	String	是	URL参数	WAF 标志符
blbId	String	是	Request Body参数	要绑定的blb标志符
listener	Object	是	Request Body参数	blb监听的 协议和端口
bindEip	int	是	Request Body参数	是否绑定 EIP
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码 。

返回头域

除公共头域外，无其他特殊头域。

返回参数

无特殊返回参数。

请求示例

```
 PUT /v2/wafUnbind/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
{
    "blbId": "lb-ecfca910"
    "listener": {
        "protocol": "HTTP",
        "port": 80,
    }
    bindEip:0
}
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
```

wafRules

接口描述

查询用户可配置的子域名数量以及自定义规则数量，需要指定 WAF 的标志符。

请求结构

```
 GET /v{version}/wafRules/{waf_id}?clientToken={clientToken}
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域。

参数名称	类型	是否必需	描述
region	region	是	详见Region

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
waf_id	String	是	URL参数	WAF 标志符
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码 。

返回头域

除公共头域外，无其他特殊头域。

返回参数

参数名称	类型	描述
domainSum	Int	子域名的个数
ruleSum	Int	规则的数量

请求示例

```
 GET /v2/wafRules/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
{
    "domainSum": 20,     //子域名数,int型:10|20|30|40|50
    "ruleSum": 40,       //规则数,int型:20|40|60|80|100
}
```

BLB-WAF 下发规则配置

接口描述

对 BLB-WAF 实例下发规则配置，需要指定 WAF 的标志符，需要传入 WAF 和 BLB 的配置。

请求结构

```
 PUT /v{version}/wafConfig/{waf_id}?clientToken={clientToken}
Host: bss.{region}.baidubce.com
Authorization: authorization string
{
    "baseConfig": {                          //基本配置信息
      "domain": "demo.com",                    //主域
      "ccDefenseSwitch": 1,                   //自定义防护开关，0关闭 | 1开启
      "ccDefenseTemplateId": 1,                //防护模版id
      "blbId": "BLBID",                      //BLB ID
      "listener":{                          //BLB 监听信息内部三个字段在wafBlb接口均有返回，请确认填写正确避免影响防
护效果
          "listenerId": "LISTENERID",           //BLB 监听ID
          "port": "PORT",                     //BLB 监听端口
          "protocol": "PROTOCOL"                //BLB 监听协议
      }
    },
    "subDomainConfigList": [                    //子域名配置信息
      {
          "subDomain": "test.baidu.com",          //子域名
          "subDomainPrefix": "test",            //子域名前缀
          "webSwitch": "0|1",                  //web防护开关,0:关闭|1:开启
          "webPolicy": "high|middle|low",        //策略等级
          "webType": "log|deny",                //执行的策略
          "ccDefenseSwitch": 1,                 //自定义防护开关，0关闭 | 1开启
          "ccDefenseTemplateId": 1,             //防护模版id
      },
      {...},
    ]
}
```

请求头域

除公共头域外，无其他特殊头域。

参数名称	类型	是否必需	描述
region	region	是	详见Region

请求参数

BLB-WAF配置详情见wafConfig。

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
waf_id	String	是	URL参数	WAF标志符
clientToken	String	是	Query参数	幂等性Token，详见幂等性
baseConfig	Object	是	Request Body参数	waf配置基本信息，具体字段详见请求结构
subDomainConfigList	List	是	Request Body参数	waf配置子域名列表及其对应配置信息，具体字段详见请求结构

返回状态码

成功返回200，失败返回见错误码 。

返回头域

除公共头域外，无其他特殊头域。

返回参数

无特殊返回参数。

请求示例

```
 PUT /v2/wafConfig/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
{
   "baseConfig": {                          //基本配置信息
      "domain": "demo.com",                    //主域
      "ccDefenseSwitch": 1,                  //自定义防护开关，0关闭｜1开启
      "ccDefenseTemplateId": 1,               //防护模版id
      "blbId":"lb-xxxxxxxxx",                //BLB ID
      "listener":{                         //BLB 监听协议和端口，cdnwaf无此字段
         "listenerId": "114762",             //BLB 监听ID
         "port": "8003",                   //BLB 监听端口
         "protocol": "HTTP"                 //BLB 监听协议
      }
   },
   "subDomainConfigList": [                  //子域名配置信息
      {
         "subDomain": "test.baidu.com",        //子域名
         "subDomainPrefix": "test",           //子域名前缀
         "webSwitch": 1,                   //web防护开关,0:关闭|1:开启
         "webPolicy": "high",               //策略等级
         "webType": "log",                 //执行的策略,log:观察模式|deny:拦截模式
         "ccDefenseSwitch": 1,               //自定义防护开关，0关闭｜1开启
         "ccDefenseTemplateId": 1,            //防护模版id
      },
      {...},
   ]
}
```

响应示例

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
```

BLB-WAF 查询规则配置

接口描述

对 BLB-WAF 实例查询当前规则配置。

请求结构

```
GET /v{version}/wafConfig/{waf_id}?clientToken={clientToken}
Host: bss.{region}.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

参数名称	类型	是否必需	描述
region	region	是	详见Region

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
waf_id	String	是	URL参数	waf标志符
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

- BLB-WAF配置详情见wafConfig

参数名称	类型	描述
baseConfig	Object	waf配置基本信息，具体字段详见响应示例
subDomainConfigList	List	waf配置子域名列表及其对应配置信息，具体字段详见响应示例

请求示例

```
GET /v2/wafConfig/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2018 08:26:52 GMT
Content-Length:
Connection: keep-alive
Content-Type: application/json;charset=UTF-8
{
   "baseConfig": {                          //基本配置信息
      "createTime": "2021-07-05T11:12:21Z",      //实例创建时间
      "domain": "demo.com",                    //主域
      "expireTime": "2022-06-05T11:12:21Z",      //服务过期时间
      "ccDefenseSwitch": 1,                    //自定义防护开关，0关闭｜1开启
      "ccDefenseTemplateId": 1,                //防护模版id
      "blbId":"lb-xxxxxxxxx",                  //BLB ID
      "listener":{                           //BLB 监听协议和端口
         "listenerId": "1234566",
         "port": "8003",
         "protocol": "HTTP"
      },
      "name": "WAF-541f2a75",                  //WAF 实例名称
      "productType": "prepay",                 //WAF 计费类型 prepay:预付费，postpay:后付费
      "region": "bj",                        //WAF 实例所属地域
      "status": "available",                   //WAF 实例状态
   },
   "subDomainConfigList": [                    //子域名配置信息
      {
         "subDomain": "test.demo.com",          //完整子域名
         "subDomainPrefix": "test",             //子域名前缀
         "webSwitch": 1,                      //web防护开关,0:关闭|1:开启
         "webPolicy": "high",                 //策略等级
         "webType": "log",                    //执行的策略,log:观察模式|deny:拦截模式
         "ccDefenseSwitch": 1,                //自定义防护开关，0关闭｜1开启
         "ccDefenseTemplateId": 1,            //防护模版id
      },
      {...},
   ]
}
```

CDN-WAF-API

Overview

描述

查询用户的 CDN-WAF 实例

请求结构

```
 GET /v{version}/cdnwaf/overview?clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
wafList	List<CdnWafInstance>	用户所有的cdn-waf实例列表

请求示例

```
GET /v2/cdnwaf/overview?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
{
    "wafList": [
        {
            "wafName": "NAME",              //WAF实例的名称
            "wafId": "WAFID",               //WAF实例的ID
            "status": "STATUS",             //WAF实例的状态，见附录InstanceStatus
            "autoRenew": "true",            //是否自动续费，true:是|false:否
            "domain": "demo.com",           //绑定的主域名
            "subDomain": {                  //已配可配子域名数量
                "used": 0,                  //已配子域名数量
                "total": "10"               //可配子域名数量
            },
            "productType": "postpay",       //计费方式，postpy:后付费|prepay:预付费
            "expireTime": "2022-06-06T06:10:00Z"，//服务过期时间
            "subDomainConfig": {
                "customSwitch": "0",        //子域名自定义防护开关,0:关闭|1:开启
                "subDomain": "test",        //子域名
                "webSwitch": "0",           //子域名web防护开关,0:关闭|1:开启
            },
            "webDomainCloseN": 0,           //关闭web防护的子域名数量
            "webDomainOpenN": 8,            //开启web防护的子域名数量
            "customDomainCloseN": 1,        //关闭自定义防护子域名数量
            "customDomainOpenN": 7,         //开启自定义防护域名数量
        },
        {...},
    ],
    "totalCount": 100                       //总条目数
}
```

DomainList

接口描述

- 返回用户所有的主域名列表

请求结构

```
 GET /v{version}/cdnwaf/domainList?clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
domainList	List	主域名列表

请求示例

```
GET /v2/cdnwaf/domainList?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
{
    "domainList": [
        {
            "domain": "demo.com",          //CDN中的主域名
        },
        {...},
    ]
}
```

querySubDomainList

接口描述

- 查询符合主域名且未添加到其他waf实例的可用子域名列表，或者该waf实例绑定的子域名

请求结构

```
PUT /v{version}/cdnwaf/querySubDomainList/{waf_id}?clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
{
    "domain": "demo.com",            //CDN 中的主域名
}
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
domain	String	是	Request Body参数	域名
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
subDomainList	List	返回用户可用的子域名列表， subDomain是子域名称，status是子域名状态

请求示例

```
    PUT /v2/cdnwaf/querySubDomainList/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20
HTTP/1.1
 HOST bss.bj.baidubce.com
   Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
   {
       "domain": "demo.com",
   }
```

响应示例

```
    HTTP/1.1 200 OK
   x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
   Date: Wed, 10 Apr 2016 08:26:52 GMT
   Transfer-Encoding: chunked
   Content-Type: application/json;charset=UTF-8
   {
      "subDomainList": [
         {
            "subDomain": "a.demo.com",      //cdn中的子域名
            "status": "1",                  //子域名状态,0:未添加|1:已添加到该waf实例
         },
         {...},
      ]
   }
```

cdnWafRules

接口描述

查询CDN WAF实例可配置的子域名和自定义规则数，需要指定waf的标志符、需要指定cdn的主域名

请求结构

```
GET /v{version}/cdnwaf/cdnWafRules/{waf_id}?clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
{
    "domain": "demo.com",                    //CDN 中的主域名
}
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
domainSum	Int	子域名数
ruleSum	Int	规则数

请求示例

```
GET /v2/cdnwaf/cdnWafRules/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
{
    "domainSum": DOMAINSUM,              //子域名数,int型:10|20|30|40|50
    "ruleSum": RULESUM,                  //规则数,int型:20|40|60|80|100
}
```

cdnWafConfig

接口描述

用于对 CDN-WAF 实例下发规则配置。

请求结构

```
 PUT /v{version}/cdnwaf/cdnWafConfig/{waf_id}?clientToken={clientToken}
Host: bss.bj.baidubce.com
Authorization: authorization string
{
   "baseConfig": {                          //基本配置信息
      "domain": "demo.com",                    //主域
   },
   "subDomainConfigList": [                  //子域名配置信息
      {
         "subDomain": "test.baidu.com",         //子域名
         "subDomainPrefix": "test",             //子域名前缀
         "webSwitch": "0|1",                   //web防护开关,0:关闭|1:开启
         "webPolicy": "high|middle|low",        //策略等级
         "webType": "log|deny",                //执行的策略
         "ccDefenseSwitch": 1,                 //自定义防护开关，0关闭｜1开启
         "ccDefenseTemplateId": 1,             //防护模版id
      },
      {...},
   ]
}
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
waf_id	String	是	URL参数	WAF标志符
clientToken	String	是	Query参数	幂等性Token，详见幂等性
baseConfig	Object	是	Request Body参数	waf配置基本信息，具体字段详见请求结构
subDomainConfigList	List	是	Request Body参数	waf配置子域名列表及其对应配置信息，具体字段详见请求结构

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

无特殊返回参数

请求示例

```
PUT /v2/cdnwaf/cdnWafConfig/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20
Host bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
{
   {
      "baseConfig": {                          //基本配置信息
         "domain": "demo.com",                    //主域
      },
      "subDomainConfigList": [                 //子域名配置信息
         {
            "subDomain": "test.baidu.com"          //子域名
            "subDomainPrefix": "test",           //子域名前缀
            "webPolicy": "high",                 //策略等级
            "webType": "log",                    //执行的策略,log:观察模式|deny:拦截模式
            "webSwitch": 1,                      //web防护开关,0:关闭|1:开启
            "ccDefenseSwitch": 1,                //自定义防护开关，0关闭｜1开启
            "ccDefenseTemplateId": 1,            //防护模版id
         },
         {...},
      ]
   }
}
```

响应示例

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
```

cdnWafConfig

接口描述

用于查询 CDN-WAF 的规则配置。

请求结构

```
GET /v{version}/cdnwaf/cdnWafConfig/{waf_id}?clientToken={clientToken}
Host: bss.bj.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
waf_id	String	是	URL参数	WAF标志符
clientToken	String	是	Query参数	幂等性Token，详见幂等性

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
baseConfig	Object	waf配置基本信息，具体字段详见响应示例
subDomainConfigList	List	waf配置子域名列表及其对应配置信息，具体字段详见响应示例

请求示例

```
GET /v2/cdnwaf/cdnWafConfig/waf-3a4b5c?clientToken=be31b98c-5e41-4838-9830-9be700de5a20
Host bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
{
    "baseConfig": {                         //基本配置信息
        "createTime": "2021-07-05T11:12:21Z",  //实例创建时间
     "domain": "dome.com",                  //主域
     "expireTime": "2022-06-05T11:12:21Z",  //服务过期时间
     "name": "WAF-541f2a75",                //实例名称
     "productType": "prepay",               //计费类型 prepay:预付费，postpay:后付费
     "region": "global",                   //资源地域,CDN-WAF 资源地域统一为 global
     "status": "available",                 //WAF实例状态
 },
    "subDomainConfigList": [                //子域名配置信息
        {
            “subDomain”: "test.baidu.com"             //子域名
            "subDomainPrefix": "test",               //子域名前缀
            "webPolicy": "high",                    //自定义策略等级,high|middle|low
            "webType": "log",                       //执行的策略：log:观察模式|deny:拦截模式
            "ccDefenseSwitch": 1,                    //自定义防护开关，0关闭｜1开启
            "ccDefenseTemplateId": 1,                //防护模版id
            "webSwitch": 1,                         //web防护开关,0:关闭|1:开启
        },
        {...},
    ]
}
```

附录

Model对象定义

WafResourceInstanceModel

参数名称	类型	描述
region	Region	资源所在region
listener	Object	listener对象2个元素，protocol和port分别表示blb监听的协议和端口
wafName	String	WAF 实例名称
wafId	String	WAF 标志符
status	InstanceStatus	WAF 实例状态
blbName	String	BLB 实例名称
blbId	String	BLB 标志符
domain	String	WAF 绑定的主域名
webSwitch	Int	web防护开关，0：关闭，1：开启
customSwitch	Int	自定义防护开关，0：关闭，1：开启

BlbListener

参数名称	类型	描述
protocol	String	只能为 https或http 两种类型
port	Int	listener端口，int型: 1-65535
rsList	List	blb绑定的bcc 列表

InstanceStatus

编码	描述
available	实例可用
paused	实例到期被暂停服务
pausing	实例到期正在被处理
updating	实例正在更新
deleting	实例正在删除
deleted	实例被删除

Region

编码	描述
bj	北京
gz	广州
su	苏州
fsh	上海
fwh	武汉
hkg	香港
bd	保定

AttackEvent

参数名称	类型	描述
time	String	攻击事件发生时间
bcc	List	受影响的资产列表
ip	String	攻击者ip
addr	String	攻击者地址
userAgent	String	攻击者伪装 ua
url	String	攻击的请求url
ruleId	String	当用户设置自定义规则后，RuleId表示自定义规则的标志符
ruleName	String	当用户设置自定义规则后，RuleId表示自定义规则的名称
ruleInfo	String	用户设置的自定义规则的内容
type	String	web防护策略，deny或者log两种模式
body	String	攻击请求的具体详情

PeriodAttackCount

参数名称	类型	描述
time	Int	表征某个时间点的数值，取值范围，[00-24]
total	Int	在这个时间点的攻击数量

BlbInstance

参数名称	类型	描述
blbName	String	BLB 实例名称
blbId	String	BLB 标志符
longId	String	BLB 长ID
listenerList	List<BlbListener>	BLB 监听的协议列表

BlbCustomRule

参数名称	类型	描述
name	String	策略名字:只支持1-65位数字、大小写字母、-/_ .必须是字母开头
type	String	自定义规则执行动作：log:观察模式,deny:拦截模式,pass:信任的流量
conditions	List<CustomCondition>	自定义规则包含的自定义规则条件，最多3条

CustomCondition

参数名称	类型	描述
key	String	匹配项,只支持这几种模式:uri、ip、referer、user_agent、get_param
match	String	匹配模式:prefix、include、suffix、equal、not_equal、not_include
value	String	匹配内容:不支持中文，支持数字大小写-._

CdnWafInstance

参数名称	类型	描述
wafName	String	WAF 实例名称
wafId	String	WAF 标志符
status	InstanceStatus	WAF 实例状态
domain	String	WAF 绑定的主域名
subdomain	SubDomainCount	WAF 配置的子域名数量统计
subDomainList	List	防护的子域名名称列表
webSwitch	Int	web防护开关,INT型：0：关闭，1：开启
customSwitch	Int	自定义防护开关,INT型：0：关闭，1：开启

CdnCustomRule

参数名称	类型	描述
name	String	策略名字:只支持1-65位数字、大小写字母、-/_ .必须是字母开头
type	String	自定义规则执行动作：log:观察模式,deny:拦截模式,pass:信任的流量
patten	String	执行动作:black:拦截，white:放行
key	String	匹配项,只支持这几种模式:uri、ip、referer、user_agent、get_param
match	String	匹配模式:prefix、include、suffix、equal、not_equal、not_include
value	String	匹配内容:不支持中文，支持数字大小写-._

更新历史

更新历史

- API 版本说明

时间	版本号	说明
2019-01-24	2	API上线
2021-06-08	2	更新了 实例购买查询、实例绑定/解除绑定、规则配置查询、规则配置下发 等 API 的部分参数

常见问题

Web攻击分类说明

Web恶意扫描

黑客攻击前多使用工具针对各种WEB应用系统以及各种典型的应用漏洞进行检测（如SQL注入、Cookie注入、XPath注入、LDAP注入、跨站脚本、代码注入、表单绕过、弱口令、敏感文件和目录、管理后台、敏感数据等）,以便收集信息后进行后续的攻击行为。

跨站脚本攻击

也称为XSS,指利用网站漏洞从用户那里恶意盗取信息.为了搜集用户信息，攻击者通常会在有漏洞的程序中插入 JavaScript、VBScript、 ActiveX或Flash以欺骗用户。一旦得手，他们可以盗取用户账户，修改用户设置，盗取/污染cookie，做虚假广告等。每天都有大量的XSS攻击的恶意代码出现。

远程文件控制

一些粗心的开发者代码部署到服务器上其参数设置可以调用读取服务器系统文件，远程攻击者可以通过恶意参数调用对这些系统文件进行操作，从而导致对WEB服务和用户隐私造成不同程度的威胁。

远程后门执行

后门程序一般是指那些绕过安全性控制而获取对程序或系统访问权的程序方法。在软件的开发阶段，程序员常常会在软件内创建后门程序以便可以修改程序设计中的缺陷。但是，如果这些后门被其他人知道，或是在发布软件之前没有删除后门程序，那么它就成了安全风险，容易被黑客当成漏洞进行攻击。

恶意文件上传

一些论坛类网站往往允许用户上传文件,导致该漏洞的原因在于代码作者没有对访客提交的数据进行检验或者过滤不严，可以直接提交修改过的数据绕过扩展名的检验。提交后的恶意程序便可作为远程后门执行。

异常文件引用

web开发程序员会在代码中引用外部文件, 异常文件引用允许攻击者利用在目标应用程序中实现的“动态文件包容”机制, 这可能会导致输出文件的内容造成Web服务器上的代码执行, 在客户端JavaScript等可导致其他攻击，如跨站点脚本代码执行。

异常文件解析

一些web服务器漏洞允许被修改的脚本文件按常用的图片文件扩展名解析但仍然执行了脚本文件的内容,这通常结合恶意文件上传攻击绕过扩展名限制提交后门文件。

系统漏洞

指一个系统的易感性或缺陷，通常严重程度比较高.攻击者利用漏洞可以直接绕过该系统的相关安全防护机制。

无效HTTP版本

HTTP 协议有多种版本，识别为主 (major).次 (minor)，例如如版本 0.9 ， 1.0 或 1.1 。无效HTTP版本指攻击者利用不受支持的http版本号构造数据包请求对web服务器攻击。

拒绝服务攻击

拒绝服务攻击即攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一。其实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。

如何获取近6个月攻击拦截日志

如何获取近6个月攻击拦截日志

用户可以通过数据统计页面浏览到180内的拦截日志信息。

告警无法关闭

WAF告警接入BCM云监控通知后，旧告警配置当前无法修改，需要根据文档进行新增告警配置并关闭生效

WAF接入云监控通知告警开关闭指南

服务等级协议 SLA

应用防火墙服务等级协议 SLA

应用防火墙服务等级协议（SLA）

百度智能云应用防火墙服务等级协议（简称“SLA”） 规定了百度智能云向客户（简称“您”）提供的应用防火墙服务的可用性等级指标及赔偿方案。特别提示，本服务等级协议仅限于使用百度智能云提供的应用防火墙服务下适用。

1. 指标定义

- **服务周期**：一个服务周期为一个自然月。

- **服务周期总分钟数**：服务周期内的总天数 * 24（小时） * 60（分钟）计算。
- **应用防火墙实例不可用**：当某一分钟内，客户所有试图与指定的应用防火墙实例建立连接的连续尝试均失败，则视为该分钟内该服务不可用。应用防火墙实例的服务不可用仅限于自身服务的不可用，不对因为客户对网络连接等各种设置原因导致的不可用适用。
- **服务不可用分钟数**：服务周期内应用防火墙实例不可用的分钟数之和。

2. 服务可用性

2.1 服务可用性计算公式

$$服务可用性=\left(\frac{服务周期总分钟数-服务不可用分钟数}{服务周期总分钟数}\right)\times 100\%$$

2.2 服务可用性承诺

百度智能云防护服务承诺应用防火墙服务可用性不低于99.9%。如未达到该承诺的，您可以根据本服务等级协议第3条约定获得相应赔偿。

3. 赔偿方案

3.1 赔偿标准

根据客户某一百度智能云账号下应用防火墙服务可用性比例，按照下表中的标准计算赔偿金额，赔偿方式仅限于用于购买应用防火墙服务的代金券，赔偿总额不超过实际支付该月应用防火墙服务费用的50%。

服务可用性	**赔偿代金券金额**
低于99.9%但等于或高于99%	月度服务费用的10%
低于99%但等于或高于95%	月度服务费用的20%
低于95%	月度服务费用的50%

但因下述原因导致的服务不可用时长，不进行赔付：

(1) 由于网络运营商严重故障导致的服务不可用。

(2) 由于您不付费或是欠款导致的服务不可用。

(3) 由于您未按规定或者违法使用百度智能云产品引发的服务不可用。

(4) 由于您或您的最终用户对百度智能云提供的服务造成安全威胁或存在欺诈或者违法行为而导致的服务不可用。

(5) 由于您或者任何第三方（不受百度智能云直接控制）设备、软件或技术引起的服务不可用。

(6) 由于您未按照百度智能云规定配置使用产品引起的服务不可用。

(7) 由于您违反任何百度智能云产品条款引起的服务不可用。

(8) 由于网络、硬件或服务的维护、升级导致的服务不可用（百度会在计划发生中断维护与升级的前3天通过邮件、短信以及官网通知中心的形式，告知您）。

(9) 由于不可抗力或紧急事件等引起的服务不可用。

(10) 其他非百度智能云原因所造成的不可用。

3.2 赔偿申请时限

赔偿申请必须限于在百度智能云应用防火墙服务没有达到服务可用性承诺比例的相关月份结束后两个月内提出。超出申请时限的赔偿申请将不被受理。百度智能云收到您的赔偿申请且在您资料提交齐全的情况下启动赔偿申请审核，审核期间可能会与您

核实相关情况，并根据核实的结果对您提出的赔偿申请依据本等级服务协议及相关协议作出处理。

4. 其他

(1) 在法律法规允许的范围内，百度智能云负责对本协议进行解释说明。

(2) 本协议一经公布立即生效，百度智能云有权对本SLA条款作出修改。如本SLA条款有任何修改，百度智能云将以网站公示的方式通知您。如您不同意百度智能云对SLA所做的修改，您有权停止使用应用防火墙服务，如您继续使用应用防火墙服务，则视为您接受修改后的SLA。

(3) 本协议项下百度智能云对于用户所有的通知均可通过网页公告、站内信、电子邮件、手机短信或其他形式等方式进行；该等通知于发送之日视为已送达收件人。因用户未及时获知百度智能云的服务变更或终止条款遭受损失的，百度智能云不承担任何责任。

(4) 本协议的订立、执行和解释及争议的解决均应适用中国法律并受中国法院管辖。如双方就本协议内容或其执行发生任何争议，双方应尽量友好协商解决；协商不成时，任何一方均可向北京市海淀区人民法院提起诉讼。

(5) 本协议构成双方对本协议之约定事项及其他有关事宜的完整协议，除本协议规定的之外，未赋予本协议各方其他权利。

(6) 如本协议中的任何协议无论因何种原因完全或部分无效或不具有执行力，本协议的其余协议仍应有效并且有约束力。

(7) 关于用户约束条款，详见百度智能云用户服务协议中的"用户的权利与义务"相关条款内容。

(8) 关于服务商免责条款，详见百度智能云用户服务协议中的"免责声明"相关条款内容。