ALIBABA CLOUD

阿里云

Web应用防火墙
网站防护配置

文档版本：20220705

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.概述 06
2.Web安全 08
2.1. 设置规则防护引擎 08
2.2. 设置深度学习引擎 13
2.3. 设置网站防篡改 15
2.4. 设置防敏感信息泄露 17
2.5. 设置主动防御 21
3.Bot管理 24
3.1. 防爬场景化配置 24
3.1.1. 概述 24
3.1.2. 配置浏览器访问网页的防爬场景化规则 25
3.1.3. 配置App防爬场景化规则 28
3.1.4. 防爬场景化配置示例 32
3.2. 设置合法爬虫规则 35
3.3. 设置爬虫威胁情报规则 36
3.4. 设置数据风控 39
3.5. App防护 43
3.5.1. 概述 43
3.5.2. SDK集成指南（新版） 45
3.5.2.1. Android应用集成SDK 45
3.5.2.2. iOS应用集成SDK 52
3.5.3. SDK集成指南（旧版） 58
3.5.3.1. 为Android应用集成SDK 58
3.5.3.2. 为iOS应用集成SDK 65
3.5.4. 设置App防护 70
4.访问控制/限流 75

4.1. 设置CC安全防护 75
4.2. 设置IP黑名单 76
4.3. 设置扫描防护 77
4.4. 设置自定义防护策略 80
5.防护白名单 85
5.1. 设置网站白名单 85
5.2. 设置Web入侵防护白名单 86
5.3. 设置数据安全白名单 88
5.4. 设置Bot管理白名单 90
5.5. 设置访问控制/限流白名单 92
6.匹配条件字段说明 95
7.自定义防护规则组 100
8.开启IPv6防护 106
9.防护配置最佳实践 108
9.1. 网站防护最佳实践 108
9.2. 规则防护引擎最佳实践 116
9.3. CC攻击防护最佳实践 118
9.4. 账户安全最佳实践 123
9.5. 使用自定义规则组提升Web攻击防护效果 125

1.概述

本文介绍了Web应用防火墙服务支持的所有网站防护配置功能。

模块	功能	描述	开启方式	相关文档
Web安全	**规则防护引擎**	基于内置的专家经验规则集，自动为网站防御SQL注入、XSS跨站、Webshell上传、命令注入、后门隔离、非法文件请求、路径穿越、常见应用漏洞攻击等通用的Web攻击。	接入后自动开启。	设置规则防护引擎 规则防护引擎最佳实践
	防护规则组	支持自由组合Web应用防火墙的防护规则，形成有针对性的防护规则组，应用到具体的网站防护。 说明 目前仅支持自定义**规则防护引擎**的防护规则组。	接入后手动开启。	自定义防护规则组 使用自定义规则组提升Web攻击防护效果
	深度学习引擎	依托于阿里云深度神经网络系统，对云上全部Web攻击数据和正常业务数据进行分类训练，从而实时防护潜在的异常攻击行为。	接入后手动开启。	设置深度学习引擎
	网站防篡改	帮助您锁定需要保护的网站页面（例如敏感页面），被锁定的页面在收到请求时，返回已设置的缓存页面，预防源站页面内容被恶意篡改。	接入后手动开启。	设置网站防篡改
	防敏感信息泄露	帮助网站过滤服务器返回内容（异常页面或关键字）中的敏感信息（例如身份证号、银行卡号、电话号码和敏感词汇），脱敏展示敏感信息或返回默认异常响应页面。	接入后手动开启。	设置防敏感信息泄露
	主动防御	采用阿里云自研的机器学习算法自主学习域名的合法流量，并自动为域名生成定制化的安全防护策略，防御未知攻击。	接入后手动开启。	设置主动防御
Bot管理	**合法爬虫**	提供合法搜索引擎白名单（例如Google、Bing、百度、搜狗、Yandex等），方便您为域名设置放行合法爬虫的访问请求。	接入后手动开启。	设置合法爬虫规则
	爬虫威胁情报	基于云平台强大的计算能力，提供拨号池IP、IDC机房IP、恶意扫描工具IP以及云端实时模型生成的恶意爬虫库等多种维度的爬虫威胁情报规则，方便您在全域名或指定路径下设置阻断恶意爬虫的访问请求。	接入后手动开启。	设置爬虫威胁情报规则
	数据风控	帮助您防御网站关键业务（例如注册、登录、活动、论坛）中可能发生的机器爬虫欺诈行为。	接入后手动开启。	设置数据风控

模块	功能	描述	开启方式	相关文档
	App防护	专门针对原生App端，提供可信通信、防机器脚本滥刷等安全防护，可以有效识别代理、模拟器、非法签名的请求。	接入后手动开启。	设置App防护
访问控制/限流	**CC安全防护**	基于CC流量特征，帮助您防御针对页面请求的CC攻击，并提供不同模式的防护策略。	接入后自动开启。	设置CC安全防护 CC攻击防护最佳实践
	IP黑名单	支持一键阻断来自指定IP地址、IP地址段以及指定地理区域的IP地址的访问请求。	接入后手动开启。	设置IP黑名单
	扫描防护	帮助网站自动阻断包含指定特征的访问请求，例如请求源IP在短期内发起多次Web攻击或目标遍历攻击、请求源IP来自常见扫描工具或阿里云恶意扫描攻击IP库。	接入后手动开启。	设置扫描防护
	自定义防护策略	支持自定义基于精确匹配条件的访问控制规则和访问频率限制规则。	接入后手动开启。	设置自定义防护策略
防护实验室	**账户安全**	帮助您识别与账户关联的业务接口（例如注册、登录等）上发生的账户安全风险事件，包括撞库、暴力破解、垃圾注册、弱口令嗅探和短信验证码接口滥刷。	接入后手动开启。	设置账户安全 账户安全最佳实践
防护白名单	**网站白名单**	通过设置网站白名单，可以让满足条件的请求不经过任何Web应用防火墙防护模块的检测，直接访问源站服务器。	接入后手动开启	设置网站白名单
	Web入侵防护白名单	通过设置Web入侵防护白名单，可以让满足条件的请求忽略指定模块（规则防护引擎、深度学习引擎）的检测。	接入后手动开启。	设置Web入侵防护白名单
	数据安全白名单	通过设置数据安全白名单，可以让满足条件的请求忽略指定模块（防敏感信息泄露、网站防篡改、账户安全）的检测。	接入后手动开启。	设置数据安全白名单
	Bot管理白名单	通过设置Bot管理白名单，可以让满足条件的请求忽略指定模块（爬虫威胁情报、数据风控、智能算法、App防护）的检测。	接入后手动开启。	设置Bot管理白名单
	访问控制/限流白名单	通过设置**访问控制/限流**白名单，可以让满足条件的请求忽略指定模块（CC安全防护、IP黑名单、扫描防护、自定义防护策略）的检测。	接入后手动开启。	设置访问控制/限流白名单

2.Web安全

2.1. 设置规则防护引擎

规则防护引擎基于内置的防护规则集，自动为网站防御SQL注入、XSS跨站、Webshell上传、命令注入、后门隔离、非法文件请求、路径穿越、常见应用漏洞攻击等通用的Web攻击。

前提条件

- 已开通Web应用防火墙实例。具体操作，请参见开通Web应用防火墙。
- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

Web应用防火墙（WAF）的规则防护引擎默认开启，所有接入WAF防护的网站业务，默认都受到规则防护引擎的检测和防护。

规则防护引擎基于阿里云安全团队在Web攻击防御实践中沉淀的大量基础防护规则，帮助网站防御各种常见的Web应用攻击。您可以根据业务防护需要，在防护规则组的维度，设置规则防护引擎采用哪些防护规则。WAF按照防护严格程度，内置了三套规则组供您选用：

- **中等规则组**：默认选用该规则组。
- **宽松规则组**：如需减少误拦截，可选用该规则组。
- **严格规则组**：如需提高攻击检测命中率，可选用该规则组。

您也可以自定义防护规则组，相关操作，请参见自定义防护规则组。

智能规则托管

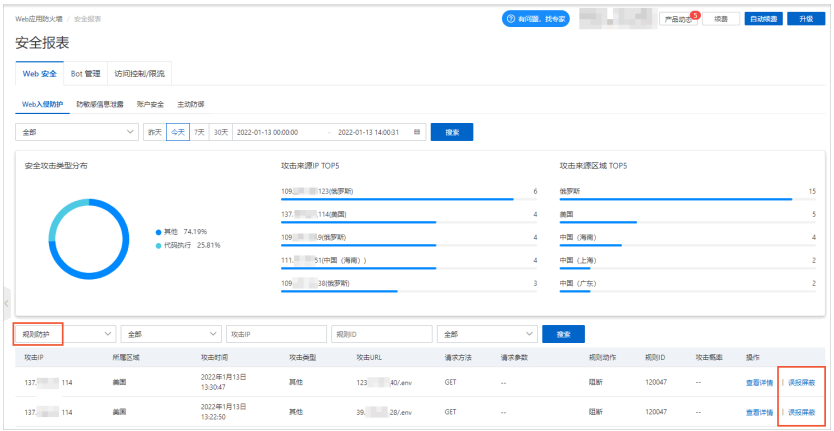
规则防护引擎默认开启**智能规则托管**，针对规则防护引擎可能对正常业务流量产生的误拦截进行自动规避。

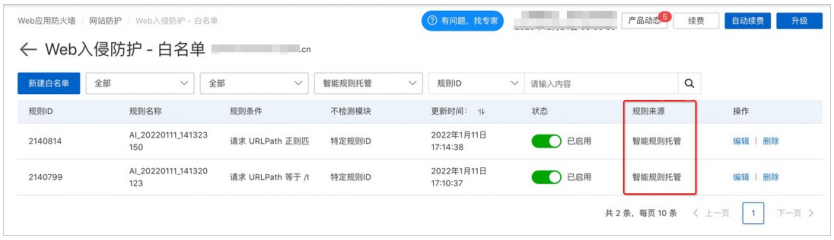
智能规则托管表示由规则防护引擎通过智能算法，自学习网站业务的历史流量特征，并结合阿里云安全威胁情报数据，自动识别不适用于防护当前业务场景或接口的规则（这类规则可能在相应场景或接口防护中产生误拦截或误报）；在规则识别的基础上，通过自动添加最小粒度的Web入侵防护白名单规则（一般针对某个特定的业务接口URL，忽略某个特定规则ID），确保在规避误报的同时不扩大攻击影响面。误报风险消除后，规则防护引擎会自动删除之前自动添加的Web入侵防护白名单规则。

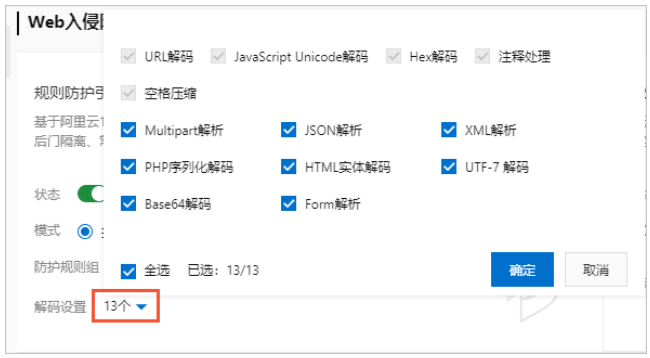
操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**Web安全**页签，定位到**规则防护引擎**区域，完成以下功能配置。

配置项	说明
状态	开启或关闭规则防护引擎。规则防护引擎默认开启，为所有接入WAF防护的网站防御常见的Web应用攻击。 您可以在**安全报表**页面，通过**Web安全 > Web入侵防护**报表，查询规则防护引擎的攻击命中记录。如果您发现某个规则误拦截了正常业务流量，可以通过**误报屏蔽**功能，屏蔽指定的规则。更多信息，请参见Web安全报表说明。 
模式	检测发现攻击请求时，对攻击请求执行的操作。可选值： ○ **拦截**：直接阻断攻击请求。 ○ **告警**：只触发告警，不阻断攻击请求。

配置项	说明
智能规则托管	开启或关闭智能规则托管。智能规则托管默认开启，通过动态管理Web入侵防护白名单，降低误拦截风险。 您可以在**规则防护引擎**配置区域，查看规则防护引擎**已智能优化XX条规则**；单击**点击查看**，可跳转到**Web入侵防护 - 白名单**页面，查看规则防护引擎自动添加的白名单规则（**规则来源**为**智能规则托管**）。您可以编辑或删除自动添加的白名单规则。  等误报风险消除后，自动添加的白名单规则会被自动删除。 **注意** - 如果您手动编辑过自动添加的白名单规则，该规则仍会在误报风险消除后，被自动删除。 - 您手动创建的Web入侵白名单规则不会被自动删除。
防护规则组	选择要应用的防护规则组。支持应用内置规则组和自定义规则组。内置规则组包括： - **中等规则组**：按照标准防护程度去检测常见的Web应用攻击。默认应用该规则组。 - **严格规则组**：按照严格防护程度去检测路径穿越、SQL注入、命令执行等Web应用攻击。 - **宽松规则组**：按照宽松防护程度去检测常见Web应用攻击。当您发现中等规则下存在较多误拦截，或者业务存在较多不可控的用户输入（例如，富文本编辑器、技术论坛等），建议您选择该规则组。 单击**前去配置**，将跳转到**防护规则组**配置页面，您可以根据业务需要自定义防护规则组及要应用的防护规则。具体操作，请参见自定义防护规则组。

配置项	说明
解码设置	设置需要规则防护引擎解码分析的内容格式。 为保证防护效果，规则防护引擎默认对请求中所有格式类型的内容进行解码分析。如果您发现规则防护引擎经常对业务中包含指定格式内容的请求造成误拦截，您可以取消解码对应格式，针对性地降低误杀率。 您可以展开**解码设置**菜单，根据需要选中或取消选中要解码的格式。 **注意** 以下解码格式不支持取消：URL解码、JavaScript Unicode解码、Hex解码、注释处理、空格压缩。 

查询防护规则

您可以参照以下方法，查询WAF规则防护引擎中最新添加的防护规则、查询规则防护引擎中目前包含的所有防护规则：

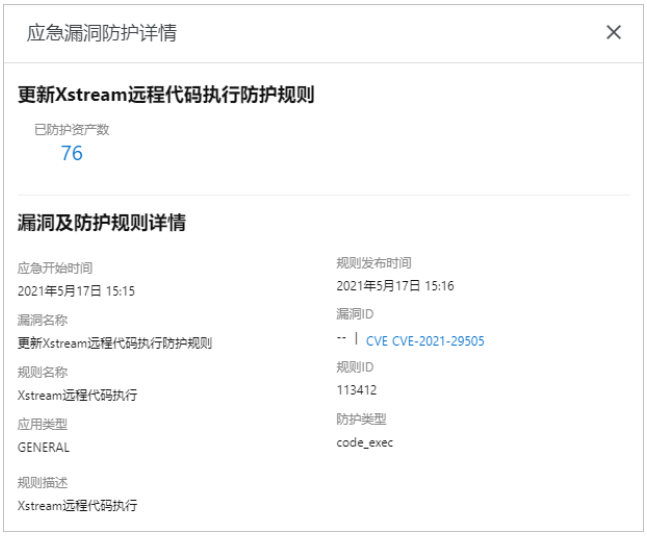
- 查询最新防护规则

  您可以在Web应用防火墙控制台的**总览**页面，通过**应急漏洞**列表，查询规则防护引擎中最新添加的防护规则。

  应急漏洞记录展示了WAF应对互联网上最新披露的安全漏洞所发布的防护规则更新。

  您可以单击某个应急漏洞记录，查看**应急漏洞防护详情**。详情页面展示了受该漏洞影响的网站域名，以及漏洞的详情和相关的WAF防护规则信息。



- 查询所有防护规则

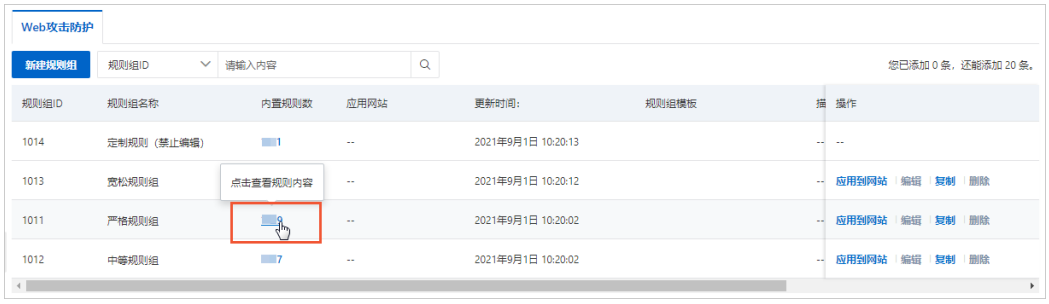
  您可以在Web应用防火墙控制台的**系统管理 > 防护规则组**页面，查询WAF规则防护引擎包含的所有防护规则。

  查询方法如下：

  i. 在**Web攻击防护**页签，定位到**严格规则组**，单击**内置规则数**列下的数字链接。

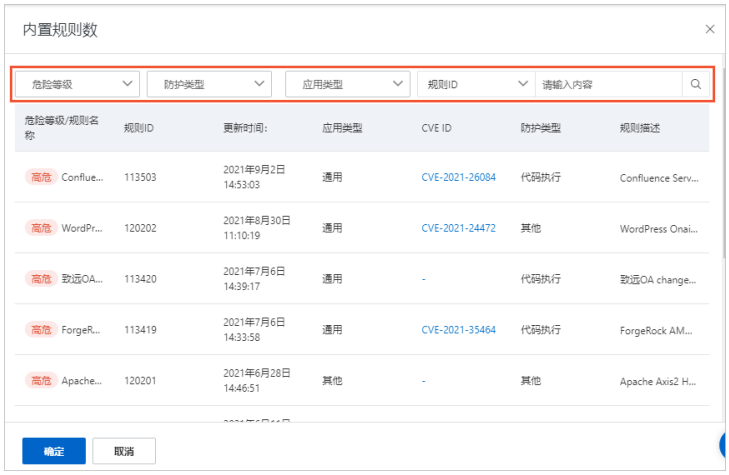
  严格规则组是规则防护引擎下默认创建的一个系统规则组（不支持编辑），包含规则防护引擎的所有防护规则。

  > **说明** 由于规则防护引擎的防护规则会动态变化，您看到的**内置规则数**可能与以下截图不一致。



  ii. 在**内置规则数**面板，查询您想要了解的防护规则。

  您可以通过**危险等级**、**防护类型**、**应用类型**筛选防护规则，或者通过**规则ID**、**CVE ID**（Common Vulnerabilities and Exposures ID）查询某个防护规则。例如，您通过**总览**或者**安全报表**页面获取到某个防护规则的ID后，可以使用规则ID查询该规则。



规则列表向您展示了防护规则的以下信息：**危险等级/规则名称**、**规则ID**、**更新时间**、**应用类型**、**CVE ID**、**防护类型**、**规则描述**。

您可以单击具体的CVE ID，查看该规则对应的漏洞详情。

相关文档

- 规则防护引擎最佳实践
- 自定义防护规则组

2.2. 设置深度学习引擎

网站接入Web应用防火墙后，您可以为其开启深度学习引擎功能。深度学习引擎依托于阿里云深度神经网络系统，对云上全部Web攻击数据和正常业务数据进行分类训练，从而实时防护潜在的异常攻击行为。

前提条件

- 已开通Web应用防火墙实例，且实例满足以下要求：
  - 包年包月实例：实例地域是**中国内地**，且实例版本是**企业版**及以上规格。

    更多信息，请参见开通Web应用防火墙。
  - 按量计费实例：已在**账单与套餐中心**，开启**Web入侵防护**模块下**大数据深度学习引擎**功能。

    更多信息，请参见账单与套餐中心（按量2.0版本）。

- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

随着互联网的发展，Web攻击手段也在不断演进，传统的单一手段的防护方式已经无法满足对复杂的互联网业务保驾护航的需求，只有通过多种检测引擎协同防护才能起到最佳的防护效果。

Web应用防火墙的深度学习引擎基于阿里云自身的海量运营数据，对正常的Web应用进行建模并从正常的模型中区分出异常情况，从繁多的Web应用攻击中提炼出异常攻击模型，最终通过模型实时地对未知风险请求进行在线检测拦截，弥补其他防御引擎对未知0day漏洞风险检测的不足。使用Web应用防火墙防御Web攻击时，被防护的业务流量先经过正则防护引擎，再经过深度学习引擎，两者互为补充。

应用场景

深度学习引擎主要针对一些弱特征的Web攻击请求，而非CC攻击。如果您对Web攻击防护有较高的要求，建议您开启深度学习引擎功能。

一般来说，规则引擎使用的正则规则的描述性比较强，对于强攻击特征的请求，正则规则的防护效果最佳。而当面对一些弱特征的攻击请求（例如XSS特征请求），即便您开启正则防护引擎的严格模式，依然可能因无法检测到而存在潜在的安全风险。这种情况下，您可以开启深度学习引擎，识别并拦截正则防护引擎的严格规则无法识别的弱特征攻击请求。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

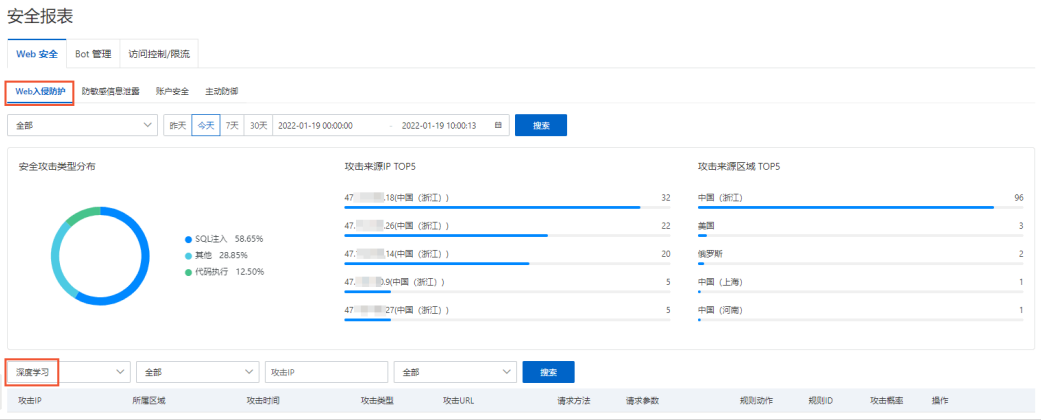
5. 单击**Web安全**页签，定位到**深度学习引擎**区域，完成以下功能配置。

参数	说明
状态	开启或关闭深度学习引擎功能。 **说明** 深度学习引擎开启后，所有网站请求默认都会经过深度学习引擎的检测。您可以通过设置Web入侵防护白名单，让满足条件的请求忽略深度学习引擎的检测。更多信息，请参见设置Web入侵防护白名单。
模式	检测发现攻击请求时，对攻击请求执行的操作。可选值： ○ **拦截**：直接阻断攻击请求。 ○ **告警**：只触发告警，不阻断攻击请求。

参数	说明
攻击概率	设置在深度学习下判定请求是攻击的概率阈值，使用50~100范围内的整数表示。 **攻击概率**阈值越大，请求被判断为攻击的标准越严格，深度学习引擎能够帮助您更精确地拦截真正的攻击，但是可能带来的漏过也会变多。 **攻击概率**阈值越小，请求被判断为攻击的标准越宽松，深度学习引擎能够帮助您拦截更多的可疑请求，但是可能带来的误杀也会变多。

后续步骤

启用深度学习引擎后，您可以在**安全报表**页面，通过**Web安全 > Web入侵防护**报表，查询深度学习引擎规则的命中纪录。更多信息，请参见WAF安全报表。



2.3. 设置网站防篡改

网站接入Web应用防火墙防护后，您可以开启网站防篡改功能。网站防篡改帮助您锁定需要保护的网站页面（例如敏感页面），被锁定的页面在收到请求时，返回已设置的缓存页面，预防源站页面内容被恶意篡改。

前提条件

- 已开通Web应用防火墙实例，且实例满足以下要求：
  - 如果是包年包月实例：已付费购买WAF包年包月实例。

    更多信息，请参见开通Web应用防火墙。
  - 如果是按量计费实例：已在**账单与套餐中心**，开启**数据安全**模块下**网站防篡改**功能。

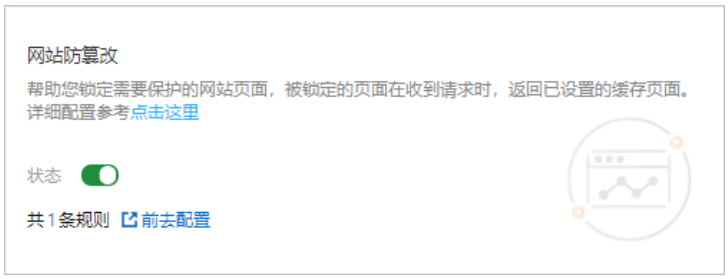
    更多信息，请参见账单与套餐中心（按量2.0版本）。
- 已完成网站接入。具体操作，请参见网站接入概述。

操作步骤

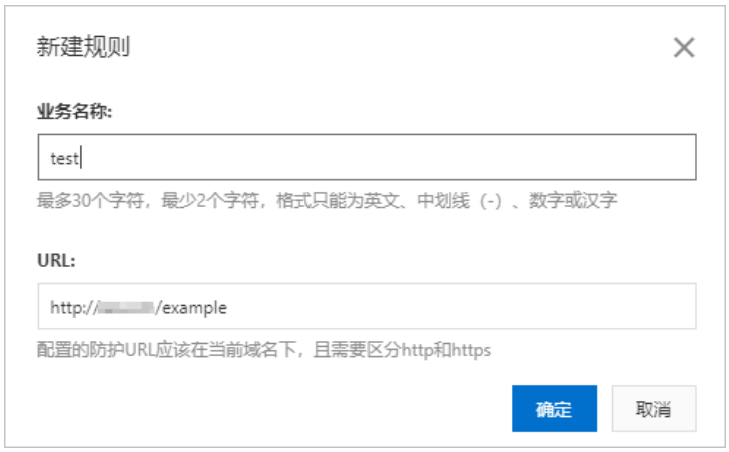
1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**Web安全**页签，定位到**网站防篡改**区域，开启**状态**开关并单击**前去配置**。

> 注意 网站防篡改开启后，所有网站请求默认都会经过网站防篡改规则的检测。您可以通过设置数据安全白名单，让满足条件的请求忽略网站防篡改规则的检测。更多信息，请参见设置数据安全白名单。



6. 新增网站防篡改规则。
   i. 在**网站防篡改**页面，单击**新增规则**。
   ii. 在**新建规则**对话框，输入要防护的网页对应的**业务名称**和URL。
   - **业务名称**：网页对应的业务名称。
   - **URL**：填写要防护的精确路径（以 `http://` 或者 `https://` 开头），不支持通配符（例如 `/*` ）或参数（例如 `/abc?xxx=` ）。该路径下的TXT、HTML和图片等内容都将受到防护。



   iii. 单击**确定**。

   成功添加网站防篡改规则后，规则默认不开启。您可以在规则列表中看到新建的规则，且**防护状态**开关未开启。

7. 开启规则。在规则列表中定位到要开启的规则，开启**防护状态**开关。
   成功开启规则后，规则对应的页面被请求时，将统一返回Web应用防火墙中的缓存记录。

8. （可选）更新缓存。在规则列表中定位到已开启的规则，单击**防护状态**列下的**更新缓存**。

> **注意** 如果被防护页面发生内容更新，您必须单击**更新缓存**，更新Web应用防火墙中的缓存记录。如果您在页面更新后未更新缓存，Web应用防火墙将始终返回最近一次缓存的记录，导致防护失效。

2.4. 设置防敏感信息泄露

网站接入Web应用防火墙后，您可以为其开启防敏感信息泄露功能。防敏感信息泄露帮助网站过滤服务器返回内容（异常页面或关键字）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。

> **注意** 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。

前提条件

- 已开通Web应用防火墙实例，且实例满足以下要求：
  - 包年包月实例：
    - 如果实例地域是**中国内地**，则实例版本必须是**高级版**及以上规格。
    - 如果实例地域是**海外地区**，则实例版本必须是**企业版**及以上规格。

    更多信息，请参见开通Web应用防火墙。
  - 按量计费实例：已在**账单与套餐中心**，开启**数据安全**模块下**防敏感信息泄露**功能。

    更多信息，请参见账单与套餐中心（按量2.0版本）。

- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

防敏感信息泄漏功能是Web应用防火墙针对《网络安全法》提出的“网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告”所给出的安全防护方案。防敏感信息泄漏针对网站中存在的敏感信息（尤其是电话号码、身份证、信用卡）泄漏、敏感词汇泄露提供脱敏和告警措施，并支持拦截指定的HTTP状态码。

功能特性

网站中造成信息泄漏的常见场景包括URL未授权访问（例如，网站管理后台未授权访问）、越权查看漏洞（例如，水平越权查看漏洞和垂直越权查看漏洞）、网页中的敏感信息被恶意爬虫爬取。针对网站中常见的敏感信息泄露场景，防敏感信息泄漏提供以下功能：

- 检测识别网站页面中出现的个人隐私敏感数据，并提供预警和屏蔽敏感信息等防护措施，避免网站经营数据泄露。这些敏感隐私数据包括但不限于身份证号、电话号码、银行卡号。

> 注意 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。

- 针对有可能暴露网站所使用的Web应用软件、操作系统类型，版本信息等服务器敏感信息，支持一键拦截，避免服务器敏感信息泄露。
- 根据内置的非法敏感关键词库，检测在网站页面中出现的相关非法敏感词，提供告警和非法关键词屏蔽等防护措施。

工作原理

防敏感信息泄露按照配置好的防护规则，检测响应页面中是否带有身份证号、电话号码、银行卡号等敏感信息，并在发现敏感信息匹配命中后，根据规则中指定的匹配动作触发告警或者敏感信息过滤。敏感信息过滤动作指以*号替换敏感信息部分，达到保护敏感信息的效果。

防敏感信息泄露功能支持的Content-Type包括 `text/*` 、 `image/*` 、 `application/*` 等，涵盖Web端、App端和API接口。

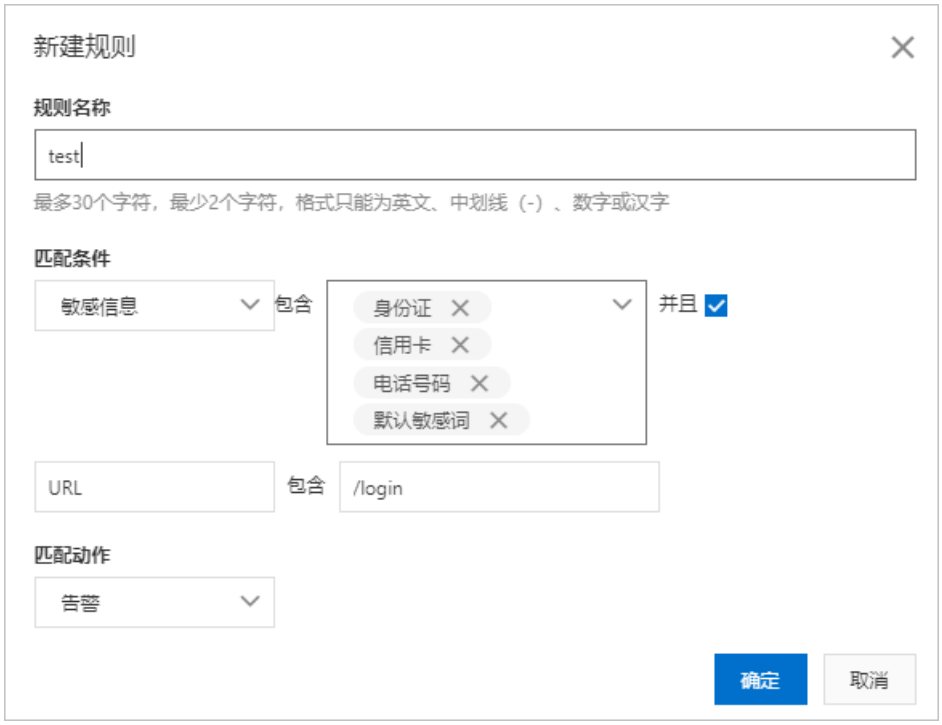
操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**Web安全**页签，定位到**防敏感信息泄露**区域，开启**状态**开关并单击**前去配置**。

> 注意
> - 您必须先开启防敏感信息泄露，才能设置防护规则。
> - 防敏感信息泄露开启后，所有网站请求默认都会经过防敏感信息泄露规则的检测。您可以通过设置数据安全白名单，让满足条件的请求忽略防敏感信息泄露规则的检测。更多信息，请参见设置数据安全白名单。

6. 新增防敏感信息泄露规则。
   i. 在**防敏感信息泄露**页面，单击**新增规则**。
   ii. 在**新建规则**对话框，完成以下规则配置。



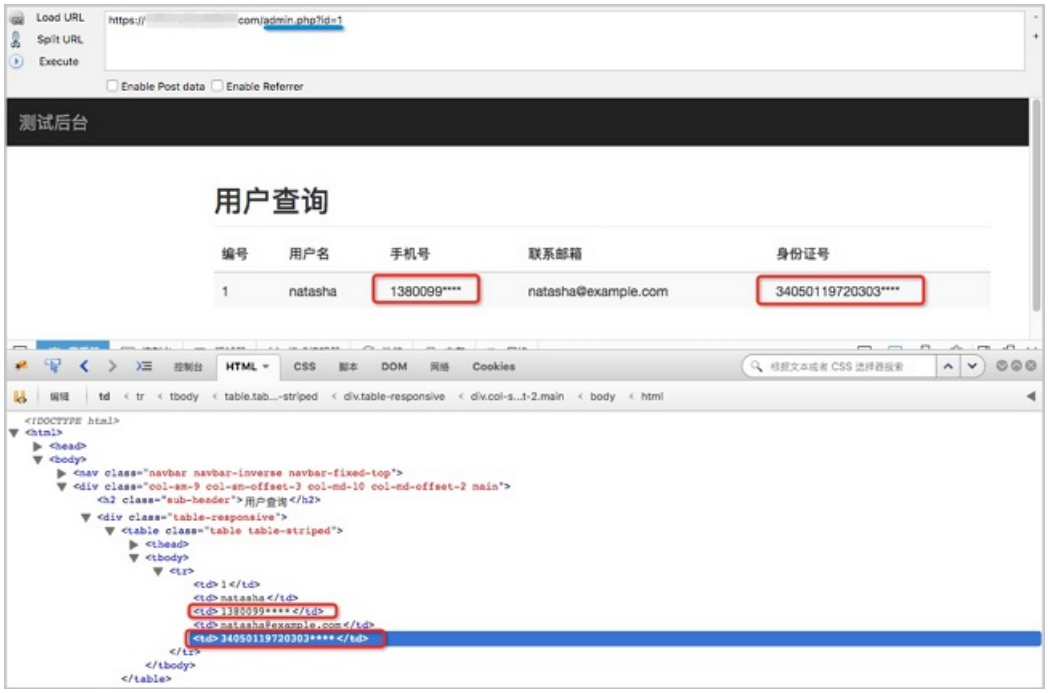
参数	说明
规则名称	为规则命名。
匹配条件	定义要在请求响应中检测的敏感信息类型，可选值： ■ **响应码**：400、401、402、403、404、500、501、502、503、504、405-499、505-599 ■ **敏感信息**：**身份证**、**信用卡**、**电话号码**、**默认敏感词** 注意 防敏感信息泄露功能目前仅支持处理中华人民共和国境内使用的数据格式（例如，身份证号、电话号码、银行卡号），暂不支持处理中国境外的身份证号、电话号码、银行卡号等数据格式。 您可以指定检测响应码、敏感信息分类下的一种或多种类型。 如果选中**并且**，则可以进一步指定要检测的**URL**，即只在指定的页面中检测敏感信息。
匹配动作	定义在请求响应中检测到敏感信息后执行的操作。 ■ 匹配条件为**响应码**时，支持以下匹配动作： ■ **告警**：触发敏感信息泄露告警通知。 ■ **拦截**：阻断访问请求，并返回默认的屏蔽提示页面。 ■ 匹配条件为**敏感信息**时，支持以下匹配动作： ■ **告警**：触发敏感信息泄露告警通知。 ■ **敏感信息过滤**：脱敏请求响应中的敏感信息。

规则配置示例

- 敏感信息过滤：针对网站页面中可能存在的电话号码和身份证等敏感信息，配置相应的规则对其进行过滤或告警。例如，您可以设置以下防护规则，过滤电话号码和身份证号敏感信息。
  - 匹配条件：敏感信息包含身份证、电话号码。
  - 匹配动作：敏感信息过滤。

  应用该规则后，则网站中的所有页面的电话号码和身份证号都会自动脱敏，效果如下图所示。

  > **注意** 网站页面中的商务合作电话、举报电话等需要对外公开的电话号码，也可能被电话号码敏感信息过滤规则过滤。



- 状态码拦截：针对特定的HTTP请求状态码，配置规则将其拦截或者告警，避免服务器敏感信息泄露。例如，您可以设置以下防护规则，拦截HTTP 404状态码。
  - 匹配条件：响应码包含404。
  - 匹配动作：拦截。

  应用该规则后，当请求一个该网站中不存在的页面时，返回特定拦截页面，效果如下图所示。

- 针对特定URL页面中的敏感信息过滤：针对特定URL页面中存在的电话号码和身份证等敏感信息，配置相应的规则对其进行过滤或告警。例如，您可以设置以下防护规则，过滤 `admin.php` 页面中的身份证号敏感信息。
  - 匹配条件：敏感信息包含身份证，并且URL包含 `admin.php` 。
  - 匹配动作：敏感信息过滤。

  应用该规则后，仅admin.php页面中的身份证号信息被自动脱敏。

iii. 单击**确定**。
成功添加防敏感信息泄露规则后，规则自动生效。您可以在规则列表中查看新建的规则，并根据需要编辑或删除规则。

后续步骤

开启防敏感信息泄露后，您可以在**安全报表**页面，通过**Web安全 > 防敏感信息泄露**报表，查询触发防敏感信息泄露规则被过滤或拦截的访问请求的日志。更多信息，请参见WAF安全报表。

2.5. 设置主动防御

网站接入Web应用防火墙防护后，您可以为网站开启主动防御功能。主动防御采用阿里云自研的机器学习算法，自主学习网站域名的合法流量，并自动为网站生成定制化的安全防护策略，防御未知攻击。

前提条件

- 已开通Web应用防火墙实例，且实例满足以下要求：
  - 包年包月实例：实例版本是**旗舰版**及以上规格。

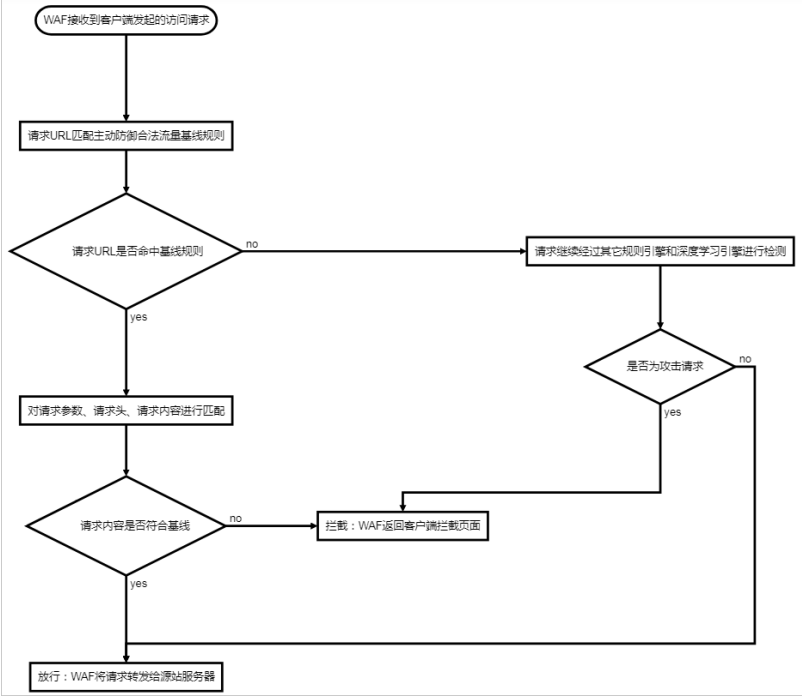
    更多信息，请参见开通Web应用防火墙。
  - 按量计费实例：已在**账单与套餐中心**，开启**Web入侵防护**模块下**主动防御**功能。

    更多信息，请参见账单与套餐中心（按量2.0版本）。

- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

传统的Web攻击防护基于安全检测规则。主动防御通过无监督学习的方式，对域名的访问流量进行深度学习，并根据机器学习算法模型为不同访问请求打分，标记正常分值。在请求分值的基础上，主动防御能够定义域名的正常访问流量基线，并基于此生成定制化的安全策略。通过将流量分层的方式，结合主动防御与Web应用防火墙的其他安全检测体系，为域名提供更加全面的攻击防护。



操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**Web安全**页签，定位到**主动防御**区域，完成以下功能配置。

参数	说明
状态	开启或关闭主动防御功能。

参数	说明
模式	检测发现攻击请求时，对攻击请求执行的操作。可选值： ○ **告警**：只触发告警，不阻断攻击请求。 ○ **拦截**：直接阻断攻击请求。 **说明** 默认情况下，主动防御采用告警模式。所有主动防御安全规则仅将命中规则的请求上报至安全报表，并不会进行拦截。建议您通过安全报表观察一段时间，确认主动防御的安全规则没有出现误拦截的情况后，再切换到拦截模式。

网站域名首次开启主动防御后，WAF将自动使用机器学习算法模型对域名的历史流量进行深度学习，并基于学习结果为该域名生成定制化的安全策略。机器学习算法模型的首次学习时长与域名的历史流量大小有关，通常需要大约一小时完成首次学习并生成安全策略。学习完成后，您将收到站内信、短信、邮件通知。

注意 主动防御的学习程序是一次性的，如果您手动关闭主动防御后再重新开启，则WAF会重新执行一遍学习程序。WAF产品版本升级不会对已有学习结果产生影响，该情形无需重新执行学习程序；但是，如果接入WAF防护的业务形态发生变化（例如，域名上的业务类型变更等），则已有学习结果将不再适用，建议您重新执行一遍学习程序。

3.Bot管理

3.1. 防爬场景化配置

3.1.1. 概述

Web应用防火墙WAF（Web Application Firewall）针对Bot管理模块进行全面升级，提供防爬场景化配置功能。您可以基于实际业务场景对防爬规则进行自定义，从而更有针对性地对业务进行爬虫风险防护。

背景信息

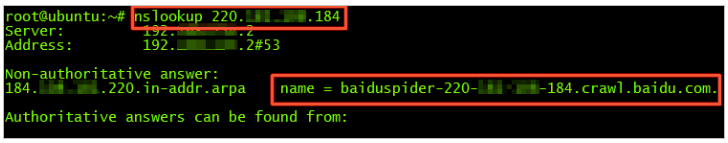
当今互联网爬虫种类繁多，专业的爬虫会不断变换爬取手段，绕过网站管理员的防爬策略。因此，很难达成依靠固定的规则来实现一劳永逸的完美防护的目标。并且，爬虫风险管理与业务自身特性强相关，需要专业的安全团队进行对抗才能取得较好的效果。

如果您对防爬效果有较高的要求，或者缺乏专业的安全团队来配置相应的安全策略，您可以使用WAF提供的防爬场景化功能，有效防护恶意爬虫风险。

WAF基于阿里云对全网威胁情报实时计算得到的恶意爬虫IP情报库、动态更新的各大公有云或IDC机房IP库等情报信息，根据配置的场景化规则，帮助您直接放行合法爬虫请求，并对来自威胁情报库的恶意请求进行防护处置。

恶意爬虫的特征和危害

正常爬虫请求的user-agent字段中通常包含 `xxspider` 标识，并且爬取的请求量不大，爬取的URL和时间段都比较分散。如果对合法的爬虫IP执行反向 `nslookup` 或 `tracert` ，一般都可以看到爬虫的来源地址。例如，对百度的爬虫IP执行反向 `nslookup` ，可查询到其来源地址信息。



恶意爬虫则可能会在某个时间段大量请求某个域名的特定地址或接口，这种情况很可能是伪装成爬虫的CC攻击，或是经第三方伪装后针对性爬取敏感信息的请求。当恶意爬虫请求量大到一定程度后，会造成服务器的CPU飙升，带来网站无法访问等业务中断问题。

适用版本

- 如果是包年包月实例：已开通高级版、企业版、旗舰版的**Bot管理**增值服务。更多信息，请参见开通Web应用防火墙。
- 如果是按量计费实例：已在**账单与套餐中心**，开启**Bot管理**模块下**场景化配置**功能。

> **说明** 使用按量计费WAF实例的防爬场景化配置功能时，阿里云将根据您已设置的场景个数来计费。相关内容，请参见按量计费2.0。

使用限制

每个域名最多可添加50个**场景化配置**规则。

相关视频

观看以下视频，快速了解如何使用防爬场景化配置方案，实现精细化爬虫防护，满足个性化的业务防护需求。

相关文档

配置浏览器访问网页的防爬场景化规则

配置App防爬场景化规则

防爬场景化配置示例

3.1.2. 配置浏览器访问网页的防爬场景化规则

Web应用防火墙WAF（Web Application Firewall）针对Bot管理模块进行全面升级，提供防爬场景化配置功能。您可以基于实际业务场景对防爬规则进行场景化定制，更有针对性地对业务进行爬虫风险防护。本文指导您针对浏览器访问网页的场景配置防爬场景化规则。

背景信息

防爬场景化配置功能支持基于不同业务场景定制防爬规则，结合智能算法，精准识别爬虫流量，并对命中规则的爬虫行为进行自动处置。同时，在定制场景化防爬规则后，您可以在测试环境中对防爬规则进行应用前的验证，避免因规则配置不合理或防护兼容性问题，对您的网站或App业务产生误拦截或防护效果低等不利影响。

前提条件

- 如果是包年包月实例：已开通高级版、企业版、旗舰版的**Bot管理**增值服务。更多信息，请参见开通Web应用防火墙。
- 如果是按量计费实例：已在**账单与套餐中心**，开启**Bot管理**模块下**场景化配置**功能。

> **说明** 使用按量计费WAF实例的防爬场景化配置功能时，阿里云将根据您已设置的场景个数来计费。相关内容，请参见按量计费2.0。

- 已完成网站接入。具体操作，请参见网站接入概述。

添加浏览器访问网页的防爬场景

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 如果您没有创建过防爬场景化规划，单击**Bot管理**页签，在**场景化配置**模块单击**点我开始**，创建您的第一条防爬场景化规则。如果您已创建过防爬场景化规则，在**Bot管理**页签右上角单击**添加**，创建更多的防爬场景化规则。

> **说明** 每个域名最多可添加50条**场景化配置**规则。

6. 在**防护场景定义**配置向导页面，设置防爬保护目标的基础信息，并单击**下一步**。

配置项	说明
防护业务场景	填写该防爬规则防护的业务场景类型。常见场景例如：登录、注册、下单等。
防护目标类型	选择**网页/浏览器**，表示对浏览器访问的网页或H5页面（包括App中使用的H5页面）进行防护。 如果网站用户从另一个域名发起对当前防护目标的访问请求，则需选择**防护目标有来自其它域名的跨域调用**，并从下拉列表中选择跨域访问的来源域名。
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。有关字段的详细内容，请参见匹配条件字段说明。最多可以添加5个条件。 **注意** 输入IP地址后需要按回车。

7. 在**防护规则推荐**向导页面，设置防爬场景规则的详细内容，并单击**下一步**。

配置项	说明
简单脚本过滤	开启此开关后，对访问防爬防护目标的客户端进行JS校验，对不支持JS校验的来自非浏览器类工具的流量进行过滤，阻断简单脚本类攻击。
动态令牌挑战	默认未开启。开启此开关后，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。您可以选择**签名验证异常**（该项为必选，指为携带签名或者签名非法）、**签名时间戳异常**、**WebDriver攻击**，开启动态令牌挑战。
AI智能防护	开启此开关后，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，生成有针对性的防护规则或黑名单。您可根据需要将AI智能防护生成的规则设置为**观察模式**或**滑块校验**模式。设置为观察模式，防爬规则会放行命中流量并将流量记录在安全报表中；设置为滑块校验模式，客户端需完成滑块校验后才能继续访问防护目标。
爬虫威胁情报库匹配	通过与阿里云威胁情报库匹配，准确识别出阿里云上对多个用户有多次恶意爬取行为的攻击源IP地址，来自这些攻击源IP地址的访问请求将需要完成滑块校验，才能继续访问防护目标。
IDC黑名单封禁	对来自阿里云和其他主流云厂商IDC黑名单库的IP地址进行封禁，阻止这些黑名单地址对防护目标发起访问请求。 

配置项	说明
IP限速	开启后即可设置访问频率限制条件，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CC攻击。 您可以自定义IP限速条件来规定在指定时长内，来自同一IP地址的访问次数超过指定阈值时，对来自该IP的访问请求执行阻断、滑块校验或观察的处置动作，并规定处置动作的生效时长。最多可以设置3个条件。相关内容，请参见设置自定义防护策略。
自定义会话限速	开启后即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CC攻击。 您可以自定义会话限速条件来规定在指定时长内，来自同一会话的访问次数超过指定阈值时，对该会话执行阻断、滑块校验或观察的处置动作，并规定处置动作的生效时长。相关内容，请参见设置自定义防护策略。

8. （可选）在**防护动作验证**页面，对防爬防护规则进行效果测试。

   本操作为可选操作，您也可以单击左下角**跳过**。我们强烈建议您（特别是首次配置时）先完成防护动作验证，再发布策略，避免出现规则配置错误、兼容性等问题引发的误拦截。

   验证步骤如下：

   i. **填写公网测试IP**：填写您测试设备（PC或手机）的公网IP。本防爬规则验证测试将仅针对该公网IP生效，不会对您的业务产生影响。

   > 注意　请不要填写通过ipconfig查询的IP地址（即内网IP地址）。如果不确定您设备的公网IP，可以通过本页面提示信息中的网络诊断工具或在线IP查询工具进行查询。

   ii. **选择动作进行测试**：将对前序步骤中配置策略所涉及到的防护动作（可选**JS校验防护效果验证**、**动态令牌验证**、**滑块验证**、**拦截验证**）生成一条只针对您测试IP生效的测试规则，供您在实际环境中测试防护动作的效果。

   在测试动作模块上单击**去测试**后，WAF会将防护策略即刻下发到测试设备，同时为您展示测试效果演示图和说明，建议您仔细阅读。

   完成测试后，单击**已完成测试**进入下一步；如果测试结果异常，可以单击**返回去再准备一下**，优化防爬规则后重新测试。

   有关测试时出现的异常情况说明和对应的解决方法，请参见防爬策略测试常见问题。

9. 在**策略预览和发布**页面，确认策略的内容，单击**发布**。

   策略发布后即刻生效。

   > 说明　首次创建场景时规则ID不会展示，正式发布防爬场景化规则后，您可以在**安全报表**页面的Bot管理页签下方，查看规则ID信息。规则ID可用于日志服务中检索特定规则的命中情况。

防爬策略测试常见问题

报错	原因	解决方法
未查询到任何有效测试请求，您可以查看帮助文档或咨询我们以分析可能的原因。	实际测试请求没有发送成功，或者没有发送到WAF。	确认测试请求已经成功发送到WAF解析的地址。
	实际测试请求的字段内容与防爬规则中定义的**防护目标特征**不一致。	在防爬策略中修改防护目标特征的内容。
	实际测试请求的源IP与配置策略中填写的公网测试IP不一致。	请确保您使用的是正确的公网IP，建议直接使用诊断工具查询您的公网IP地址。
请求未通过校验，您可以查看帮助文档或咨询我们以分析可能的原因。	没有模拟真实用户访问，例如使用了调试模式、自动化工具等。	测试时使用客户端真实模拟用户访问。
	防护场景选择错误，例如实际需要配置App防爬场景规则，但错选为**网页/浏览器**。	在防爬场景化规则中修改防护场景类型。
	访问请求存在跨域的情况，但在防爬场景化规则中未正确配置。	修改防爬场景化规则，选中**防护目标有来自其它域名的跨域调用**并从下拉列表中选择跨域访问的来源域名。
	前端兼容性问题。	您可以通过钉钉群或工单联系我们排查。
请求未触发校验，您可以查看帮助文档或咨询我们以分析可能的原因。	测试规则没有下发完毕。	建议您多测试几次，等待防爬测试规则下发完成。
未拦截且查询到任何有效测试请求，您可以查看帮助文档或咨询我们以分析可能的原因。	实际测试请求没有发送成功，或者没有发送到WAF。	确认测试请求已经成功发送到WAF解析的地址。
	实际测试请求的字段内容与防爬规则中定义的**防护目标特征**不一致。	在防爬策略中修改防护目标特征的内容。
	实际测试请求的源IP与配置策略中填写的公网测试IP不一致。	请确保您使用的是正确的公网IP，建议直接使用诊断工具查询您的公网IP地址。

后续步骤

前往安全报表中的**Bot管理**页签，查看防护效果和规则命中的详细内容，并且根据防护效果，对防爬场景化策略进行优化。

3.1.3. 配置App防爬场景化规则

Web应用防火墙WAF（Web Application Firewall）针对Bot管理模块进行全面升级，提供防爬场景化配置功能。您可以基于实际业务场景定制防爬规则，更有针对性地对业务进行爬虫风险防护。本文指导您针对App的场景配置防爬场景化规则。

背景信息

防爬场景化配置功能支持基于不同业务场景定制防爬规则，结合智能算法，精准识别爬虫流量，并对命中规则的爬虫行为进行自动处置。同时，在定制场景化防爬规则后，您可以在测试环境中对防爬规则进行应用前的验证，避免因规则配置不合理或防护兼容性问题，对您的网站或App业务产生误拦截或防护效果低等不利影响。

前提条件

- 如果是包年包月实例：已开通高级版、企业版、旗舰版的**Bot管理**增值服务。更多信息，请参见开通Web应用防火墙。
- 如果是按量计费实例：已在**账单与套餐中心**，开启**Bot管理**模块下**场景化配置**功能。

> **说明** 使用按量计费WAF实例的防爬场景化配置功能时，阿里云将根据您已设置的场景个数来计费。相关内容，请参见按量计费2.0。

- 已完成网站接入。具体操作，请参见网站接入概述。
- 需要防护的App已集成Web应用防火墙SDK。详细内容，请参见集成SDK。

添加网页/浏览器场景

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 如果您没有创建过防爬场景化规划，单击**Bot管理**页签，在**场景化配置**模块单击**点我开始**，创建您的第一条防爬场景化规则。如果您已创建过防爬场景化规则，在**Bot管理**页签右上角单击**添加**，创建更多的防爬场景化规则。

> **说明** 每个域名最多可添加50条**场景化配置**规则。

6. 在**防护场景定义**配置向导页面，设置防爬保护目标的基础信息，并单击**下一步**。

配置项	说明
防护业务场景	填写该防爬规则防护的业务场景类型。常见场景例如：登录、注册、下单等。
防护目标类型	选择**App**，表示对使用iOS和Android系统开发的原生App进行防护。 **说明** App中使用的H5页面不属于此类防护目标。如果您需要对App中使用的H5页面进行防爬场景化防护，**防护目标类型**需要选择**网页/浏览器**。

配置项	说明
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。有关字段的详细内容，请参见匹配条件字段说明。最多可以添加5个条件。 **注意** 输入IP地址后需要按回车。

7. 在**防护规则推荐**向导页面，设置防爬场景规则的详细内容，并单击**下一步**。

配置项	说明
App签名异常	对使用未携带签名或签名非法的App访问防爬防护目标的请求进行检测和管控。此项不支持关闭，您可以在下方设置**防护动作**，对App签名异常的流量进行相应的处置。设置为观察模式，防爬规则会放行命中流量并将流量记录在安全报表和日志服务中；设置为拦截模式，防爬规则会对命中流量进行拦截。
设备特征异常	启用此项后，防爬规则会对具有异常特征的设备发起的请求进行检测和管控。 设备的异常特征包括： ○ **使用模拟器**：表示设备上使用了模拟器。 ○ **使用代理**：表示设备上使用了代理服务。 ○ **Root设备**：表示设备开放了Root权限。 ○ **调试模式**：表示设备开启了调试模式。 ○ **App被hook**：表示设备上存在 `hook` 程序。 ○ **App多开**：表示设备上同时打开了多个被防护App的进程。 您可根据需要将规则设置为**观察**或**拦截**。
防护动作	支持**观察**和**拦截**两种处置动作。此项配置针对**App签名异常**和**设备特征异常**同时生效。
IP限速	开启后即可设置访问频率限制条件，有针对性地过滤异常请求，有效缓解CC攻击。 您可以自定义IP限速条件来规定在指定的统计时长内，来自同一IP地址的访问次数超过指定阈值时，对该访问请求执行阻断或观察的处置动作，并规定处置动作的生效时长。最多可以设置3个条件。相关内容，请参见设置自定义防护策略。
设备限速	开启后即可设置访问频率限制条件，有针对性地过滤异常请求，有效缓解CC攻击。 您可以自定义终端设备限速条件来规定在指定的统计时长内，来自同一终端设备的访问次数超过指定阈值时，对该访问请求执行阻断或观察的处置动作，并规定处置动作的生效时长。最多可以设置3个条件。

配置项	说明
自定义会话限速	开启后即可自定义访问频率限制条件，有针对性地过滤异常请求，有效缓解CC攻击。 您可以自定义会话限速条件来规定在指定的统计时长内，来自同一会话的访问次数超过指定阈值时，对该访问请求执行阻断或观察的处置动作，并规定处置动作的生效时长。最多可以设置3个条件。相关内容，请参见设置自定义防护策略。

8. （可选）在**防护动作**校验页面，对防爬防护规则进行效果测试。

   本步骤为可选操作，您也可以单击左下角**跳过**。建议您先完成防护动作验证后，再发布策略。

   关键配置项说明：

   - **公网测试IP**：填写您测试设备（手机）的公网IP。防爬规则将仅针对该公网IP生效，不会对您的业务产生影响。

     > **注意** 如果不确定您设备的公网IP，可以通过本页面提示信息中的网络诊断工具或在线IP查询工具进行查询。

   - **SDK签名验证**：单击**去测试**，验证该App的SDK签名是否正常。

     > **说明** 请务必使用已经集成好App防护SDK的真实设备进行测试，否则会导致验证签名失败，访问请求被拦截，无法正常完成测试。

   - **测试动作**：针对命中规则的访问请求进行拦截验证。在测试动作模块上单击**去测试**后，WAF会将防护策略即刻下发到测试设备，同时为您展示测试效果演示图和说明，建议您仔细阅读。

     完成测试后，单击**已完成测试**进入下一步；如果测试结果异常，可以单击**返回去再准备一下**，优化防爬规则后重新测试。

     有关测试时出现的异常情况说明和对应的解决方法，请参见防爬策略测试常见问题。

9. 在**策略预览和发布**页面，确认策略的内容，单击**发布**。

   策略发布后即刻生效。

   > **说明** 首次创建场景时规则ID不会展示，正式发布防爬场景化规则后，您可以在**安全报表**页面的Bot管理页签下方，查看规则ID信息。规则ID可用于日志服务中检索特定规则的命中情况。

防爬策略测试常见问题

报错	原因	解决方法
未查询到任何有效测试请求，您可以查看帮助文档或咨询我们以分析可能的原因。	实际测试请求没有发送成功，或者没有发送到WAF。	确认测试请求已经成功发送到WAF解析的地址。
	实际测试请求的字段内容与防爬规则中定义的**防护目标特征**不一致。	在防爬策略中修改防护目标特征的内容。

报错	原因	解决方法
	实际测试请求的源IP与配置策略中填写的公网测试IP不一致。	请确保您使用的是正确的公网IP，建议直接使用诊断工具查询您的公网IP地址。
请求未通过校验，您可以查看帮助文档或咨询我们以分析可能的原因。	没有模拟真实用户访问，例如使用了调试模式、自动化工具等。	测试时使用客户端真实模拟用户访问。
	防护场景选择错误，例如实际需要配置防爬场景规则，但错选为**网页/浏览器**。	在防爬场景化规则中修改防护场景类型。
	访问请求存在跨域的情况，但在防爬场景化规则中未正确配置。	修改防爬场景化规则，选中**防护目标存在跨域调用其他域名**并从下拉列表中选择跨域访问的来源域名。
	前端兼容性问题。	您可以通过钉钉群或工单联系我们排查。
请求未触发校验，您可以查看帮助文档或咨询我们以分析可能的原因。	测试规则没有下发完毕。	建议您多测试几次，等待防爬测试规则下发完成。
未拦截且查询到任何有效测试请求，您可以查看帮助文档或咨询我们以分析可能的原因。	实际测试请求没有发送成功，或者没有发送到WAF。	确认测试请求已经成功发送到WAF解析的地址。
	实际测试请求的字段内容与防爬规则中定义的**防护目标特征**不一致。	在防爬策略中修改防护目标特征的内容。
	实际测试请求的源IP与配置策略中填写的公网测试IP不一致。	请确保您使用的是正确的公网IP，建议直接使用诊断工具查询您的公网IP地址。
请求验签失败被拦截，您可以查看帮助文档或咨询我们以分析可能的原因。	集成SDK时部分代码逻辑有问题导致签名非法，例如签名的内容跟实际请求不一致，或签名缺失。	检查签名是否存在问题并进行修复。相关内容，请参见App防护。
	测试时未使用真实设备或开启了代理。	使用真实的设备重新进行测试。

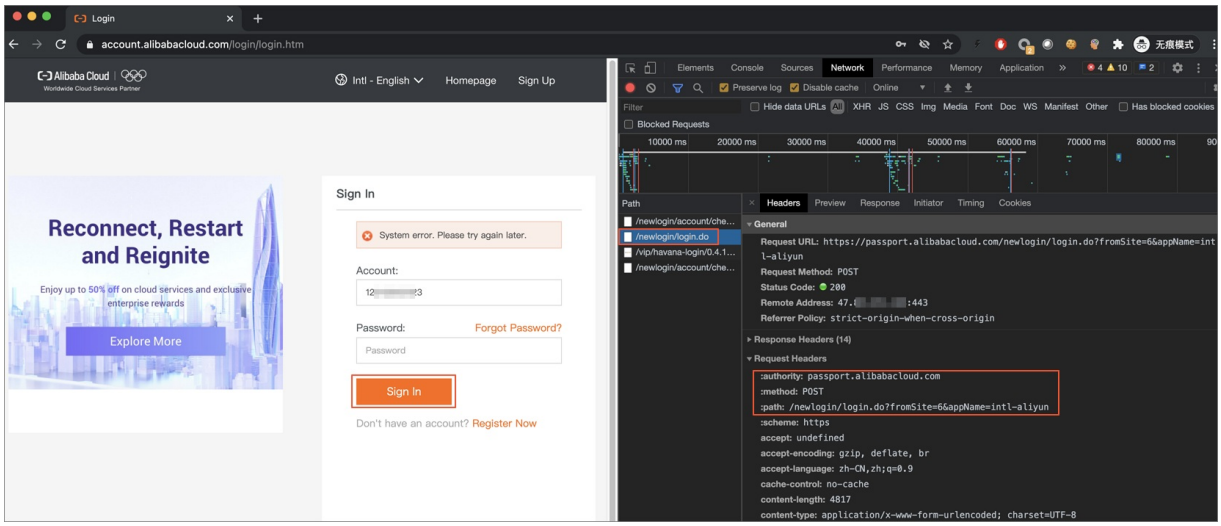
3.1.4. 防爬场景化配置示例

本文以网页登录和网页存在多个子域名为例，介绍如何自定义防爬场景化规则。

示例一：阿里云官网登录页面

本示例以阿里云国际站官网登录页面（account.alibabacloud.com）为例，介绍防爬场景化防护规则的具体配置。

在阿里云官网单击登录按钮后，触发的网页请求字段如下：



场景化防爬规则配置示意图如下：

规则配置说明：

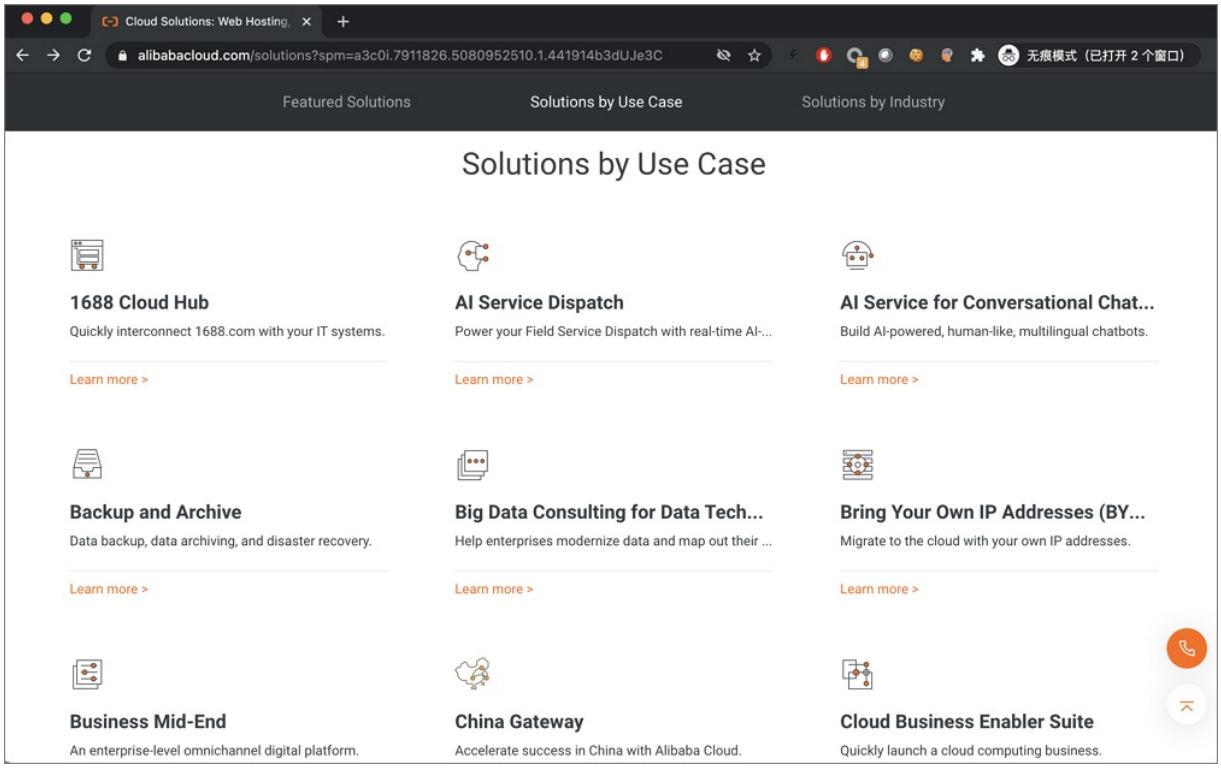
- 执行登录操作时，需要在阿里云官网页面上单击Sign In图标来触发登录请求。这是此次示例场景中防护的最终目标，因此，防护业务场景填写**登录**。
- 网页登录流程是在浏览器环境下完成的，防护目标类型选择**网页/浏览器**。
- 登录按钮位于account.alibabacloud.com这个域名下的页面中，但登录请求是提交到passport.alibabacloud.com这个域名的，存在跨域的情况。因此，防护策略本身应该配置在passport.alibabacloud.com域名下，但同时需要选中**防护目标有来自其它域名的跨域调用**，并填写**account.alibaba.com**域名。
- 登录请求本身的特征是URL包含/newlogin/login.do，且请求方法为POST。因此，防护目标特征需要按该

特征进行定义。

示例二：阿里云官网解决方案详情页面

本示例以阿里云国际站官网解决方案详情页面（alibabacloud.com/solutions）为例，介绍防爬场景化防护规则的具体配置。

以下是本示例中提及的阿里云解决方案详情页面：



场景化防爬规则配置示意图如下：

规则配置说明如下：

- 此次示例场景中防护的最终目标是alibabacloud.com/solutions页面下的各个解决方案子页面。因此，防护业务场景填写**解决方案详情页**。
- 访问该页面是在浏览器环境下完成的，防护目标类型选择**网页/浏览器**。
- 在阿里云解决方案详情页面（alibabacloud.com/solutions），访问单个解决方案页面，其URL结构为 `/solutions/xxx` 。因此，防护目标特征设置为 `URLPath`**包含**`/solutions/` 、请求方法为 `GET` 。本示例中不涉及跨域请求，因此，无需选择**防护目标有来自其它域名的跨域调用**。您也可以根据业务场景的实际情况，添加更多防护条件，例如user-agent、param、referer等。

3.2. 设置合法爬虫规则

合法爬虫功能提供合法搜索引擎白名单（例如Google、Bing、百度、搜狗、Yandex等），为域名放行合法爬虫的访问请求。

前提条件

- 已开通Web应用防火墙实例，且实例满足以下要求：
  - 包年包月实例：已开启**Bot管理**模块。更多信息，请参见开通Web应用防火墙。
  - 按量计费实例：已在**账单与套餐中心**开启**Bot管理**模块下**合法爬虫**功能。更多信息，请参见账单与套餐中心（按量2.0版本）。
- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

合法爬虫规则依据阿里云爬虫情报库，帮助您直接放行合法爬虫请求。阿里云爬虫情报库基于阿里云全网流量计算得出并可实时更新，涵盖合法爬虫访问请求来源的特征信息。合法爬虫支持主流搜索引擎的爬虫IP信息，可动态更新，目前包含Google、百度、搜狗、Bing、Yandex。

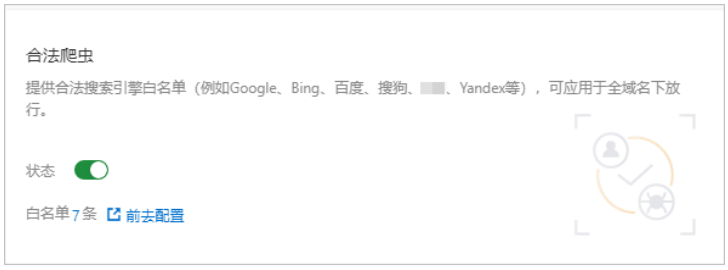
启用合法爬虫规则后，来自相关搜索引擎的合法爬虫IP将被直接放行，不经过Bot管理模块的防护检测。

> **说明** 在Bot管理模块外，您还可以使用**访问控制/限流**规则进一步过滤来自于合法爬虫白名单IP的请求。更多信息，请参见设置自定义防护策略。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**Bot管理**页签，定位到**合法爬虫**区域，开启**状态**开关并单击**前去配置**。



6. 在**合法爬虫**规则列表，根据**情报名称**选择要放行的合法爬虫，开启对应的**启用状态**开关。

规则ID	情报规则名称	防护路径	处置动作	最新修改时间	启用状态
1589409	百度蜘蛛白名单	全路径	放行	2021年5月26日 11:09	
1589410	搜狗蜘蛛白名单	全路径	放行	2021年5月26日 11:09	
1589412	Google蜘蛛白名单	全路径	放行	2021年5月26日 11:09	
1589413	Bing蜘蛛白名单	全路径	放行	2021年5月26日 11:09	

默认规则支持单独设置放行来自以下搜索引擎的爬虫请求：Google、Bing、百度、搜狗、Yandex。您也可以只开启**合法搜索引擎白名单**规则，放行所有支持的搜索引擎白名单。

3.3. 设置爬虫威胁情报规则

爬虫威胁情报功能提供拨号池IP、IDC机房IP、恶意扫描工具IP以及云端实时模型生成的恶意爬虫库等多种维度的爬虫威胁情报规则，方便您在全域名或指定路径下设置阻断恶意爬虫的访问请求。

前提条件

- 已开通Web应用防火墙实例，且实例满足以下要求：
  - 包年包月实例：已开启**Bot管理**模块。更多信息，请参见开通Web应用防火墙。
  - 按量计费实例：已在**账单与套餐中心**开启**Bot管理**模块下**威胁情报**功能。更多信息，请参见账单与套餐中心（按量2.0版本）。

- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

爬虫威胁情报规则基于阿里云爬虫情报库，帮助您阻断来自威胁情报库的爬虫请求。阿里云爬虫情报库基于阿里云全网流量和威胁情报计算得出并实时更新，可有效检测恶意爬虫IP，并提供恶意访问请求来源的特征信息。

> **说明** 阿里云爬虫情报库覆盖公有云和线下IDC网络。

您可以设置威胁情报规则，针对不同类型的威胁情报库选择不同的处置动作（例如直接拦截、进行JavaScript校验、弹出滑块验证或观察），也可以为某些关键接口配置针对特定类型威胁情报库的防护，以避免正常业务受到影响。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**Bot管理**页签，定位到**爬虫威胁情报**区域，开启**状态**开关并单击**前去配置**。

> **说明** 爬虫威胁情报开启后，所有网站请求默认都会经过爬虫威胁情报规则的检测。您可以通过设置Bot管理白名单，让满足条件的请求忽略爬虫威胁情报规则的检测。更多信息，请参见设置Bot管理白名单。

6. 在**爬虫威胁情报**规则列表中，根据**情报名称**选择要使用的威胁情报库，开启对应的**启用状态**开关。

下表描述了支持的爬虫威胁情报库。

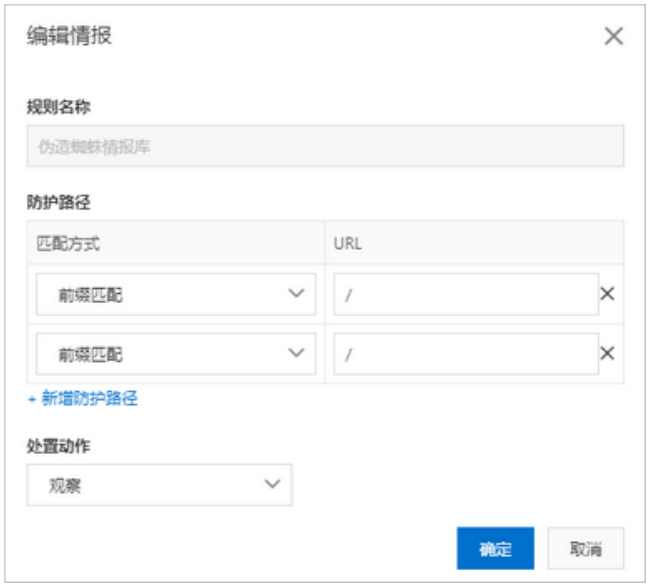
情报库	描述
扫描器恶意指纹库	常见扫描器的特征库。

情报库	描述
恶意扫描IP情报库	基于阿里云全网实时检测到的恶意扫描行为攻击源IP进行分析，得到的动态IP情报库。
撞库IP情报库	基于阿里云全网实时检测到的撞库、暴力破解行为攻击源IP进行分析，得到的动态IP情报库。
伪造蜘蛛情报库	识别爬虫程序伪造合法搜索引擎的user-agent（如BaiduSpider）来逃避检测的行为。 **注意** 开启该威胁情报库之前，请确保已经放行合法爬虫白名单，否则可能导致误拦截。更多信息，请参见设置合法爬虫规则。
恶意爬虫情报库	基于阿里云全网实时检测到的爬虫行为攻击源IP进行分析，得出的动态IP情报库。该IP情报有低级、中级、高级三个等级。级别越高，对应的情报库内IP数量越多，相应的误判概率更大。 **说明** 建议您对高级情报库规则中风险等级为高级的规则（误报较多）设置二次校验（即使用滑块验证、JS校验等处置动作），避免误报。 对二次校验不适用的场景（规则风险等级为低级），建议配置低级别的情报库规则。
IDC情报库	相关公有云和IDC机房的IP库，包括：阿里云、腾讯云、美团云、世纪互联、其他。这些IP段经常被爬虫用于部署爬虫程序或用作代理，而不会被正常用户使用。

开启默认规则后，当目标情报库内的来源IP向域名下任意路径发起访问请求时，一律触发**观察**处置，即放行请求同时进行记录。

如果您希望进一步调整默认规则（例如指定要防护的关键路径或者修改处置动作），请参照下一步自定义威胁情报规则。

7. （可选）自定义威胁情报规则。
   i. 定位到要调整的默认规则，单击其操作列下的**编辑**。
   ii. 在**编辑情报**对话框，完成以下规则配置。



参数	说明
防护路径	填写要防护的具体**URL**（例如“/abc”、“/login/abc”，“/”表示所有路径），并选择对应的**匹配方式**。可选值： ■ **精确匹配**：访问地址与防护路径完全匹配时，会命中威胁情报规则。 ■ **前缀匹配**：访问地址与防护路径的前缀相同时，会命中威胁情报规则。 ■ **正则匹配**：访问地址满足防护路径的正则表达式时，会命中威胁情报规则。 单击**新增防护路径**可以添加最多10个路径。
处置动作	指定命中规则后的操作。可选值： ■ **观察**：放行请求并进行记录。 ■ **阻断**：直接阻断访问请求。 ■ **JS验证**：通过JavaScript校验请求数据，验证通过后放行请求。 ■ **滑块**：在客户端跳出滑块验证页面，客户端完成验证后放行请求。 **说明** 滑块验证仅支持同步请求，如有异步请求（如AJAX）防护需求请联系阿里云安全团队。如果不确定您防护的接口能否正常使用滑块验证，建议您先在自定义防护策略（ACL访问控制）中配置针对测试IP和URL的规则来验证和调试。更多信息，请参见设置自定义防护策略。 ■ **严格滑块**：在客户端跳出滑块验证页面，客户端完成验证后放行请求。滑块验证的通过标准更严格。

iii. 单击**确定**。

3.4. 设置数据风控

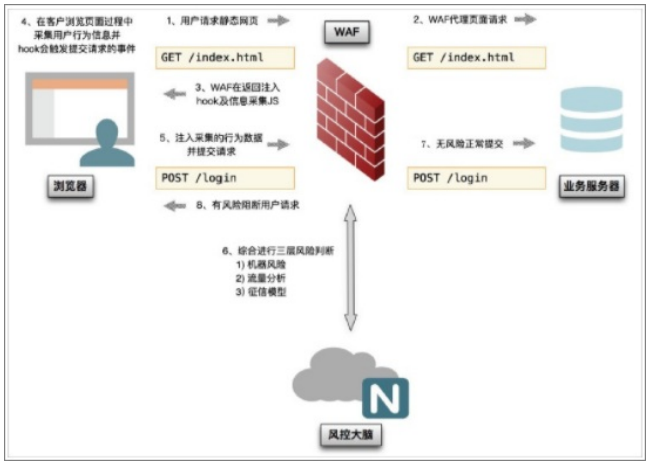
网站接入Web应用防火墙WAF（Web Application Firewall）后，您可以为其开启数据风控功能。数据风控帮助防御网站关键业务（例如注册、登录、活动、论坛）中可能发生的机器爬虫欺诈行为。本文介绍如何设置数据风控的防护策略。

背景信息

数据风控基于阿里云的大数据能力，通过风险决策引擎，结合人机识别技术，防止各类场景的关键业务欺诈行为。您只需将业务接入WAF即可使用数据风控功能，且无需在服务器或客户端进行任何改造。

数据风控支持防护的场景包括但不限于以下内容：垃圾注册、短信验证码滥刷、撞库、暴力破解、恶意抢购、秒杀、薅羊毛、抢红包、机器人抢票、刷票、恶意投票、垃圾消息。

下图描述了数据风控的工作流程。关于接入数据风控的应用场景示例和实际效果，请参见数据风控应用示例。



兼容性说明

数据风控仅适用于网页或H5环境。在某些情况下，可能存在页面中插入的用于安全防护的JS插件与原页面不兼容的问题，导致数据风控的滑块验证功能出现异常。目前，常见的存在不兼容问题的页面包括：

- 访问者可以直接通过URL地址访问的静态页面，例如各种通过HTML直接展示数据的详情页、分享页、网站首页、文档页等，页面跳转方式为直接修改 `location.href` 和使用 `window.open` 、 `<a>` 标签的页面。
- 业务代码重写页面的请求发送方法或自定义请求提交，例如重写表单提交、重写XHR、自定义ajax提交等情况。
- 业务代码中存在hook相关请求提交的内容。

如果您的业务中可能存在不兼容问题，建议您在接入数据风控功能初期，选用预警模式并结合Web应用防火墙的实时日志分析服务进行兼容性和效果测试。更多信息，请参见日志服务概述。

如果出现不兼容的问题，您可以使用人机验证服务配合Web应用防火墙一起实现防护。

关于原生App业务的防护，建议您使用App增强防护SDK方案。更多信息，请参见设置App防护。

前提条件

- 已开通Web应用防火墙实例，且实例满足以下要求：
  - 包年包月实例：实例地域是**中国内地**，且实例开启了**Bot管理**模块。更多信息，请参见开通Web应用防火墙。
  - 按量计费实例：已在**账单与套餐中心**开启**Bot管理**模块下**数据风控**功能。更多信息，请参见账单与套餐中心（按量2.0版本）。
- 已完成网站接入。具体操作，请参见网站接入概述。

> **注意** WAF已上线防爬场景化配置功能，支持您基于实际业务场景对防爬规则进行定制，从而更有针对性地对业务进行爬虫风险防护。如果您有网站防爬的需求，建议您直接使用防爬场景化配置功能。配置防爬场景化规则后，无需再设置数据风控规则，即可实现网页防爬的效果。此外，数据风控功能已不再维护和更新，为您带来的不便，敬请谅解。

操作步骤

1. 登录Web应用防火墙3.0控制台。在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
2. 在左侧导航栏，选择**防护配置 > 网站防护**。
3. 在**网站防护**页面上方，切换到要设置的域名。

4. 单击**Bot管理**页签，定位到**数据风控**区域，完成以下功能配置并单击**前去配置**。

参数	说明
状态	开启或关闭数据风控。开启数据风控后，Web应用防火墙默认将在网站所有（或指定的）页面中插入JS插件用于安全防护，页面响应内容将以非GZIP压缩方式进行传输。即使您的网站配置使用非标端口访问，也无需添加额外配置。 **说明** ○ 您必须先开启数据风控，才能调整防护模式和设置防护规则。 ○ 数据风控开启后，所有网站请求默认都会经过数据风控规则的检测。您可以通过设置Bot管理白名单，让满足条件的请求忽略数据风控规则的检测。更多信息，请参见设置Bot管理白名单。
模式	数据风控的防护模式。可选值： ○ **强拦截**：识别到业务攻击时，网站将被重定向至验证页面进行严格的二次验证。 ○ **拦截**：识别到业务攻击时，网站将被重定向至验证页面进行二次验证。 ○ **告警**：识别到业务攻击时，只记录风险日志、不进行拦截，可通过业务风控报表查看详细风险情况。 **说明** 默认使用预警模式，数据风控不会对任何请求进行拦截，但依然会在静态页面中插入JS脚本分析客户端行为。

5. 添加数据风控防护规则。
   i. 在**数据风控**页面，单击**防护请求**页签，并单击**新增防护请求**。
   ii. 在**新增防护请求**对话框，输入**防护请求URL**。更多信息，请参见什么是防护请求URL。
   iii. 单击**确定**。

   防护请求添加成功后，10分钟左右生效。您可以在防护请求列表中查看新增的防护请求，并根据需要编辑或删除防护请求。

6. （可选）指定JS插入页面。

   由于部分页面前端代码与数据风控的JavaScript脚本可能存在兼容性问题。如果遇到此类问题，建议您通过指定页面插入JS功能仅添加部分页面进行安全防护。

   > **说明** 仅在部分页面插入JS插件时，数据风控将可能无法获取完整的用户访问行为，并对最终的防护效果产生影响。

   i. 在**数据风控**页面，单击**JS插入页面**页签。

   ii. 选中**指定页面插入JS**，并单击**添加页面**。

   > **说明** 最多支持添加20个页面地址。

   iii. 在**添加URL**对话框，输入要插入JS的页面的地址（必须以“/”开头），并单击**确定**。

   成功添加URL后，数据风控将仅在您所添加的URL路径下的页面中插入JS插件。

开启数据风控后，您可以使用Web应用防火墙的日志服务功能查看防护结果。相关操作，请参见查看防护结果。

什么是防护请求URL

防护请求URL是执行业务动作的接口地址，而不是页面本身的URL地址。例如，下图所示注册页面本身的URL地址为 `www.aliyundoc.com/new_user` ，获取验证码按钮对应的业务接口地址是 `www.aliyundoc.com/getsmscode` ，注册按钮对应的业务接口地址是 `www.aliyundoc.com/register.do` 。

这种情况下，您应该为获取验证码按钮的接口地址 `www.aliyundoc.com/getsmscode` 和注册按钮对应的接口地址 `www.aliyundoc.com/register.do` 分别添加防护请求，并设置为防护请求URL，防止验证码的短信接口被刷和垃圾注册风险。如果将注册页面地址 `www.aliyundoc.com/new_user` 设置为防护请求URL，当正常用户访问该页面时也将收到滑块验证提示，影响用户体验。

设置防护请求URL时，请注意以下信息：

- 防护请求URL必须精确到实际请求URL，不支持模糊匹配。

  例如，将 `www.aliyundoc.com/test` 设置为防护请求URL，则数据风控只匹配test路径的访问请求，不会匹配test路径下所有页面的访问请求。

- 数据风控支持对网页目录进行防护。

  例如，您将防护请求URL设置为 `www.aliyundoc.com/book/*` ，即可对 `www.aliyundoc.com/book` 路径下所有页面的请求实现数据风控防护。但是，不建议您为全站配置防护。假如设置 `www.aliyundoc.com/*` 为防护请求URL，将导致用户访问网站首页时也需要通过滑块验证，影响用户体验。

- 直接请求数据风控已防护的URL一定会触发滑块验证。因此，请确保所配置的防护请求URL在正常情况下不会被用户直接请求，即正常用户通常需要经过一系列的前置访问后才会请求该URL地址。
- 直接调用API接口的场景不适合使用数据风控进行防护。由于API调用是直接发起的机器行为，无法通过数据风控的人机识别验证。但是，对于正常用户单击页面中的某按钮调用API接口的情况，可以通过数据风控功能进行防护。

查看防护结果

您可以使用Web应用防火墙的日志服务功能来排查数据风控的监控和拦截情况。

为域名开启日志采集后，您可以在**日志查询**页签，通过**高级搜索**功能下的**数据风控**筛选项，快速查询数据风控的监控和拦截情况。具体操作，请参见查询和分析日志。

数据风控应用示例

阿里云用户小丁在互联网上搭建网站业务，网站域名是 `www.aliyundoc.com` ，普通用户可以通过 `www.aliyundoc.com/register.html` 注册成为网站会员。近来，小丁发现存在黑客通过一些恶意脚步频繁提交注册请求，并注册大量垃圾账户来参与网站的抽奖活动。所提交的请求与正常用户请求相似度很高，且请求频率不高，传统的CC攻击防护功能难以分辨出这些恶意请求。

配置示例

小丁将网站业务接入Web应用防火墙并为 `www.aliyundoc.com` 域名开启数据风控功能。小丁当前最关心的注册业务的请求URL是 `www.aliyundoc.com/register.html` ，因此将该URL设置为防护请求URL。

防护效果

防护配置生效后，数据风控通过在所有页面中插入的JS插件，观察并分析每一个访问 `www.aliyundoc.com` 网站域名（包括首页及其子路径）的用户的各种行为，判断是否存在异常。同时，结合阿里云的大数据信誉库判断访问源IP是否存在风险。

当用户向 `www.aliyundoc.com/register.html` 地址提交注册请求时，Web应用防火墙将基于该用户自开始访问该网站，到提交注册请求间的所有行为和环境征来判断用户是否可疑。例如，如果用户没有任何前置操作直接提交注册请求，则可基本判断该请求为可疑请求。具体说明如下：

- 如果基于之前的行为，数据风控判断该请求来自正常用户，则该用户在注册过程中将无任何感知。
- 当数据风控判断该请求为可疑请求，或者该访问源IP曾有不良记录，将通过滑块验证的方式验证用户身份。只有通过验证的用户，才能继续进行注册。

  如果通过滑块验证方式可疑（例如，使用脚本模仿真人滑动过程等），数据风控将继续通过其他方式再次进行验证，直到验证通过且通过方式可信。如果无法通过验证，数据风控将阻断该请求。

整个过程中，由于数据风控是针对整个网站域名（ `www.aliyundoc.com` ）开启的，数据风控需要对该域名下的所有页面插入JS插件来判断用户行为是否可信。而真正的防护和验证，仅针对 `www.aliyundoc.com/register.html` 注册接口URL生效，只有在提交注册请求时数据风控才会对请求进行干涉。

3.5. App防护

3.5.1. 概述

App防护是Web应用防火墙（WAF）针对原生App端提供的SDK安全解决方案，为您的App提供可信通信、防机器脚本滥刷等安全防护。

App防护能够解决哪些安全问题

App防护集成了阿里巴巴集团多年来对抗黑灰产、羊毛党的经验和技术积累。为App集成App防护SDK后，您的App将获得与天猫、淘宝、支付宝等App端相同的可信通信技术能力，并可共享阿里巴巴集团多年对抗黑灰产、羊毛党所积累的恶意设备指纹库，从根本上解决App端的安全问题。

App防护提供的SDK安全方案帮助您解决以下原生App端的安全问题：

- 恶意注册、撞库、暴力破解
- 针对App的大流量CC攻击
- 短信、验证码接口被刷

- 薅羊毛、抢红包
- 恶意秒杀限时限购商品
- 恶意查票、刷票（例如，机票、酒店等场景）
- 价值资讯爬取（例如，价格、征信、融资、小说等内容）
- 机器批量投票
- 灌水、恶意评论

如何为应用开启App防护

为应用开启App防护的操作流程如下：

1. 开通WAF App防护模块。

   App防护是WAF提供的增值服务，只有开通后才能使用。您可以通过以下方式开通App防护：

   - 未开通WAF：通过开通WAF，选择开启**App防护**模块。相关操作，请参见开通Web应用防火墙。

   - 已开通WAF：
     - 包年包月计费模式下，通过升级WAF，选择开启**App防护**模块。相关操作，请参见续费与升级（包年包月）。
     - 按量计费模式下，通过修改套餐，选择开启**App防护**模块。相关操作，请参见账单与套餐中心（按量2.0版本）。

2. 在Web应用防火墙控制台的**防护配置 > 网站防护**页面，开启**App防护**状态开关，并设置App防护策略，自定义需要防护的接口并根据需要开启版本防护。相关操作，请参见设置App防护。

   开启**App防护**后，您可以单击**获取并复制appkey**，获取SDK认证密钥（即 `appkey` ）。该密钥用于发起SDK初始化请求，需要在集成代码中使用。

3. 联系WAF技术支持人员获取App防护SDK包，并在App中集成SDK。

   关于在App中集中SDK的具体操作，请参见以下文档：

- Android应用集成SDK
- iOS应用集成SDK

> **说明** 集成SDK可能需要1~2人天的工作量。

4. 使用App域名完成网站接入。相关操作，请参见添加域名。
5. 更新App域名的DNS解析，将域名解析到对应的WAF CNAME地址。相关操作，请参见修改域名DNS。
6. 使用集成了SDK的App发送测试请求，并通过响应和日志分析调试错误和异常，直到确认App中已正确集成SDK。
7. 发布正确集成SDK的新版本App。

> **注意** 发布新版本App时，建议您进行强制更新，否则旧版本App依然存在安全风险。

SDK隐私政策

关于App防护提供的SDK服务所涉及的隐私政策，请参见Web应用防火墙App防护SDK隐私政策。

3.5.2. SDK集成指南（新版）

3.5.2.1. Android应用集成SDK

本文介绍了为您的Android应用集成WAF App防护SDK（以下简称SDK）的操作方法。您必须在应用中集成SDK，才能为应用开启App防护。

使用限制

Android应用的API版本必须是16及以上，否则无法正常使用SDK。

前提条件

- 已开通WAF App防护模块且开启了App防护状态开关。

  相关操作，请参见如何为应用开启App防护。
- 已获取Android应用对应的SDK。

  您开通WAF App防护模块后，可以通过钉钉、工单等方式联系WAF售后技术支持人员获取SDK。

  Android应用对应的SDK包含1个**AAR**文件，文件名为*AliTigerTally_X.Y.Z.aar*，其中*X.Y.Z*表示版本号。
- 已获取SDK认证密钥（即 `appkey` ）。

  您在Web应用防火墙控制台的**防护配置 > 网站防护**页面开启**App防护**后，即可单击**获取并复制appkey**，获取SDK认证密钥。该密钥用于发起SDK初始化请求，需要在集成代码中使用。

  > **说明** 每个阿里云账号拥有唯一的 `appkey` （适用于所有接入WAF防护的域名），且Android和iOS应用集成SDK时都使用该 `appkey` 。

认证密钥示例：

```
****OpKLvM6zliu6KopyHIhmneb_****u4ekci2W8i6F9vrgpEezqAzEzj2ANrVUhvAXMwYzgY_****vc51aEQlRovkRoUhRlVsf4IzO9dZp6nN_****Wz8pk2TDLuMo4pVIQvGaxH3vrsnSQiK****
```

背景信息

App防护SDK主要用于对通过App客户端发起的请求进行签名。WAF服务端通过校验App请求签名，识别App业务中的风险、拦截恶意请求，实现App防护的目的。

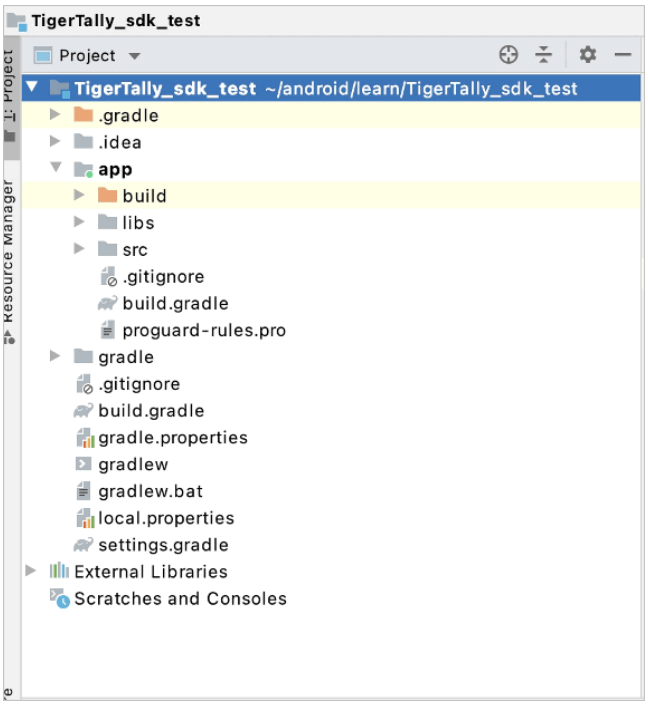
关于App防护提供的SDK所涉及的隐私政策，请参见Web应用防火墙App防护SDK隐私政策。

创建一个测试工程（可选）

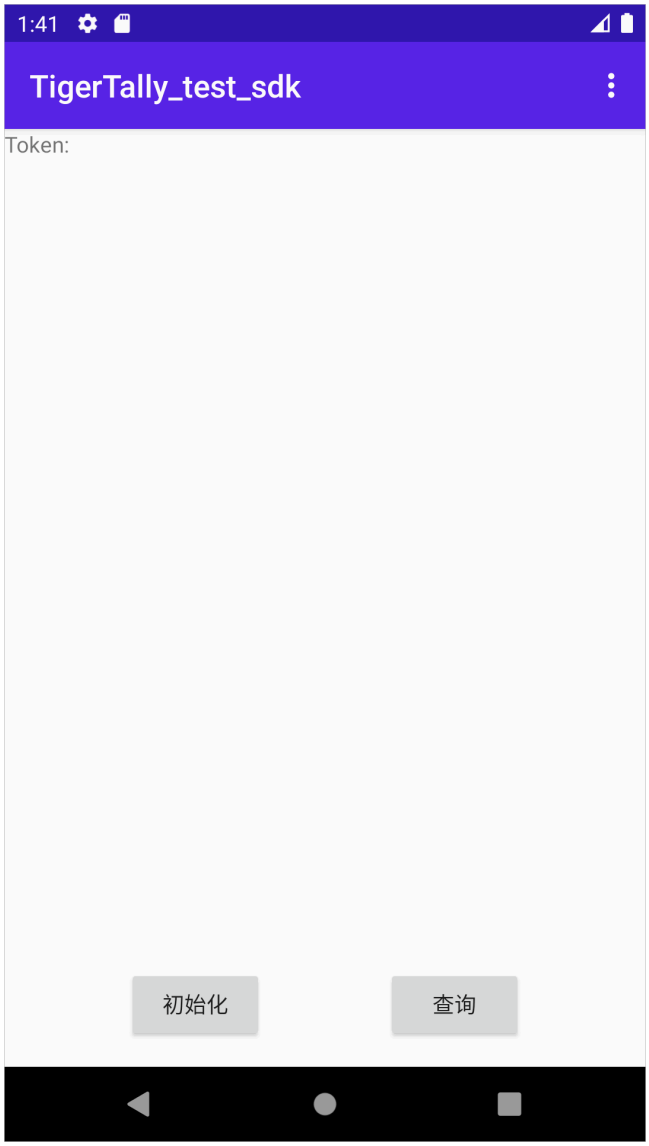
您可以直接在真实的Android工程中集成SDK，或者先创建一个测试工程进行测试，等熟悉操作后，再在真实环境中进行操作。

以Android Studio工具为例，新建一个测试用Android工程，并按照配置向导完成创建。

本文将测试工程命名为*TigerTally_sdk_test*，创建好的工程目录如下图所示。

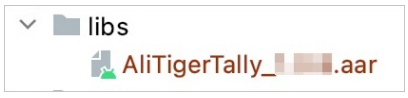


在集成SDK前，请确认测试工程可以正常运行。



操作步骤

1. 使用Android Studio打开App工程，进入文件目录。
2. 引用AAR包。
   i. 将您获取的*AliTigerTally.aar*文件复制到*libs*目录（可以直接拖放进去）。



ii. 打开build.gradle文件，修改以下配置：

- 将*libs*目录添加为查找依赖的源。

```
repositories{
   flatDir {
     dirs 'libs'
   }
}
```

- 添加编译依赖。

> 注意 您需要将以下代码中AliTigerTally文件的版本号（X.Y.Z）替换成您获取的AAR文件的版本号。

```
dependencies {
  compile(name: 'AliTigerTally_X.Y.Z', ext: 'aar')
}
```

iii. 在页面上方的提示信息中，单击Sync Now，将修改的配置同步到项目中。

3. 添加SO引用。

   如果您的项目已经使用过SO，请跳过该步骤；如果项目在此之前未使用过SO，请在build.gradle中添加以下配置：

```
android {
    defaultConfig {
    ndk {
        abiFilters 'arm64-v8a', 'x86', "armeabi-v7a"
        //abiFilters "armeabi-v7a"
      }
    }
}
```

4. 为应用申请以下权限。

权限	是否必须	说明
android.permission.INTERNET	是	用于连接网络。
android.permission.ACCESS_NETWORK_STATE	否	用于获取设备的网络状态。
android.permission.ACCESS_WIFI_STATE	否	用于获取设备的WIFI状态。
android.permission.READ_PHONE_STATE	否	用于读取设备状态和身份。 注意 该权限在Android 6.0及以上需要动态申请。
android.permission.BLUETOOTH	否	用于获取设备的蓝牙权限。

权限	是否必须	说明
android.permission. READ_EXTERNAL_STORAGE	否	用于读取设备的外部存储。 **注意** 该权限在Android 6.0及以上需要动态申请。
android.permission.CHANGE_NETWORK_ STATE	否	用于修改设备的网络状态。

5. 添加集成代码。
   i. 设置用户标识。

   接口定义：

   ```
   int setAccount(String account);
   ```

   功能：设置您业务中自定义的终端用户标识，方便您更灵活地配置WAF防护策略。

   接口参数：<account>，String类型，表示标识一个用户的字符串（建议您使用脱敏后的格式）。

   返回值：int类型，返回是否设置成功，*0*表示成功，*-1*表示失败。

   示例代码：

   ```
   final String account="account";
   TigerTallyAPI.setAccount(account); // 如果当前登录的用户是游客身份，可以跳过这步，直接调用初始化函数。
   ```

ii. SDK初始化。

接口定义：

```
int init(Context context, String appkey, int type);
```

功能：初始化SDK，执行一次初始化采集。一次初始化采集表示采集一次终端设备信息，您可以根据业务的不同，重新调用 `init` 函数进行初始化采集。

初始化采集分为两种模式：采集全量数据、采集除需授权字段外的数据（不采集涉及终端设备用户隐私的字段，包括：imei、imsi、simSerial、wifiMac、wifiList、bluetoothMac）。

> **说明** 建议您在终端用户同意App的隐私政策前，采集除需授权字段外的数据；在终端用户同意App的隐私政策后，再采集全量数据。采集全量数据有利于更好地识别风险。

接口参数：

- <context>：Context类型，传入您应用的上下文。
- <appkey>：String类型，设置为您的SDK认证密钥。
- <type>：CollectType类型，设置采集模式。取值：
  - *DEFAULT*：表示采集全量数据。
  - *NO_GRANTED*：表示采集除需授权字段外的数据。

返回值：int类型，返回初始化结果，*0*表示成功，*-1*表示失败。

示例代码：

```
final String appkey="your_appkey";
// 采集全量数据。
int ret = TigerTallyAPI.init(this.getApplicationContext(), appkey, TigerTallyAPI.Co
llectType.DEFAULT);
// 采集除需授权字段外的数据。
int ret = TigerTallyAPI.init(this.getApplicationContext(), appkey, TigerTallyAPI.Co
llectType.NOT_GRANTED);
Log.d("AliSDK", "ret:" + ret);
```

iii. 签名请求数据。

接口定义：

```
String vmpSign(int signType, byte[] input);
```

功能：对输入的数据进行签名，并且返回签名串。

接口参数：

- <signType>：int类型，取值固定为1，表示默认的签名算法。
- <input>：byte[]类型，表示待签名的数据。

  待签名数据一般是整个请求体（RequestBody）。如果请求体为空（例如，POST请求的Body为空或者使用了GET请求），则设置成空对象（`null`）或者空字符串的Bytes值（例如，`"".getBytes("UTF-8")`）。

返回值：String类型，返回签名串。

示例代码：

> **说明** 示例代码中将签名串定义为*wToken*。

```
String request_body = "i am the request body, encrypted or not!";
String wToken = null;
try {
    wToken = TigerTallyAPI.vmpSign(1, request_body.getBytes("UTF-8"));
} catch (UnsupportedEncodingException e) {
    e.printStackTrace();
}
Log.d("AliSDK", "wToken:" + wToken);
```

iv. 将签名串添加到HTTP协议头。

例如，如果您的项目使用`HttpURLConnection`，则可以将签名串（*wToken*）字段的内容添加到`HttpURLConnection`类的对象中。

示例代码：

```
String request_body = "i am the request body, encrypted or not!";
new Thread(new Runnable() {
    @Override
    public void run() {
        try {
            URL url = new URL("https://www.aliyundoc.com");
            HttpURLConnection conn = (HttpURLConnection) url.openConnection();
            conn.setReadTimeout(5000);
            conn.setRequestMethod("POST");
            // set wToken info to header
            conn.setRequestProperty("wToken", wToken);
            OutputStream os = conn.getOutputStream();
            // set request body info
            byte[] requestBody = request_body.getBytes("UTF-8");
            os.write(requestBody);
            os.flush();
            os.close();
            int code = conn.getResponseCode();
            Log.d("respCode", Integer.toString(code));
        } catch (MalformedURLException e) {
            e.printStackTrace();
        } catch (UnsupportedEncodingException e) {
            e.printStackTrace();
        } catch (ProtocolException e) {
            e.printStackTrace();
        } catch (IOException e) {
            e.printStackTrace();
        }
    };
    }).start();
```

v. 将修改好HTTP协议头的数据发送到应用服务器。

WAF服务端获得应用服务器收到的请求后，通过解析签名串（*wToken*）进行风险识别、拦截恶意请求，然后将合法请求转发回源站。

接口混淆配置

如果您使用ProGuard进行代码混淆，则可以使用 `-keep` 选项对SDK的接口函数进行设置，保护SDK接口函数不被移除混淆。

示例代码：

```
-keep class com.aliyun.TigerTally.* {*;}
```

3.5.2.2. iOS应用集成SDK

本文介绍了为您的iOS应用集成WAF App防护SDK（以下简称SDK）的操作方法。您必须在应用中集成SDK，才能为应用开启App防护。

使用限制

iOS应用对应的iOS版本是9.0及以上，否则不支持集成App防护SDK。

前提条件

- 已开通WAF App防护模块且开启了App防护状态开关。

  相关操作，请参见如何为应用开启App防护。

- 已获取iOS应用对应的SDK。

  您开通WAF App防护模块后，可以通过钉钉、工单等方式联系WAF售后技术支持人员获取SDK。

  iOS应用对应的SDK分为广告标识符（Identifier for Advertising，简称IDFA）版本和非IDFA版本，对应的SDK文件分别是：

  - *AliTigerTally_IDFA.framework*
  - *AliTigerTally_NOIDFA.framework*

  如果您的iOS项目中使用了IDFA，推荐您集成AliTigerTally_IDFA版本SDK，否则请使用AliTigerTally_NOIDFA版本SDK。

- 已获取SDK认证密钥（即 `appkey` ）。

  您在Web应用防火墙控制台的**防护配置 > 网站防护**页面开启**App防护**后，即可单击**获取并复制appkey**，获取SDK认证密钥。该密钥用于发起SDK初始化请求，需要在集成代码中使用。

  > **说明** 每个阿里云账号拥有唯一的 `appkey` （适用于所有接入WAF防护的域名），且Android和iOS应用集成SDK时都使用该 `appkey` 。

  认证密钥示例：

  ```
  ****OpKLvM6zliu6KopyHIhmneb_****u4ekci2W8i6F9vrgpEezqAzEzj2ANrVUhvAXMwYzgY_****vc51aEQlRo
  vkRoUhRlVsf4IzO9dZp6nN_****Wz8pk2TDLuMo4pVIQvGaxH3vrsnSQiK****
  ```

背景信息

App防护SDK主要用于对通过App客户端发起的请求进行签名。WAF服务端通过校验App请求签名，识别App业务中的风险、拦截恶意请求，实现App防护的目的。

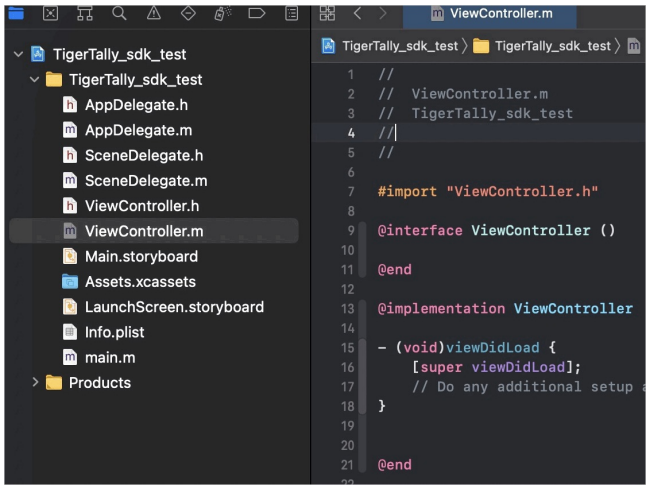
关于App防护提供的SDK所涉及的隐私政策，请参见Web应用防火墙App防护SDK隐私政策。

创建一个测试工程（可选）

您可以直接在真实的iOS工程中集成SDK，或者先创建一个测试工程进行测试，等熟悉操作后，再在真实环境中进行操作。

以Xcode环境为例，新建一个iOS工程，并按照配置向导完成创建。

本文将测试工程命名为*TigerTally_sdk_test*，创建好的工程目录如下图所示。



操作步骤

1. 使用Xcode打开App工程，进入文件目录。
2. 将SDK复制到项目中。
3. 在项目中添加以下依赖库。

依赖库	非IDFA版本是否需要	IDFA版本是否需要
libc++.tbd	是	是
CoreTelephony.framework	是	是
libresolv.9.tbd	是	是
AdSupport.framework	否	是

4. 打开编译选项设置（Build Settings），在Other Linker Flags选项中添加-ObjC。
5. 添加集成代码。

i. 在需要集成SDK的源文件中，添加头文件。

示例代码：

- Objective-C语言

```
// 非IDFA版本。
#import <AliTigerTally_NOIDFA/AliTigerTally.h>
// IDFA版本。
#import <AliTigerTally_IDFA/AliTigerTally.h>
```

- Swift语言

```
// 创建头文件。
#ifndef TigerTally_sdk_Swift_h
#define TigerTally_sdk_Swift_h
// 非IDFA版本。
#import <AliTigerTally_NOIDFA/AliTigerTally.h>
// IDFA版本。
#import <AliTigerTally_IDFA/AliTigerTally.h>
#endif /* TigerTally_sdk_Swift_h */
```

您需要在编译选项设置（Build Settings）的Objective-C Bridging Header选项中，添加已创建的头文件。

ii. 设置用户标识。

接口定义：

```
-(void)setAccount:(NSString*)account
```

功能：设置您业务中自定义的终端用户标识，方便您更灵活地配置WAF防护策略。

接口参数：<account>，NSString*类型，表示标识一个用户的字符串（建议您使用脱敏后的格式）。

返回值：无。

示例代码：

- Objective-C语言

```
// testAccount表示用户标识字符串示例。
// 如果当前登录的用户是游客身份，可以跳过这步，直接调用初始化函数。
[[AliTigerTally sharedInstance] setAccount:@"testAccount"];
```

- Swift语言

```
// testAccount表示用户标识字符串示例。
// 如果当前登录的用户是游客身份，可以跳过这步，直接调用初始化函数。
AliTigerTally.sharedInstance().setAccount("testAccount")
```

iii. 添加初始化函数。

接口定义：

```
-(bool)initialize:(NSString*)appKey
```

功能：初始化SDK，执行一次初始化采集。一次初始化采集表示采集一次终端设备信息，您可以根据业务的不同，重新调用initialize函数进行初始化采集。

接口参数：<appKey>，NSString*类型，设置成您的SDK认证密钥。

返回值：bool类型，返回是否初始化成功，true表示成功，false表示失败。

示例代码：

- Objective-C语言

```
NSString *appKey=@"****OpKLvM6zliu6KopyHIhmneb_****u4ekci2W8i6F9vrgpEezqAzEzj2ANrVUhvAXMwYzgY_****vc51aEQlRovkRoUhRlVsf4IzO9dZp6nN_****Wz8pk2TDLuMo4pVIQvGaxH3vrsnSQiK****";
if([[AliTigerTally sharedInstance]initialize:appKey]){
    NSLog(@"初始化成功");
 }else{
     NSLog(@"初始化失败");
}
```

- Swift语言

```
let binit = AliTigerTally.sharedInstance().initialize("****OpKLvM6zliu6KopyHIhmneb_****u4ekci2W8i6F9vrgpEezqAzEzj2ANrVUhvAXMwYzgY_****vc51aEQlRovkRoUhRlVsf4IzO9dZp6nN_****Wz8pk2TDLuMo4pVIQvGaxH3vrsnSQiK****")
if(binit){
    NSLog("初始化成功");
}else{
    NSLog("初始化失败");
}
```

iv. 签名请求数据。

接口定义：

```
-(NSString*)vmpSign:(NSData*)inputBody
```

功能：对输入的数据进行签名，并且返回签名串。

接口参数：<inputBody>，NSData*类型，表示待签名的数据体。

返回值：

- 正常返回结果：NSString* 类型，返回签名串。

- 异常返回结果：

返回结果	说明	建议操作
`you must call initialize`	表示您没有调用 `initialize` 函数。	请先调用 `initialize` 函数初始化SDK，然后再调用 `vmpSign` 函数。
`you must input body`	表示您没有设置待签名的数据体。	您在调用 `vmpSign` 函数时，必须设置要签名的数据体（<inputBody>）。
`NULL`	表示初始化未完成，签名失败。	建议您重新调用 `vmpSign` 函数。 如果该问题反复出现，请通过钉钉、工单等方式联系WAF售后技术支持人员获取帮助。

示例代码：

> **说明** 示例代码中将签名串定义为*wToken*。

- Objective-C语言

```
if(![[AliTigerTally sharedInstance]initialize:@"****OpKLvM6zliu6KopyHIhmneb_****u4ekci2W8i6F9vrgpEezqAzEzj2ANrVUhvAXMwYzgY_****vc51aEQlRovkRoUhRlVsf4IzO9dZp6nN_******Wz8pk2TDLuMo4pVIQvGaxH3vrsnSQiK****"])
{
        NSLog(@"初始化失败");
        return;
}
NSString *signBody =@"hello";
NSString *wToken= [[AliTigerTally sharedInstance] vmpSign:[signBody dataUsingEncoding:NSUTF8StringEncoding]];
NSLog(@"wToken== %@",wToken);
```

- Swift语言

```
if(!AliTigerTally.sharedInstance().initialize("****OpKLvM6zliu6KopyHIhmneb_****u4ekci2W8i6F9vrgpEezqAzEzj2ANrVUhvAXMwYzgY_****vc51aEQlRovkRoUhRlVsf4IzO9dZp6nN_****Wz8pk2TDLuMo4pVIQvGaxH3vrsnSQiK****")){
    NSLog("初始化失败");
   return
}
let signBody = "hello"
var token = AliTigerTally.sharedInstance().vmpSign(signData)
NSLog(token);
```

v. 将签名串添加到协议头，并发送数据到服务器。

在业务关键事件（例如，客户端登录请求事件）中，将签名串提交到应用服务器。WAF服务端在获取应用服务器收到的请求后，通过解析签名串（*wToken*）进行风险识别、拦截恶意请求，然后将合法请求转发回源站。

示例代码：

- Objective-C语言

```
NSURL * url = [NSURL URLWithString:@"https://xxxxxx/test?id=123"];
NSMutableURLRequest *request=[NSMutableURLRequest requestWithURL:url cachePolicy:
NSURLRequestUseProtocolCachePolicy timeoutInterval:10];
[request setValue: wToken forHTTPHeaderField: @"wToken"];
request.HTTPMethod=@"post";
request.HTTPBody=[signBody dataUsingEncoding:NSUTF8StringEncoding];
NSURLSessionDataTask *dataTask = [[NSURLSession sharedSession] dataTaskWithReques
t:request completionHandler:^(NSData * _Nullable data, NSURLResponse * _Nullable
response, NSError * _Nullable error) {
    if(error){
        NSLog(@"发送失败%@", error);
    }else
    {
        NSLog(@"发送成功");
    }
}];
[dataTask resume];
```

- Swift语言

```
guard let url = URL(string: "https://xxxxxx/test?id=123") else { return }
var request = URLRequest(url: url)
request.httpMethod = "POST"
request.addValue(token, forHTTPHeaderField: "wToken")
let session = URLSession.shared
session.dataTask(with: request) { (data, response, error) in
    if let data = data {
        do {
            print("OK")
        } catch {
            print("ERROR")
            print(error)
        }
    }
}.resume()
}
```

3.5.3. SDK集成指南（旧版）

3.5.3.1. 为Android应用集成SDK

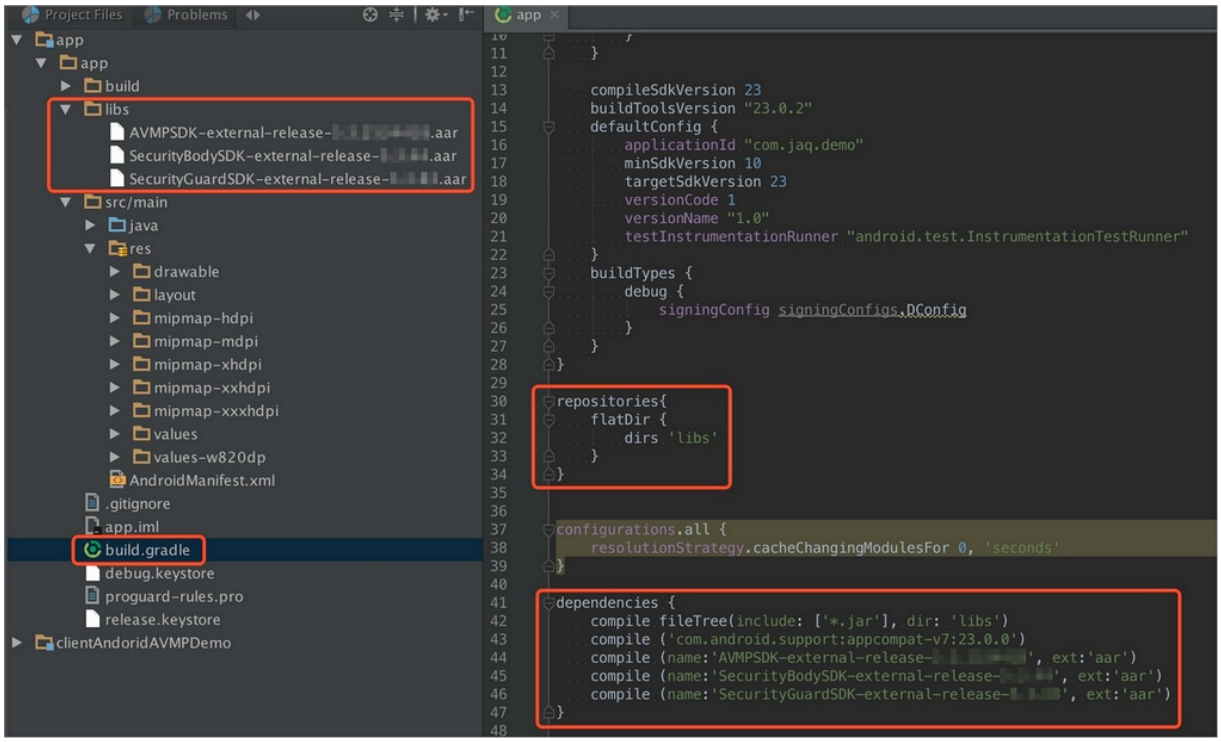
参考以下SDK集成说明为您的Android应用集成爬虫防护SDK。

Android SDK文件

联系阿里云技术支持人员获取对应的SDK包后，将其解压至本地。下表描述了解压获得的*sdk-Android*文件夹中包含的文件。

文件名	说明
SecurityGuardSDK-xxx.aar	主框架SDK文件
AVMPSDK-xxx.aar	虚拟机引擎插件
SecurityBodySDK-xxx.aar	人机识别插件
yw_1222_0335_mwua.jpg	虚拟机引擎配置文件

配置Android工程



1. 在Android Studio中导入解压SDK获得的.aar文件。将sdk-Android文件夹中所有.aar文件复制到Android应用工程的*libs*目录中。

   > **说明** 如果当前工程中不存在*libs*目录，请在指定路径下手动创建*libs*文件夹。

2. 编辑配置信息。打开该Module的*build.gradle*文件，完成以下配置修改。
   - 将*libs*目录添加为查找依赖的源。

     ```
     repositories{
        flatDir {
          dirs 'libs'
        }
     }
     ```

   - 添加编译依赖。

> **说明** .aar文件的版本号可能有所不同，以您下载解压得到的文件名为准。

```
dependencies {
  compile fileTree(include: ['*.jar'], dir: 'libs')
  compile ('com.android.support:appcompat-v7:23.0.0')
  compile (name:'AVMPSDK-external-release-xxx', ext:'aar')
  compile (name:'SecurityBodySDK-external-release-xxx', ext:'aar')
  compile (name:'SecurityGuardSDK-external-release-xxx', ext:'aar')
}
```

3. 将解压SDK获得的.jpg配置文件导入*drawable*目录。将*sdk-Android*文件夹中的*yw_1222_0335_mwua.jpg*配置文件复制到Android应用工程的*drawable*目录中。

   > **说明** 如果当前工程中不存在*drawable*目录，请在指定路径下手动创建*drawable*文件夹。

4. 过滤ABI（删除多余架构SO）。爬虫防护SDK目前仅支持armeabi、armeabi-v7a、arm64-v8a架构的SO。

   > **警告** 您必须对最终导出的ABI进行过滤，否则可能导致应用崩溃。

   i. 在Android应用工程的*lib*目录中，删除*armeabi*、*armeabi-v7a*、*arm64-v8a*文件夹以外所有其他CPU架构的文件夹，包括*x86*、*x86_64*、*mips*、*mips64*等，只保留*armeabi*、*armeabi-v7a*、*arm64-v8a*文件夹。

   ii. 参考以下代码示例，在应用工程的*build.gradle*配置文件中增加过滤规则，被abiFilters指定的架构将会被包含在APK文件中。

   > **说明** 本代码示例中仅指定了armeabi架构，您可以根据实际情况指定或兼容armeabi-v7a、arm64-v8a架构。

   ```
   defaultConfig{
     applicationId "com.xx.yy"
     minSdkVersion xx
     targetSdkVersion xx
     versionCode xx
     versionName "x.x.x"
     ndk {
       abiFilters "armeabi"
       // abiFilters "armeabi-v7a"
       // abiFilters "arm64-v8a"
     }
   }
   ```

   > **说明** 只保留armeabi架构的SO，不会影响应用的兼容性，还能大幅减小应用的体积。

5. 添加应用权限。
   - 如果是Android Studio项目，并且使用了aar方式进行集成，由于在.aar文件中已经声明了相关权限，因此不需要在项目中额外配置权限。
   - 如果是Eclipse项目，您需要在*AndroidMenifest.xml*文件中添加以下权限配置：

```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" />
```

6. 添加ProGuard配置。

> **说明** 如果您使用了Proguard进行混淆，则需要添加ProGuard配置。ProGuard的配置根据集成方式的不同，分为Eclipse和Android Studio两种情况。

- Android Studio

  如果在*build.gradle*中配置了proguardFiles，并且开启了minifyEnabled，则表明使用了*proguard-rules.pro*配置文件进行混淆。

```
buildTypes {
    release {
        minifyEnabled true
        proguardFiles getDefaultProguardFile('proguard-android.txt'), 'proguard-rules.pro'
    }
}
```

- Eclipse

  如果在*project.properties*中指定了proguard配置，例如在*project.properties*中存在`proguard.config=proguard.cfg`语句，则表明使用了proguard进行混淆。

> **说明** 混淆配置在*proguard.cfg*文件中。

添加keep规则

为了保证一些需要的类不被混淆，需要在proguard的配置文件中添加以下规则：

```
-keep class com.taobao.securityjni.**{*;}
-keep class com.taobao.wireless.security.**{*;}
-keep class com.ut.secbody.**{*;}
-keep class com.taobao.dp.**{*;}
-keep class com.alibaba.wireless.security.**{*;}
```

调用SDK接口

步骤1：导入包

```
import com.alibaba.wireless.security.jaq.JAQException;
import com.alibaba.wireless.security.jaq.avmp.IJAQAVMPSignComponent;
import com.alibaba.wireless.security.open.SecurityGuardManager;
import com.alibaba.wireless.security.open.avmp.IAVMPGenericComponent;
```

步骤2：初始化

接口定义：`boolean initialize();`

功能：初始化SDK。

接口参数：无。

返回值：Boolean类型。初始化成功返回true，失败返回false。

示例代码

```
IJAQAVMPSignComponent jaqVMPComp = SecurityGuardManager.getInstance(getApplicationContext()
).getInterface(IJAQAVMPSignComponent.class);
boolean result = jaqVMPComp.initialize();
```

步骤3：签名请求数据

接口定义：`byte[] avmpSign(int signType, byte[] input);`

功能：使用avmp技术对input的数据进行签名处理，并且返回签名串。

接口参数

名称	类型	是否必须	描述
signType	int	是	签名使用的算法。目前是固定值，填写 `3` 。
input	byte[]	否	待签名的数据，一般是整个请求体（request body）。 **说明** 如果请求体为空（例如POST请求的body为空、或者GET请求），则填写空对象null或空字符串的Bytes值（例如，"".getBytes("UTF-8"))。

返回值：byte[]类型，返回签名串。

示例代码：客户端向服务器端发送数据时，需要调用avmpSign接口对整个body数据进行签名处理，所得到的签名串就是wToken。

```
int VMP_SIGN_WITH_GENERAL_WUA2 = 3;
String request_body = "i am the request body, encrypted or not!";
byte[] result = jaqVMPComp.avmpSign(VMP_SIGN_WITH_GENERAL_WUA2, request_body.getBytes("UTF-8"));
String wToken = new String(result, "UTF-8");
Log.d("wToken", wToken);
```

步骤4：将wToken放进协议头

在HttpURLConnection类的对象中添加wToken字段的内容。

示例代码

```
String request_body = "i am the request body, encrypted or not!";
URL url = new URL("http://www.aliyundoc.com");
HttpURLConnection conn = (HttpURLConnection) url.openConnection();
conn.setRequestMethod("POST");
// set wToken info to header
conn.setRequestProperty("wToken", wToken);
OutputStream os = conn.getOutputStream();
// set request body info
byte[] requestBody = request_body.getBytes("UTF-8");
os.write(requestBody);
os.flush();
os.close();
```

步骤5：发送数据到服务器

将修改好协议头的数据发送到App自有服务器，中间会由Anti-Bot截获，并通过解析wToken进行风险识别。

警告 被签名的请求体应该与客户端实际发送的请求体完全一致。完全一致的含义包括请求体中字符串的编码格式、空格、特殊字符以及参数的顺序等均一致，否则将导致签名验证失败。

错误码

上述initialize和avmpSign接口的调用过程中可能出现异常。如果生成签名串异常或失败，请在Log中搜索与 `SecException` 相关的信息。

下表描述了常见错误码及含义。

错误码	含义
1901	参数不正确，请检查输入的参数。
1902	图片文件有问题。一般是获取图片文件时的APK签名和当前程序的APK签名不一致。请使用当前程序的APK重新生成图片。
1903	图片文件格式有问题。
1904	请升级新版本图片。AVMP签名功能仅支持V5图片。

错误码	含义
1905	没有找到图片文件。请确保图片文件在*res\drawable*目录下，与AVMP相关的图片为*yw_1222_0335_mwua.jpg*。
1906	图片中缺少AVMP签名对应的byteCode。请检查使用的图片是否正确。
1907	初始化AVMP失败，请重试。
1910	非法的avmpInstance实例。可能由于以下原因导致： • AVMPInstance被destroy后，调用InvokeAVMP。 • 图片byteCode版本与SDK不匹配。
1911	加密图片的byteCode没有相应导出的函数。
1912	AVMP调用失败。请联系我们。
1913	AVMPInstance被destroy后，调用InvokeAVMP出现该错误。
1915	AVMP调用内存不足，请重试。
1999	未知错误，请重试。

确认集成效果

您可以参考以下步骤，确认您的应用已正确集成了爬虫防护SDK。

1. 将打包生成的APK文件通过修改扩展名的方式转换成ZIP压缩文件，并将该压缩文件解压至本地。
2. 定位到工程的*lib*目录，确保文件夹中只存在*armeabi*、*armeabi-v7a*、*arm64-v8a*文件夹。

   > **说明** 如果存在其他架构的文件夹，请参见配置Android工程，移除其他架构的文件夹。

3. 定位到工程的*res/drawable*目录，确认存在*yw_1222_0335_mwua.jpg*文件，且文件大小不为0。
4. 通过打印日志，确保调用avmpSign接口后能生成正确的签名信息。

   > **说明** 如果签名信息未生成，请参见错误码信息进行排查。

常见问题

为什么指定shrinkResources后，密钥图片被错误地优化？

在Android Studio中，如果指定shrinkResources为true，在工程编译时可能对未在代码中引用的资源文件进行优化。该操作可能导致爬虫防护SDK中的.jpg文件无法正常工作。如果打包后得到APK中，*yw_1222_0335.jpg*配置文件的大小为0KB，则表明该图片文件已被优化。

解决方法

1. 在工程的*res*目录中新建*raw*目录，并在raw目录中创建*keep.xml*文件。
2. 在*keep.xml*文件中，添加以下内容。

```
<?xml version="1.0" encoding="utf-8"?>
<resources xmlns:tools="http://schemas.android.com/tools"
tools:keep="@drawable/yw_1222_0335.jpg,@drawable/yw_1222_0335_mwua.jpg" />
```

3. 添加完成后，重新编译工程APK即可。

3.5.3.2. 为iOS应用集成SDK

参考以下SDK集成说明为您的iOS应用集成爬虫防护SDK。

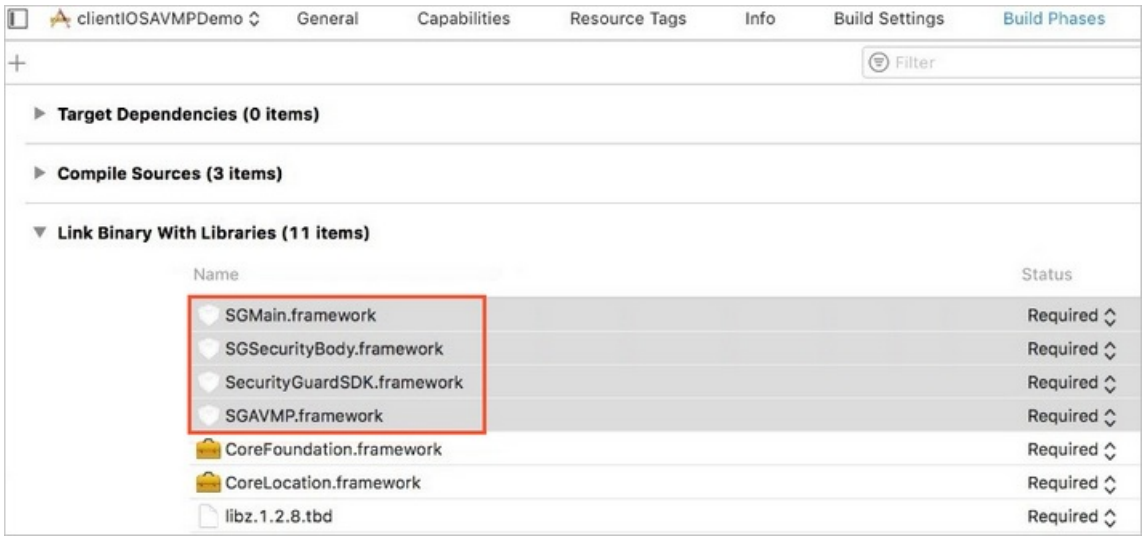
iOS SDK文件

联系阿里云技术支持人员获取对应的SDK包后，将其解压至本地。下表描述了解压获得的*sdk-iOS*文件夹中包含的文件。

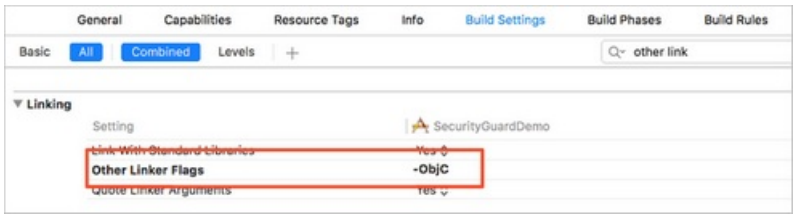
文件名	说明
SGMain.framework	主框架SDK文件
SecurityGuardSDK.framework	基础安全插件
SGSecurityBody.framework	人机识别插件
SGAVMP.framework	虚拟机插件
yw_1222_0335_mwua.jpg	配置文件

配置iOS工程

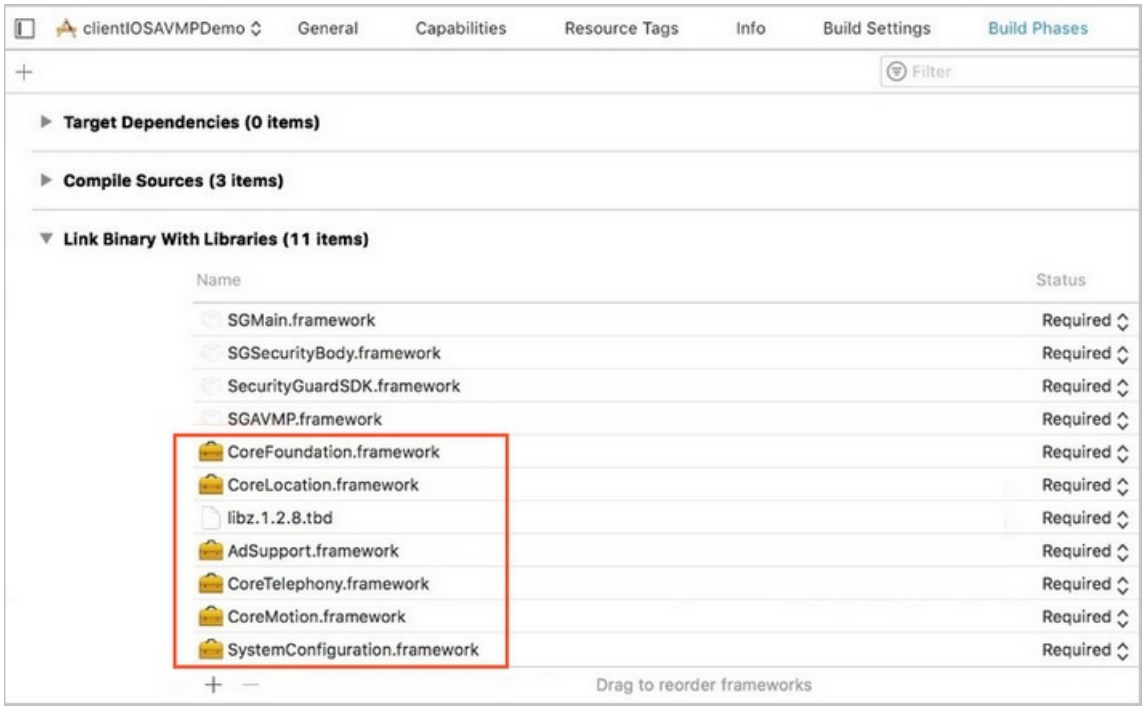
1. 引用SDK依赖文件。在iOS工程的依赖库中（**Build Phases**页签下的**Link Binary With Libraries**菜单）引入解压SDK包获得的四个.framework文件：
   - *SGMain.framework*
   - *SecurityGuardSDK.framework*
   - *SGSecurityBody.framework*
   - *SGAVMP.framework*



2. 添加链接选项。在Build Settings页签下，将Linking > Other Linker Flags设置为-ObjC。



3. 引入系统依赖文件。在iOS工程的依赖库中引入以下文件：
   - *CoreFoundation.framework*
   - *CoreLocation.framework*
   - *AdSupport.framework*
   - *CoreTelephony.framework*
   - *CoreMotion.framework*
   - *SystemConfiguration.framework*



4. 引入配置文件。将SDK包中的*yw_1222_0335_mwua.jpg*配置文件添加到*mainbundle*目录。

> 注意 在应用集成多个target的情况下，请确认将 `yw_1222_0335_mwua.jpg` 配置文件添加到正确的Target Membership中。

调用SDK接口

步骤1：初始化SDK

接口定义： `+ (BOOL) initialize;`

功能：初始化SDK。

接口参数：无。

返回值：BOOL类型。初始化成功返回YES，失败返回NO。

调用方式：`[JAQAVMPSignature initialize];`

示例代码

```
static BOOL avmpInit = NO;
- (BOOL) initAVMP{
  @synchronized(self) { // just initialize once
    if(avmpInit == YES){
      return YES;
    }
    avmpInit = [JAQAVMPSignature initialize];
    return avmpInit;
  }
}
```

步骤2：签名请求数据

接口定义：`+ (NSData*) avmpSign: (NSInteger) signType input: (NSData*) input;`

功能：使用avmp技术对input的数据进行签名处理，并返回签名串。

警告 被签名的请求体应该与客户端实际发送的请求体完全一致。完全一致的含义包括请求体中字符串的编码格式、空格、特殊字符以及参数的顺序等均一致，否则将导致签名验证失败。

接口参数

名称	类型	是否必须	描述
signType	NSInteger	是	签名使用的算法。目前是固定值，填写`3`。
input	NSData*	否	待签名的数据，一般是整个请求体（request body）。 **说明** 如果请求体为空（例如POST请求的body为空、或者GET请求），则填写空对象null或空字符串的Bytes值。

返回值：NSData*类型，返回签名串。

调用方式：`[JAQAVMPSignature avmpSign: 3 input: request_body];`

示例代码

说明 客户端向服务器端发送数据时，需要调用avmpSign接口对整个body数据进行签名处理，所得到的签名串就是wToken。

```
# define VMP_SIGN_WITH_GENERAL_WUA2 (3)
- (NSString*) avmpSign{
  @synchronized(self) {
    NSString* request_body = @"i am the request body, encrypted or not!";
    if(![self initAVMP]){
      [self toast:@"Error: init failed"];
        return nil;
    }
    NSString* wToken = nil;
    NSData* data = [request_body dataUsingEncoding:NSUTF8StringEncoding];
    NSData* sign = [JAQAVMPSignature avmpSign: VMP_SIGN_WITH_GENERAL_WUA2 input:data];
    if(sign == nil || sign.length <= 0){
      return nil;
    }else{
      wToken = [[NSString alloc] initWithData:sign encoding: NSUTF8StringEncoding];
      return wToken;
    }
  }
}
```

如果请求体为空，仍需要调用avmpSign接口生成wToken，第二个参数直接传入空值即可。示例如下：

```
NSData* sign = [JAQAVMPSignature avmpSign: VMP_SIGN_WITH_GENERAL_WUA2 input:nil];
```

步骤3：将wToken放进协议头

示例代码

```
#define VMP_SIGN_WITH_GENERAL_WUA2 (3)
-(void)setHeader
{ NSString* request_body = @"i am the request body, encrypted or not!";
  NSData* body_data = [request_body dataUsingEncoding:NSUTF8StringEncoding];
  NSString* wToken = nil;
  NSData* sign = [JAQAVMPSignature avmpSign: VMP_SIGN_WITH_GENERAL_WUA2 input:body_data];
  wToken = [[NSString alloc] initWithData:sign encoding: NSUTF8StringEncoding];
  NSString *strUrl = [NSString stringWithFormat:@"http://www.aliyundoc.com/login"];
  NSURL *url = [NSURL URLWithString:strUrl];
  NSMutableURLRequest *request =
    [[NSMutableURLRequest alloc]initWithURL:url cachePolicy:NSURLRequestReloadIgnoringCache
Data timeoutInterval:20];
  [request setHTTPMethod:@"POST"];
  // set request body info
  [request setHTTPBody:body_data];
  // set wToken info to header
  [request setValue:wToken forHTTPHeaderField:@"wToken"];
  NSURLConnection *mConn = [[NSURLConnection alloc]initWithRequest:request delegate:self st
artImmediately:true];
  [mConn start];
  // ...
}
```

步骤4：发送数据到服务器

将修改好协议头的数据发送到云盾，通过解析wToken进行风险识别、拦截恶意请求，然后将合法请求转发回源站。

错误码

上述initialize和avmpSign接口的调用过程中可能出现异常。如果生成签名串异常或失败，请在console中搜索与SG Error相关的错误码信息。

下表描述了常见错误码及含义。

错误码	含义
1901	参数不正确，请检查输入的参数。
1902	图片文件错误。可能是由于BundleID不匹配导致。
1903	图片文件格式有问题。
1904	请升级新版本图片。AVMP签名功能仅支持v5图片。
1905	无法找到图片文件。请确保图片文件yw_1222_0335_mwua.jpg已正确添加在工程中。
1906	图片中缺少AVMP签名对应的byteCode。请检查使用的图片是否正确。
1907	初始化AVMP失败，请重试。

错误码	含义
1910	非法的avmpInstance实例。可能由于以下原因导致： • AVMPInstance被destroy后，调用InvokeAVMP。 • 图片byteCode版本与SDK不匹配。
1911	加密图片的byteCode没有相应导出的函数。
1912	AVMP调用失败，请联系我们。
1913	AVMPInstance被destroy后，调用InvokeAVMP时出现该错误。
1915	AVMP调用内存不足，请重试。
1999	未知错误，请重试。

3.5.4. 设置App防护

App防护专门针对原生App端，提供可信通信、防机器脚本滥刷等安全防护，可以有效识别代理、模拟器、非法签名的请求。本文介绍了在应用端集成App防护SDK后，如何在Web应用防火墙控制台设置App防护的防护路径和版本防护功能，以及如何开启App防护。

前提条件

- 已开通Web应用防火墙实例，且实例满足以下要求：
  - 包年包月实例：已开启**App防护**模块。更多信息，请参见开通Web应用防火墙。
  - 按量计费实例：已在**账单与套餐中心**开启**Bot管理**模块下**App防护**功能。更多信息，请参见账单与套餐中心（按量2.0版本）。
- 已在App中集成Web应用防火墙的App防护SDK。更多信息，请参见概述。

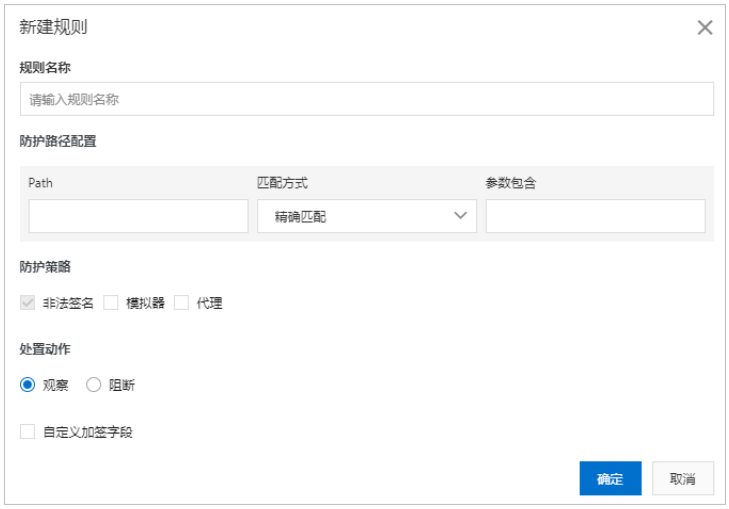
操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**Bot管理**页签，定位到**App防护**，单击**前去配置**。

> **说明** App防护开启后，所有业务请求默认都会经过App防护规则的检测。您可以通过设置Bot管理白名单，让满足条件的请求忽略App防护规则的检测。更多信息，请参见设置Bot管理白名单。

6. 设置路径防护规则。
   i. 在**App防护**页面，定位到**路径防护**区域，单击**新建规则**。
   ii. 在**新建规则**对话框，完成以下规则配置。



> **说明** 建议您在测试阶段设置全路径防护（Path设置为 `/`，**匹配方式**选择**前缀匹配**），并将**处置动作**设置为**观察**（如果是测试域名，可以设置为**阻断**）。这样可以在不影响线上业务的前提下进行调试。

参数	说明
规则名称	为规则命名。

参数	说明
防护路径配置	设置要防护的路径信息，包含以下参数： ■ **Path**：要防护的路径地址。使用正斜杠（/）表示全路径。 **说明** POST请求的body长度超过8 KB的情况下，可能会造成验签失败。如果该类型接口没有防护必要（如上传大图片等），建议不要经过SDK防护；如确实有防护必要，请使用自定义加签字段。 ■ **匹配方式**：支持**前缀匹配**、**精确匹配**和**正则匹配**。 前缀匹配会匹配指定路径下的所有接口，精确匹配只匹配指定路径，正则匹配支持以正则表达式的方式描述指定路径。 ■ **参数包含**：要防护的路径下包含固定参数时，指定要匹配的参数内容，更准确地定位接口。参数内容指请求地址中问号后面的内容。 示例：假设要防护的URL包括 **域名**`/?action=login&name=test` 。您可以将**Path**设置为“/”，**匹配方式**设置为“前缀匹配”，并在**参数包含**中填写“name”、“login”、“name=test”、“action=login”。
防护策略	选择要应用的防护策略： ■ **非法签名**：默认选中（不支持取消），验证对指定路径的请求的签名是否正确。签名不正确则命中规则。 ■ **模拟器**：选中后，检测用户是否使用模拟器对指定路径发起请求。使用模拟器则命中规则。 ■ **代理**：选中后，检测用户是否使用代理工具对指定路径发起请求。使用代理工具则命中规则。
处置动作	选择对命中防护策略的用户请求执行的操作： ■ **观察**： 只记录日志，不阻断请求。 ■ **阻断**： 阻断请求，返回405状态码。 **注意** 未集成SDK或未调试完成前，请不要为生产环境中的域名开启阻断模式，否则可能会因为SDK没有正确集成导致合法请求被拦截。在测试接入阶段，可以开启观察模式，通过日志调试SDK集成。
自定义加签字段	启用自定义加签字段后，系统将根据所设置的需要加签的请求字段和对应的字段值进行加签验证，判断是否命中该防护策略。 系统默认情况对请求的body加签，如果body长度超过8 KB则可能导致验签失败。这种情况下，您可以启用自定义加签字段，使用您指定的请求字段来取代系统默认的加签字段。 启用自定义加签字段后，您可以选择请求Header、参数或Cookie类型，然后填写需要加签的字段即可。例如，您可以选择**cookie**，填写“DG_ZUID”，请求Cookie中的DG_ZUID字段将取代系统默认的body字段作为加签字段。

iii. 单击**确定**。

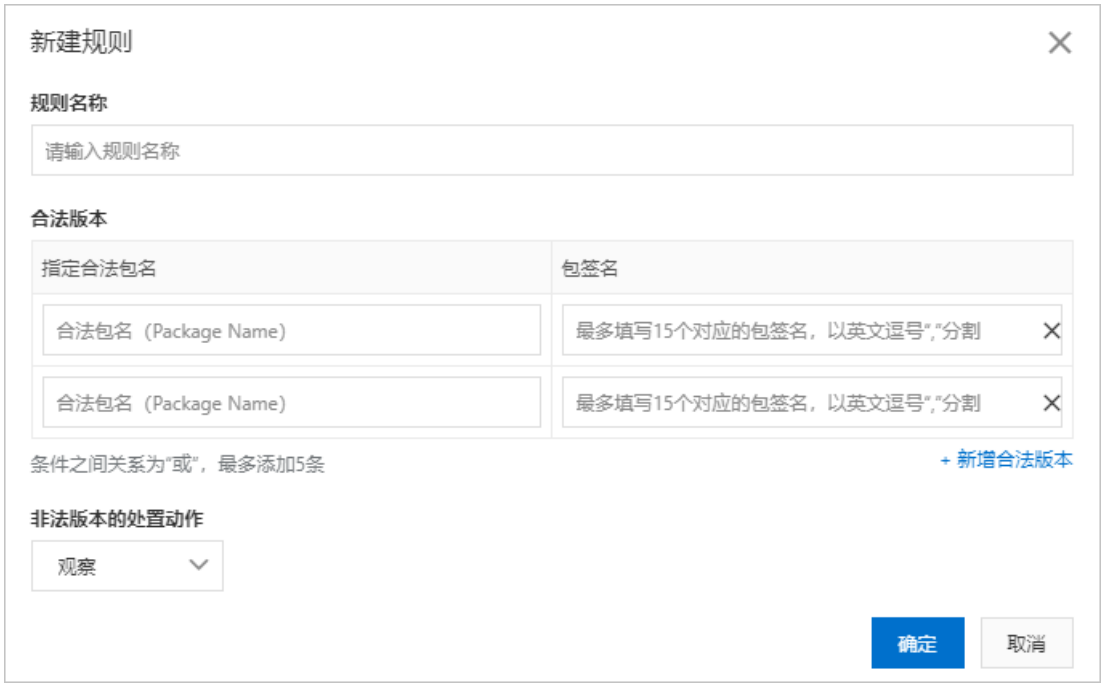
7. 开启版本防护。

通过配置版本防护可以拦截来自非官方App的请求。如果您需要验证App合法性，可通过配置该策略实现。

> **说明** 如果不需要进行App合法性验证，则可不配置版本防护策略。

i. 在**App防护**页面，定位到**版本防护**，开启**仅允许指定版本通过**开关。

ii. 在**新建规则**对话框，完成以下规则配置。



参数	说明
规则名称	为规则命名。
合法版本	设置合法版本信息： ■ **指定合法包名**：指定合法的App包名称。例如，*com.aliyundemo.example*。 ■ **包签名**：请联系阿里云相关安全技术人员获取。如果无需验证对应的App包签名，则包签名项为空即可，将只验证所设定的合法App包名称。 **注意** 包签名不是App证书签名。 单击**新增合法版本**可以添加最多5条版本记录，包名称不允许重复。iOS和Android包都支持，合法的记录都可以填写进去以匹配多个包名。
非法版本的处置操作	■ **观察**：只记录日志，不阻断请求。 ■ **阻断**：阻断请求，返回405状态码。

iii. 单击**确定**。

8. 开启App防护。回到**App防护**区域，开启**状态**开关。

> **说明** 建议您通过调试确定已在App中正确集成SDK并发布新版App后，再开启App防护，使防护配置生效。

4.访问控制/限流

4.1. 设置CC安全防护

网站接入Web应用防火墙后，CC安全防护功能默认开启，为网站拦截针对页面请求的CC攻击（拦截后返回405拦截提示页面）。您可以根据实际需求修改CC安全防护的防护策略。

前提条件

- 已开通Web应用防火墙实例。具体操作，请参见开通Web应用防火墙。
- 已完成网站接入。具体操作，请参见网站接入概述。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**访问控制/限流**页签，定位到**CC安全防护**区域，完成以下功能配置。

参数	说明
状态	开启或关闭CC安全防护功能。网站接入Web应用防火墙后默认开启CC安全防护。 **说明** CC安全防护开启后，所有网站请求默认都会经过CC安全防护的检测。您可以通过设置**访问控制/限流**白名单，让满足条件的请求忽略CC安全防护的检测。更多信息，请参见设置访问控制/限流白名单。

参数	说明
模式	要应用的防护模式。可选值： ○ **防护**：只针对特别异常的请求进行拦截，误杀较少。建议您在网站无明显流量异常时应用此模式，避免误杀。 ○ **防护-紧急**：高效拦截CC攻击，可能造成较多误杀。当您发现有防护模式无法拦截的CC攻击，并出现网站响应缓慢，流量、CPU、内存等指标异常时，可以应用此模式。 **说明** 防护-紧急模式适用于网页或H5页面，但不适用于API或Native App业务，因为会造成大量误杀。对于后者，建议您使用自定义防护策略。更多信息，请参见设置自定义防护策略。

相关操作

- 如果您发现使用了**防护-紧急**模式后，仍有较多攻击未被成功拦截，建议您检查流量来源是否为WAF回源IP。如果发现有攻击直接攻击源站，您可以设置只允许WAF回源IP访问源站。更多信息，请参见设置源站保护。
- 如果您希望有更好的防护效果，同时误杀率更低，您可以使用自定义防护策略。更多信息，请参见设置自定义防护策略。

4.2. 设置IP黑名单

网站接入Web应用防火墙WAF（Web Application Firewall）后，您可以为其开启IP黑名单功能。IP黑名单功能帮助您阻断来自指定IP地址、IP地址段以及指定地域的IP地址的访问请求。本文介绍如何设置普通IP黑名单和地域级IP黑名单。

背景信息

IP黑名单分为普通IP黑名单和地域级IP黑名单。

- 普通IP黑名单：阻断来自指定IP地址、IP地址段的访问请求。
- 地域级IP黑名单：阻断来自指定中国境内或中国境外的IP访问请求。

前提条件

- 已开通Web应用防火墙实例，且实例满足以下要求：
  - 包年包月实例：实例版本为**高级版**、**企业版**、**旗舰版**或**独享版**。更多信息，请参见开通Web应用防火墙。

    注意 **高级版**实例只支持普通**IP黑名单**（针对指定的IP地址），不支持**地域级IP黑名单**（针对指定地域下的所有IP地址）。

    如需要使用**地域级IP黑名单**，则实例版本必须是**企业版**、**旗舰版**或**独享版**。
  - 按量计费实例：已在**账单与套餐中心**，开启**访问控制**模块下**IP黑名单/区域封禁**功能。更多信息，请参见账单与套餐中心（按量2.0版本）。
- 已完成网站接入。具体操作，请参见网站接入概述。

操作步骤

1. 登录Web应用防火墙控制台，并在顶部菜单栏，选择WAF实例的资源组和地域（**中国内地**、**非中国内地**）。
2. 在左侧导航栏，选择**防护配置 > 网站防护**。
3. 在**网站防护**页面上方，切换到要设置的域名。

4. 单击**访问控制/限流**页签，定位到**IP黑名单**卡片，开启**状态**开关并单击**前去配置**。

> **说明** IP黑名单开启后，所有网站请求默认都会经过IP黑名单的检测。您可以通过设置**访问控制/限流**白名单，让满足条件的请求忽略IP黑名单的检测。更多信息，请参见设置访问控制/限流白名单。

5. 在**IP黑名单**页面，分别配置**IP黑名单**和**地域级IP 黑名单**。
   - **IP黑名单**：输入要封禁的IP地址，并单击页面下方的**保存**。多个IP间以英文逗号（,）分隔，最多支持添加200个IP地址。
   - **地域级IP 黑名单**：分别从**中国境内**、**中国境外**页签下选中要封禁的中国或国际地区，并单击页面下方的**保存**。

     IP黑名单开启后自动生效，黑名单中IP对网站发起的所有访问请求都将被阻断。

相关操作

- 如果您希望配置更精细的IP黑名单访问控制，建议您使用自定义防护策略。更多信息，请参见设置自定义防护策略。
- 如果您希望加白放行特定IP的访问流量，建议您设置**访问控制/限流**白名单。更多信息，请参见设置访问控制/限流白名单。

4.3. 设置扫描防护

网站接入Web应用防火墙后，您可以为其开启扫描防护功能。扫描防护帮助网站自动阻断包含指定特征的访问请求，例如请求源IP在短期内发起多次Web攻击或目录遍历攻击、请求源IP来自常见扫描工具或阿里云恶意扫描攻击IP库。

前提条件

- 已开通Web应用防火墙实例，且实例满足以下要求：
  - 包年包月实例：实例版本是**高级版**及以上规格。

    > **注意** 高级版实例只支持使用默认扫描防护策略，不支持自定义扫描防护策略。如需自定义**高频Web攻击封禁**和**目录遍历防护**的防护策略，则实例版本必须是**企业版**及以上规格。

    更多信息，请参见开通Web应用防火墙。

- 按量计费实例：已在**账单与套餐中心**，开启**Web入侵防护**模块下**自定义扫描防护**功能。

  更多信息，请参见账单与套餐中心（按量2.0版本）。

- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

扫描防护功能包括以下防护策略：

- **高频Web攻击封禁**：自动封禁在短时间内发起多次Web攻击的客户端IP。支持自定义防护策略。封禁期间支持手动解封。
- **目录遍历防护**：自动封禁在短时间内发起多次目录遍历攻击的客户端IP。支持自定义防护策略。封禁期间支持手动解封。
- **扫描工具封禁**：自动阻断常见扫描工具IP的访问请求。支持封禁的扫描工具包括Sqlmap、AWVS、Nessus、Appscan、Webinspect、Netsparker、Nikto、Rsas等。
- **协同防御**：自动阻断阿里云全球恶意扫描攻击IP库中IP的访问请求。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**访问控制/限流**页签，定位到**扫描防护**区域，完成以下功能配置。

> **说明** 扫描防护下任意功能开启后，所有网站请求默认都会经过扫描防护的检测。您可以通过设置**访问控制/限流**白名单，让满足条件的请求忽略扫描防护的检测。更多信息，请参见设置访问控制/限流白名单。

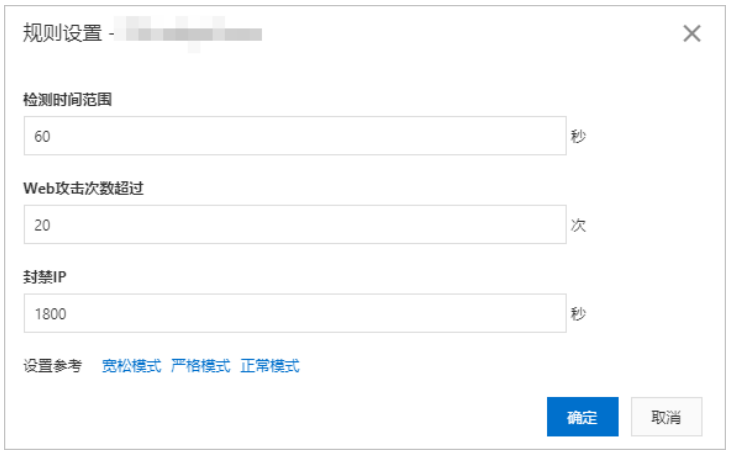
- **高频Web攻击封禁**：开启或关闭高频Web攻击封禁。

配置高频Web攻击封禁的防护策略

a. 开启高频Web攻击封禁。

b. 单击**前去配置**。

c. 在**规则设置**对话框，配置以下参数：**检测时间范围**（秒）、**Web攻击次数超过**（次）、**封禁IP**（秒）。



规则释义：如果某个客户端IP在指定的**检测时间范围**内发起的**Web攻击次数超过**指定数量，则在指定的**封禁IP**时长内阻断该IP的访问请求。

> **说明** 建议您使用**设置参考**，单击选择一种内置的配置模式（**宽松模式**、**严格模式**、**正常模式**），并在此基础上进行调整。

d. 单击**确定**。

解除当前封禁IP：单击**解封当前封禁IP**，直接解除由该功能封禁的IP。

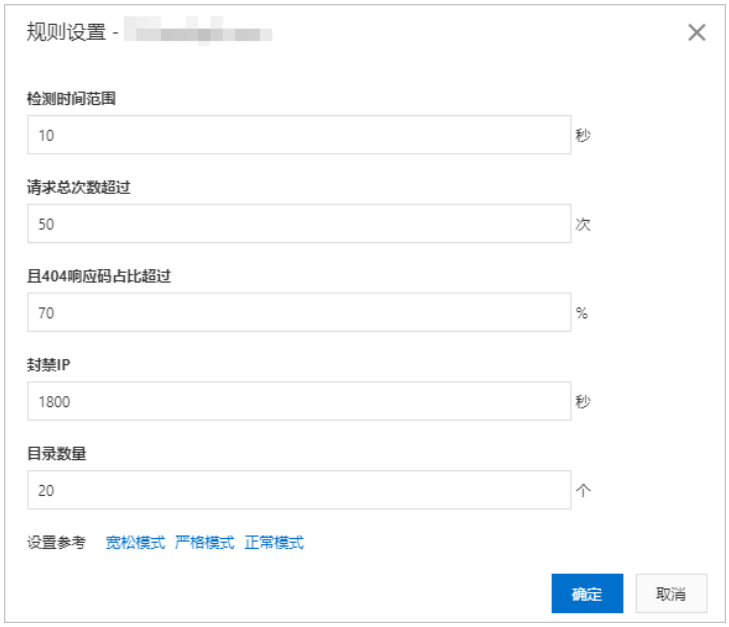
- **目录遍历防护**：开启或关闭目录遍历防护。

  配置目录遍历防护的防护策略

  a. 开启目录遍历防护。

  b. 单击**前去配置**。

c. 在**规则设置**对话框，配置以下参数：**检测时间范围**（秒）、**请求总次数超过**（次）、**且404响应码占比超过**（%）、**封禁IP**（秒）、**目录数量**。



规则释义：如果某个客户端IP在指定的**检测时间范围**内发起的**请求总次数超过**指定数量**且404响应码占比超过**指定比例，或者在指定的**检测时间范围**内请求访问的**目录数量**超过指定值，则在指定的**封禁IP**时长内阻断该IP的访问请求。

> **说明** 建议您使用**设置参考**，单击选择一种内置的配置模式（**宽松模式**、**严格模式**、**正常模式**），并在此基础上进行调整。

d. 单击**确定**。

解除当前封禁IP：单击**解封当前封禁IP**，直接解除由该功能封禁的IP。

- **扫描工具封禁**：开启或关闭扫描工具封禁。

  开启后，智能识别常见的扫描工具行为。如果访问行为满足扫描特征，将一直阻断其访问请求。关闭后，将不再拦截扫描行为。

- **协同防御**：开启或关闭协同防御。

  开启后，自动阻断来自阿里云全球恶意扫描攻击IP库中IP的访问请求。

4.4. 设置自定义防护策略

网站接入Web应用防火墙（WAF）后，您可以为其开启自定义防护策略功能。自定义防护策略允许您自定义基于精确匹配条件的访问控制规则和访问频率限制规则。自定义防护策略支持随业务场景定制，可用于盗链防护、网站管理后台保护等场景。

前提条件

- 已开通Web应用防火墙实例。具体操作，请参见开通Web应用防火墙。
- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

自定义防护策略通过自定义规则实现。自定义规则分为以下类型：

- ACL访问控制规则：根据客户端IP、请求URL、以及常见的请求头字段定义精确匹配条件，过滤访问请求。
- CC攻击防护规则：在精确匹配条件的基础上，定义访问频率限制条件，针对性过滤异常请求。

使用限制

包年包月WAF实例版本不同，支持配置的自定义规则的数量及规格不同，具体如下表所示。

规格	说明	高级版	企业版	旗舰版及以上
自定义规则数量	最多支持添加的自定义规则的数量。	200条/域名	200条/域名	200条/域名
高级匹配字段	在自定义规则的匹配条件中使用除IP和URL外的高级匹配字段。	不支持	支持	支持
频率设置	在自定义规则中开启频率设置，即自定义CC攻击防护规则。	不支持	支持	支持
自定义统计对象	在频率设置中使用除IP和Session外的自定义统计对象字段。	不支持	支持	支持

按量计费WAF实例支持配置的自定义规则的数量及规格说明如下：

- 支持创建的自定义规则的数量：50条/域名。
- 默认不支持在自定义规则中使用高级匹配字段。

  如需使用高级匹配字段，必须先在**账单与套餐中心**，开启**访问控制**模块下的**高级精准条件**功能。
- 默认不支持在自定义规则中启用频率设置。

  如需使用频率设置功能，必须先在**账单与套餐中心**，开启**访问控制**模块下的**自定义限速**功能。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**访问控制/限流**页签，定位到**自定义防护策略**区域，开启**状态**开关并单击**前去配置**。

说明 自定义防护策略开启后，所有网站请求默认都会经过自定义防护策略的检测。您可以通过设置访问控制/限流白名单，让满足条件的请求忽略自定义防护策略的检测。更多信息，请参见设置访问控制/限流白名单。

6. 新建自定义规则。
   i. 在**自定义防护策略**页面，单击**新建自定义防护策略**。
   ii. 在**新建规则**对话框，完成以下规则配置。

参数	说明
规则名称	为规则命名。
匹配条件	定义规则的检测逻辑，只有命中匹配条件的请求才会触发规则。单击**新增条件**可以设置最多5个条件。存在多个条件时，多个条件必须同时满足才算命中条件。 关于匹配条件的配置描述，请参见匹配条件字段说明。

参数	说明
频率设置	开启或关闭频率设置。频率统计在匹配条件检测后生效。开启频率设置时，需要完成统计参数配置。  关于频率设置参数的描述，请参见频率设置参数描述。
处置动作	定义触发规则后执行的操作。可选值： ■ **观察**：触发告警，不阻断请求。 ■ **阻断**：阻断访问请求。 ■ **滑块**：重定向访问请求到滑块验证页面。 ■ **严格滑块**：重定向访问请求到严格的滑块验证页面。 ■ **JS验证**：触发JS校验。 如果开启了**频率设置**，则需要指定**超时时间（秒）**，即处置动作的生效时长。 **说明** 由于WAF需要将集群中的多台服务器的数据进行汇总来统计访问频率，统计过程中可能存在一定延时，因此处置动作的实际生效时间可能稍有滞后。
防护类型	自定义规则的类型。无需手动配置，根据是否开启**频率设置**自动选择。 ■ 开启频率设置后，取值为**CC攻击防护**。 ■ 未开启频率设置，取值为**ACL访问控制**。

下表描述了频率设置中需要配置的参数。

参数	说明

参数	说明
统计对象	统计请求数量的依据。可选值： ■ **IP**：单一源IP的请求数量。 ■ **Session**：单一会话的请求数量。 ■ **自定义header**：具有相同自定义header内容的请求数量。 ■ **自定义参数**：具有相同自定义参数内容的请求数量。 ■ **自定义cookie**：具有相同自定义cookie内容的请求数量。
统计时长（秒）	统计周期。
阈值（次）	统计时长内统计对象的允许数量，超过阈值，则触发频率限制。
响应码	在统计检测逻辑后生效，验证统计时长内请求响应中指定**响应码**的数量或比例。数量和比例二选一。 ■ **数量**：允许指定响应码出现的最大次数。 ■ **比例（%）**：允许指定响应码占请求响应中的最大比例。
生效范围	频率设置校验的生效范围。可选值： ■ **当前特征匹配范围内**：表示只统计命中当前规则**匹配条件**的请求。 ■ **当前规则作用的域名范围内**：表示统计当前域名的所有请求。

iii. 单击**保存**。

成功添加自定义防护策略规则后，规则自动启用。您可以在规则列表中查看新建的规则，并根据需要禁用、编辑或删除规则。

相关文档

- 匹配条件字段说明

5.防护白名单

5.1. 设置网站白名单

网站接入Web应用防火墙后，您可以通过设置网站白名单，让满足条件的请求不经过任何Web应用防火墙防护模块的检测，直接访问源站服务器。网站白名单一般用于放行您完全信任的流量，例如受信任的自身漏洞检测扫描工具的访问、已知且已认证的第三方系统接口的访问等。

前提条件

- 已开通Web应用防火墙实例。具体操作，请参见开通Web应用防火墙。
- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

Web应用防火墙网站防护包含多个防护模块，接入防护的网站访问请求默认需要经过所有已开启的防护模块的检测。如果您的业务中有完全受信任的访问流量，您可以设置网站白名单，让满足条件的请求不经过任何防护模块的检测，直接访问源站服务器。

您也可以为不同网站防护模块单独设置白名单，让满足条件的请求只忽略指定模块的检测。支持设置的模块白名单包括：

- Web入侵防护白名单：可以让满足条件的请求不经过规则防护引擎、深度学习引擎模块的检测。
- 数据安全白名单：可以让满足条件的请求不经过防敏感信息泄露、网站防篡改、账户安全模块的检测。
- Bot管理白名单：可以让满足条件的请求不经过爬虫威胁情报、数据风控、智能算法、App防护模块的检测。
- 访问控制/限流白名单：可以让满足条件的请求不经过CC安全防护、IP黑名单、扫描防护、自定义防护策略模块的检测。

> **说明** 强烈建议您根据需要设置对应的模块白名单。越精细的白名单规则安全性越高，模块白名单的安全性高于网站白名单。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击页面右上角的**网站白名单**。
6. 新建网站白名单。
   i. 在**网站白名单**页面，单击**新建白名单**。

ii. 在**新建规则**对话框，完成以下规则配置。

参数	说明
规则名称	为规则命名。
匹配条件	定义白名单请求要满足的条件。单击**新增条件**可以设置最多5个条件。存在多个条件时，多个条件必须同时满足才算命中条件。 关于匹配条件的配置描述，请参见匹配条件字段说明。

iii. 单击**保存**。

成功添加网站白名单规则后，规则自动生效。您可以在规则列表中查看新建的规则，并根据需要禁用、编辑或删除规则。

相关文档

匹配条件字段说明

5.2. 设置Web入侵防护白名单

网站接入Web应用防火墙防护后，您可以通过设置Web入侵防护白名单，让满足指定特征的请求不经过规则防护引擎、深度学习引擎的检测。Web入侵防护白名单一般用于放行因触发Web入侵防护相关规则被误拦截的特殊业务请求。

前提条件

- 已开通Web应用防火墙实例。具体操作，请参见开通Web应用防火墙。
- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

Web入侵防护为网站提供针对Web通用攻击的防护能力和对0day漏洞的快速响应能力，保证网站安全性，具体包含以下检测模块：

- 规则防护引擎
- 深度学习引擎

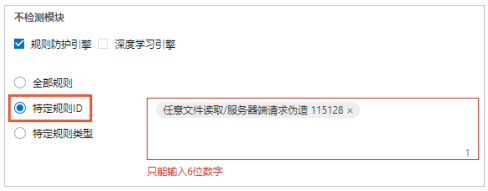
如果上述模块开启后对正常网站请求造成误拦截，您可以设置Web入侵防护白名单，让满足条件的请求不经过指定模块的检测。建议您在设置Web入侵防护白名单规则时，结合实际业务需求，确保放行的都是预期的访问请求。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**Web安全**页签，定位到**Web入侵防护**区域，单击右侧的**前去配置**。
6. 新建Web入侵防护白名单规则。
   i. 在**Web入侵防护 - 白名单**页面，单击**新建白名单**。
   ii. 在**新建规则**对话框，完成以下规则配置。

参数	说明
规则名称	为规则设置一个名称。 仅支持使用英文字符（包含大写和小写格式）、数字、汉字，且不能超过50个字符。
匹配条件	设置白名单请求需要满足的条件（即特征）。单击**新增条件**可以设置最多5个条件。存在多个条件时，多个条件必须同时满足才算命中条件。 关于匹配条件的配置描述，请参见匹配条件字段说明。

参数	说明
不检测模块	设置白名单请求不需要检测的模块。可选值：**规则防护引擎**、**深度学习引擎**。 选中**规则防护引擎**后，默认不检测规则防护引擎中包含的**全部规则**。您也可以根据需要，设置只忽略检测指定的规则、规则类型。设置方法如下： a. 选中**规则防护引擎**。 b. （可选）如果只忽略检测指定的规则，选中**特定规则ID**，并输入不检测的规则ID。  您可以在**防护规则组**页面，通过**新建规则组**，查询WAF包含的所有Web攻击防护规则，获取相关规则的ID。具体操作，请参见自定义防护规则组。 每输入一个规则ID，需要按回车进行确认。最多支持输入50个规则ID。 **说明** 您也可以在**安全报表**页面，通过**Web入侵防护**报表的**误报屏蔽**功能，添加针对特定规则ID的Web入侵防护白名单规则。**误报屏蔽**功能支持根据攻击请求特征自动生成对应的白名单规则，无需您手动设置匹配条件和查询规则ID。关于误报屏蔽的相关操作，请参见Web安全报表说明。 c. （可选）如果只忽略检测指定的规则类型，选中**特定规则类型**，并选择不检测的规则类型，然后单击**确定**。 

iii. 单击**保存**。

成功添加Web入侵防护白名单规则后，规则自动启用。您可以在规则列表中查看新建的规则，并根据需要禁用、编辑或删除规则。

注意 白名单规则经创建后，默认永久有效。如果您不再需要某条白名单规则，可以将其禁用、删除。

相关文档

匹配条件字段说明

5.3. 设置数据安全白名单

网站接入Web应用防火墙后，您可以通过设置数据安全白名单，让满足条件的请求忽略指定模块（防敏感信息泄露、网站防篡改、账户安全）的检测。数据安全白名单可以放行因触发数据安全相关规则被误拦截的业务请求。

前提条件

- 已开通Web应用防火墙实例。具体操作，请参见开通Web应用防火墙。
- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

数据安全为网站提供基于页面内容防泄漏和篡改的响应防护，保护网站数据的完整性和保密性，具体包括以下检测模块：

- 网站防篡改
- 防敏感信息泄露
- 账户安全

如果上述模块开启后对正常网站请求造成误拦截，您可以设置数据安全白名单，让满足条件的请求不经过指定模块的检测。

建议您设置更详细的规则，确保放行的都是合法的访问请求。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**Web安全**页签，定位到**数据安全**区域，单击右侧的**前去配置**。
6. 新建数据安全白名单。
   i. 在**数据安全 - 白名单**页面，单击**新建白名单**。

ii. 在**新建规则**对话框，完成以下规则配置。

参数	说明
规则名称	为规则命名。
匹配条件	定义白名单请求要满足的条件。单击**新增条件**可以设置最多5个条件。存在多个条件时，多个条件必须同时满足才算命中条件。 关于匹配条件的配置描述，请参见匹配条件字段说明。
不检测模块	命中条件后，要忽略的检测模块，可选值： ■ **防敏感信息泄露** ■ **网站防篡改** ■ **账户安全**

iii. 单击**保存**。

成功添加数据安全白名单规则后，规则自动启用。您可以在规则列表中查看新建的规则，并根据需要禁用、编辑或删除规则。

相关文档

匹配条件字段说明

5.4. 设置Bot管理白名单

网站接入Web应用防火墙后，您可以通过设置Bot管理白名单，让满足条件的请求忽略指定模块（爬虫威胁情报、数据风控、智能算法、App防护）的检测。Bot管理白名单可以放行因触发Bot管理相关规则被误拦截的业务请求。

前提条件

- 已开通Web应用防火墙实例，且实例满足以下要求：
  - 使用包年包月方式开通。

> **说明** 按量计费开通的Web应用防火墙实例暂不支持Bot管理增值服务。

- 已开启**Bot管理**增值服务。

- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

Bot管理为接入Web应用防火墙的域名提供从Web、应用到API接口的全面的恶意爬虫防护检测，具体包括以下检测模块：

- 合法爬虫
- 爬虫威胁情报
- 数据风控
- App防护
- 智能算法

如果上述模块（除合法爬虫以外）开启后对正常网站请求造成误拦截，您可以设置Bot管理白名单，让满足条件的请求不经过指定模块的检测。

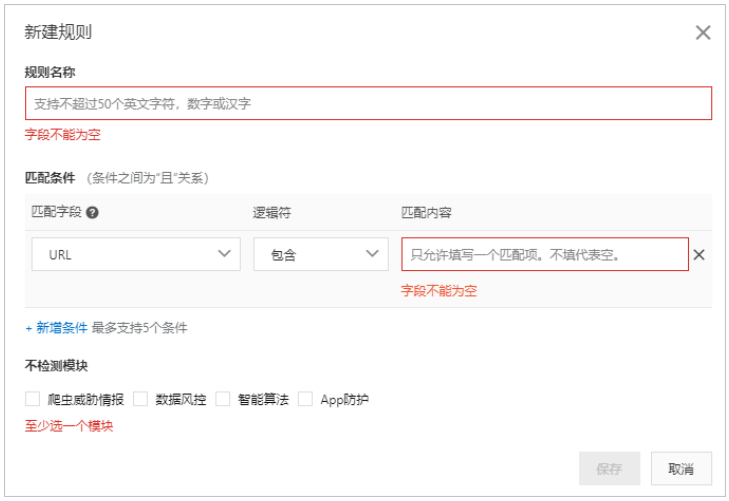
建议您设置更详细的规则，确保放行的都是合法的访问请求。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**Bot管理**页签，定位到**精细化配置**区域，单击右侧的**前去配置**。
6. 新建Bot管理白名单。
   i. 在**Bot管理-白名单**页面，单击**新建白名单**。

ii. 在**新建规则**对话框，完成以下规则配置。



参数	说明
规则名称	为规则命名。
匹配条件	定义白名单请求要满足的条件。单击**新增条件**可以设置最多5个条件。存在多个条件时，多个条件必须同时满足才能命中条件。 关于匹配条件的配置描述，请参见匹配条件字段说明。
不检测模块	命中条件后，要忽略的检测模块，可选值： ■ **爬虫威胁情报** ■ **数据风控** ■ **智能算法** ■ **App防护**

iii. 单击**保存**。

成功添加Bot管理白名单规则后，规则自动启用。您可以在规则列表中查看新建的规则，并根据需要禁用、编辑或删除规则。

相关文档

匹配条件字段说明

5.5. 设置访问控制/限流白名单

网站接入Web应用防火墙后，您可以通过设置访问控制/限流白名单，让满足条件的请求忽略指定模块（CC安全防护、IP黑名单、扫描防护、自定义防护策略）的检测。访问控制/限流白名单可以放行因触发访问控制/限流相关规则被误拦截的业务请求。

前提条件

- 已开通Web应用防火墙实例。具体操作，请参见开通Web应用防火墙。
- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

访问控制/限流为网站提供基于应用层的自定义访问控制策略和流量管理策略，保证网站的可访问性，具体包含以下检测模块：

- CC安全防护
- IP黑名单
- 扫描防护
- 自定义防护策略

如果上述模块开启后对正常网站请求造成误拦截，您可以设置访问控制/限流白名单，让满足条件的请求不经过指定模块的检测。

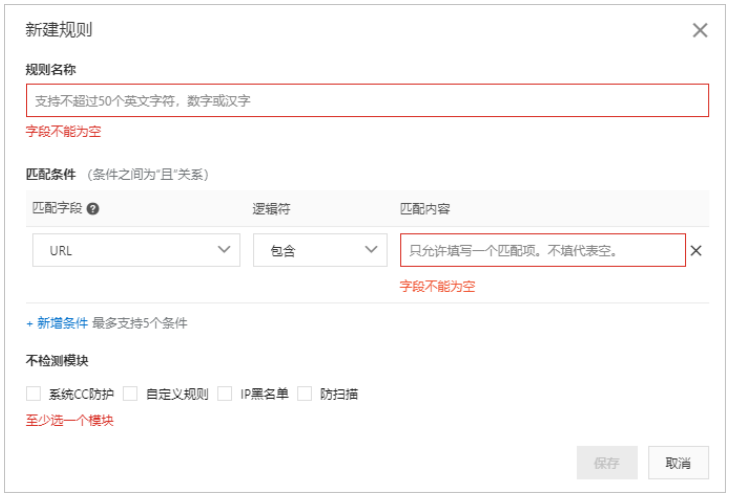
建议您设置更详细的规则，确保放行的都是合法的访问请求。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

5. 单击**访问控制/限流**页签，定位到**访问控制/限流**区域，单击右侧的**前去配置**。
6. 新建访问控制/限流白名单。
   i. 在**访问控制/限流 - 白名单**页面，单击**新建白名单**。

ii. 在**新建规则**对话框，完成以下规则配置。



参数	说明
规则名称	为规则命名。
匹配条件	定义白名单请求要满足的条件。单击**新增条件**可以设置最多5个条件。存在多个条件时，多个条件必须同时满足才算命中条件。 关于匹配条件的配置描述，请参见匹配条件字段说明。
不检测模块	命中条件后，要忽略的检测模块，可选值： ■ **系统CC防护** ■ **自定义规则** ■ **IP黑名单** ■ **防扫描**

iii. 单击**保存**。

成功添加访问控制/限流白名单规则后，规则自动启用。您可以在规则列表中查看新建的规则，并根据需要禁用、编辑或删除规则。

相关文档

匹配条件字段说明

6.匹配条件字段说明

Web应用防火墙的白名单设置和自定义防护策略都需要定义规则匹配条件。本文具体描述了规则匹配条件中支持使用的字段及其释义。

什么是匹配条件、匹配动作

在Web应用防火墙中，您可以自定义防护白名单规则和自定义防护策略规则。自定义规则由匹配条件与匹配动作构成。在创建规则时，您通过设置匹配字段、逻辑符和相应的匹配内容定义匹配条件，并针对符合匹配条件规则的访问请求定义相应的动作。

- **匹配条件**

  匹配条件包含匹配字段、逻辑符、匹配内容。匹配内容暂时不支持通过正则表达式描述。每一条自定义规则中最多允许设置5个匹配条件组合，且各个条件间是“与”的逻辑关系，即访问请求必须同时满足所有匹配条件才算命中该规则，并执行相应的匹配动作。

- **匹配动作**

  防护白名单中的匹配动作表示不检测模块，自定义防护策略的匹配动作表示处置动作，具体请参见以下文档：

  - 设置网站白名单
  - 设置Web入侵防护白名单
  - 设置访问控制/限流白名单
  - 设置Bot管理白名单
  - 设置数据安全白名单
  - 设置自定义防护策略

支持的匹配字段

下表描述了匹配条件中支持使用的匹配字段。

匹配字段	支持的版本	适用的逻辑符	字段描述
IP	高级版及以上	属于、不属于	访问请求的来源IP，支持填写IP或IP/掩码（例如，47.100.XX.XX/24）。 **说明** 最多可以填写50个值，多个值之间使用英文逗号（,）分隔。

匹配字段	支持的版本	适用的逻辑符	字段描述
URL	高级版及以上	• 等于、不等于、等于多值之一、不等于任一值 • 包含、不包含、包含多值之一、不包含任一值 • 长度等于、长度大于、长度小于 • 前缀匹配、后缀匹配 • 正则匹配、正则不匹配	访问请求的URL地址。
Referer	高级版及以上	• 等于、不等于、等于多值之一、不等于任一值 • 包含、不包含、包含多值之一、不包含任一值 • 存在、不存在、内容为空 • 长度等于、长度大于、长度小于 • 前缀匹配、后缀匹配	访问请求的来源网址，即该访问请求是从哪个页面跳转产生的。
User-Agent	高级版及以上	• 等于、不等于、等于多值之一、不等于任一值 • 包含、不包含、包含多值之一、不包含任一值 • 存在、不存在、内容为空 • 长度等于、长度大于、长度小于 • 前缀匹配、后缀匹配	发起访问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。

匹配字段	支持的版本	适用的逻辑符	字段描述
Params	高级版及以上	• 等于、不等于、等于多值之一、不等于任一值 • 包含、不包含、包含多值之一、不包含任一值 • 存在、不存在、内容为空 • 长度等于、长度大于、长度小于 • 前缀匹配、后缀匹配	访问请求的URL地址中的参数部分，通常指URL中”?”后面的部分。例如，`www.example.com/index.html?action=login` 中的 `action=login` 就是参数部分。
Query-Arg	高级版及以上	• 等于、不等于、等于多值之一、不等于任一值 • 包含、不包含、包含多值之一、不包含任一值 • 存在、不存在、内容为空 • 长度等于、长度大于、长度小于 • 前缀匹配、后缀匹配	访问请求的URL地址中的参数部分，通常指URL中”?”后面的部分。例如 `www.example.com/request_path?arg1=a&arg2=b` 中，`query-arg` 字段为arg1或arg2。 **说明** 访问请求里 `query-arg` 参数包含多个字段时，自定义防护策略中如果设置的是 `query-arg包含arg` ，WAF会命中取值为arg1和arg2的两条访问请求。如果您需要精确匹配访问请求，建议策略设置为 `query-arg包含arg1` 或 `query-arg包含arg2` 。
URLPath	高级版及以上	• 等于、不等于、等于多值之一、不等于任一值 • 包含、不包含、包含多值之一、不包含任一值 • 长度等于、长度大于、长度小于 • 前缀匹配、后缀匹配 • 正则匹配、正则不匹配	访问请求的URL路径。

匹配字段	支持的版本	适用的逻辑符	字段描述
Cookie	企业版及以上	• 等于、不等于、等于多值之一、不等于任一值 • 包含、不包含、包含多值之一、不包含任一值 • 存在、不存在、内容为空 • 长度等于、长度大于、长度小于	访问请求中的Cookie信息。
Content-Type	企业版及以上	• 等于、不等于、等于多值之一、不等于任一值 • 包含、不包含、包含多值之一、不包含任一值 • 长度等于、长度大于、长度小于	访问请求指定的响应HTTP内容类型，即MIME类型信息。
Content-Length	企业版及以上	值小于、等于、值大于	访问请求的响应内容所包含的字节数。
X-Forwarded-For	企业版及以上	• 等于、不等于、等于多值之一、不等于任一值 • 包含、不包含、包含多值之一、不包含任一值 • 长度等于、长度大于、长度小于	访问请求的客户端真实IP。X-Forwarded-For（XFF）用来识别通过HTTP代理或负载均衡方式转发的访问请求的客户端最原始的IP地址的HTTP请求头字段，只有通过HTTP代理或者负载均衡服务器转发的访问请求才会包含该项。
Post-Body	企业版及以上	• 等于、不等于 • 包含、不包含 • 存在、不存在、内容为空 • 不存在 • 前缀匹配、后缀匹配	访问请求的请求内容信息。
Server-Port	企业版及以上	等于、不等于、等于多值之一、不等于任一值	源站服务器的端口号。例如 `www.example.com:9999`，中，`server_port` 为9999。
Http-Method	企业版及以上	等于、不等于、等于多值之一、不等于任一值	访问请求的方法，例如GET、POST、DELETE、PUT、OPTIONS等。

匹配字段	支持的版本	适用的逻辑符	字段描述
Header	企业版及以上	• 等于、不等于、等于多值之一、不等于任一值 • 包含、不包含、包含多值之一、不包含任一值 • 存在、不存在、内容为空 • 长度等于、长度大于、长度小于	访问请求的头部信息，用于自定义HTTP头部字段。

7.自定义防护规则组

您可以使用Web应用防火墙提供的防护规则自定义搭建防护规则组，为具体的防护功能（例如，规则防护引擎）创建有针对性的防护策略。在设置网站防护功能时，如果默认的防护规则组不能满足您的需求，建议您使用自定义防护规则组。

前提条件

- 已开通了Web应用防火墙，且实例满足以下要求：
  - 使用包年包月方式开通。

    > **说明** 按量付费开通的Web应用防火墙实例暂不支持使用防护规则组。

  - 如果实例地域是**中国内地**，则实例套餐必须是**企业版**及以上规格。
  - 如果实例地域是**非中国内地**，则实例套餐必须是**旗舰版**及以上规格。

  更多信息，请参见开通Web应用防火墙。
- 已完成网站接入。具体操作，请参见网站接入概述。

背景信息

目前仅**规则防护引擎**支持自定义防护规则组，即您可以自定义**规则防护引擎**功能的防护规则组。关于**规则防护引擎**的更多信息，请参见设置规则防护引擎。

使用流程

防护规则组的使用流程如下：

1. 新建规则组：为具体防护功能创建自定义防护规则组，形成有针对性的防护策略。
2. 应用规则组：已添加自定义防护规则组后，您可以为网站域名应用自定义防护规则组。

新建规则组

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**系统管理 > 防护规则组**。
4. （可选）在**防护规则组**页面，单击要操作的防护功能页签。

   > **说明** 由于目前仅**Web攻击防护**（对应**规则防护引擎**）支持防护规则组，页面自动跳转到**Web攻击防护**页签，该步骤无需手动操作。

   规则组列表展示了Web攻击防护（规则防护引擎）的系统规则和自定义防护规则组。
   - 系统默认规则组：规则组名称为**宽松规则组**、**中等规则组**、**严格规则组**。

您可以单击系统规则的**内置规则数**，查看系统规则包含的内置规则信息。

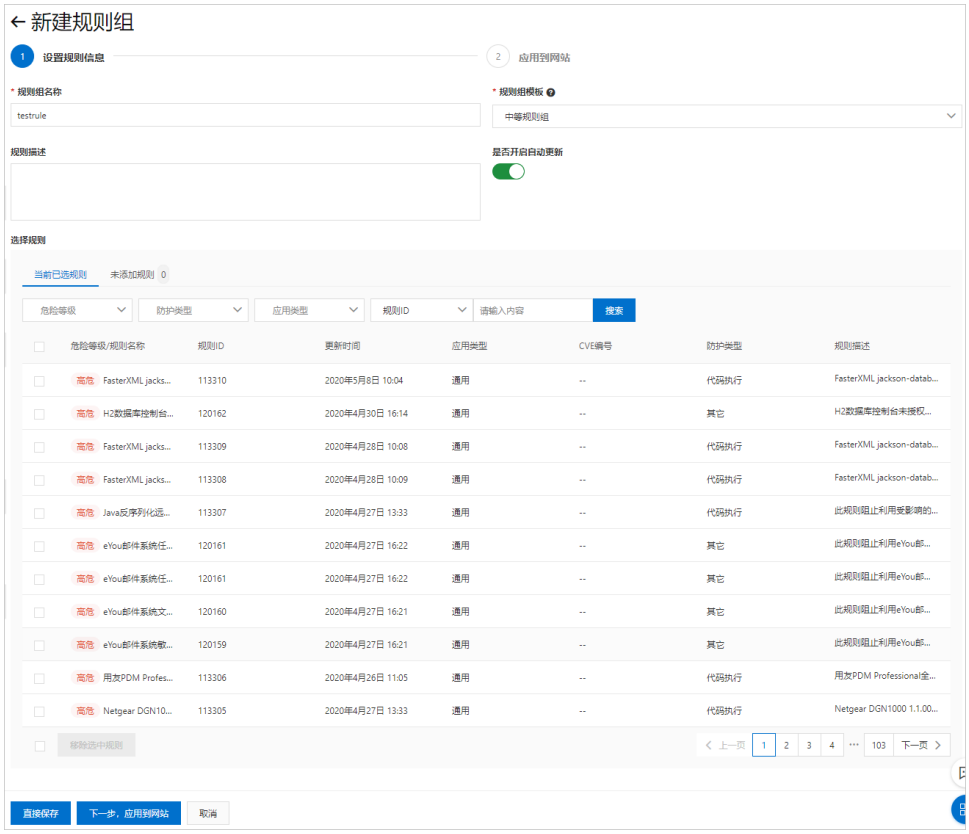
> **说明** 系统规则组不支持编辑和删除。

- 自定义规则组：表示您在**Web攻击防护**页签新建的规则组。

5. 单击**新建规则组**。

> **说明** 您最多可以手动添加10个Web攻击防护（规则防护引擎）防护规则组。

6. 完成**新建规则组**配置向导。
   i. **设置规则信息**。完成以下规则组参数设置，并单击**下一步，应用到网站**。



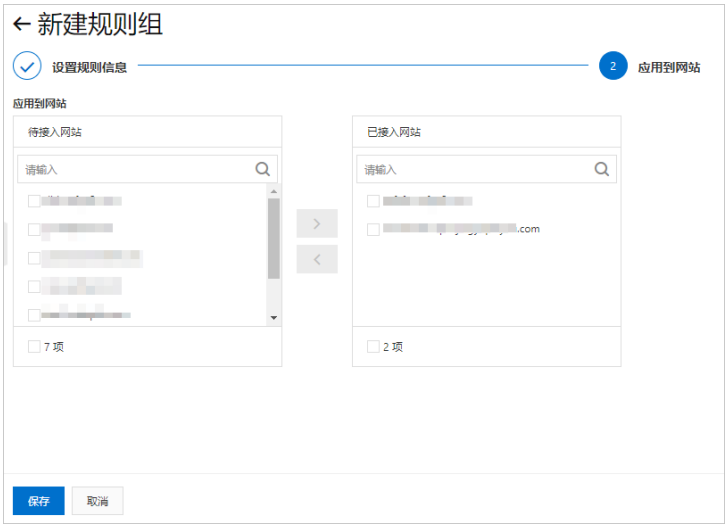
参数	描述
规则组名称	设置规则组的名称。 规则组名称用于标识当前规则组，建议您使用有明确含义的名称。

参数	描述
规则组模板	选择要应用的规则组模板。可选项： ■ **严格规则组** ■ **中等规则组** ■ **宽松规则组** 规则组模板是系统同步更新安全防护规则的基础，不同规则组模板包含的规则不同。选择规则组模板并开启自动更新后，应用了该模板的规则组会自动同步规则组模板内规则的更新。
规则描述	输入规则组的描述信息。
是否开启自动更新	开启自动更新后，当规则组模板包含的规则更新时，会自动同步到应用了该模板的规则组。 **说明** 部分旧版本自定义规则组不支持规则组自动更新，建议您重新自定义规则组替换此类规则组，实现规则组自动更新。
选择规则	选择当前规则组要应用的防护规则。 **当前已选规则**列表默认展示您所选的规则组模板中的所有规则，您需要从中选择不适用或者可能造成误拦截的规则并单击**移除选中规则**。 您可以使用筛选和搜索功能查询规则，例如通过**防护类型**、**应用类型**、**危险等级**筛选规则，或者输入规则名称、ID搜索规则。 ■ **危险等级**：表示规则防御的Web攻击的危险等级，包括**高危**、**中危**、**低危**。 ■ **防护类型**：表示规则防御的Web攻击类型，包括**SQL注入**、**跨站脚本**、**代码执行**、**本地文件包含**、**远程文件包含**、**webshell**、**其它**。 ■ **应用类型**：表示规则防护的Web应用类型，包括**通用**、**Wordpress**、**Dedecms**、**Discuz**、**Phpcms**、**Ecshop**、**Shopex**、**Drupal**、**Joomla**、**Metinfo**、**Struts2**、**Spring Boot**、**Jboss**、**Weblogic**、**Websphere**、**Tomcat**、**Elastic Search**、**Thinkphp**、**Fastjson**、**ImageMagick**、**PHPwind**、**phpMyAdmin**、**其它**。

说明 如果您暂时无需应用新建的规则组，您可以在完成规则组配置后，单击**直接保存**，完成配置向导，后续需要应用该规则组的时候再编辑该规则组即可。

ii. （可选）**应用到网站**。从**待接入网站**列表选择要应用当前防护规则组的网站域名，添加到**已接入网站**列表。

> 注意 每个网站域名仅支持应用一个防护规则组。



iii. 单击**保存**。

完成操作后，您可以在规则组列表中查看新建的规则组，并根据需要设置应用防护规则组的网站，具体操作，请参见应用规则组。

创建规则组后，您可以在**防护规则组**列表中查看该规则组的**更新时间**（即规则组创建的时间），确定是否需要更新该规则组。

应用规则组

已添加自定义防护规则组后，您可以使用以下任意一种方式应用自定义防护规则组：

- 在**防护规则组**页面为网站应用自定义防护规则组。以下操作步骤以此为例进行描述。
- 在**网站防护**页面设置规则防护引擎防护规则组时，单击下拉列表，选择需要该网站应用的自定义防护规则组。

更多信息，请参见设置规则防护引擎。

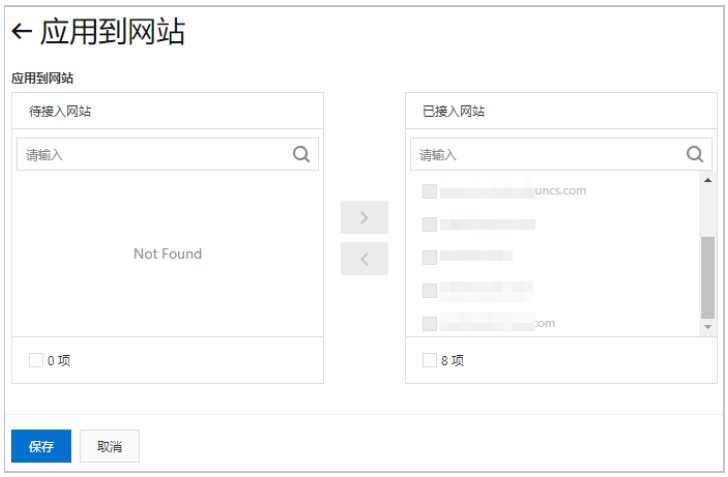
1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。

3. 在左侧导航栏，选择**系统管理 > 防护规则组**。
4. （可选）在**防护规则组**页面，单击要操作的防护功能页签。

   > **说明** 由于目前仅Web攻击防护（规则防护引擎）支持防护规则组，页面自动跳转到Web攻击防护页签，该步骤无需操作。

5. 在规则组列表，定位到要应用的防护规则组，单击其操作列下的**应用到网站**。
6. 在**应用到网站**页面，从**待接入网站**列表选择要应用当前防护规则组的网站域名，添加到**已接入网站**列表，并单击**保存**。

   > **注意** 每个网站域名仅支持应用一个防护规则组，且必须应用一个防护规则组。



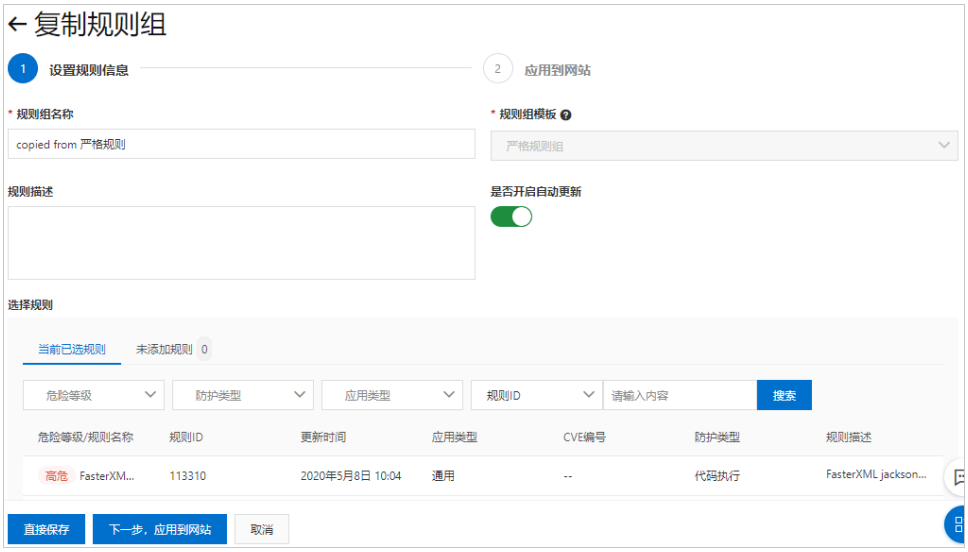
完成操作后，您可以在规则组列表的**应用网站**列，查看规则组应用生效的网站域名。

相关操作

在**防护规则组**页面，您可以对已创建的规则组执行以下操作：

- **复制**：复制某个规则组的规则配置。

  复制规则组的配置页面如下图所示，其中您可以修改**规则组名称**、**规则描述**、**是否开启自动更新**，不可以修改**规则组模板**和规则设置。如果您需要修改规则设置，建议您在复制完成后，编辑通过复制添加的规则组。



- **编辑**：编辑自定义防护规则组的名称、描述和规则配置。系统规则组不支持编辑。
- **删除**：删除自定义防护规则组。系统规则组不支持删除。

  删除自定义防护规则组前，请确保规则组未被应用到任何网站上。如果需要删除的规则组被应用到网站上，您必须先为网站应用其他规则组，才能删除当前规则组。

8.开启IPv6防护

网站接入WAF防护后，您可以为网站一键开启IPv6防护功能。IPv6防护为网站防御IPv6环境下发起的攻击，帮助源站实现对IPv6协议请求的安全防护。

前提条件

- 已开通WAF包年包月服务的企业版、旗舰版、独享版实例，或者按量计费WAF服务。更多信息，请参见开通Web应用防火墙。
- WAF实例的地域是中国内地。

> **说明** 海外地区的WAF实例暂不支持IPv6防护。

- 已使用CNAME接入模式完成网站接入。更多信息，请参见添加域名。

> **说明** 使用透明接入模式的网站暂不支持IPv6防护。

背景信息

开启IPv6安全防护功能后，WAF自动生成的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。

> **注意** 只有使用CNAME接入模式将网站接入WAF防护，才能够正常实现双路解析。

您可以在WAF网站配置中开启IPv6回源，即同时设置IPv4和IPv6回源服务器地址，并启用**IPv4/IPv6回源协议跟随**，使来自IPv6客户端的请求转发到IPv6源站，来自IPv4客户端的请求转发到IPv4源站。更多信息，请参见添加域名。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**资产中心 > 网站接入**。
4. 在**域名列表**中，定位到要操作的域名，在**快捷操作**列为域名打开**IPv6**开关。

5. 在**提示**对话框，单击**确定**。

成功开启IPv6防护后，IPv6开关的状态将变更为已开启。

后续步骤

开启IPv6防护后，WAF在将IPv6客户端请求转发到您的源站服务器时，将使用新增的回源IP网段。

为了保证您的源站服务器能够正常接收WAF转发的回源请求，您必须在源站服务器上设置放行新增的WAF回源IP网段，尤其是当您已经开启了源站保护（即在源站上只允许放行WAF回源IP网段的请求），否则会导致IPv6客户端访问异常或无法访问。具体操作，请参见放行WAF回源IP段、设置源站保护。

9.防护配置最佳实践

9.1. 网站防护最佳实践

当您第一次完成域名接入，面对网站防护设置时，可能会不知道从何下手。本文将引导您从不同场景、角色的视角快速熟悉Web应用防火墙的防护模块选择和防护策略设置，帮助您从自己最关心的需求入手，了解Web应用防火墙的防护逻辑。

前提条件

已完成网站接入。更多信息，请参见添加域名。

使用前须知

本文所有描述建立在您已经开通了相关防护功能的基础上。如果您还没有启用推荐的防护功能，您可以参考功能描述文档开启并设置对应功能。

除特殊说明外，本文推荐的防护设置均在**网站防护**页面完成。您可以参照以下步骤访问**网站防护**页面：

1. 登录Web应用防火墙控制台。
2.
3. 在左侧导航栏，选择**防护配置 > 网站防护**。
4. 在**网站防护**页面上方，切换到要设置的域名。

概述

本文从以下不同角色视角或业务需求视角出发，提供了网站防护的设置建议。您可以选择最贴近您自身实际需求的场景，了解相关的防护设置：

- 我是新手，不懂安全，也没有特殊需求
- 我是运维人员，希望业务安全平稳，出问题时可以快速排查问题
- 我是专业的安全人员，需要做全面的Web入侵运营
- 我的业务需要严格的安全防护，有攻击时宁可错杀不可漏掉
- 我的业务经常受到爬虫骚扰或面临数据泄露、被篡改的风险

我是新手，不懂安全，也没有特殊需求

您可能是基于等保要求或出于提升企业安全水位（达到预防目的）等考虑购买了Web应用防火墙。这种情况下，您可以在完成网站接入后直接使用WAF的默认防护设置，不做任何调整。WAF提供的默认防护能力足够为网站抵御绝大部分的基础Web威胁。

建议您多关注Web应用防火墙控制台的**总览**和**安全报表**页面，了解业务情况和攻击情况。具体操作，请参见以下文档：

- WAF总览
- WAF安全报表

我是运维人员，希望业务安全平稳，出问题时可以快速排查问题

针对您的需求，推荐您在完成网站接入后，为网站设置以下防护功能：

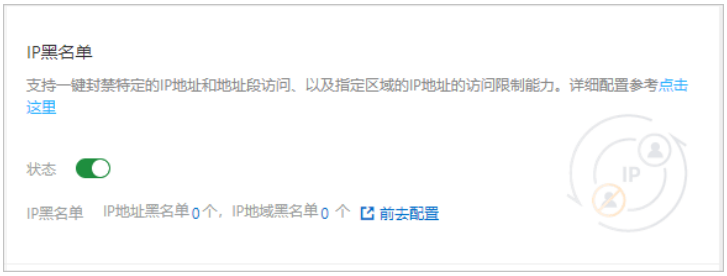
- **网站白名单**：设置网站访问白名单，直接放行满足条件的请求，不进行任何防护检测。

  操作导航：单击**网站防护**页面右上角的**网站白名单**，完成相关设置。具体操作，请参见设置网站白名单。

  您也可以设置具体防护模块的白名单，只加白部分防护模块，这样防护会更加精确。具体操作，请参见以下文档：

  - Web入侵防护白名单：可以让满足条件的请求不经过规则防护引擎、深度学习引擎模块的检测。
  - 数据安全白名单：可以让满足条件的请求不经过防敏感信息泄露、网站防篡改、账户安全模块的检测。
  - Bot管理白名单：可以让满足条件的请求不经过爬虫威胁情报、数据风控、智能算法、App防护模块的检测。
  - 访问控制/限流白名单：可以让满足条件的请求不经过CC安全防护、IP黑名单、扫描防护、自定义防护策略模块的检测。

- **IP黑名单**：封禁与业务不相关的IP地址和地址段，以及指定地域区域的来源IP的访问请求。例如，不存在外省IP访问的地方政府论坛，可以将外省地区加入地域级黑名单；不存在海外用户的站点，可以将全部海外地区加入地域级黑名单。



  操作导航：在**网站防护**页面，单击**访问控制/限流**页签，定位到**IP黑名单**区域，完成相关设置。具体操作，请参见设置IP黑名单。

- **自定义防护策略**：为网站自定义访问控制（ACL）或访问限流策略。例如，限制某些接口只允许特定IP或者UA访问、限制某些特定类型请求的请求频率不能过高等。您也可以通过自定义防护策略防护CC攻击、爬虫攻击或者某些特殊的Web攻击等。

  操作导航：在**网站防护**页面，单击**访问控制/限流**页签，定位到**自定义防护策略**区域，完成相关设置。具体操作，请参见设置自定义防护策略。

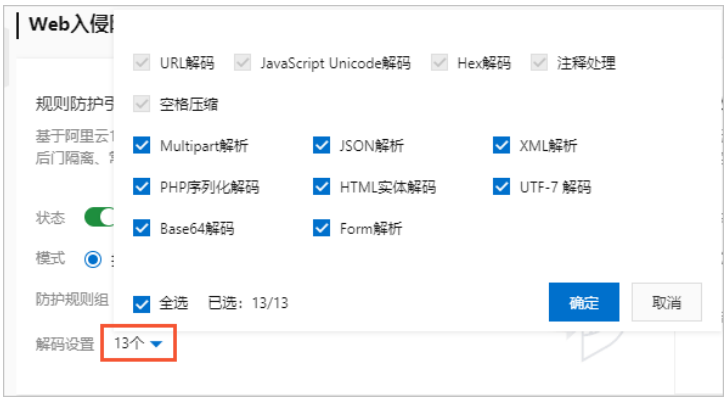
- **账户安全**：帮助您识别与账户关联的业务接口（例如注册、登录等）上发生的账户安全风险事件，具体包括撞库、暴力破解、垃圾注册、弱口令嗅探和短信验证码接口滥刷。

操作导航：在**网站防护**页面，单击**Web安全**页签，定位到**数据安全 > 账户安全**区域，单击**前去配置**，完成相关设置。具体操作，请参见设置账户安全。

我是专业的安全人员，需要做全面的Web入侵运营

针对您的需求，推荐您在完成网站接入后，为网站设置以下防护功能：

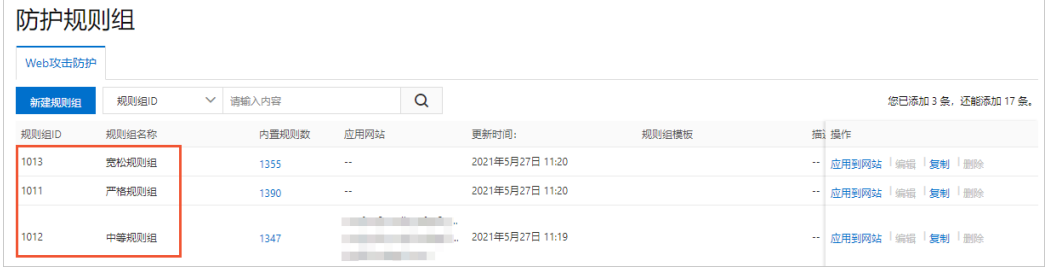
- **解码设置**：根据自身业务实际的编码情况，设置需要WAF防护引擎进行解码的内容格式，最大化地做到精确防护。选择合适的解码方式能够帮助WAF更好地识别流量。WAF默认应用全部13种解码方式，您可以过滤不需要的方式，避免不必要的解析和可能的误拦截。



操作导航：在**网站防护**页面，单击**Web安全**页签，定位到**Web入侵防护 > 规则防护引擎**区域，完成**解码设置**。具体操作，请参见设置规则防护引擎。

- **防护规则组**：基于内置的防护规则集进行删减，选择最适合您业务系统形态、框架、中间件等实际情况的防护规则集合，使用这些规则自定义Web攻击防护的防护规则组，并将其应用到网站。建议您使用防护规则组设置针对网站整体的Web入侵防御策略。如果仅是针对单个URL的防护策略，建议您使用自定义防护策略。

  操作导航：访问Web应用防火墙控制台的**系统管理 > 防护规则组**页面，自定义Web攻击防护的防护规则组，并将自定义规则组应用到网站。具体操作，请参见自定义防护规则组。



- **自定义防护策略**：为网站自定义访问控制（ACL）或访问限流策略。例如，限制某些接口只允许特定IP或者UA访问、限制某些特定类型请求的请求频率不能过高等。您也可以通过自定义防护策略防护CC攻击、

爬虫攻击或者某些特殊的Web攻击等。

操作导航：在**网站防护**页面，单击**访问控制/限流**页签，定位到**自定义防护策略**区域，完成相关设置。具体操作，请参见设置自定义防护策略。

- **深度学习引擎（告警模式）**：深度学习引擎基于云上每天上亿的威胁情报样本训练，能很好地弥补规则防护引擎的短板，特别是针对各种变形或未知的攻击特征。对于专业的安全人员，建议您先开启深度学习引擎的**告警**模式，观察一到两周被深度学习引擎检测出来的异常。如果没有明显问题，再切换到**拦截**模式。

操作导航：在**网站防护**页面，单击**Web安全**页签，定位到**Web入侵防护 > 深度学习引擎**区域，开启**状态**开关并将**模式**设置为**告警**。具体操作，请参见设置深度学习引擎。

- **主动防御（告警模式）**：主动防御基于对当前域名流量的学习建立正常流量的模型，包括请求参数的类型、长度、是否必须等信息。模型建成后，一旦发现请求不符合模型所描述的特征即告警。主动防御**告警**模式帮助您更有效地发现业务中的异常和威胁。如果被检测出来的请求对您的业务没有意义，则可以开启**拦截**模式。

操作导航：在**网站防护**页面，单击**Web安全**页签，定位到**高级防护 > 主动防御**区域，开启**状态**开关并将**模式**设置为**告警**。具体操作，请参见设置主动防御。

- **扫描防护（高频Web攻击封禁、目录遍历防护、扫描工具封禁、协同防御）**：扫描防护功能从情报、扫描器特征、扫描行为检测等多个维度，帮助您更好地降低来自扫描器的威胁。

操作导航：在**网站防护**页面，单击**访问控制/限流**页签，定位到**扫描防护**区域，开启全部功能并设置合适的阈值。具体操作，请参见设置扫描防护。

我的业务需要严格的安全防护，有攻击时宁可错杀不可漏掉

针对您的需求，推荐您在完成网站接入后，为网站设置以下防护功能：

- **规则防护引擎（严格规则组）**

操作导航：在**网站防护**页面，单击**访问控制/限流**页签，定位到**Web入侵防护 > 规则防护引擎**区域，将**防护规则组**设置为**严格规则组**。具体操作，请参见设置自定义防护策略。

- **深度学习引擎（拦截模式）**：深度学习引擎基于云上每天上亿的威胁情报样本训练，能很好地弥补规则防护引擎的短板，特别是针对各种变形或未知的攻击特征。在高强度防护场景下，建议您直接开启**拦截**模式。

操作导航：在**网站防护**页面，单击**Web安全**页签，定位到**Web入侵防护 > 深度学习引擎**区域，开启**状态**开关并将**模式**设置为**拦截**。具体操作，请参见设置深度学习引擎。

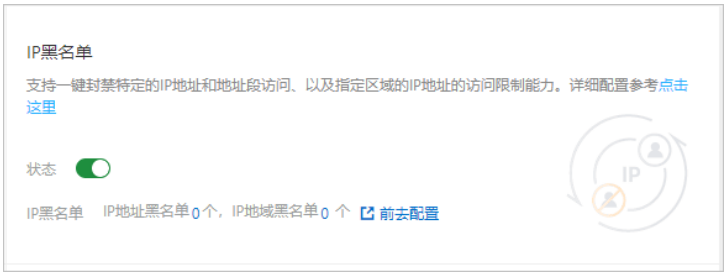
- **主动防御（拦截模式）**：主动防御基于对当前域名流量的学习建立正常流量的模型，包括请求参数的类型、长度、是否必须等信息。模型建成后，一旦发现请求不符合模型所描述的特征即告警。在高强度保护场景下，建议您直接开启**拦截**模式。

操作导航：在**网站防护**页面，单击**Web安全**页签，定位到**高级防护 > 主动防御**区域，开启**状态**开关并将**模式**设置为**拦截**。具体操作，请参见设置主动防御。

- **扫描防护（高频Web攻击封禁、目录遍历防护、扫描工具封禁、协同防御）**：扫描防护功能从情报、扫描器特征、扫描行为检测等多个维度，帮助您更好地降低来自扫描器的威胁。

操作导航：在**网站防护**页面，单击**访问控制/限流**页签，定位到**扫描防护**区域，开启全部功能并设置合适的阈值。具体操作，请参见设置扫描防护。

- **IP黑名单**：封禁与业务不相关的IP地址和地址段，以及指定地域区域的来源IP的访问请求。例如，不存在外省IP访问的地方政府论坛，可以将外省地区加入地域级黑名单；不存在海外用户的站点，可以将全部海外地区加入地域级黑名单。



操作导航：在**网站防护**页面，单击**访问控制/限流**页签，定位到**IP黑名单**区域，完成相关设置。具体操作，请参见设置IP黑名单。

我的业务经常受到爬虫骚扰或面临数据泄露、被篡改的风险

针对您的需求，推荐您在完成网站接入后，为网站设置以下防护功能：

- **数据风控**：数据风控适合防护针对特定接口发出的机器流量（例如脚本、自动化工具等），例如登录、注册、下单等场景。

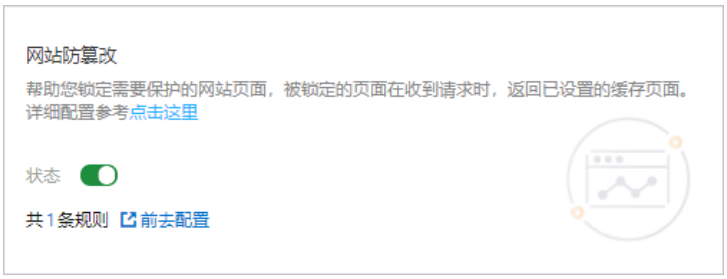
> **说明** 数据风控依赖于JS注入，只适用于网页环境。请不要在App中启用该功能。如果您不是很确定要防护的接口是否适用，请通过工单或钉钉联系我们帮助您判断。

操作导航：在**网站防护**页面，单击**Bot管理**页签，定位到**数据风控**区域，完成相关设置。具体操作，请参见设置数据风控。

- **防敏感信息泄露**：帮助您过滤服务器返回内容（异常页面或关键字）中的敏感信息，如身份证号、银行卡号、电话号码和敏感词汇等，进行打码显示。

操作导航：在**网站防护**页面，单击**Web安全**页签，定位到**数据安全 > 防敏感信息泄露**区域，完成相关设置。具体操作，请参见设置防敏感信息泄露。

- **网站防篡改**：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。



操作导航：在**网站防护**页面，单击**Web安全**页签，定位到**数据安全 > 网站防篡改**区域，完成相关设置。具体操作，请参见设置网站防篡改。

- **自定义防护策略**：例如您可以针对某些经常被爬取的静态页面一键开启JS验证，拦截大多数脚本和自动化程序。您也可以基于精细化的频率控制对访问过快的session等开启滑块校验。

操作导航：在**网站防护**页面，单击**访问控制/限流**页签，定位到**自定义防护策略**区域，完成相关设置。具体操作，请参见设置自定义防护策略。

- **账户安全**：帮助您识别与账户关联的业务接口（例如注册、登录等）上发生的账户安全风险事件，具体包括撞库、暴力破解、垃圾注册、弱口令嗅探和短信验证码接口滥刷。

操作导航：在**网站防护**页面，单击**Web安全**页签，定位到**数据安全 > 账户安全**区域，单击**前去配置**，完成相关设置。具体操作，请参见设置账户安全。

- **合法爬虫**：提供合法搜索引擎白名单（例如Google、Bing、百度、搜狗、Yandex等），方便您为域名设置放行合法爬虫的访问请求。

操作导航：在**网站防护**页面，单击**Bot管理**页签，定位到**合法爬虫**区域，完成相关设置。具体操作，请参见设置合法爬虫规则。

- **爬虫威胁情报**：提供拨号池IP、IDC机房IP、恶意扫描工具IP以及云端实时模型生成的恶意爬虫库等多种维度的爬虫威胁情报规则，方便您在全域名或指定路径下设置阻断恶意爬虫的访问请求。

操作导航：在**网站防护**页面，单击**Bot管理**页签，定位到**爬虫威胁情报**区域，完成相关设置。具体操作，请参见设置爬虫威胁情报规则。

- **App防护**：专门针对原生App端，提供可信通信、防机器脚本滥刷等安全防护，可以有效识别代理、模拟器、非法签名的请求。

操作导航：在**网站防护**页面，单击**Bot管理**页签，定位到**App防护**区域，完成相关设置。具体操作，请参见设置App防护。

9.2. 规则防护引擎最佳实践

本文介绍了使用Web应用防火墙（WAF）的规则防护引擎功能进行Web应用攻击防护的最佳实践，包含应用场景、防护策略、防护效果、规则更新四个方面。

应用场景

WAF主要帮助网站防御不同类型的Web应用攻击，例如SQL注入、XSS跨站攻击、远程命令执行、Webshell上传等攻击。关于Web攻击的更多信息，请参见常见Web漏洞释义。

> **说明** 主机层服务的安全问题（例如，Redis、MySQL未授权访问等）导致的服务器入侵不在WAF的防护范围之内。

设置防护策略

您在完成网站接入后，WAF的**规则防护引擎**功能默认开启，并使用正常模式的防护策略，为网站防御常见的Web攻击。您可以在**网站防护**页面定位到**规则防护引擎**区域，设置防护策略和查看规则防护引擎的防护状态。具体操作，请参见操作步骤。

防护状态解读

- **状态**：是否开启规则防护引擎模块，默认开启。
- **模式**：WAF检测发现网站的访问请求中包含Web攻击时要执行的动作，包含**拦截**和**告警**两种模式。
  - **拦截**模式：WAF自动拦截攻击请求，并在后台记录攻击日志。
  - **告警**模式：WAF不会拦截攻击请求，仅在后台记录攻击日志。
- **防护规则组**：规则防护引擎使用的防护规则合集，默认提供**中等规则组**、**严格规则组**、**宽松规则组**，分别表示正常、严格、宽松的检测强度。

- **中等规则组**：防护粒度较宽松且防护规则策略精准，可以拦截常见的具有绕过特征的攻击请求。
- **严格规则组**：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，相比中等规则组带来的误拦截可能更多。
- **宽松规则组**：防护粒度较粗，只拦截攻击特征比较明显的请求。

> **说明** 防护规则组设置仅在开启规则防护引擎后生效。

如果您开通了企业版或旗舰版的中国内地WAF实例，或者旗舰版的海外地区WAF实例，则您可以自定义防护规则组。自定义防护规则组允许您自由组合WAF提供的所有防护规则，形成有针对性的防护策略，并将其应用到网站防护。具体操作，请参见自定义防护规则组。

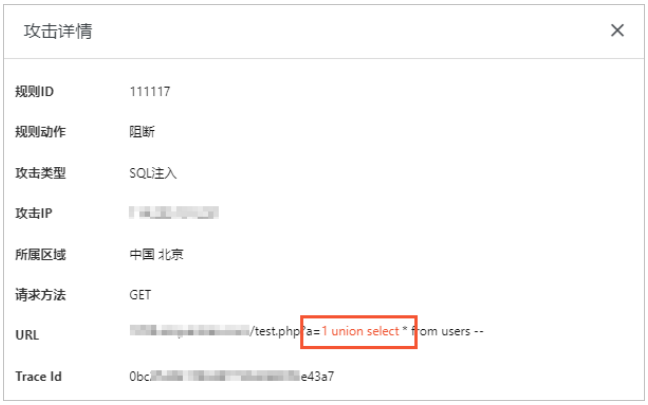
使用建议

- 如果您对自己的业务流量特征还不完全清楚，建议您先切换到**告警**模式进行观察。一般情况下，建议您观察一至两周，然后分析告警模式下的攻击日志：
  - 如果没有发现任何正常业务流量被拦截的记录，则可以切换到**拦截**模式。
  - 如果发现攻击日志中有正常的业务流量，您可以联系阿里云安全专家（更多信息，请参见安全专家指导服务），沟通具体的解决方案。
- PHPMyAdmin、开发技术类论坛接入WAF防护可能会存在误拦截的问题，建议您联系阿里云安全专家（更多信息，请参见安全专家指导服务），沟通具体的解决方案。
- 业务操作方面应注意以下问题：
  - 正常业务的HTTP请求中尽量不要直接传递原始的SQL语句、JavaScript代码。
  - 正常业务的URL尽量不要使用一些特殊的关键字（UPDATE、SET等）作为路径，例如 `www.aliyundoc.com/abc/update/mod.php?set=1` 。
  - 如果业务中需要上传文件，不建议直接通过Web方式上传超过50 MB的文件，建议使用OSS或者其他方式上传。更多信息，请参见开始使用OSS。

查看防护效果

开启规则防护引擎后，您可以在**安全报表**页面查询**Web安全 > Web入侵防护**报表，了解规则防护引擎的防护记录。具体操作，请参见WAF安全报表。

Web入侵防护报表支持查询最近30天内的攻击记录。报表下方提供了详细的攻击记录列表，您可以筛选出**规则防护**记录，然后单击某条记录后的**查看详情**，查询攻击详情。例如，下图中的**攻击详情**表示一条已被WAF拦截的SQL注入请求。



> **说明** 如果您发现WAF误拦截了正常的业务流量，建议您先通过**Web入侵防护白名单**功能，对受影响的URL配置白名单策略，然后联系阿里云安全专家（更多信息，请参见安全专家指导服务），沟通具体的解决方案。具体操作，请参见设置Web入侵防护白名单。

查看规则更新通知

对于互联网披露的已知漏洞和未披露的0day漏洞，WAF将及时完成防护规则的更新并发布规则更新通知。您可以在**产品信息**页面，查询WAF最新发布的**规则更新通知**。具体操作，请参见查看产品信息。

> **说明** Web攻击往往存在不止一种概念证明方法（Proof of Concept，简称PoC），阿里云安全专家会对漏洞原理进行深度分析，从而确保发布的Web防护规则覆盖已公开和未公开的各种漏洞利用方式。

更多信息

安全管家服务可以为您提供包括安全检测、安全加固、安全监控、安全应急等一系列专业的安全服务项目，帮助您更加及时、有效地应对漏洞及黑客攻击。更多信息，请参见安全管家服务。

9.3. CC攻击防护最佳实践

本文介绍了常见的CC攻击场景，并结合阿里云Web应用防火墙WAF（Web Application Firewall）的相关功能给出具体的防护策略和配置，帮助您有针对性地防御CC攻击。

概述

您可以从以下不同的CC攻击防护场景中选择贴近您自身实际需求的场景，了解相关的防护设置：

- 大流量高频CC攻击
- 攻击源来自海外或公有云
- 请求特征畸形或不合理
- 滥刷接口（登录、注册、短信、投票等）
- 恶意扫描
- App攻击
- 恶意爬取

大流量高频CC攻击

在大规模CC攻击中，单台傀儡机发包的速率往往远超过正常用户的请求频率。针对这种场景，直接对请求源设置限速规则是最有效的办法。推荐您使用WAF**自定义防护策略**功能的**频率设置**，配置限速策略，具体操作，请参见设置自定义防护策略。

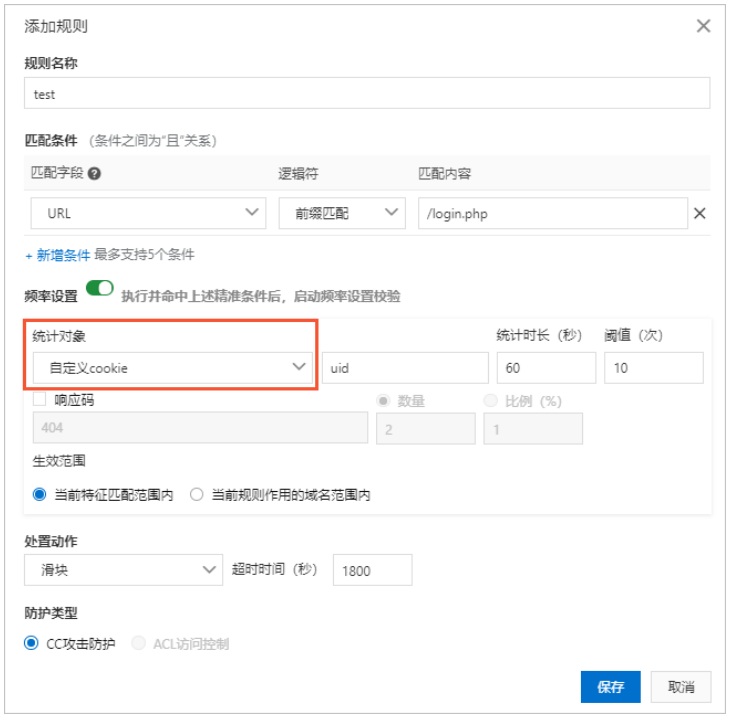
配置示例：您可以配置以下规则，当一个IP在30秒内访问当前域名下任意路径的次数超过1000次，则封禁该IP的请求10个小时。该规则可以作为一般中小型站点的预防性配置。

在实际场景中，您需要根据自身业务需求调整防护路径和触发防护的阈值，并选择合适的处置动作，以达到更有针对性、更精细化的防护效果。例如，为了预防登录接口受到恶意高频撞库攻击的影响，您可以配置登录接口的地址（示例：使用**前缀匹配**逻辑符，将**匹配内容**设置为`/login.php`），并设置60秒内超过20次请求则进行封禁。

在使用CC防护时，请注意以下内容：

- **处置动作**中的**滑块**和**严格滑块**验证用于校验请求是否来自于真实浏览器（而非自动化工具脚本），适用范围仅限于网页或H5，不适用于原生App、API等环境。针对原生App、API等环境，请将**处置动作**设置为**阻断**。
- 针对有可能被CC攻击防护策略误伤的接口或IP，您可以通过**访问控制/限流**白名单功能将其统一加白。具体操作，请参见设置访问控制/限流白名单。
- 请勿对App、API环境开启**CC安全防护**的**防护-紧急**模式。

如果您开通了旗舰版的WAF实例，则您可以在频率设置中使用除IP和Session外的自定义统计对象字段，设置更细粒度、更多维度的限速功能。例如，由于针对IP的封禁会影响NAT出口，您可以使用cookie或者业务中自带的用户级别参数作为统计对象。下图配置针对业务中标记用户的cookie（假设cookie格式为 `uid=12345` ）进行统计，并使用滑块作为处置动作，避免误拦截。



攻击源来自海外或公有云

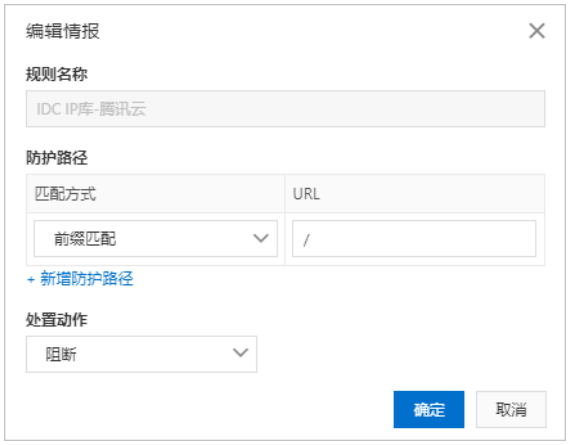
CC攻击中经常出现很大比例的攻击来源于海外IP、公有云IP、IDC机房IP的情形。

对于面向中国用户的站点，在遭受攻击时可以通过封禁海外访问来缓解攻击压力。推荐您使用WAF的**地域级IP黑名单**功能，封禁中国境外IP地址的访问，具体操作，请参见设置IP黑名单。

如果您已经开启了WAF的**Bot管理**模块，则您可以使用**爬虫威胁情报**功能，封禁常见IDC IP库的爬虫IP，例如阿里云、腾讯云、IDC机房的IP段。

> **说明** 许多爬虫程序选择部署在云服务器上，而正常用户很少通过公有云和IDC的源IP访问您的业务。

配置示例：您可以开启以下爬虫威胁情报规则，封禁腾讯云爬虫IP的访问。具体操作，请参见设置爬虫威胁情报规则。



请求特征畸形或不合理

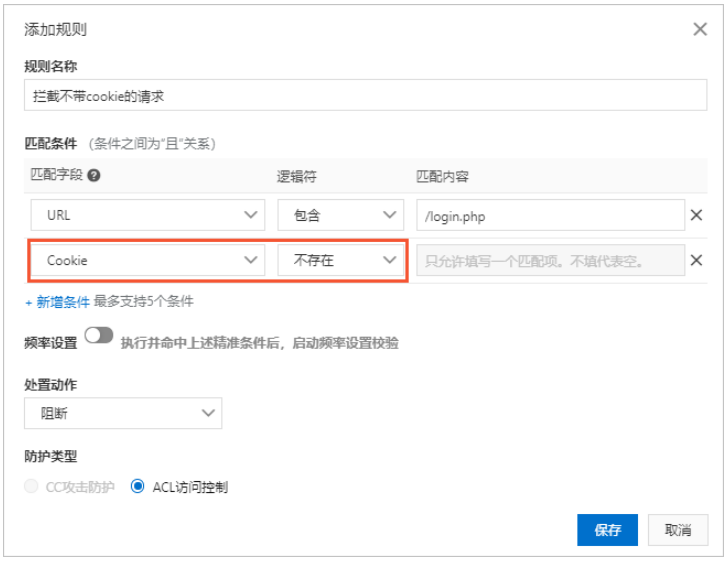
由于很多CC攻击请求是攻击者随意构造的，在仔细观察日志后，往往会发现这些请求有很多与正常请求不相符的畸形报文特征。常见的畸形报文特征包括：

- user-agent异常或畸形：例如，包含Python等自动化工具特征、明显格式错乱的UA（例如 `Mozilla///` ）、明显不合理的UA（例如 `www.example.com` ）。如果存在以上请求特征，可以直接封禁请求。
- user-agent不合理：例如，对于微信推广的H5页面，正常用户都应该通过微信发起访问，如果UA来自于Windows桌面浏览器（例如MSIE 6.0），则明显是不合理的。如果存在以上请求特征，可以直接封禁请求。
- referer异常：例如，不带referer或referer固定且来自于非法站点，则可以封禁这种请求（访问网站首页或第一次访问页面的情形除外）。针对只能通过某个站内地址跳转访问的URL，您可以从referer角度分析行为异常，决定是否封禁。
- cookie异常：正常用户往往会在请求中带上属于网站本身业务集的一些cookie（第一次访问页面的情形除外）。很多情况下，CC攻击的报文不会携带任何cookie。您可以从这个角度出发，封禁不带cookie的访问请求。
- 缺少某些HTTP header：例如，针对一些业务中需要的认证头等，正常用户的请求会携带，而攻击报文则不会。
- 不正确的请求方法：例如，本来只有POST请求的接口被大量GET请求攻击，则可以直接封禁GET请求。

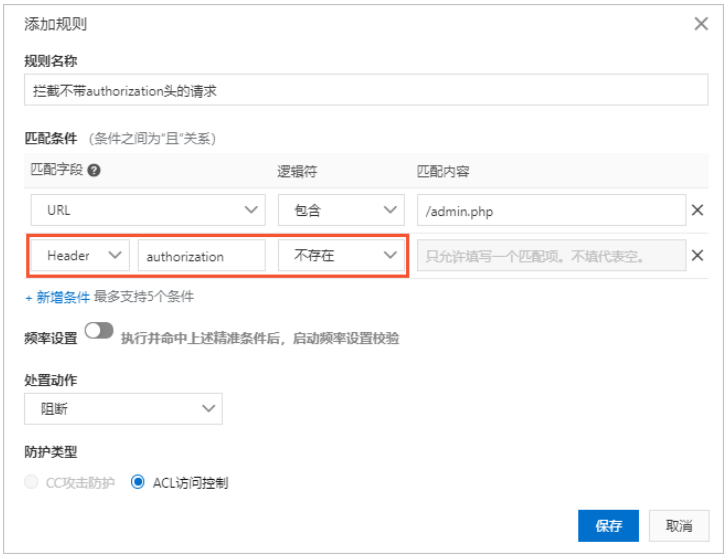
对于上述异常的请求特征，您都可以在特征分析的基础上，使用WAF**自定义防护策略**的**ACL访问控制**规则设置对应的封禁策略。具体操作，请参见设置自定义防护策略。

配置示例：

- 拦截不带cookie的请求。



- 拦截不带authorization头的请求。



滥刷接口（登录、注册、短信、投票等）

对于网页环境（包括H5）中的一些关键接口，例如登录、注册、投票、短信验证码等，推荐您使用数据风控功能进行防护。

数据风控在关键接口页面中插入JS代码，采集用户在页面上的操作行为和环境信息，综合判断发送至关键接口的请求是否来自于真实的用户（而不是自动化工具脚本）。数据风控判定的依据主要来自于人机识别的结果，跟发送请求的频率、来源IP没有关系，针对一些低频、分散的攻击请求有很好的效果。

> **注意** 数据风控的判定依赖于开启防护后在正常请求中附带的验证参数，该功能不适用于不能执行JS的环境（例如API、Native App等）。为避免误拦截，建议您在启用数据风控前先在测试环境进行测试，或是先开启观察模式并跟云盾工程师确认后，再开启防护模式。

具体操作，请参见设置数据风控。

恶意扫描

大规模的扫描行为会给服务器带来很大压力，除了限制访问请求频率外，您还可以使用**扫描防护**功能来加强防护效果。扫描防护支持以下设置：

- **高频Web攻击封禁**：自动封禁连续触发Web防护规则的客户端IP。
- **目录遍历防护**：自动封禁在短时间内进行多次目录遍历攻击的客户端IP。
- **扫描工具封禁**：自动封禁来自常见扫描工具或阿里云恶意扫描攻击IP库中IP的访问请求。
- **协同防御**：自动阻断阿里云全球恶意扫描攻击IP库中IP的访问请求。

具体操作，请参见设置扫描防护。

App攻击

针对App攻击，除上述频率设置、地域级IP黑名单、ACL访问控制等手段，您也可以接入云盾SDK进行防护。

SDK方案通过将SDK集成到App中，对请求进行安全签名和校验，并结合各种硬件信息，综合识别请求是否来自于合法的App。只要不是来自于官方App的合法请求，一概拦截。这是一种“白名单”思路，只放行合法的请求，而不用去分析非法请求的特征。

SDK防护需要开启**App防护**模块后才可以使用。具体操作，请参见设置App防护。

恶意爬取

对于很多资讯类网站（例如征信、租房、机票、小说等），大量的爬虫往往会造成带宽增大、负载飙升等异常，以及数据泄露等问题。针对爬虫问题，如果上述手段不能起到很好的防御效果，推荐您开启并使用**Bot管理**模块，更有针对性地防御爬虫。具体操作，请参见设置Bot管理白名单。

9.4. 账户安全最佳实践

Web应用防火墙（WAF）的账户安全功能为您提供账户风险的识别能力。本文针对如何防护账户风险给出不同攻击场景和业务场景下的防护建议，指导您更好地保护自己业务中与账户关联的接口。

背景信息

WAF支持账户安全检测，在Web攻击防护基础上帮助您识别与账户关联的业务接口（例如注册、登录接口等）上发生的账户安全风险事件，具体包括撞库、暴力破解、垃圾注册、弱口令嗅探和短信验证码接口滥刷。配置WAF账户安全检测后，您可以在WAF安全报表中查看相关检测结果。更多信息，请参见设置账户安全。

使用验证码（适用于普通网页或H5）

为普通PC页面或H5页面启用验证码是防护重点接口的最简单和有效的手段。接入验证码服务通常需要您在业务代码中做少许改动，一般一至二个工作日即可完成。

一般的验证码能够有效拦截使用简单工具脚本发起的接口直接调用，但随着黑灰产攻击手段和攻击工具的进化，普通的验证码越来越容易被绕过。当您需要更高强度的攻防对抗时，建议您选择专业的验证码服务，例如阿里云验证码服务。

阿里云验证码服务基于阿里巴巴集团多年来对抗黑灰产的经验所形成的一套完整的人机识别和风控体系，提供包括无痕验证在内的多种验证方式，帮助您有效对抗职业黑灰产的攻击，同时避免对正常用户的干扰。

更多信息，请参见人机验证在线体验页面。

使用SDK签名（适用于App）

对于不适合使用验证码的原生App，阿里云提供了一套SDK方案。SDK方案通过采集移动端的各种硬件信息、环境信息，并且对请求进行签名和验签，确保只有通过合法的官方App（而不是来自脚本、自动化程序、模拟器等非正常途径）发出来的请求才会被放行回源站。

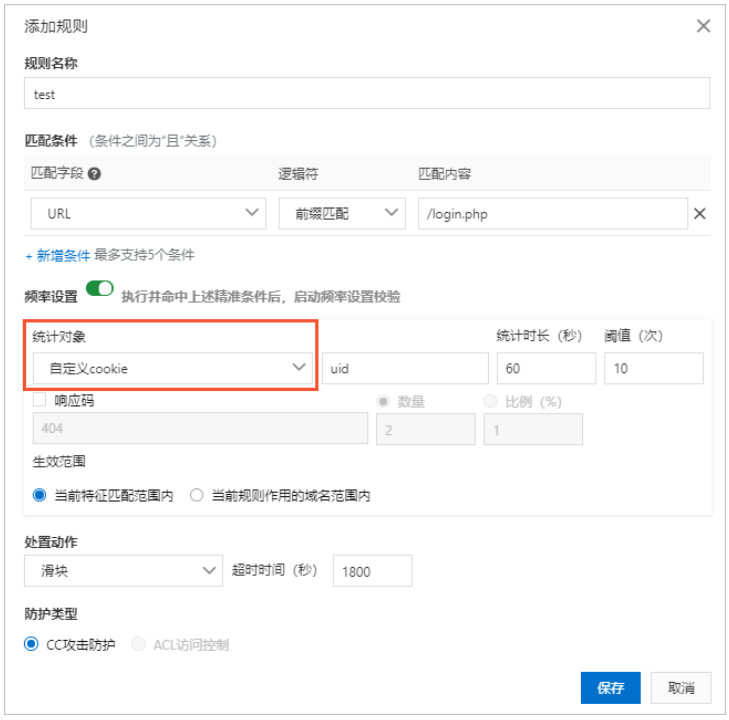
> **说明** 您必须先开通Web应用防火墙的**App防护**模块，才能使用SDK方案。更多信息，请参见App防护概述。

多维度的频次限制（适用于高频攻击）

对于攻击请求中包含某个高频特征字段（例如IP、session、cookie、参数、header等）的行为，您可以使用多维度的频次限制，将攻击源拉黑。例如，当攻击请求使用大量代理、秒拨IP，但复用同一个登录态的cookie（例如uid）时，您可以基于cookie设置限速，这样就将防护对象由原始的IP转变为跟业务逻辑有关的“账号”维度。

推荐您使用WAF**自定义防护策略**中的**频率设置**，以下是频率设置的配置示例。具体操作请参见设置自定义防护策略。

> **说明** 只有旗舰版的Web应用防火墙实例支持在**频率设置**中使用除IP和Session外的自定义统计对象字段，例如自定义cookie、自定义header、自定义参数。



分析异常的请求特征

对于绝大部分攻击，通过细心观察和分析，总会发现攻击请求与正常用户请求在特征上的差异。以下是一些常见的异常请求特征，供您参考。

- HTTP Header不完整。例如缺失referer、cookie、content-type等字段。
- User-agent的值异常。例如对于普通Web站点的请求中出现大量Java或是Python的UA特征，或者对于微信小程序应用的请求中出现大量桌面版PC浏览器的UA特征等。
- Cookie不完整。一般的应用都会有多个具备业务含义的cookie，例如SessionID、userid、deviceid、lastvisit等，而爬虫程序在编写的时候有可能只会提交获取结果所必需的一到二个cookie，而缺少其他具有业务含义的cookie。
- 参数内容异常。类似cookie异常，有些参数对于爬虫来说意义不大，缺失或者重复提交都不影响获取结果，这也可以作为同一类异常来处理。
- 业务字段异常。例如邮箱、手机号、账户信息中包含某一些异常或不合理的关键字等。

推荐您使用WAF日志服务进行日志查询，方便您快速地分析请求特征，例如Top IP排序、某一特征在整体流量中的占比等。

> **说明** 您必须先开通Web应用防火墙的**日志服务**模块，才能使用日志服务。更多信息，请参见步骤1：开通WAF日志服务。

开启撞库、爬虫威胁情报

WAF的**Bot管理**模块将基于阿里云全网流量监测到的有撞库行为聚集的恶意IP通过算法提取出来，形成撞库IP情报库，并动态更新。您可以使用Bot管理模块的**爬虫威胁情报**功能，一键开启撞库IP检测（观察模式）或是对命中的IP进行拦截、滑块验证等处置。更多信息，请参见设置爬虫威胁情报规则。

> **说明** 您必须先开通Web应用防火墙的**Bot管理**模块，才能使用**爬虫威胁情报**功能。

使用安全托管服务

如果上述解决方案都不能满足您的防护需求，或者防护效果不够理想，或是您希望有专业的安全团队直接帮助您解决问题，推荐您使用安全托管服务。阿里云提供专业的攻防技术团队，根据您的具体业务场景和需求来定制防护方案，并提供实时的分析、监控、攻防对抗，最大程度地保证防护效果。

更多信息，请参见安全托管服务。

9.5. 使用自定义规则组提升Web攻击防护效果

当您发现网站业务的正常请求被Web应用防火墙的规则防护引擎误拦截时，您可以通过自定义防护规则组的方式避免该类误拦截。

前提条件

- 已开通了Web应用防火墙，且实例满足以下要求：
  - 使用包年包月方式开通。

    > **说明** 按量付费开通的Web应用防火墙实例暂不支持使用防护规则组。

  - 如果实例地域是**中国内地**，则实例套餐必须是**企业版**及以上规格。
  - 如果实例地域是**非中国内地**，则实例套餐必须是**旗舰版**及以上规格。

  更多信息，请参见开通Web应用防火墙。
- 已完成网站接入。具体操作，请参见网站接入概述。

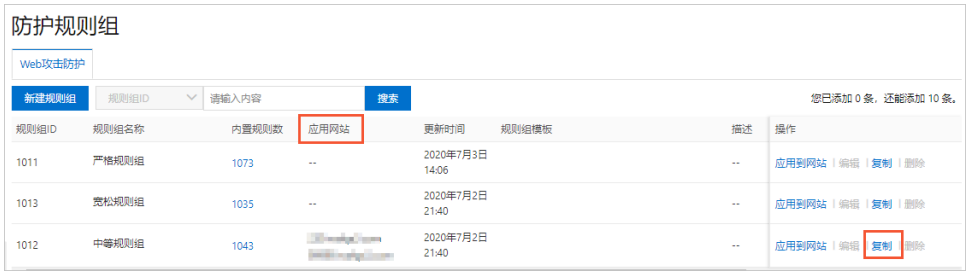
背景信息

当业务正常请求被WAF的规则防护引擎误拦截时，您首先要确定触发本次拦截的防护规则ID，然后为网站域名设置自定义防护规则组，移除造成误拦截的规则，使WAF针对受影响的网站业务不再拦截同样的正常请求。

操作步骤

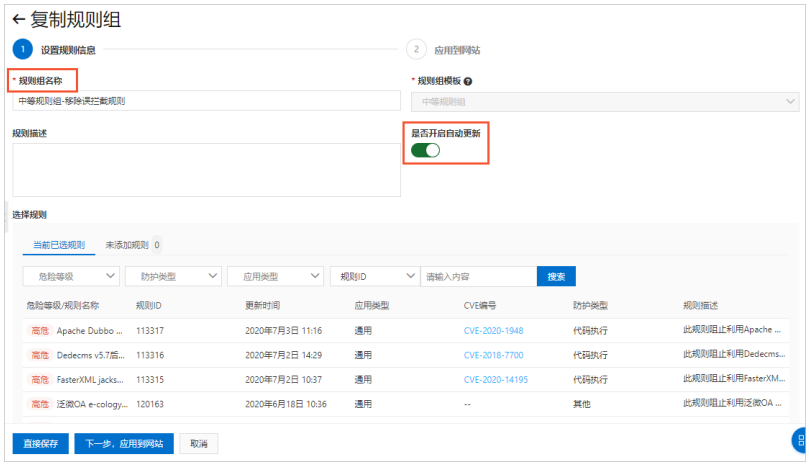
1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**非中国内地**）。
3. 在左侧导航栏，选择**安全运营 > 安全报表**。
4. 获取触发误拦截的WAF防护规则ID。
   i. 查询**Web安全 > Web入侵防护**报表，选择发生误拦截的网站域名，并在下方攻击记录列表中筛选出**规则防护**攻击记录。
   ii. 在**规则防护**攻击记录列表中，定位到误拦截记录（可以使用攻击IP筛选），记录对应的**规则ID**。
5. 在左侧导航栏，选择**系统管理 > 防护规则组**。
6. 自定义防护规则组，移除造成误拦截的防护规则。
   i. 在**Web攻击防护**规则组列表中，定位到发生误拦截的网站域名所应用的规则组。

   > **说明** 您可以在**应用网站**列搜索发生误拦截的网站域名，定位到目标规则组。

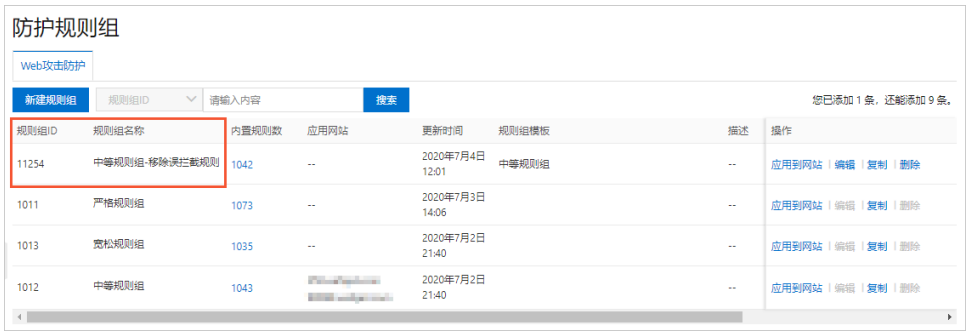
   

   ii. 单击目标规则组操作列下的**复制**（假设造成误拦截的是**中等规则组**）。

iii. 在**复制规则组**页面，修改**规则组名称**（示例：中等规则组-移除误拦截规则），开启**是否开启自动更新**开关，并单击**直接保存**。



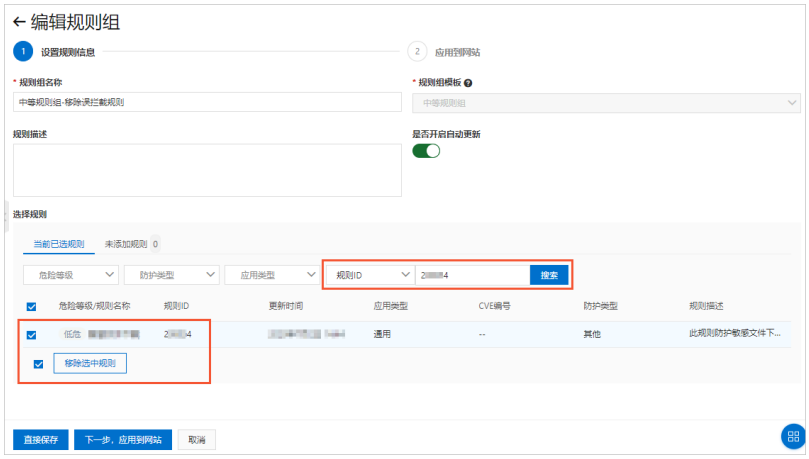
成功复制规则组后，您可以在规则组列表中查看复制生成的规则组。



iv. 定位到复制生成的规则组，单击其操作列下的**编辑**。

v. 在**编辑规则组**页面，使用**规则组ID**搜索造成误拦截的规则，选中规则，并单击**移除选中规则**。

> 注意 在将防护规则从自定义规则组移除时，请务必确认防护规则误拦截了网站业务的正常请求。

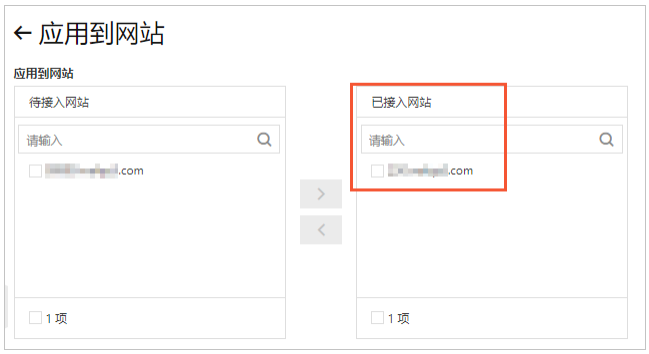


vi. 单击**直接保存**。

7. 为网站应用自定义防护规则组。

i. 定位到复制生成的规则组，单击其操作列下的**应用到网站**。

ii. 在**应用到网站**页面，将发生误拦截的网站域名添加到**已接入网站**，并单击**保存**。



自定义规则组应用完成后，您可以在**网站防护**页面查看网站域名的**规则防护引擎**设置，其中**防护规则组**将变更为所应用的自定义规则组。具体操作，请参见设置规则防护引擎。

当网站域名再次收到同样的访问请求时，WAF不会对其拦截。

> **说明** 如果访问请求仍然被WAF拦截，您可以根据上述步骤再次确定本次触发拦截的防护规则ID，并在自定义规则组中将该规则移除，避免误拦截。