阿里云
Web应用防火墙

旧版引擎指南

文档版本：20200702

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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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
	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。	 **禁止：** 重置操作将丢失用户配置数据。
	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。
	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。
	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。	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 防护引擎全面升级

自2020年3月11日起，Web应用防火墙将陆续为所有老用户全面升级防护引擎，为您提供更全面的防护能力和更便捷的操作体验。

升级至新版防护引擎后，您将获得以下体验升级：

- 防护体验全面升级

  分类聚合后的防护模块，从Web入侵防护、数据安全、Bot管理、访问控制/限流等多维度为您的业务提供全面防护。

  同时，更强大的精准限流能力和账户安全防护能力，帮助您有效抵御非法流量访问、CC攻击、撞库、弱口令攻击、暴力破解等威胁。升级后的趋势分析报表，为您更直观地展示防护效果，安全可视。
- 自定义防护策略满足精细化限流需求

  自定义策略防护支持更多精准访问控制字段和规则数，为您提供复杂条件下的精准限流访问能力，满足各种业务场景下的非法访问请求限制管理。

  - 原自定义CC防护规则整合至自定义防护策略，提供更精准的限流能力。详细信息，请参见#unique_4。
  - 原精准访问控制规则中的特定流量放行配置调整至各防护功能模块对应的白名单规则配置，提供更便捷的合法流量配置方式。详细信息，请参见#unique_5。
- 更便捷的IP黑名单配置体验

  一键添加基于IP、IP段以及IP所属地域的黑名单，实现访问控制的快捷操作，方便您快速拦截特定流量。

防护能力/用户体验-全面升级

自定义防护能力
强势升级

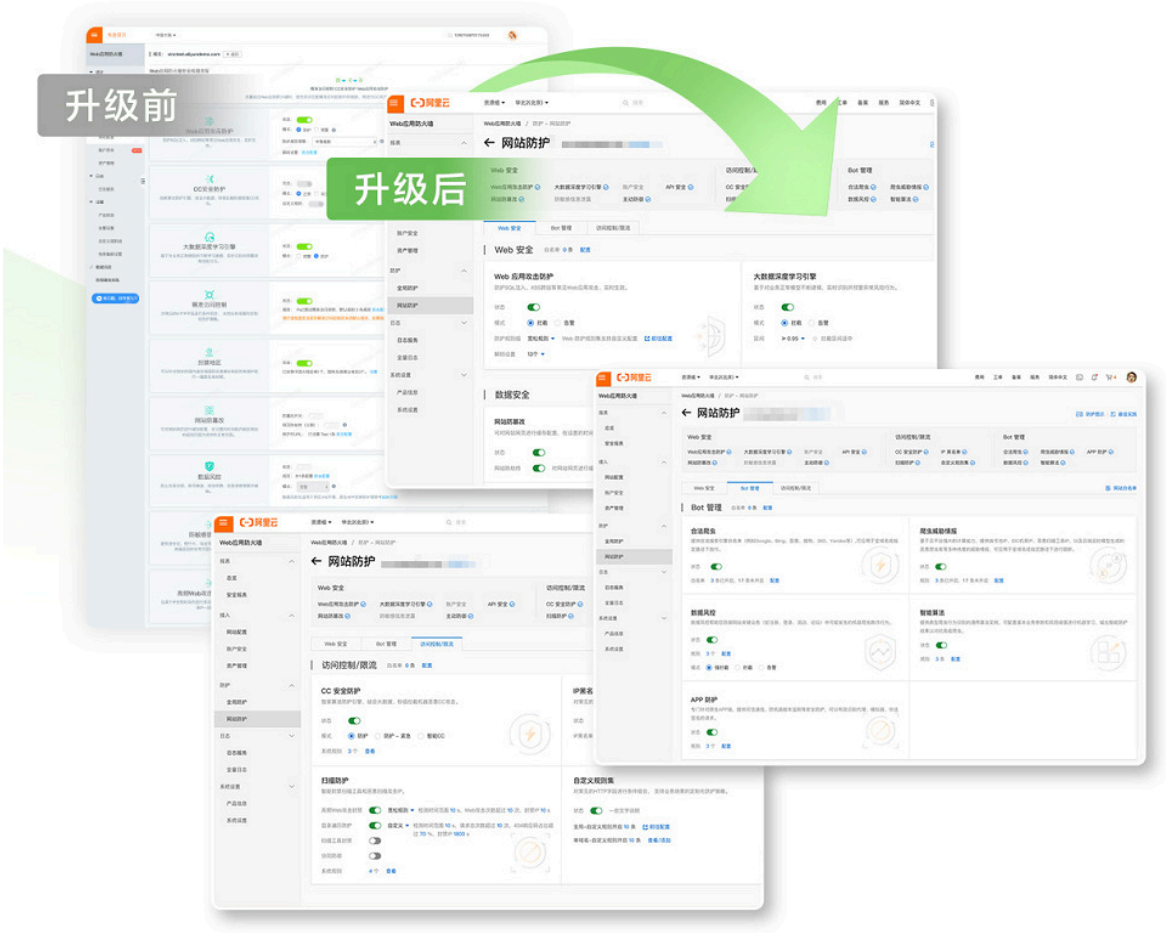
账户安全防护能力
隆重上线

扫描防护详情
可视化呈现

多种白名单管理
全面发布

Bot管理能力
重磅推出

自定义防护能力全面升级



频次限流防护能力升级

频次规则的流量范围条件由单维（url）升级到多维（全部精准条件），限流目标由源IP提升至源IP、用户、自定义header和参数等多个条件，完美支持各种复杂业务访问流量管理，更强大！

频次规则支持高级自定义

支持用户自定义频次限流访问规则的限流名单库的生效范围，规则防护范围随您把控，更安全！

精准访问控制条件升级

自定义规则组合参数扩充支持“源IP所属区域”条件，规则组合条件数量升级支持5个不同的复杂条件，有效支持精细化流量的访问控制，更精细！

IP黑名单实现一键拉黑

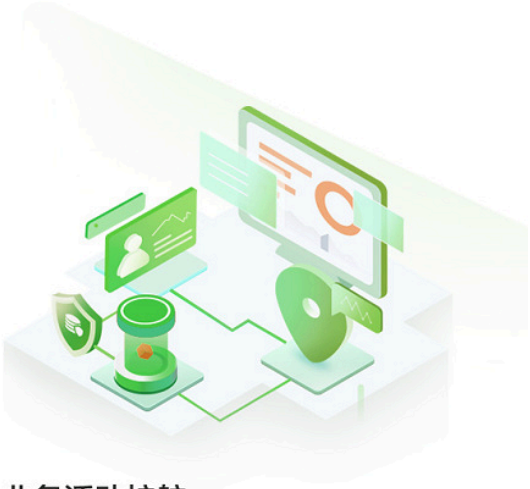
支持用户快捷的一键拉黑指定的源IP或地址段、以及流量来源地域的流量封禁，更快捷！

防护模块级别的白名单策略、扫描防护报表、放行优先的规则生效顺序等更多功能，等您发现。更多详细信息，请参见网站防护（新版引擎）相关文档。

全新防护场景

CC攻击和爬虫攻击防护：

支持随“心”所欲自定义精细化频次限流防护策略，提供智能防御的Bot管理能力，强力缓解恶意流量攻击对系统及业务造成的安全威胁



业务活动护航：

通过灵活的自定义访问控制防护策略和自定义支持频次防护策略能力，结合业务活动的目标用户的访问流量特征、用户来源设备、地域等多种组合特性，进行精细化防护配置，为业务安全保驾护航。

撞库、爆破，弱口令攻击防护：

账户安全上线拦截能力，可一键开启对抗账户相关的攻击行为的防护能力，全面保障账户安全。

扫描防护：

默认开启扫描防护和协同防护，云端威胁情况效应最大化，助力各种扫描探测拦截，将风险扼杀在摇篮节点。

升级方法

我们将陆续为所有2020年1月前开通Web应用防火墙的老用户安排防护引擎升级。当后端防护引擎升级完成后，您登录Web应用防火墙控制台时将收到升级提示，单击**立即体验**即可享受全新防护引擎为您带来的体验升级。

说明：

本次升级暂不包含海外地域WAF实例，请您耐心等待。

2 使用透明代理模式接入WAF

如果您的源站服务器部署在具有公网IP的阿里云ECS实例，则您可以使用透明代理模式将网站接入Web应用防火墙进行防护。透明代理模式的配置简便，无需修改域名DNS解析，支持直接牵引源站ECS的流量到Web应用防火墙进行防护。

前提条件

- 已开通包年包月的Web应用防火墙服务，且使用旧版防护引擎。

  注意：
  透明代理模式目前仅对旧版防护引擎开放。如果您使用的是新版防护引擎，建议您使用DNS配置模式进行网站接入。更多信息，请参见#unique_8。
- 源站服务器部署在华北2（北京）地域的阿里云ECS实例，且源站ECS实例拥有公网IP或已绑定弹性公网IP（EIP）。

  说明：
  透明代理模式暂不支持通过负载均衡SLB的公网IP牵引源站ECS实例的流量。

背景信息

使用透明代理模式将网站接入Web应用防火墙进行防护后，源站ECS实例的公网IP 80端口接收到的HTTP协议的流量将被直接牵引到Web应用防火墙，经Web应用防火墙处理后返回到源站服务器。

使用透明代理模式接入Web应用防火墙具有以下优势：

- 自动支持基于目标ECS、EIP（源站服务器）的全流量防护，避免因未配置源站保护而导致的潜在安全风险。
- 自动透明的流量牵引，无需修改域名DNS解析，避免对业务造成影响。

透明代理模式需要您授权Web应用防火墙读取ECS实例信息。配置过程中只需添加域名和选择对应的服务器IP即可。

注意：
除了透明代理模式，您还可以使用DNS配置模式接入Web应用防火墙。透明代理模式和DNS配置模式只能选择一种，即如果使用透明代理模式，必须先清空DNS配置模式下的域名配置记录。关于使用DNS配置模式接入Web应用防火墙的更多信息，请参见#unique_8。

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**、）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 在**网站配置**页面顶部菜单栏，选择**透明代理模式**。

> **注意：**
> 如果您已经使用DNS配置模式接入网站到Web应用防火墙，则必须先清空DNS配置模式下的域名记录，才能使用透明代理模式。

5. （可选） 授权Web应用防火墙访问ECS实例信息。

> **说明：**
> 首次使用透明代理模式时，您需要授权Web应用防火墙访问您的ECS实例信息。若已完成过授权，请跳过此步骤。

a) 单击**立即授权**。

> **说明：**
> 如果您已经完成授权，则**立即授权**按钮不会出现。

b) 在**云资源访问授权**页面，单击**同意授权**。

完成授权后，页面将跳转到**添加域名**页面。

6. （可选） 单击**添加域名**。

> **说明：**
> 如果您刚刚完成上一步授权操作，请跳过此步骤，直接参照下一步进行后续操作。

7. 在**添加域名**页面，输入要防护的**域名**，并从**服务器IP**列表中选择域名对应的源站ECS IP地址，单击**确定**。

   服务器IP列表罗列了Web应用防火墙读取到的当前阿里云账号下符合前提条件的ECS IP地址。

   > **注意：**
   > 选择服务器IP表示允许将该IP的80端口接收到的HTTP协议访问流量牵引至Web应用防火墙进行分析、处理。

   成功添加域名后，自动触发流量牵引。Web应用防火墙将依据域名对应的防护策略检测访问请求，并将处理后的正常请求返回到源站服务器。

8. （可选） 管理服务器IP。

a) 在域名列表右上方，单击**服务器IP管理**。

b) 在服务器IP列表的**状态**列查看IP的流量牵引状态。

流量牵引状态的说明如下：

- **已牵引**：表示该服务器IP 80端口接收到的所有HTTP协议流量已自动牵引到Web应用防火墙。
- **牵引中**：表示正在牵引流量。
- **牵引失败**：表示流量牵引失败。
- **删除中**：表示正在移除该IP。

c) 对于不再需要流量牵引的服务器IP，您可以在单击其操作列下的**删除**。

注意：

在**网站配置**页面删除域名时，对应的服务器IP流量牵引不会随之删除。要取消流量牵引，您必须在**服务器IP管理**中执行删除操作。

3 网站防护（旧版引擎）

3.1 使用概览

本文介绍在开通和使用阿里云Web应用防火墙（WAF）过程中的常用操作和最佳实践，便于您快速了解WAF，熟悉配置方法。

WAF使用流程

WAF是阿里云云盾提供的Web应用防火墙，帮助您监控网站上的HTTP/HTTPS访问请求，并通过自定义过滤规则和启用Web攻击防护等功能，帮助您部署网站访问控制。

参照以下步骤使用WAF：

1. 开通WAF并将网站接入WAF，使网站的访问流量全部流转到WAF进行监控。
2. 完成接入后，配置WAF防护功能。WAF将按照配置的防护策略检测并过滤恶意访问请求，只放行合法请求到源站服务器。
3. WAF正常工作后，随时查看WAF安全报表，了解业务和安全信息；或通过设置功能，查看WAF资源使用情况，调整告警配置等。
4. 应用WAF最佳实践，完善安全管理；联系安全专家，解决技术问题。

开通WAF

支持通过按量付费或包年包月的计费方式开通WAF。

- 按量付费：按当日被防护网站的访问QPS峰值和当日选用的WAF防护功能，生成后付费账单；每日结算前一日费用。
- 包年包月：按月/年计费，选购适用的WAF套餐，生成账单后直接付费；在选购的时长内享用套餐内的防护服务。

开通WAF后，您将获得一个WAF实例（对应一个WAF IP）；您可以使用这个WAF实例接入防护最多10个域名，为其开启防护，这10个域名只能使用同一个一级域名。

操作导航

- WAF计费方式
- 开通Web应用防火墙
- WAF续费与升级
- 关闭Web应用防火墙

WAF实例规格

- WAF版本功能说明

  WAF包年包月模式提供高级版、企业版、旗舰版、独享版四种规格。您可以根据要防护网站的业务规模和实际防护需求，选择合适的规格。

- （仅按量付费）功能与规格配置

  按量付费模式支持实时调整WAF的功能与规格，享受更贴近业务现状的安全防护。功能与规格调整保存后实时生效；每日账单依据当天最高配置进行计算。

- 额外带宽

  通过包年包月方式选购WAF套餐时，我们需要了解您的正常业务流量，以便区分DDoS攻击等异常流量。每种WAF套餐支持不同的业务带宽，如果您的实际业务正常流量大于套餐内的带宽限制，您需要购买额外带宽。

- 域名扩展包

  如果您希望防护具有不同一级域名的网站，您需要购买域名扩展包。

- 独享IP包

  如果您有很重要的域名需要单独防护，而非使用同一个WAF IP防护所有域名，您可以购买独享IP包。

接入WAF

开通WAF后，您可以使用透明代理模式或DNS配置模式将网站接入WAF进行防护。

> **注意：**
> 透明代理模式和DNS配置模式只能选择一种，即如果要使用透明代理模式，必须先清空DNS配置模式下的域名配置记录，反之亦然。

- 透明代理模式：将所配置的源站服务器公网IP的80端口接收到的HTTP协议的流量直接牵引到WAF，经WAF处理后再将正常的访问流量回注给源站服务器。

  该方式需要您授权WAF读取您的ECS实例信息。配置过程中只用在WAF控制台添加域名和勾选相应的服务器IP。

- DNS配置模式：通过修改域名解析的方式，将被防护域名的访问流量指向WAF；WAF根据域名配置的源站服务器地址，将处理后的请求转发回源站服务器。

  该方式需要您在WAF控制台添加网站配置来关联要防护的域名，并通过域名解析（DNS），将网站访问请求流转到WAF进行监控。

  - 添加网站配置：网站配置描述了被防护网站的流量转发关系。您可以使用自动或手动的方式添加网站配置。在网站配置中，您需要指定要防护的网站域名和源站服务器地址等信息。完成网站配置后，WAF分配给这个域名一个专用的CNAME地址。

    说明：

    如果您的域名使用阿里云云解析DNS进行域名解析，在添加网站配置时支持一键自动创建，完成WAF接入；否则，您需要手动创建网站配置并修改DNS解析。

  - 修改DNS解析：只有当您在对应域名的解析记录中添加并应用WAF CNAME记录后，才可以正式将网站访问流量导向WAF实例进行监控。

网站接入WAF后，WAF帮助您过滤恶意请求，放行合法的访问请求至源站服务器。

操作导航

- 使用透明代理模式接入WAF
- （DNS配置模式）网站配置
- （DNS配置模式）业务接入WAF配置

防护配置

WAF提供多种防护功能，您可以随时调整已接入网站的防护配置，按照实际需求过滤网站访问请求。

您可以自定义ACL访问控制规则，或直接使用封装好的常见Web防护功能。我们结合Web攻击特征，分析请求头和请求主体，编写了精准的过滤算法，并将这些复杂的过滤算法封装各类防护功能，方便您直接使用。

说明：

WAF使用多层过滤的机制，即您在启用WAF并配置防护功能后，一个客户端请求在经过WAF时，实际上按顺序经过了多层过滤。默认的防护检测顺序为：**精准访问控制 > CC防护 > Web应用攻击防护**。

操作导航

- 精准访问控制、黑白名单配置

  自定义访问规则，根据客户端IP、请求URL以及常见的请求头字段过滤访问请求。

- Web应用攻击防护

  帮助您防护SQL注入、XSS跨站攻击等常见的Web攻击。

- CC安全模式、自定义CC防护

  帮助您防护针对页面请求的CC攻击。

- 大数据深度学习引擎

  对请求做语义分析，检测经伪装或隐藏的恶意请求，帮助您防护通过攻击混淆、变种等方式发起的恶意攻击。

- 高频Web攻击IP自动封禁

  帮助您自动封禁在短时间内进行多次Web攻击的客户端IP。

- 目录扫描防护

  帮助您自动封禁在短时间内进行多次目录遍历攻击的客户端IP。

- 扫描威胁情报

  帮助您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。

- 封禁地区

  帮助您一键封禁来自指定中国省份（地区）或海外地区的IP的访问请求。

- 数据风控

  帮助您对抗机器威胁，如垃圾注册、账号被盗、活动作弊、垃圾消息等欺诈行为。

- 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。

- 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。

- 主动防御

  采用阿里云自研的机器学习算法自动学习域名的合法流量，为域名自动生成定制化的安全策略，防护未知攻击。

安全报表

WAF提供方便的数据可视化和统计功能，方便您查看网站业务信息和安全统计数据。

操作导航

- 总览

  查看图表化的业务访问数据以及安全防护统计信息。

- 安全报表

  查询被防护域名在30天内受到的攻击详情和风险预警信息。

- 全量日志

  搜索网站日志并使用在线分析快速定位请求。

  > **说明:**
  > 只有在**网站配置**页面为域名开启**日志检索**后，WAF才会收集指定域名的访问日志。

- 数据大屏：接入可视化大屏，查看WAF的实时攻防态势监控和告警。

WAF设置

WAF提供实例层面的设置功能，帮助您了解和管理WAF实例资源。

操作导航

- 产品信息

  查看WAF实例的资源详情、WAF的防护规则更新通知、功能更新通知和WAF回源IP段。

- 告警设置

  WAF通过短信或邮件的方式推送安全事件和系统告警，您可以设置告警触发方式、告警周期以及告警信息接收方式。

- 自定义规则组

  查看WAF内置防护规则，自由组合规则生成有针对性的防护策略（即自定义规则组），并在相应防护功能中应用自定义策略。

最佳实践

阅读WAF最佳实践，更好地将WAF应用于您的实际业务。

- 获取访问者真实IP

  启用WAF后，源站服务器收到的所有请求都来自WAF实例，无法直接显示客户端IP。本实践指导您查看访问者真实IP。

- 源站保护

  启用WAF后，源站服务器IP对客户端是隐藏的。如果您的源站服务器IP已公开或不慎泄露，攻击者可能越过WAF，直接对您的源站发动攻击。配置源站保护可以有效防护这种情形。

- 同时部署WAF和DDoS高防IP

  如果您同时开通了阿里云DDoS高防IP服务和Web应用防火墙，您可以参照本实践进行配置。

- 同时部署WAF和CDN

  如果您同时开通了阿里云CDN服务和Web应用防火墙，您可以参照本实践进行配置。

技术支持

在使用WAF过程中遇到问题时，将鼠标移动到云盾Web应用防火墙控制台左侧导航栏**有问题，找专家**图标上，您可以看到WAF技术支持钉钉群的二维码。

通过钉钉软件扫描该二维码，加入技术支持群，您可以直接向安全专家咨询关于WAF使用的任何技术问题或解决紧急问题。

说明：

请前往钉钉官网，下载并安装钉钉聊天软件。

3.2 设置Web应用攻击防护

网站接入Web应用防火墙后，Web应用攻击防护功能默认开启。Web应用攻击防护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。您可以根据实际需求调整Web应用攻击防护的防护模式和策略。

说明：

本文介绍的Web应用攻击防护功能不适用2020年1月发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_6。

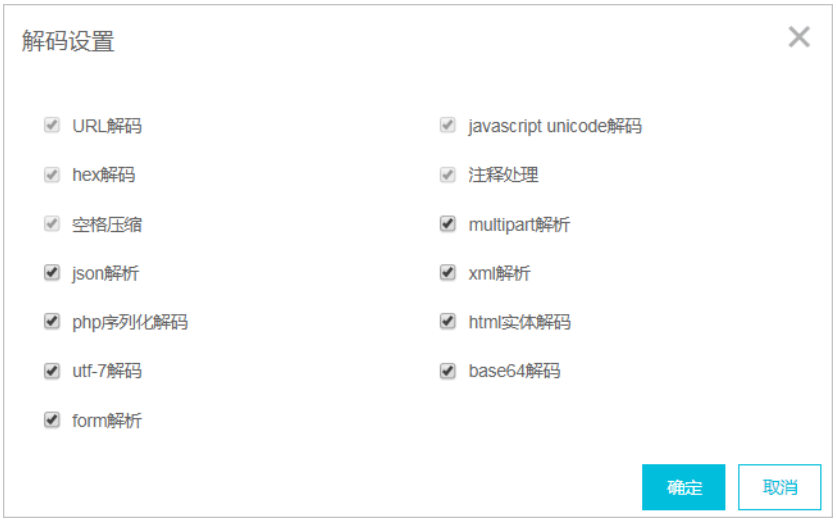
前提条件

已完成网站接入。更多信息，请参见#unique_8。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。
5. 定位到**Web应用攻击防护**配置区域，完成以下功能配置。

参数	描述
状态	开启或关闭Web应用攻击防护功能。
模式	检测发现攻击请求时，对攻击请求执行的操作。可选值： • **防护**：发现攻击后直接阻断。 • **预警**：发现攻击后只告警，不阻断。
防护规则策略	要应用的检测策略，可选值： • **中等规则**：标准检测常见Web应用攻击，默认应用。 • **严格规则**：严格检测路径穿越、SQL注入、命令执行等Web应用攻击。 • **宽松规则**：宽松检测常见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），建议您选择该模式。

参数	描述
解码设置	设置需要Web应用攻击防护解码分析的内容格式。 为保证防护效果，Web应用攻击防护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Web应用攻击防护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。 操作步骤 **a.** 展开配置菜单。 **b.** 勾选或取消勾选要解码的格式。 • 不支持取消的格式：URL解码、javascript unicode解码、hex解码、注释处理、空格压缩。 • 支持取消的格式：multipart解析、json解析、xml解析、php序列化解码、html实体解码、utf-7解码、base64解码、form解析。  **c.** 单击**确定**。

预期结果

Web应用攻击防护的功能配置调整后自动生效。

3.3 大数据深度学习引擎

网站接入Web应用防火墙后，您可以为其开启大数据深度学习引擎功能。大数据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。您可以根据实际需求调整大数据深度学习引擎的防护策略。

前提条件

> **说明：**
> 本文介绍的大数据深度学习引擎功能不适用发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_55。

- 按量付费开通的Web应用防火墙实例，必须在**功能与规格设置**中开启**Web攻击防护**的**高级防护**模式。更多信息，请参见#unique_56。

- 已完成网站接入。更多信息，请参见#unique_57。

背景信息

一般来说，Web应用攻击防护使用的正则规则的描述性比较强，对于强攻击特征的请求，Web应用攻击防护的防护效果最佳。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Web应用攻击防护的严格模式，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，您可以开启大数据深度学习引擎，识别并拦截Web应用攻击防护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. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。
5. 定位到**大数据深度学习引擎**配置区域，完成以下功能配置。

配置项	说明
状态	开启或关闭大数据深度学习引擎功能。

配置项	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： • **防护**：发现攻击后直接阻断。 • **预警**：发现攻击后只告警，不阻断。

3.4 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。CC安全防护以关闭连接的方式阻断检测出的CC攻击请求。您可以根据实际需求调整CC安全防护的防护策略。

前提条件

说明：
本文介绍的CC安全防护功能不适用发布的新版控制台界面，如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_59。

已完成网站接入。更多信息，请参见#unique_57。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。
5. 定位到**CC安全防护**配置区域，完成以下功能配置。开启**状态**开关，并选择相应防护**模式**。

配置项	说明
状态	开启或关闭CC安全防护功能。

配置项	说明
模式	要应用的防护模式。可选值： • **正常**：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。 • **攻击紧急**：高效拦截CC攻击，可能造成较多误杀。当您发现有正常模式无法拦截的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：** 攻击紧急模式适用于网页/H5页面，但不适用于API/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CC防护。更多信息，请参见自定义CC防护。

说明：

- 如果发现**攻击紧急**模式仍然漏过较多攻击，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，您可以设置源站保护，只允许WAF回源IP访问服务器。
- 如果您希望有更好的防护效果，同时有更低的误杀，您可以升级到Web应用防火墙企业版或旗舰版，自定义或找安全专家定制针对性的防护算法。

FAQ

不同WAF规格对应的CC安全防护能力有什么区别？

不同WAF产品规格针对各种复杂的CC攻击提供不同的防护效果：

- 高级版：支持默认的防护模式（正常、攻击紧急），阻拦攻击特征明显的CC攻击。
- 企业版：支持自定义访问控制规则，防护某些具有特定攻击特征的CC攻击。具体操作请参见自定义CC防护。
- 旗舰版：专家定制防护规则，保障防护效果。

规格详情请参见Web应用防火墙价格详情页。

关于如何升级WAF规格，请参见续费与升级。

说明：

对于按量付费版Web应用防火墙，您必须登录云盾Web应用防火墙控制台，前往**设置** > **功能与规格**页面，启用缓解CC攻击的**高级防护**功能选项，才能选择开启**攻击紧急**模式。

为什么有些CC攻击需要升级企业版才能防护？

云盾Web应用防火墙通过人机识别、大数据分析、模型分析等技术识别攻击，对攻击进行拦截。不同于与程序交互，安全攻防是人与人的对抗，每个网站的性能瓶颈也不同。黑客在发现一种攻击无效后，可以调整策略并重新发动定向攻击。此时，通过云盾安全专家介入分析，可以获得更高的防护等级和效果。

3.5 自定义CC防护

WAF企业版和旗舰版支持CC自定义防护功能。您可以在控制台自定义防护规则，限制单个IP对您的网站上特定路径（URL）的访问频率。

说明：

本文介绍的自定义CC防护功能不适用2020年1月发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_4。

前提条件

- 包年包月开通的Web应用防火墙实例，实例套餐必须是企业版及以上规格。更多信息，请参见#unique_22。
- 按量付费开通的Web应用防火墙实例，必须在**功能与规格设置**中开启**缓解CC攻击**的**高级防护**模式。更多信息，请参见功能与规格配置。

- 已完成网站接入。更多信息，请参见#unique_57。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。

5. 定位到**CC安全防护**配置区域，选择**正常**防护模式，并单击**前去配置**。

6. 单击**新增规则**，添加一条规则。

参数	说明
规则名称	为该规则命名。
URI	指定需要防护的具体地址，如/register。支持在地址中包含参数，如/user?action=login。

参数	说明
匹配规则	• **完全匹配**：即精确匹配，请求地址必须与配置的URI完全一样才会被统计。 • **前缀匹配**：即包含匹配，只要是请求的URI以此处配置的URI开头就会被统计。例如，如果设置URI为/register，则/register.html会被统计。
检测时长	指定统计访问次数的周期。需要和单一IP访问次数配合。
单一IP访问次数	指定在检测时长内，允许单个源IP访问被防护地址的次数。
阻断类型	指定触发条件后的操作（封禁、人机识别），以及请求被阻断后阻断动作的时长。 • **封禁**：触发条件后，直接断开连接。 • **人机识别**：触发条件后，用重定向的方式去访问客户端（返回200状态码），通过验证后才放行。例如，单个IP在20s内访问超过5次则进行人机识别判断，在10分钟内该IP的访问请求都需要通过人机识别，如果被识别为非法将会被拦截，只有被识别为合法才会放行。

以截图的配置为例，其含义为：单个IP访问目标地址（精确匹配）时，一旦在10秒内访问超过20次，就直接阻断该IP的访问，阻断操作持续600分钟。

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单一IP的访问频率，统计过程中可能存在一定延时，因此封禁的实际生效时间可能稍有滞后。

3.6 精准访问控制

精准访问控制支持自定义访问规则，根据客户端IP、请求URL、以及常见的请求头字段过滤访问请求。

前提条件

说明：

本文介绍的精确访问控制功能不适用发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_4。

已完成网站接入。更多信息，请参见#unique_57。

背景信息

精准访问控制允许您设置访问控制规则，对常见的HTTP字段（如IP、URL、Referer、UA、参数等）进行条件组合，用来筛选访问请求，并对命中条件的请求设置放行、阻断、告警操作。精确访问控制支持业务场景定制化的防护策略，可用于盗链防护、网站管理后台保护等场景。

说明：

按量付费的WAF实例提供两种规格的精准访问控制：基础防护和高级防护。您可以在**规格与配置**中进行调整。具体操作，请参见功能与规格配置。

- 基础防护仅支持基于IP和URL的匹配条件，且每个域名可设置10条规则。
- 高级防护支持基于IP、URL、Cookie、User-Agent、Referer、提交参数、X-Forwarded-For等各类常见HTTP头部的逻辑组合判断功能，每个域名可设置100条规则。

包年包月模式下，高级版WAF实例仅支持IP、URL、Referer、User-Agent、Params匹配字段，且每个域名最多只能定义20条规则；企业版和旗舰版的WAF实例支持所有匹配字段（见支持的匹配字段），支持为每个域名定义的规则数分别为100条、200条。

精准访问控制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，但允许设置为空值。

  每一条精准访问控制规则中最多允许设置三个匹配条件组合，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

  精准访问控制规则支持以下匹配动作：

  - **阻断**：阻断命中匹配条件的访问请求。
  - **放行**：放行命中匹配条件的访问请求。
  - **告警**：放行命中匹配条件的访问请求，并针对该请求进行告警。

  选择**放行**、**告警**匹配动作后，您可以进一步设置该请求是否需要继续经过其它WAF防护功能检测过滤，如Web应用攻击防护、CC应用攻击防护、智能防护、地区封禁、数据风控、SDK防护等。

- 规则匹配顺序

  如果您设置了多条规则，则多条规则间有先后匹配顺序，即访问请求将根据您设定的精准访问控制规则顺序依次进行匹配，顺序较前的精准访问控制规则优先匹配。

  您可以通过规则排序功能对所有精准访问控制规则进行排序，以获得最优的防护效果。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。
5. 定位到**精准访问控制**配置区域，开启**状态**开关，并单击**前去配置**。

6. 单击**添加规则**，并设置规则的**匹配条件**和相应的**处置动作**，完成后单击**确认**。

> **说明：**
> 关于规则参数说明，请参见精准访问控制规则；关于应用示例，请参见配置示例。

7. 成功创建规则后，您可以选择执行以下操作。

   - **编辑**规则内容或**删除**规则。
   - 规则排序。如果有多条规则，单击**规则排序**，并操作**上移**、**下移**、**置顶**、**置底**调整规则的匹配顺序。

     说明：
     越靠上的规则越优先匹配。

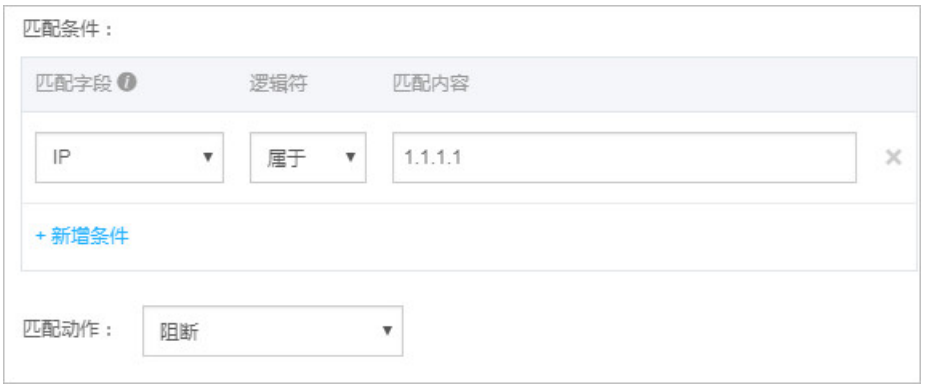
配置示例

精准访问控制规则支持多种配置方法，您可以结合自身业务特点定义相应的规则。通过设置精准访问控制规则也可以实现特定的Web漏洞防护。

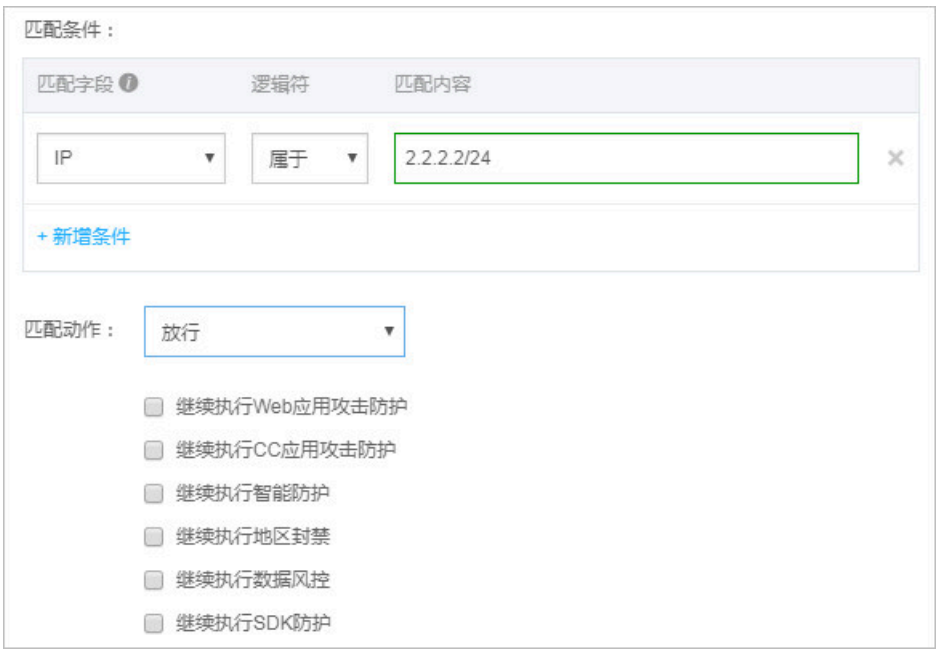
以下罗列了一些常用的精确访问控制配置示例，供您参考。

- 配置IP黑白名单

  通过设置以下精准访问控制规则，阻断来自1.1.1.1的所有访问请求。



  通过设置以下精准访问控制规则，放行来自2.2.2.0/24网段的所有访问请求。



  说明：

  应用此白名单配置规则时，请不要勾选**继续执行Web应用攻击防护**和**继续执行CC应用攻击防护**等选项，不然访问请求仍可能被WAF的其它防护功能拦截。

  更多关于配置IP黑白名单的操作及注意事项，请参见IP黑白名单配置。

- 拦截特定的攻击请求

  通过分析某类特定的WordPress反弹攻击，发现其特征是User-Agent字段都包含WordPress，如下图所示。

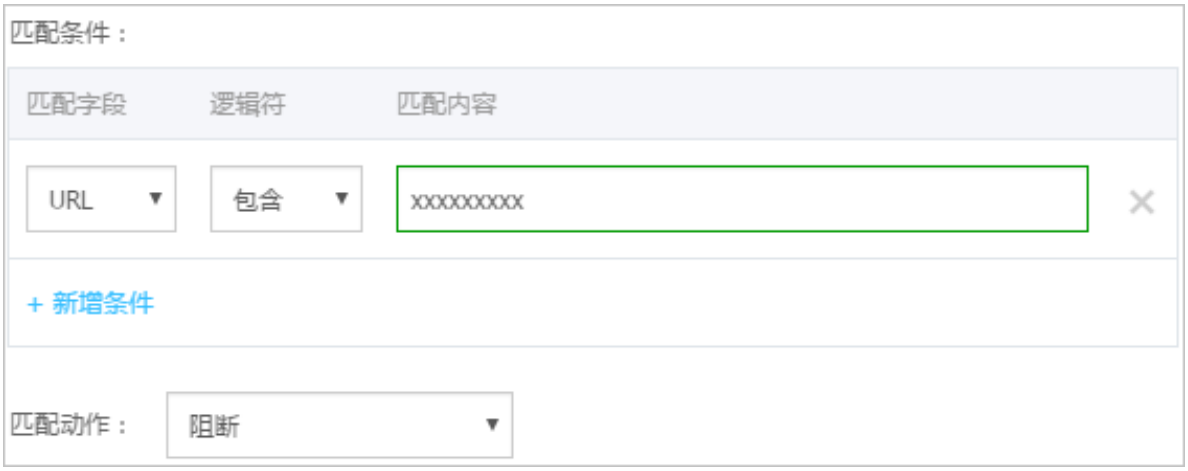
UA
WordPress/4.2.10; http://ascsolutions.vn; verifying pingback from 191.96.249.54
WordPress/4.0.1; http://146.148.63.90; verifying pingback from 191.96.249.54
WordPress/4.6.1; https://www.nokhostinsabt.com; verifying pingback from 191.96.249.54
WordPress/4.5.3; http://eadastage.lib.umd.edu; verifying pingback from 191.96.249.54
WordPress/3.5.1; http://danieljromo.com
WordPress/4.2.4; http://wd.icopy.net.tw; verifying pingback from 191.96.249.54
WordPress/4.6.1; http://kmgproje.com; verifying pingback from 191.96.249.54
WordPress/4.1.6; http://www.vv-atalanta.nl; verifying pingback from 191.96.249.54
WordPress/4.5; http://23.83.236.52; verifying pingback from 191.96.249.54
WordPress/4.6.1; http://playadelrey.news; verifying pingback from 191.96.249.54
WordPress/4.1; http://hostclick.us; verifying pingback from 191.96.249.54
WordPress/4.5.3; http://mosaics.pro; verifying pingback from 191.96.249.54
WordPress/4.0; http://www.chinavrheadset.com; verifying pingback from 191.96.249.54

  因此，可以设置以下精准访问控制规则，拦截该类WordPress反弹攻击请求。

  关于WordPress攻击的详细防护配置，请参见防御WordPress反射。

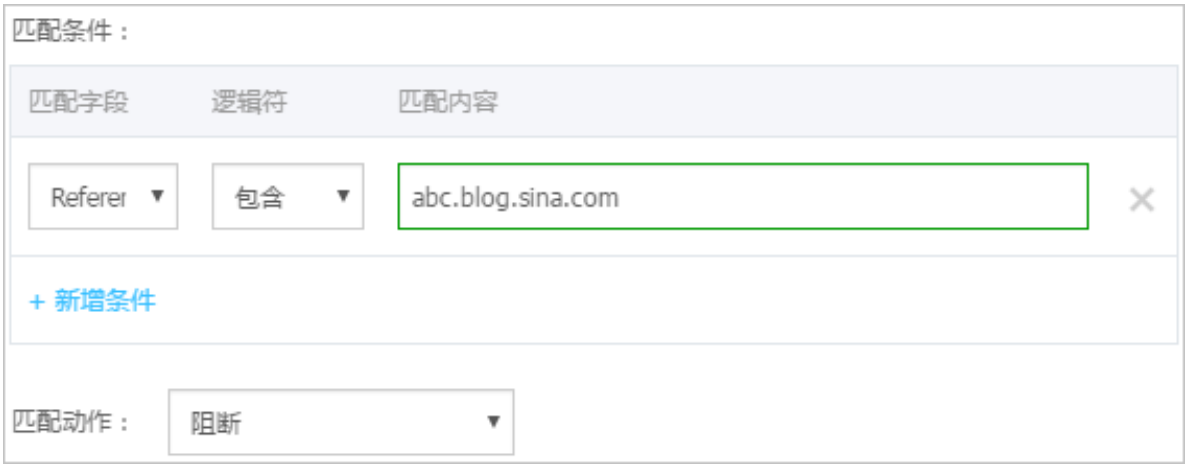
- 封禁特定的URL

  如果您遇到有大量IP在刷某个特定且不存在的URL，您可以通过配置以下精准访问控制规则直接阻断所有该类请求，降低源站服务器的资源消耗。



- 防盗链

  通过配置Referer匹配字段的访问控制规则，您可以阻断特定网站的盗链。例如，您发现abc.blog.sina.com大量盗用本站的图片，您可以配置以下精准访问控制规则阻断相关访问请求。



支持的匹配字段

下表罗列了精确访问控制支持的匹配字段及其描述。

匹配字段	字段描述	适用逻辑符
IP	访问请求的来源IP，支持填写IP或IP段（例如，1.1.1.1/24）。 **说明：** 您可以填写最多50个IP或IP段，以英文逗号（,）分隔。	• 属于 • 不属于

URL	访问请求的URL地址。	• 包含 • 不包含 • 等于 • 不等于
Referer	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。	• 包含 • 不包含 • 等于 • 不等于 • 长度小于 • 长度等于 • 长度大于 • 不存在
User-Agent	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。	• 包含 • 不包含 • 等于 • 不等于 • 长度小于 • 长度等于 • 长度大于
Params	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.abc.com/index.html?action=login中的action=login就是参数部分。	• 包含 • 不包含 • 等于 • 不等于 • 长度小于 • 长度等于 • 长度大于
Cookie	访问请求中的Cookie信息。	• 包含 • 不包含 • 等于 • 不等于 • 长度小于 • 长度等于 • 长度大于 • 不存在

Content-Type	访问请求指定的响应HTTP内容类型，即MIME类型信息。	• 包含 • 不包含 • 等于 • 不等于 • 长度小于 • 长度等于 • 长度大于
X-Forwarded-For	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。	• 包含 • 不包含 • 等于 • 不等于 • 长度小于 • 长度等于 • 长度大于 • 不存在
Content-Length	访问请求的响应内容所包含的字节数。	• 值小于 • 值等于 • 值大于
Post-Body	访问请求的响应内容信息。	• 包含 • 不包含 • 等于 • 不等于
Http-Method	访问请求的方法，如GET、POST等。	• 等于 • 不等于
Header	访问请求的头部信息，用于自定义HTTP头部字段。	• 包含 • 不包含 • 等于 • 不等于 • 长度小于 • 长度等于 • 长度大于 • 不存在

3.7 设置封禁地区

使用封禁地区可以对指定的中国内地各省份及港澳台特别行政区或全球多达247个国家或地区的来源IP进行一键黑名单封禁，阻断所有来自指定地区的访问请求。

说明：

本文介绍的封禁地区功能不适用2020年1月发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_64。

前提条件

- 包年包月开通的Web应用防火墙实例，实例套餐必须是企业版及以上规格。更多信息，请参见#unique_22。

  说明：

  海外地域WAF实例必须是旗舰版。
- 按量付费开通的Web应用防火墙实例，必须在**功能与规格设置**中开启**支持基于地理位置的区域封禁**。更多信息，请参见功能与规格配置。

- 已完成网站接入。更多信息，请参见#unique_57。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。
5. 定位到**封禁地区**配置区域，开启**状态**开关。

   说明：

为确保封禁地区的拦截策略生效，请务必确认您已启用精准访问控制防护功能中的系统默认规则。

6. 单击**设置**，选择中国境内或中国境外范围并勾选需要封禁的地区，完成后单击**确定**。

说明：
选择中国境外范围时，您可以通过国家名称的首字母或者搜索国家名称快速找到需要封禁的国家或地区。

预期结果

完成设置后，来自被封禁地区IP的所有访问请求都将被阻断。

说明：
访问来源IP的归属地信息以淘宝IP地址库为准。更多信息，请参见淘宝IP地址库。

3.8 IP黑白名单配置

业务接入Web应用防火墙（WAF）后，您可以配置精确访问控制规则来阻断或放行指定IP的访问请求，即设置IP黑名单、白名单。IP黑白名单仅针对配置的特定域名生效。

前提条件

说明：
本文介绍的IP黑白名单配置不适用发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_64。

已完成网站接入。更多信息，请参见#unique_57。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。

5. 定位到**精确访问控制**配置区域，开启**状态**开关，并单击**前去配置**。

6. 单击**新增规则**，新增一条防护规则。

- 白名单配置示例：使用下图配置，放行源IP为1.1.1.1的所有访问。

说明：

如果想完全放行这个IP的所有请求，则不要勾选匹配动作下方的继续执行其它防护选项。如果勾选，则来自这个IP的部分请求仍然可能被相应防护的规则拦截。

- 黑名单配置示例：使用下图配置，阻断源IP为1.1.1.1的所有访问。

说明：

- 防护规则中的IP支持掩码格式（如1.1.1.0/24），且逻辑符支持选择“不属于”。因此，如果您想只允许来自某个网段（如公司网段）的请求访问某个域名时，可参见下图配置。

- 多条防护规则之间存在匹配优先级，按照规则列表中从上到下的顺序进行匹配，通过单击右上角的**规则排序**可以调整防护规则之间的优先级。

3.9 设置数据风控

数据风控帮助您防御网站关键业务（如注册、登录、活动、论坛）中可能发生的欺诈行为。

说明：

本文介绍的数据风控功能不适用2020年1月发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_67。

前提条件

已将网站接入WAF进行防护。具体操作请参见业务接入WAF配置。

背景信息

数据风控基于阿里云的大数据能力，通过业内领先的风险决策引擎，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，轻松获取风控能力，且无需在服务器或客户端进行任何改造。

说明：

目前，仅中国内地的WAF实例提供数据风控功能。

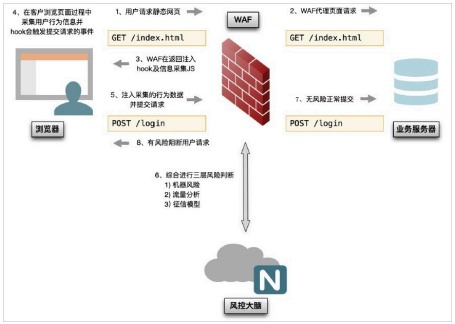
对于按量付费的WAF实例，您必须在**功能与规格**中启用**数据风控**，才能使用该功能。具体操作请参见功能与规格配置。

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

数据风控的工作流程如下图所示。



关于接入数据风控的应用场景示例和实际效果，请参见应用示例。

兼容性说明

数据风控仅适用于网页、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，包括：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，包括：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相关请求提交的情况

建议您在接入数据风控功能初期，选用预警模式并结合WAF全量日志服务进行兼容性和效果测试。更多信息，请参见WAF实时日志分析服务。

如果您发现存在不兼容的情况，您可以使用人机验证服务配合WAF一起实现防护。更多信息，请参见人机验证服务。

原生App业务防护请使用爬虫风险管理提供的SDK解决方案。更多信息，请参见App增强防护SDK方案。

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 前往**管理** > **网站配置**页面，并在页面上方选择**中国内地**地域。
3. 选择要操作的域名，单击其操作列下的**防护配置**。

4. 开启**数据风控**状态开关并确认开启。

> **说明：**
> 启用数据风控功能后，WAF将在您网站的所有（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的是非标端口访问，配置数据风控也无需进行额外配置。关于如何指定JS插入页面，请参见指定JS插入页面。

5. 选择防护**模式**：

- **预警**：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。
- **防护**：识别到业务攻击时，用户将被重定向至验证页面进行二次验证。

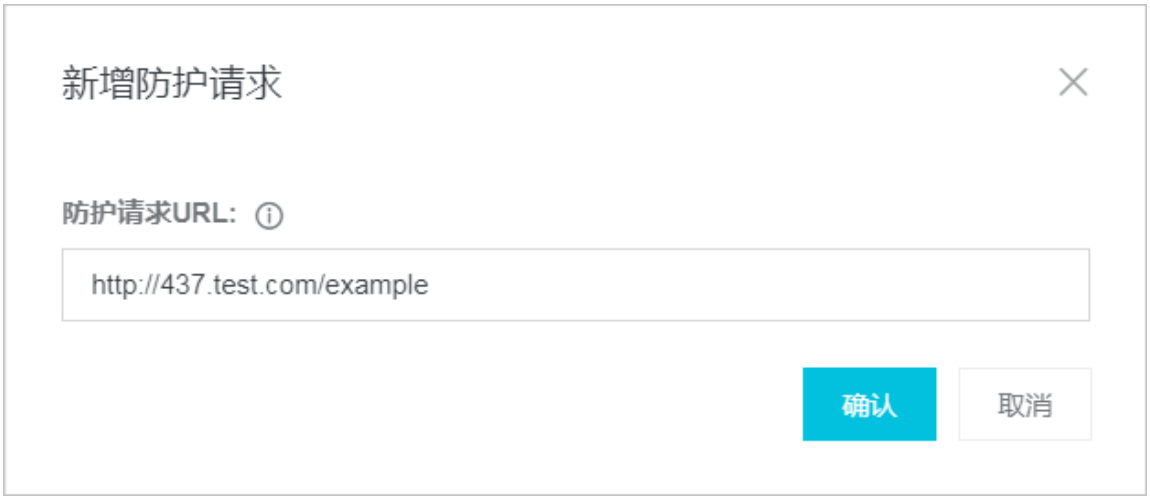
> **说明：**
> 默认使用预警模式，数据风控不会对任何请求进行拦截，但依然会在静态页面中插入JS脚本分析客户端行为。

6. 单击**前去配置**。

7. 添加防护请求。

a) 在**防护请求**页签下，单击**新增防护请求**。

b) 在**新增防护请求**对话框，指定**防护请求URL**。



什么是防护请求URL

防护请求URL指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.abc.com/new_user，获取验证码按钮对应的业务接口地址是www.abc.com/getsmscode，注册按钮对应的业务接口地址是www.abc.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.abc.com/getsmscode和注册按钮对应的接口地址www.abc.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.abc.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。

防护请求URL注意事项

- 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.test.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.abc.com/book/*，即可对www.abc.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.

abc.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。

c) 单击**确认**。

防护请求添加成功后，10分钟左右生效。

8. 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，可通过指定页面插入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。

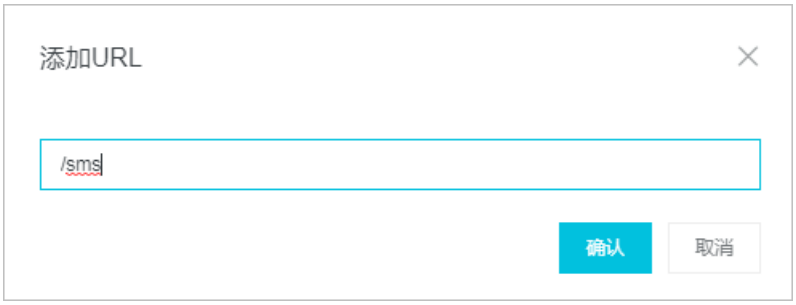
a) 在**JS插入页面**页签下，单击**指定页面插入JS**。

b) 单击**添加页面**。

说明：

最多可以添加20个页面地址。

c) 在**添加URL**对话框中，输入要插入JS的页面地址（以“/”开头），单击**确认**。



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。

启用数据风控后，您还可以使用WAF的全量日志功能查看防护结果。关于日志示例，请参见查看防护结果。

数据风控应用示例

阿里云用户小白在互联网上搭建网站业务，网站域名是www.abc.com，普通用户可以通过www.abc.com/register.html注册成为网站会员。

近来，小白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。

于是，小白将网站业务接入WAF并为www.abc.com域名开启数据风控功能。小白当前最关心的注册业务的请求URL是www.abc.com/register.html，因此将该URL设置为防护请求URL。

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.abc.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.abc.com/register.html地址提交注册请求时，WAF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征信特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。
  - 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。

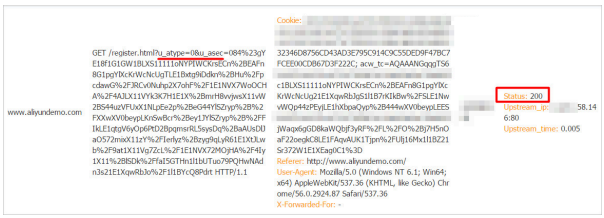
    - 如果通过滑块验证方式可疑（例如，使用脚本模仿真人滑动过程等），数据风控将继续通过其它方式再次进行验证，直到验证通过且通过方式可信。
    - 如果无法通过验证，数据风控将阻断该请求。
  - 如果基于之前的行为，数据风控判断该请求来自正常用户，则该用户在注册过程中将无任何感知。

整个过程中，由于数据风控是针对整个网站域名（www.abc.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.abc.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。

查看防护结果

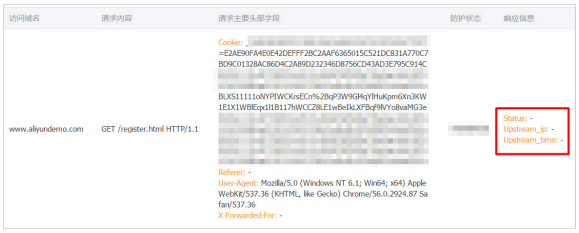
您可以使用WAF的全量日志查询功能来排查数据风控的监控和拦截情况。更多信息，请参见全量日志查询。

- 通过数据风控验证的日志情况。



正常用户经过数据风控验证的访问请求URL将包含一个以ua开头的参数，请求会被WAF转发回源站，源站服务器正常响应该请求。

- 被数据风控拦截的日志情况。



如果直接请求业务接口URL，一般不会包含以ua开头的参数（或带有伪造的ua参数），这类请求将被WAF拦截，且请求日志中无源站响应信息。

因此，您可以使用全量日志查询功能，在**高级搜索** > **URL关键字**中配置启用数据风控的接口，来排查数据风控的监控和拦截情况。

3.10 网站防篡改

您可以使用网站防篡改对指定的敏感页面设置缓存，缓存后即使源站页面内容被恶意篡改，WAF也会向访问者返回预先缓存好的页面内容，确保用户看到正确的页面。

前提条件

> **说明：**
> 本文介绍的网站防篡改功能不适用发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_70。

- 按量付费开通的Web应用防火墙实例，必须在**功能与规格设置**中开启**网页防篡改、敏感信息防泄露**。更多信息，请参见#unique_56。

- 已完成网站接入。更多信息，请参见#unique_57。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。

5. 定位到**网站防篡改**配置区域，开启**防篡改开关**，并单击**前去配置**。

6. 单击**新增规则**，在**添加URL**对话框配置要防护的具体页面。

- **业务名称**：为该规则命名。
- **URL**：填写精确的要防护的路径，不支持通配符（如`/*`）或参数（如`/abc?xxx=`）。WAF可以防护该路径下的text、html和图片等内容。

7. 添加规则后，手动打开对应规则**防护状态**下的开关。如果您在添加规则后未打开防护开关，则设置不会生效。

8. 如果被防护页面进行了内容更新，您必须单击**更新缓存**来更新缓存。如果您在页面更新后未更新缓存，WAF将始终返回最近一次缓存的页面内容。

3.11 防敏感信息泄露

防敏感信息泄漏是Web应用防火墙针对网安法提出的“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。

前提条件

说明：
本文介绍的防敏感信息泄露功能不适用发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_72。

- 按量付费开通的Web应用防火墙实例，必须在**功能与规格设置**中开启**网页防篡改、敏感信息防泄露**。更多信息，请参见#unique_56。

- 已完成网站接入。更多信息，请参见#unique_57。

背景信息

防敏感信息泄漏功能针对网站中存在的敏感信息（尤其是手机号、身份证、信用卡等信息）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。

网站中常见的造成信息泄漏的场景包括：

- 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：

- 针对网站页面中出现的个人隐私敏感数据进行检测识别，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、手机号、银行卡号等。
- 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，针对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。

防敏感信息泄露通过检测响应页面中是否带有身份证号、手机号、银行卡号等敏感信息，发现敏感信息匹配命中后，根据所设置的匹配动作进行告警或者过滤敏感信息。其中，敏感信息过滤动作以*号替换敏感信息部分，从而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. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。
5. 定位到**防敏感信息泄露**配置区域，开启**状态**开关，并单击**前去配置**。

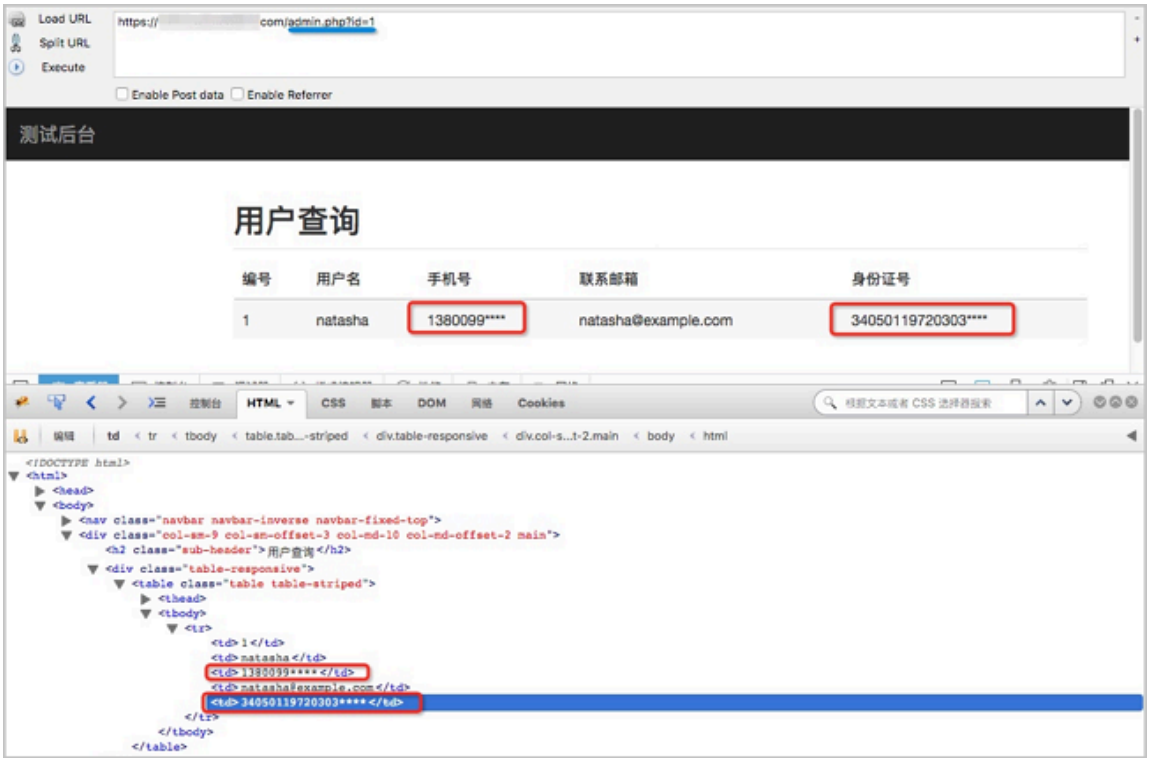
6. 单击**新增规则**，添加敏感信息防护规则。

说明：

在规则设置对话框中，您可以单击**并且**增加URL匹配条件实现对特定URL进行匹配检测。

- 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，您可以通过设置以下防护规则，过滤手机号和身份证号敏感信息。

配置该防护规则后，该网站域名中的所有页面中的手机号和身份证号都会自动脱敏，效果如下图所示。



说明：

网站页面中的商务合作电话、举报电话等需要对外公开的手机号码，也可能被所配置的手机号敏感信息过滤规则所过滤。

- 状态码拦截：针对特定的HTTP请求状态码，可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，您可以通过设置以下防护规则，拦截HTTP 404状态码。

配置该防护规则后，当请求一个该网站域名中不存在的页面时，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，您可以通过设置以下防护规则，过滤admin.php页面中的身份证号敏感信息。

配置该防护规则后，仅admin.php页面中的身份证号信息被脱敏。

7. 成功添加规则后，您可以**编辑**或**删除**规则。

后续步骤

启用防敏感信息泄露后，您可以登录云盾Web应用防火墙控制台，前往**统计** > **安全报表**页面查看**Web应用攻击**报表，查询被防敏感信息泄露规则过滤或拦截的访问请求日志。

3.12 高频Web攻击IP自动封禁

高频Web攻击IP自动封禁功能帮助您自动封禁在短时间内进行多次Web攻击的客户端IP。

前提条件

说明：

本文介绍的高频Web攻击IP自动封禁功能不适用2020年1月发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_73。

- 已开启Web应用攻击防护和CC安全防护功能。更多信息，请参见Web应用攻击防护和CC安全防护。
- 已完成网站接入。更多信息，请参见#unique_57。

背景信息

您可以开启高频Web攻击IP自动封禁功能，使WAF自动检测并封禁在短时间内进行多次Web攻击的客户端IP；被封禁IP在封禁时间内的请求将被直接拦截，封禁时间过后自动解除封禁。开启防护后，您可以自定义防护策略（见步骤5）；也可以一键解除已封禁的客户端IP（见步骤6）。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。
5. 定位到**高频Web攻击IP自动封禁**配置区域，开启**状态**开关。

成功开启高频Web攻击IP自动封禁后，默认启用的防护策略为：当WAF检测到某个客户端IP在60秒内发起Web攻击请求超过20次，则封禁该IP的访问请求1,800秒。

6. （可选） 如果您想自定义防护策略，请参照以下步骤进行操作：

a) 在**高频Web攻击IP自动封禁**下，单击**前去配置**。

b) 在**规则设置**对话框中，完成以下配置。

配置	描述
检测时间范围	设置检测时间间隔，单位为秒。

配置	描述
Web攻击次数超过	设置在检测时间范围内，客户端发起多少次以上攻击请求，则触发封禁。
封禁IP	设置触发封禁时，封禁客户端IP多长时间，单位为秒。

> **说明：**
> 如果您不清楚如何设置，请在**设置参考**下单击选择一种模式：**宽松模式**、**严格模式**、**正常模式**。每种模式对应不同严格程度的策略，您可以在其基础上进行调整。

c) 单击**确定**。

7. （可选）如果您想手动解除已被封禁的客户端IP，在**高频Web攻击IP自动封禁**下，单击**解封当前封禁IP**。

3.13 目录遍历防护

目录遍历防护帮助您自动封禁在短时间内进行多次目录遍历攻击的客户端IP。

前提条件

> **说明：**
> 本文介绍的目录遍历防护功能不适用2020年1月发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_73。

- 已开启Web应用攻击防护和CC安全防护功能。更多信息，请参见Web应用攻击防护和CC安全防护。
- 已完成网站接入。更多信息，请参见#unique_57。

背景信息

您可以开启目录遍历防护功能，使WAF自动检测并封禁在短时间内进行多次目录遍历攻击的客户端IP；被封禁IP在封禁时间内的请求将被直接拦截，封禁时间过后自动解除封禁。开启防护后，您可以自定义防护策略（见步骤5）；也可以一键解除已封禁的客户端IP（见步骤6）。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。

5. 定位到**目录遍历防护**配置区域，开启**状态**开关。

成功开启目录遍历防护后，默认启用的防护策略为：当WAF检测到某个客户端IP在10秒总请求次数超过50次，且响应码404占比超过总请求的70%，则封禁该IP的访问请求1,800秒。

6. （可选）如果您想自定义防护策略，请参照以下步骤进行操作：

a) 在**目录遍历防护**下，单击**前去配置**。

b) 在**规则设置**对话框中，完成以下配置。

配置	描述
检测时间范围	设置检测时间间隔，单位为秒。
请求总数超过	设置在检测时间范围内，客户端发起多少次以上访问请求，且这些请求中404响应码的占比超过多少（%），则触发封禁。
且404响应码占比超过	
封禁IP	设置触发封禁时，封禁客户端IP多长时间，单位为秒。

说明：

如果您不清楚如何设置，请在**设置参考**下单击选择一种模式：**宽松模式**、**严格模式**、**正常模式**。每种模式对应不同严格程度的策略，您可以在其基础上进行调整。

c) 单击**确定**。

7. （可选）如果您想手动解除已被封禁的客户端IP，在**目录遍历攻击**下，单击**解封当前封禁IP**。

3.14 扫描威胁情报

扫描威胁情报帮助您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。

前提条件

> **说明：**
> 本文介绍的扫描威胁情报功能不适用发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_73。

- 已开启Web应用攻击防护和CC安全防护功能。更多信息，请参见Web应用攻击防护和CC安全防护。
- 已完成网站接入。更多信息，请参见#unique_57。

背景信息

您可以开启扫描威胁情报功能，使WAF自动封禁常见扫描工具的访问请求，支持封禁的扫描工具包括：Sqlmap、AWVS、Nessus、Appscan、Webinspect、Netsparker、Nikto、Rsas等；也可以开启协同防御，使WAF自动封禁来自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. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。
5. 定位到**扫描威胁情报**配置区域，根据实际需求开启以下防护功能。
   - **扫描工具封禁**：开启以后，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，将一直封禁其访问请求。关闭后，将不再拦截扫描行为。
   - **协同防御**：开启以后，自动封禁来自阿里云全球恶意扫描攻击IP库中IP的访问请求。

3.15 主动防御

主动防御功能采用阿里云自研的机器学习算法自动学习域名的合法流量，从而为域名自动生成定制化的安全策略，防护未知攻击。

前提条件

> **说明：**
> 本文介绍的主动防御功能不适用2020年1月发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_74。

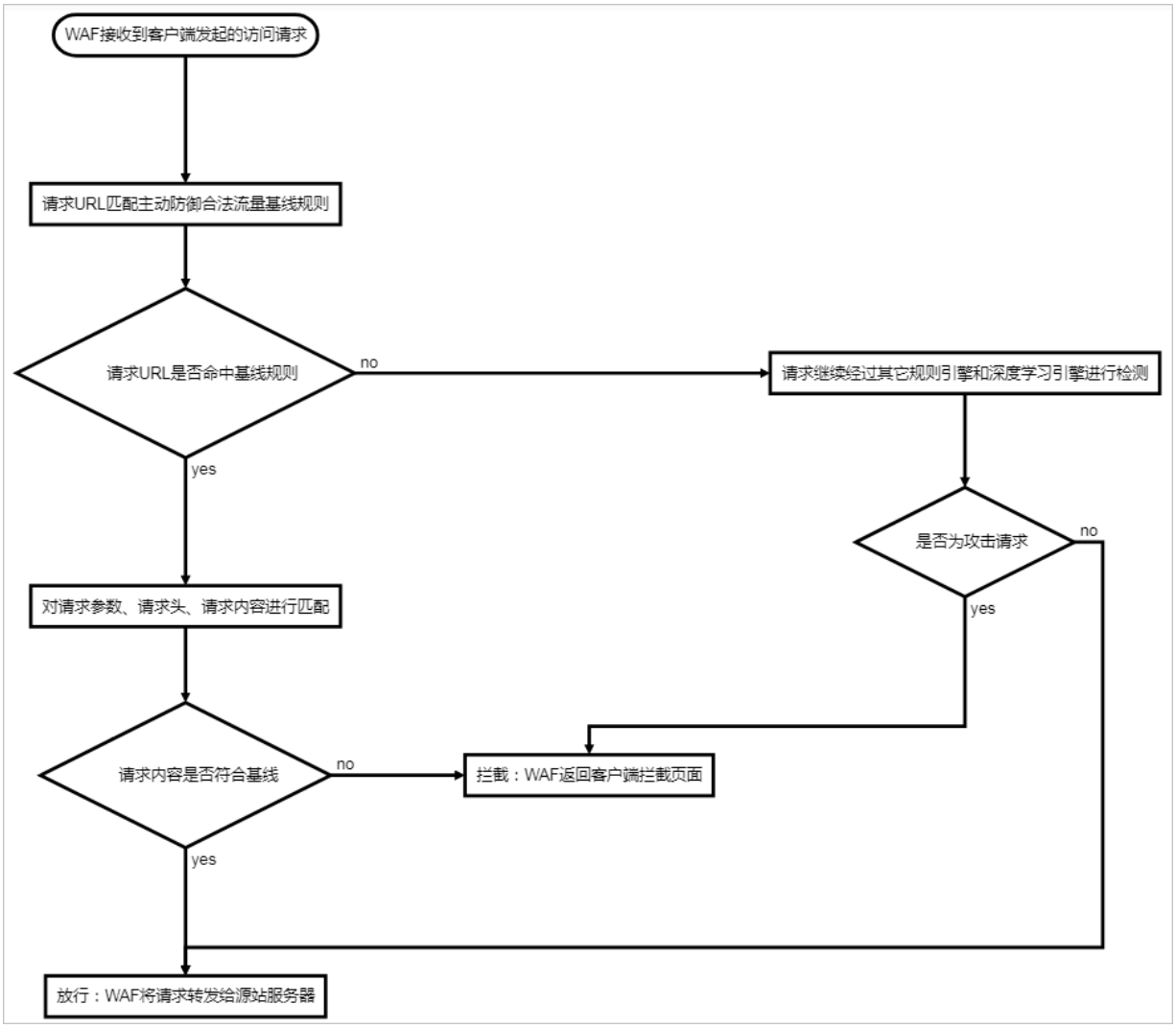
- 包年包月开通的Web应用防火墙实例，实例套餐必须是旗舰版及以上规格。更多信息，请参见#unique_22。

  > **说明：**
  > 按量付费开通的Web应用防火墙实例，暂不支持主动防御功能。

- 已完成网站接入。更多信息，请参见#unique_57。

背景信息

有别于传统的基于安全检测规则的防护模式，Web应用防火墙的主动防御功能通过无监督学习的方式针对域名的访问流量进行深度学习，根据机器学习算法模型为访问请求标记正常分值，从而定义该域名的正常访问流量基线并生成定制化的安全策略。通过将流量分层的方式，将主动防御能力与Web应用防火墙的其它安全检测体系有机结合，为域名提供全面的攻击防护。



操作步骤

1. 登录Web应用防火墙控制台。
2. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **网站配置**。
4. 选择要操作的域名，单击其操作列下的**防护配置**。

5. 定位到**主动防御**配置区域，开启**状态**开关。

域名首次启用主动防御功能后，系统将自动使用机器学习算法模型对该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。

> **说明：**
> 主动防御的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。

3.16 账户安全

Web应用防火墙（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。使用账户安全检测时，您只需在WAF中配置防护接口，即可在WAF安全报表中查看相关检测结果。

前提条件

> **说明：**
> 本文介绍的账户安全功能不适用发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_76。

- 包年包月开通的Web应用防火墙实例，实例套餐必须是企业版及以上规格。

  > **说明：**
  > 按量付费开通的Web应用防火墙实例，暂不支持账户安全功能。

- 已完成网站接入。更多信息，请参见#unique_57。

背景信息

开启账户安全检测前，您必须了解业务中与账户安全有关的接口信息，以便完成后续配置，例如域名、提交账号信息的URL、具体的账号/密码字段的参数名称。

使用限制

每个WAF实例最多支持为三个接口开启账户安全检测。

新增防护接口

1. 登录Web应用防火墙控制台。
2. 在页面上方选择Web应用防火墙实例的地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，单击**管理** > **账户安全**。
4. 在**账户安全**页面，单击**新增接口**。

> **说明：**
> 每个WAF实例最多可以添加三个检测接口。若接口数量达到限制，则**新增接口**按钮不可操作。

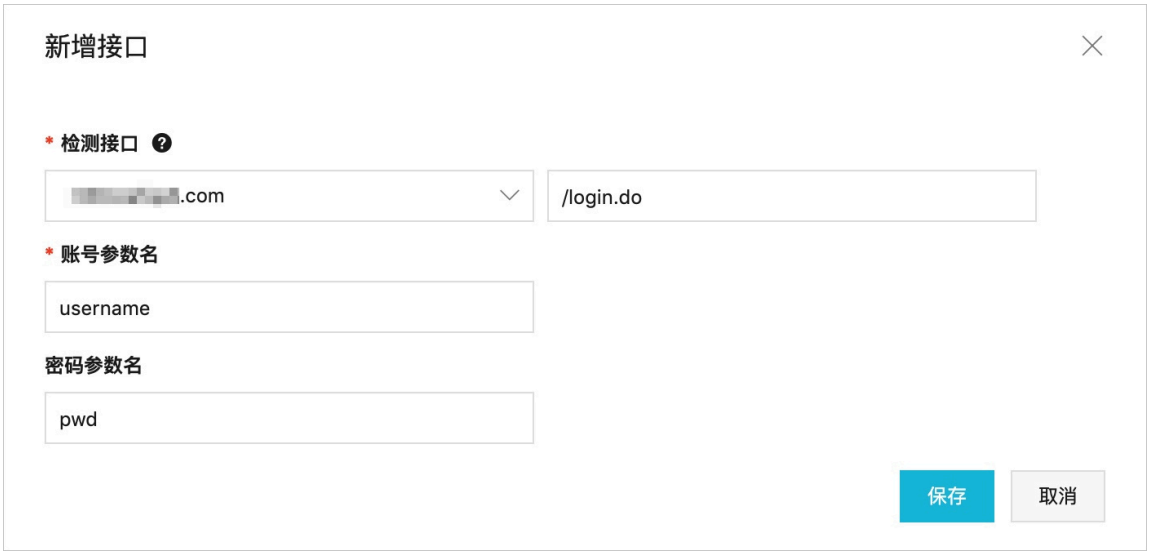
5. 在**新增接口**对话框中，完成接口配置，并单击**保存**。接口配置的描述见下表。

配置项	说明
检测接口	选择要检测的域名并填写账号信息提交接口的URI。 **说明：** • 检测接口不是登录接口所在页面的地址（例如/login.html），而是最终提交登录用户名和密码信息的接口地址。 • 如果您已开通资产管理，则WAF帮助您自动补全已接入域名的全部接口，您可以在这里直接选择要检测的接口。更多信息，请参见资产管理。
账号参数名	填写账号字段对应的参数名称。

配置项	说明
密码参数名	填写密码字段对应的参数名称。若检测接口无需提交密码，则该配置留空。

配置示例

- 假设用户登录接口是/login.do，提交的POST请求body中内容样例为username=Jammy&pwd=123456，则**账户参数名**是username，**密码参数名**是pwd，可以按下图所示进行配置。



- 如果登录账号参数位于GET请求的URL中，例如/login.do?username=Jammy&pwd=123456，则配置方法与上图一样。
- 如果业务接口不需要密码参数，例如注册账号接口，则只需要填写**账号参数名**，**密码参数名**留空。
- 如果业务接口要求传入手机号作为用户凭证，则手机号可以视作账号参数。例如/sendsms.do?mobile=13811111111，则**检测接口**填写/sendsms.do，**账号参数名**填写mobile，**密码参数名**留空。

成功添加检测接口。配置好检测接口后，WAF后台会下发检测任务。若被检测接口的流量命中检测逻辑，一般几个小时后就开始产出账户安全风险事件。

查看账户安全报表

您可以在**账户安全**页面单击目标接口操作列下的**查看报表**，直接访问接口的账户安全报表，或者前往WAF**安全报表**页面查看账户安全报表。

以下内容介绍了通过**安全报表**页面查看账户安全报表的操作方法。

1. 在左侧导航栏，单击**统计** > **安全报表**。
2. 在**账户安全**页签下，选择要查看的域名、接口、数据范围（**昨日数据**、**今日数据**、**7日数据**、**30日数据**），查看对应的账户安全风险事件。

账户安全报表的字段描述见下表。

字段	说明
接口	检测到账户安全事件的接口URI。
所属域名	接口隶属的域名。
异常时间段	检测到账户安全事件的时间段。
已拦截量	在**异常时间段**内，接口上发生的所有被当前WAF防护策略拦截的请求的数量。 这里的策略指全部已经生效的防护策略，例如Web攻击防护规则、精准访问控制、CC攻击防护、区域封禁等。这个数字占总请求量的比值在一定程度上反映了当前接口的账户风险防控效果。
总请求量	在**异常时间段**内，接口上发生的总请求数量。

字段	说明
告警原因	产生告警的依据，目前包括以下几个维度： • 命中撞库或暴力破解的行为模型。 • 该接口在对应时段内的流量基线异常。 • 该接口在对应时段内命中威胁情报库的量较大。 • 该接口在对应时间内命中了较多弱口令，有暴力破解或撞库的风险。

更多信息

WAF账户安全检测只提供账户安全风险的检测能力。由于账户安全涉及到的业务和技术场景复杂，所以在防护上需要依据不同的情况采取对应的方案。更多信息，请参见账户安全最佳实践。

4 查看安全报表（旧版引擎）

WAF提供安全报表，集中展示Web应用攻击、CC攻击的防护记录和访问控制事件，帮助您了解WAF的所有防护动作。您可以查看WAF已防护域名的攻击防护统计和攻击详情。

> **说明：**
> 本文介绍的安全报表功能不适用2020年1月发布的新版控制台界面。如果您使用在此日期后开通的Web应用防火墙实例，请参见#unique_79。

前提条件

- 已完成网站接入。更多信息，请参见#unique_8。
- 按量付费开通的Web应用防火墙实例，必须在中开启**提供业务分析报表**。更多信息，请参见#unique_56。

操作步骤

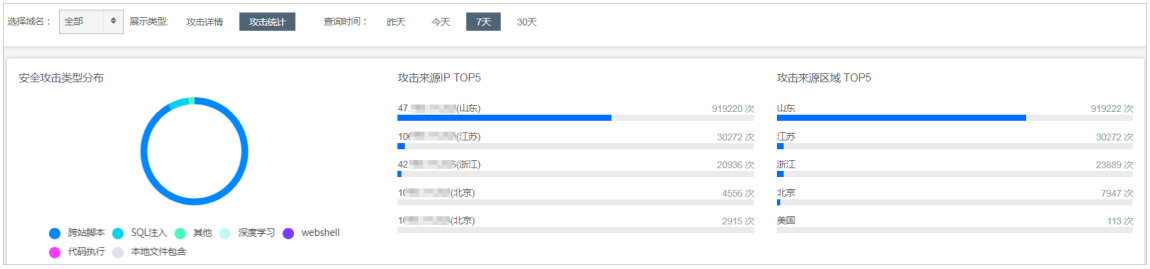
1. 登录云盾Web应用防火墙控制台。
2. 前往**统计** > **安全报表**页面。
3. 在**攻击防护**页签，选择要查看的记录类型，查看其防护记录。
   - **Web应用攻击**：展示WAF阻断的所有Web攻击记录。您可以使用域名、攻击IP、和攻击时间来筛选您关注的记录。

> **说明：**
> 关于Web应用攻击防护的功能描述和操作方法，请参见设置Web应用攻击防护。

> **说明：**

攻击请求中命中相应Web攻击防护规则的字段将以红色显示。

默认以攻击详情的形式展示结果，您可以选择查看攻击统计。攻击统计显示了安全攻击类型分布、攻击来源IP TOP5、和攻击来源区域 TOP5。



- **CC攻击**：展示WAF拦截的针对某个域名的CC攻击记录。您可以选择域名和查询时间，来查看相应记录。

说明：

关于CC安全防护的功能描述和操作方法，请参考CC安全防护。

页面上方展示指定时间段内的总QPS和攻击QPS的趋势信息，下方则列出所有遭受到的恶意CC攻击事件。WAF对CC攻击事件的定义是：攻击持续时间 > 3分钟，且每秒攻击次数 > 100。

- **访问控制事件**：展示针对某个域名的访问控制事件记录。您可以选择域名和查询时间，来查看相应记录。

说明：

关于精准访问控制的功能描述和操作方法，请参见精准访问控制。

5 API参考

5.1 旧版引擎（2018-01-17版本）

5.1.1 API概览

Web应用防火墙提供以下相关API接口。

实例信息

API	描述
DescribeRegions	调用DescribeRegions接口获取当前WAF支持的地域信息。
DescribePayInfo	调用DescribePayInfo接口获取指定地域的WAF实例当前信息。
DescribeWafSourceIpSegment	调用DescribeWafSourceIpSegment接口获取WAF实例的回源IP网段列表。

域名配置

API	描述
DescribeDomainNames	调用DescribeDomainNames接口获取指定WAF实例中已添加的域名名称列表。
DescribeDomainConfig	调用DescribeDomainConfig接口获取指定域名的转发配置信息。
DescribeDomainConfigStatus	调用DescribeDomainConfigStatus接口查询指定域名的转发配置是否生效。
CreateDomainConfig	调用CreateDomainConfig接口添加域名配置信息。
ModifyDomainConfig	调用ModifyDomainConfig接口修改指定域名配置信息。
DeleteDomainConfig	调用DeleteDomainConfig接口删除指定域名配置信息。
CreateCertAndKey	调用CreateCertAndKey接口为已添加的域名配置记录上传证书及私钥信息。

Web攻击防护配置

API	描述
ModifyWafSwitch	调用ModifyWafSwitch接口打开或关闭Web攻击防护功能开关。

精准访问控制配置

API	描述
CreateAclRule	调用CreateAclRule接口为指定域名添加精准访问控制规则。
DeleteAclRule	调用DeleteAclRule接口删除指定精准访问控制规则。
ModifyAclRule	调用ModifyAclRule接口修改指定精准访问控制规则。
DescribeAclRules	调用DescribeAclRules接口获取指定域名的精准访问控制规则列表。

异步任务信息

API	描述
DescribeAsyncTaskStatus	调用DescribeAsyncTaskStatus接口查询WAF任务执行状态。

5.1.2 调用方式

Web应用防火墙接口调用是向WAF API的服务端地址发送HTTP GET请求，并按照接口说明在请求中加入相应请求参数，调用后系统会返回处理结果。请求及返回结果都使用UTF-8字符集进行编码。

请求结构

Web应用防火墙的API是RPC风格，您可以通过发送HTTP GET请求调用WAF API。

其请求结构如下：

```
https://Endpoint/?Action=xx&Parameters
```

其中：

- **Endpoint**：WAF API的服务接入地址为wafopenapi.cn-hangzhou.aliyuncs.com。
- **Action**：要执行的操作，如使用**DescribeDomainNames**查询已添加的域名名称列表。
- **Version**：要使用的API版本，WAF的API版本是2018-01-17。
- **Parameters**：请求参数，每个参数之间用“&”分隔。

  请求参数由公共请求参数和API自定义参数组成。公共参数中包含API版本号、身份验证等信息，详情请参见公共参数。

下面是一个调用**DescribeDomainNames**接口查询指定WAF实例中已添加的域名名称列表的示例：

说明：

为了便于用户查看，本文档中的示例都做了格式化处理。

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
```

```
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Format=xml
&Version=2018-01-17
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
...
```

API授权

为了确保您的账号安全，建议您使用子账号的身份凭证调用API。如果您使用RAM账号调用WAF API，您需要为该RAM账号创建、附加相应的授权策略。

API签名

WAF服务会对每个API请求进行身份验证，无论使用HTTP还是HTTPS协议提交请求，都需要在请求中包含签名（Signature）信息。

WAF通过使用AccessKey ID和AccessKey Secret进行对称加密的方法来验证请求的发送者身份。AccessKey是为阿里云账号和RAM用户发布的一种身份凭证（类似于用户的登录密码），其中AccessKey ID 用于标识访问者的身份，AccessKey Secret是用于加密签名字符串和服务器端验证签名字符串的密钥，必须严格保密。

RPC API需按如下格式在请求中增加签名（Signature）：

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=
CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-
4e0ad82fd6cf
```

以**DescribeDomainNames**为例，假设AccessKey ID是testid， AccessKey Secret是testsecret，则签名前的请求URL如下：

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2018-01-17
&SignatureVersion=1.0
```

完成以下步骤计算签名：

1. 使用请求参数创建待签名字符串：

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeDomainNames&Region%3Dcn
&InstanceId%3Dwaf_elasticity-cn-0xldbqtm005&Format%3DXML&SignatureMethod
%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&
```

```
SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A46%253A24Z&Version
%3D2018-01-17
```

2. 计算待签名的HMAC的值。

   在AccessKey Secret后添加一个“&”作为计算HMAC值的key。本示例中的key为testsecret&。

```
CT9X0VtwR86fNWSnsc6v8YGOjuE=
```

3. 将签名加到请求参数中：

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2018-01-17
&SignatureVersion=1.0
&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

5.1.3 公共参数

公共请求参数

公共请求参数是每个接口都需要使用到的请求参数。

表 5-1: 公共请求参数表

名称	类型	是否必须	描述
Region	String	是	WAF实例所在的地域。取值： • cn：表示中国大陆地区。 • cn-hongkong：表示海外地区。
InstanceId	String	是	WAF实例ID。 **说明：** 您可以通过调用**DescribePayInfo**接口查看您当前WAF实例ID。
Format	String	否	返回消息的格式。取值： • JSON（默认） • XML
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值： 2018-01-17

名称	类型	是否必须	描述
AccessKeyId	String	是	访问服务使用的密钥ID。
Signature	String	是	签名结果串。
SignatureMethod	String	是	签名方式，取值： HMAC-SHA1
Timestamp	String	是	请求的时间戳，为日期格式。使用UTC时间按照ISO8601标，格式为YYYY-MM-DDThh:mm:ssZ。 例如，北京时间2013年1月10日20点0分0秒，表示为2013-01-10T20:00:00Z。
SignatureVersion	String	是	签名算法版本，取值： 1.0
SignatureNonce	String	是	唯一随机数，用于防止网络重放攻击。 在不同请求间要使用不同的随机数值。
ResourceOwnerAccount	String	否	本次API请求访问到的资源拥有者账户，即登录用户名。

示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2018-01-17
&SignatureVersion=1.0
&Signature=Signature
```

公共返回参数

API返回结果采用统一格式，返回2xx HTTP状态码代表调用成功；返回4xx或5xx HTTP状态码代表调用失败。调用成功返回的数据格式有XML和JSON两种，可以在发送请求时指定返回的数据格式，默认为XML格式。

每次接口调用，无论成功与否，系统都会返回一个唯一识别码**RequestId**。

- XML格式

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<!—结果的根结点-->
<接口名称+Response>
  <!—返回请求标签-->
  <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
  <!—返回结果数据-->
</接口名称+Response>
```

- JSON格式

```
{
  "RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
  /*返回结果数据*/
  }
```

5.1.4 调用示例

Web应用防火墙的接口调用是向WAF API的服务端地址发送HTTP GET请求，并按照接口说明在请求中加入相应请求参数，调用后系统会返回处理结果。

以下Python示例代码演示了如何添加公共参数和接口请求参数、如何用请求参数构造规范化请求字符串、如何构造StringToSign字符串，以及如何获得OpenAPI服务端地址，最终以Get方式发送HTTP请求获取相应的响应结果。

下载Python示例代码

说明:

如果您需要使用以下示例，请替换示例中的公共参数及接口请求参数信息。

定义公共参数

```
#! /usr/bin/env python
# -*- coding: utf-8 -*-
import hashlib
import urllib
import requests
import hmac
import random
import datetime
import sys

class OpenAPI(object):
    def __init__(self, signature_version='1.0', api_url=None, ak=None, sk=None, api_version
=None):
        assert api_url is not None
        assert ak is not None
        assert sk is not None
        assert api_version is not None

        self.signature_once = 0
        self.signature_method = 'HMAC-SHA1'
        self.signature_version = signature_version
        self.api_version = api_version
        self.format = 'json'
        self.signature_method = 'HMAC-SHA1'
        self.api_url = api_url
```

```
        self.access_key = ak
        self.access_secret = sk

    def __gen_common_params(self, req_type, api_version, access_key, access_secret,
http_params):
        while 1:
            rand_int = random.randint(10, 999999999)
            if rand_int != self.signature_once:
                self.signature_once = rand_int
                break

        # 当前步骤中是否含有AccessKey参数
        if access_key == None:
            return None

        http_params.append(('AccessKeyId', access_key))
        http_params.append(('Format', self.format))
        http_params.append(('Version', api_version))
        timestamp = datetime.datetime.utcnow().strftime("%Y-%m-%dT%H:%M:%SZ")
        http_params.append(('Timestamp', timestamp))
        http_params.append(('SignatureMethod', self.signature_method))
        http_params.append(('SignatureVersion', self.signature_version))
        http_params.append(('SignatureNonce', str(self.signature_once)))
        # 签名
        http_params = self.sign(req_type, http_params, access_secret)
        return urllib.urlencode(http_params)

    def get(self, http_params=[], host=None, execute=True):
        data = self.__gen_common_params('GET', self.api_version, self.access_key, self.
access_secret, http_params)
        api_url = self.api_url

        if data == None:
            url = "%s" % (api_url)
        else:
            url = "%s/?" % api_url + data
        print ("URL: %s"%url)
        if execute is False:
            return url
        ret = {}
        try:
            if host is not None:
                response = requests.get(url,headers={'Host':host}, verify=False)
            else:
                response = requests.get(url, verify=False)
            ret['code'] = response.status_code
            ret['data'] = response.text
        except Exception as e:
            ret['data'] = str(e)

        return ret

    def __get_data(self, http_params):
        params = self.__gen_common_params('POST', self.api_version, self.access_key, self.
access_secret, http_params)
        if params == []:
            data = None
        else:
            data = params.replace("+", "%20")
            data = data.replace("*", "%2A")
            data = data.replace("%7E", "~")
        return data

    def post(self, http_params=[], out_fd=sys.stdout):
```

```
        data = self.__get_data(self.api_version, self.access_key, self.access_secret,
http_params)
        api_url = self.api_url
        out_fd.write(u"[%s] --> (POST):%s\n%s\n" % (datetime.datetime.now(), api_url, data
))
        ret = requests.post(api_url, data, verify=False)
        print (ret.text)
        return ret

    def sign(self, http_method, http_params, secret):
        list_params = sorted(http_params, key=lambda d: d[0])
        #print list_params
        url_encode_str = urllib.urlencode(list_params)
        #print url_encode_str
        url_encode_str = url_encode_str.replace("+", "%20")
        url_encode_str = url_encode_str.replace("*", "%2A")
        url_encode_str = url_encode_str.replace("%7E", "~")
        string_to_sign = http_method + "&%2F&" + urllib.quote(url_encode_str)
        #print string_to_sign
        hmac_key = str(secret + "&")
        sign_value = str(hmac.new(hmac_key, string_to_sign, hashlib.sha1).digest().encode
('base64').rstrip())
        http_params.append(('Signature', sign_value))
        return http_params
```

生成接口调用请求

说明:

以下代码示例以调用**ModifyWafSwitch**接口开启Web应用攻击防护功能为例。

```
from open_api import OpenAPI

class Waf(OpenAPI):
    def __init__(self, api_url, ak, sk, api_version, instance_id, region):

        super(Waf, self).__init__(api_url=api_url, ak=ak, sk=sk, api_version=api_version)
        self.instance_id = instance_id
        self.region = region

    def ModifyWafSwitch(self,domain, instance_id=None, region='cn', service_on=1,
execute=True):
        if instance_id is None:
            instance_id = self.instance_id
        if region is None:
            region = self.region

        params = [
            ('Action', 'ModifyWafSwitch'),
            ('InstanceId', instance_id),
            ('Domain', domain),
            ('Region',region),
            ('ServiceOn', service_on)
        ]

        print (params)

        return self.get(http_params=params,execute=execute)

if __name__ == "__main__":
    api_url = "https://wafopenapi.cn-hangzhou.aliyuncs.com"
    # 填写您账号的AccessKeyId信息
```

```
    ak = ""
    # 填写您账号的AccessKeyScecret信息
    sk = ""
    # 填写您WAF的实例ID，您可以通过调用GetPayInfo接口获取InstanceID信息
    instance_id = ""
    # 填写您WAF实例所在地域信息
    region = ""
    api_version = "2018-01-17"

    t = Waf(api_url=api_url, ak=ak, sk=sk, api_version=api_version, instance_id=instance_id
, region=region)
    print (t.ModifyWafSwitch(domain="", service_on=1))
```

发送HTTP GET请求

通过上述代码得到HTTP请求，向WAF API的服务端地址发送该HTTP GET请求。

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=ModifyWafSwitch&Domain=
www.aliyun.com&ServiceOn=1&Region=cn&InstanceId=waf_elasticity-cn-0xldbqtm005&
TimeStamp=2018-08-23T12:46:24Z&Format=JSON&AccessKeyId=testid&SignatureMethod
=HMAC-SHA1&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&Version=2018-
01-17&SignatureVersion=1.0&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

获得响应结果

最终收到WAF API服务端返回的响应结果。

返回示例

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
 "Result":{
   "Status":2,
   "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 }
}
```

5.1.5 实例信息

5.1.5.1 DescribePayInfo

调用DescribePayInfo接口获取指定地域的WAF实例当前信息。

说明:

请求该API接口时，无需指定**InstanceId**公共请求参数。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePayInfo	要执行的操作。取值：**DescribePayInfo**。
InstanceSource	String	否	waf-cloud	实例来源。默认值：**waf-cloud**。
Region	String	否	cn	地域ID，取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

返回数据

名称	类型	示例值	描述
RequestId	String	276D7566-31C9-4192-9DD1-51B10DAC29D2	请求ID。
Result			返回结果。
EndDate	Long	1512921600	实例到期时间。 **说明：** 对于按量付费实例，表示试用版到期时间。
InDebt	Integer	1	当前实例是否欠费： • **0**：表示已欠费。 • **1**：表示正常。 **说明：** 该参数按量计费WAF实例有意义。
InstanceId	String	waf_elasticity-cn-0xldbqtm005	实例ID。
PayType	Integer	2	WAF实例类型： • **0**：表示未购买或未开通。 • **1**：表示包年包月实例。 • **2**：表示按量付费实例。

名称	类型	示例值	描述
Region	String	cn	所属地域： • **cn**：表示中国大陆地区。 • **cn-hongkong**：表示海外地区。
RemainDay	Integer	0	试用版WAF实例剩余可用天数。 **说明：** 该参数仅对按量计费WAF实例有意义。
Status	Integer	0	WAF实例当前状态： • **0**：表示已到期。 • **1**：表示正常。 **说明：** 该参数仅对包年包月WAF实例有意义。
Trial	Integer	0	是否试用版WAF实例： • **0**：表示否。 • **1**：表示是。 **说明：** 该参数仅对按量计费WAF实例有意义。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribePayInfo
&Region=cn
&公共请求参数
```

正常返回示例

`XML` 格式

```
<DescribePayInfoResponse>
    <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
    <Result>
        <Status>1</Status>
        <Trial>0</Trial>
        <InstanceId>waf_elasticity-cn-0xldbqtm005</InstanceId>
        <InDebt>1</InDebt>
        <Region>cn</Region>
        <RemainDay>0</RemainDay>
```

```
        <PayType>2</PayType>
        <EndDate>1512921600</EndDate>
    </Result>
</DescribePayInfoResponse>
```

JSON 格式

```
{
 "Result":{
  "Status":1,
  "EndDate":1512921600,
  "Region":"cn",
  "InDebt":1,
  "Trial":0,
  "InstanceId":"waf_elasticity-cn-0xldbqtm005",
  "RemainDay":0,
  "PayType":2
 },
 "RequestId":"276D7566-31C9-4192-9DD1-51B10DAC29D2"
}
```

错误码

访问错误中心查看更多错误码。

5.1.5.2 DescribeRegions

调用DescribeRegions接口获取当前WAF支持的地域信息。

说明:

请求该API接口时，无需指定**Region**和**InstanceId**这两个公共请求参数。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeRegions	要执行的操作。取值：**DescribeRegions**。

返回数据

名称	类型	示例值	描述
Regions			地域列表信息。
Region			地域列表信息。

名称	类型	示例值	描述
Display	String	ture	是否在该地域提供WAF服务： • **true**：表示是。 • **false**：表示否。
Region	String	cn	地域ID。
RequestId	String	276D7566-31C9-4192-9DD1-51B10DAC29D2	请求ID。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeRegions
&公共请求参数
```

正常返回示例

XML 格式

```
<DescribeRegionsResponse>
    <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
    <Regions>
        <Region>
            <Region>cn</Region>
            <Display>true</Display>
        </Region>
        <Region>
            <Region>cn-hongkong</Region>
            <Display>true</Display>
        </Region>
    </Regions>
</DescribeRegionsResponse>
```

JSON 格式

```
{
 "RequestId":"276D7566-31C9-4192-9DD1-51B10DAC29D2",
 "Regions":{
  "Region":[
   {
    "region":"cn",
    "display":"true"
   },
   {
    "region":"cn-hongkong",
    "display":"true"
   }
  ]
 }
```

```
}
```

错误码

访问错误中心查看更多错误码。

5.1.5.3 DescribeWafSourceIpSegment

调用DescribeWafSourceIpSegment接口获取WAF实例的回源IP网段列表。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeWafSourceIpSegment	要执行的操作。取值：**DescribeWafSourceIpSegment**。
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明：** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

返回数据

名称	类型	示例值	描述
Ips	String	121.43.18.0/24,120.25.115.0/24,101.200.106.0/24	WAF回源IP网段，网段间以逗号（,）分隔。
RequestId	String	9087ADDC-9047-4D02-82A7-33021B58083C	请求ID。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeWafSourceIpSegment
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Region=cn
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeWafSourceIpSegmentResponse>
    <Ips>121.43.18.0/24,120.25.115.0/24,101.200.106.0/24</Ips>
    <RequestId>9087ADDC-9047-4D02-82A7-33021B58083C</RequestId>
</DescribeWafSourceIpSegmentResponse>
```

JSON 格式

```
{
 "RequestId":"9087ADDC-9047-4D02-82A7-33021B58083C",
 "Ips":"121.43.18.0/24,120.25.115.0/24,101.200.106.0/24"
}
```

错误码

访问错误中心查看更多错误码。

5.1.6 域名配置

5.1.6.1 DescribeDomainNames

调用DescribeDomainNames接口获取指定WAF实例中已添加的域名名称列表。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainNames	要执行的操作。取值：**DescribeDomainNames**。

名称	类型	是否必选	示例值	描述
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	WAF实例ID。 **说明:** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
Region	String	否	cn	WAF实例所在的地域。取值: • **cn**：表示中国内地地区（默认） • **cn-hongkong**：表示海外地区
ResourceGroupId	String	否	default	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	56B40D30-4960-4F19-B7D5-2B1F0EE6CB70	请求ID。
Result	List	{"DomainNames":["1.example.com","2.example.com","3.example.com"]}	已添加的域名名称列表。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&InstanceId=waf_elasticity-cn-0xldbqt****
&公共请求参数
```

正常返回示例

`XML` 格式

```
<DescribeDomainNamesResponse>
  <Result>
    <DomainNames>1.example.com</DomainNames>
    <DomainNames>2.example.com</DomainNames>
    <DomainNames>3.example.com</DomainNames>
  </Result>
  <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
```

```
</DescribeDomainNamesResponse>
```

JSON 格式

```
{
 "Result":{
  "DomainNames":[
   "1.example.com",
   "2.example.com",
   "3.example.com"
  ]
 },
 "RequestId":"56B40D30-4960-4F19-B7D5-2B1F0EE6CB70"
}
```

错误码

访问错误中心查看更多错误码。

5.1.6.2 DescribeDomainConfig

调用DescribeDomainConfig接口获取指定域名的转发配置信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainConfig	要执行的操作。取值：**DescribeDomainConfig**。
Domain	String	是	rstest.cdn.com	已添加的域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明:** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

返回数据

名称	类型	示例值	描述
RequestId	String	56B40D30-4960-4F19-B7D5-2B1F0EE6CB70	请求ID。
Result			返回结果。
DomainConfig			域名配置结构体。
Cname	String	xxxxxxxxxxxxxx.fakewaf.com	WAF实例分配的CNAME。
ProtocolType	Integer	2	协议类型： • **0**：表示支持HTTP协议。 • **1**：表示支持HTTPS协议。 • **2**：表示同时支持HTTP和HTTPS协议。
SourceIps	String	1.1.1.1	源站IP。
Status	Integer	2	请求执行状态： • **0**：表示该请求等待执行。 • **1**：表示该请求正在执行中。 • **2**：表示该请求已执行完成。
WafTaskId	String	aliyun.waf.20180712180229702.Y6re3d	WAF的请求ID。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainConfig
&Domain=www.aliyun.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&公共请求参数
```

正常返回示例

XML 格式

```
<DescribeDomainConfigResponse>
    <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
    <Result>
```

```
        <Status>2</Status>
        <DomainConfig>
            <ProtocolType>2</ProtocolType>
            <SourceIps>x.x.x.x</SourceIps>
            <SourceIps>x.x.x.x</SourceIps>
            <Cname>xxxxxxxxxxxxxx.fakewaf.com</Cname>
        </DomainConfig>
        <WafTaskId>aliyun.waf.20180712180229702.Y6re3d</WafTaskId>
    </Result>
</DescribeDomainConfigResponse>
```

JSON 格式

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712180229702.Y6re3d",
  "DomainConfig":{
   "Cname":"xxxxxxxxxxxxx.fakewaf.com",
   "ProtocolType":2,
   "SourceIps":[
    "x.x.x.x",
    "x.x.x.x"
   ]
  },
 "RequestId":"56B40D30-4960-4F19-B7D5-2B1F0EE6CB70"
}
```

错误码

访问错误中心查看更多错误码。

5.1.6.3 DescribeDomainConfigStatus

调用DescribeDomainConfigStatus接口查询指定域名的转发配置是否生效。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainConfigStatus	要执行的操作。取值：**DescribeDomainConfigStatus**。
Domain	String	是	rstest.cdn.com	已添加的域名名称。

名称	类型	是否必选	示例值	描述
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明:** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
Region	String	否	cn	WAF实例所在的地域。取值: • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。
Result			返回结果。
DomainConfig			域名转发配置结构体。
ConfigStatus	String	1	域名转发配置生效状态: • **0**：表示未生效。 • **1**：表示已生效。 • **-1**：表示尚未检测完成。
Status	Integer	2	请求执行状态: • **0**：表示该请求等待执行。 • **1**：表示该请求正在执行中。 • **2**：表示该请求已执行完成。
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	WAF的请求ID。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainConfigStatus
```

```
&Domain=www.aliyun.com
&公共请求参数
```

正常返回示例

XML 格式

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
<Result>
   <Status>2</Status>
   <DomainConfig>
      <ConfigStatus>1</ConfigStatus>
   </DomainConfig>
   <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
</Result>
```

JSON 格式

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a",
  "DomainConfig":{
   "ConfigStatus":1
  }
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.1.6.4 CreateDomainConfig

调用CreateDomainConfig接口添加域名配置信息。

通过调用API接口，将您的域名接入WAF实例实现Web安全防护，建议您参考以下步骤：

1. 调用CreateDomainConfig接口添加域名配置信息。

2. 根据返回结果中的**WafTaskId**值，调用DescribeAsyncTaskStatus接口查看添加域名配置任务的执行进度。当该任务已完成时，说明域名配置信息已成功添加。

3. 调用DescribeDomainConfigStatus接口确认该域名配置是否生效。

说明：

只有当返回结果显示配置已经生效后，您才可以将业务流量切换至WAF实例。

4. 调用DescribeDomainConfig接口查看WAF实例为该域名分配的CNAME。

5. 在域名DNS解析服务提供商处，修改该域名的解析记录，将业务流量切换至WAF。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateDomainConfig	要执行的操作。取值：**CreateDomainConfig**。
Domain	String	是	rstest.cdn.com	域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明：** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
IsAccessProduct	Integer	是	0	该域名在WAF前是否配置有七层代理（例如，高防、CDN等），取值： • **0**：表示无。 • **1**：表示有。
Protocols	String	是	["http"]	该域名所支持的访问协议，取值： • **http**：表示支持HTTP协议。 • **https**：表示支持HTTPS协议。 • **http,https**：同时支持HTTP、HTTPS协议。
SourceIps	String	否	["1.1.1.1"]	源站IP，支持指定多个IP。数组类型，示例值：["1.1.1.1"]。

名称	类型	是否必选	示例值	描述
HttpPort	String	否	[80]	HTTP协议配置的端口。指定多个HTTP端口时，使用“,”进行分隔。示例值：[80]。  **说明：** 配置协议为HTTP时，该参数为必填项。默认值为**80**。**HttpPort**与**HttpsPort**两个请求参数至少需要填一个。
HttpsPort	String	否	[443]	HTTPS协议配置的端口。指定多个HTTPS端口时，使用“,”进行分隔。示例值：[443]。  **说明：** 配置协议为HTTPS时，该参数为必填项。默认值为**443**。**HttpPort**与**HttpsPort**两个请求参数至少需要填一个。
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区
LoadBalancing	Integer	否	0	回源负载均衡策略，取值： • **0**：表示IP Hash方式。 • **1**：表示轮询方式。
HttpToUserIp	Integer	否	0	是否开启HTTPS访问请求通过HTTP协议转发回源站，取值： • **0**：表示关闭 （默认） • **1**：表示开启  **说明：** 如果您的网站不支持HTTPS回源，开启HTTP回源（默认回源端口是80端口）功能项，即可通过WAF实现HTTPS访问。

名称	类型	是否必选	示例值	描述
HttpsRedirect	Integer	否	0	是否开启HTTPS强制跳转，取值： • **0**：表示关闭 （默认） • **1**：表示开启 **说明：** 仅使用HTTPS访问协议时需填写该请求参数。开启强制跳转后HTTP请求将显示为HTTPS，默认跳转至443端口。
RsType	Integer	否	0	该域名的回源地址类型，取值： • **0**：表示回源到IP。 • **1**：表示回源到域名。
ResourceGroupId	String	否	rs1234	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。
Result	Struct		返回结果。
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	WAF的请求ID。
Status	Integer	2	请求执行状态： • **0**：表示该请求等待执行。 • **1**：表示该请求正在执行中。 • **2**：表示该请求已执行完成。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=CreateDomainConfig
&Domain=www.aliyun.com
&SourceIps=["x.x.x.x","x.x.x.x"]
&Protocols=["http","https"]
```

```
&HttpPort=[80]
&HttpsPort=[443]
&RsType=0
&IsAccessProduct=0
&LoadBalancing=0
&HttpsRedirect=1
&HttpToUserIp=0
&公共请求参数
```

正常返回示例

XML 格式

```
<CreateDomainConfigResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</CreateDomainConfigResponse>
```

JSON 格式

```
{
   "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
   "Result":{
      "Status":2,
      "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
   }
}
```

错误码

访问错误中心查看更多错误码。

5.1.6.5 ModifyDomainConfig

调用ModifyDomainConfig接口修改指定域名配置信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyDomainConfig	要执行的操作。取值：**ModifyDomainConfig**。
Domain	String	是	rstest.cdn.com	域名名称。

名称	类型	是否必选	示例值	描述
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。  **说明:** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
IsAccessProduct	Integer	是	0	该域名在WAF前是否配置有七层代理（例如，高防、CDN等），取值： • **0**：表示无。 • **1**：表示有。
Protocols	String	是	["http"]	该域名所支持的访问协议，取值： • **http**：表示支持HTTP协议。 • **https**：表示支持HTTPS协议。 • **http,https**：同时支持HTTP、HTTPS协议。
HttpPort	String	否	[80]	HTTP协议配置的端口。指定多个HTTP端口时，使用“,”进行分隔。示例值：[80]。  **说明:** 配置协议为HTTP时，该参数为必填项。默认值为**80**。**HttpPort**与**HttpsPort**两个请求参数至少需要填一个。
HttpToUserIp	Integer	否	0	是否开启HTTPS访问请求通过HTTP协议转发回源站，取值： • **0**：表示关闭 （默认） • **1**：表示开启  **说明:** 如果您的网站不支持HTTPS回源，开启HTTP回源（默认回源端口是80端口）功能项，即可通过WAF实现HTTPS访问。

名称	类型	是否必选	示例值	描述
HttpsPort	String	否	[443]	HTTPS协议配置的端口。指定多个HTTPS端口时，使用“,”进行分隔。示例值：[443]。 **说明：** 配置协议为HTTPS时，该参数为必填项。默认值为**443**。**HttpPort**与**HttpsPort**两个请求参数至少需要填一个。
HttpsRedirect	Integer	否	1	Https跳转状态。取值： • **1**：开启 • **0**：关闭（默认）
LoadBalancing	Integer	否	0	负载均衡的方式，取值： • **0**：IP hash • **1**：轮询
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区
SourceIps	String	否	["1.1.1.1"]	源站IP，支持指定多个IP。示例：["1.1.1.1"]。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。
Result			返回结果。
Status	Integer	2	请求执行状态： • **0**：表示该请求等待执行。 • **1**：表示该请求正在执行中。 • **2**：表示该请求已执行完成。

名称	类型	示例值	描述
WafTaskId	String	aliyun.waf.2018071221 4032277.qmxI9a	WAF的请求ID。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=ModifyDomainConfig
&Domain=www.aliyun.com
&SourceIps=["x.x.x.x","x.x.x.x"]
&Protocols=["http","https"]
&HttpPort=[80]
&HttpsPort=[443]
&IsAccessProduct=0
&HttpsRedirect=1
&HttpToUserIp=0
&公共请求参数
```

正常返回示例

XML 格式

```
<ModifyDomainConfigResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</ModifyDomainConfigResponse>
```

JSON 格式

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.1.6.6 DeleteDomainConfig

调用DeleteDomainConfig接口删除指定域名配置信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteDomainConfig	要执行的操作。取值：**DeleteDomainConfig**。
Domain	String	是	rstest.cdn.com	已添加的域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明：** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。
Result			返回结果。
Status	Integer	2	请求执行状态： • **0**：表示该请求等待执行。 • **1**：表示该请求正在执行中。 • **2**：表示该请求已执行完成。

名称	类型	示例值	描述
WafTaskId	String	aliyun.waf.2018071221 4032277.qmxI9a	WAF的请求ID。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DeleteDomainConfig
&Domain=www.aliyun.com
&公共请求参数
```

正常返回示例

`XML` 格式

```
<DeleteDomainConfigResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</DeleteDomainConfigResponse>
```

`JSON` 格式

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.1.6.7 CreateCertAndKey

调用CreateCertAndKey接口为已添加的域名配置记录上传证书及私钥信息。

说明:

您也可以调用该接口为指定域名配置更新已上传的证书及私钥信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateCertAndKey	要执行的操作。取值：**CreateCertAndKey**。
Cert	String	是	-----BEGIN CERTIFICATE----------END CERTIFICATE-----	证书文件内容。
Domain	String	是	rstest.cdn.com	域名名称。
HttpsCertName	String	是	www.aliyun.com	证书名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明:** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
Key	String	是	-----BEGIN RSA PRIVATE KEY----------END RSA PRIVATE KEY-----	私钥文件内容
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。
Result			返回结果。

名称	类型	示例值	描述
Status	Integer	2	请求执行状态： • **0**：表示该请求等待执行。 • **1**：表示该请求正在执行中。 • **2**：表示该请求已执行完成。
WafTaskId	String	aliyun.waf.2018071221 4032277.qmxI9a	WAF的请求ID。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DeleteDomainConfig
&Domain=www.aliyun.com
&Cert="-----BEGIN CERTIFICATE----------END CERTIFICATE-----"
&Key="-----BEGIN RSA PRIVATE KEY----------END RSA PRIVATE KEY-----"
&HttpsCertName=www.aliyun.com
&公共请求参数
```

正常返回示例

`XML` 格式

```
<CreateCertAndKeyResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</CreateCertAndKeyResponse>
```

`JSON` 格式

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.1.7 Web攻击防护配置

5.1.7.1 ModifyWafSwitch

调用ModifyWafSwitch接口打开或关闭Web攻击防护功能开关。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyWafSwitch	要执行的操作。取值：**ModifyWafSwitch**。
Domain	String	是	rstest.cdn.com	域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明：** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
ServiceOn	Integer	是	1	Web攻击防护功能开关，取值： • **0**：表示关闭。 • **1**：表示开启。
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。
Result			返回结果。

名称	类型	示例值	描述
Status	Integer	2	请求执行状态： • **0**：表示该请求等待执行。 • **1**：表示该请求正在执行中。 • **2**：表示该请求已执行完成。
WafTaskId	String	aliyun.waf.2018071221 4032277.qmxI9a	WAF的请求ID。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=ModifyWafSwitch
&Domain=www.aliyun.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&ServiceOn=1
&公共请求参数
```

正常返回示例

`XML` 格式

```
<ModifyWafSwitchResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</ModifyWafSwitchResponse>
```

`JSON` 格式

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.1.8 精准访问控制配置

5.1.8.1 DescribeAclRules

调用DescribeAclRules接口获取指定域名的精准访问控制规则列表。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeAclRules	要执行的操作。取值：**DescribeAclRules**。
CurrentPage	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。
Domain	String	是	www.aliyun.com	域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明:** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
PageSize	Integer	是	10	页面显示最大记录数量。
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。
Result			返回结果。

名称	类型	示例值	描述
AclRules			精准访问控制规则列表，其中每条精准访问控制规则都会以AclRule子参数表述。AclRule子参数以JSON格式的字符串表述。
AclRule			精准访问控制规则列表，其中每条精准访问控制规则都会以AclRule子参数表述。AclRule子参数以JSON格式的字符串表述。
Action	Integer	1	规则的匹配动作，取值： • **0**：表示阻断，即命中该规则的匹配条件，则阻断该访问请求。 • **1**：表示放行，即命中该规则的匹配条件，则放行该访问请求。 • **2**：表示告警，即命中该规则的匹配条件，将放行该访问请求，但会记录该请求并告警。
Conditions			规则匹配条件结构体。
condition			规则匹配条件结构体。
Contain	String	1	逻辑符： • **0**：表示不包含。 • **1**：表示包含。 • **2**：表示不存在。 • **10**：表示不等于。 • **11**：表示等于。 • **20**：表示长度小于。 • **21**：表示长度等于。 • **22**：表示长度大于。 • **30**：表示值小于。 • **31**：表示值等于。 • **32**：表示值大于。

名称	类型	示例值	描述
Key	String	url	匹配字段，包括IP、URL、Referer、User-Agent、Params、Cookie、Content-Type、X-Forwarded-For、Content-Length、Post-Body、Http-Method、Header。 **说明：** 说明：不同版本的WAF实例支持的匹配字段不同，您可以在Web应用防火墙管理控制台中查看您的实例当前所支持的匹配字段。
Value	String	login	匹配内容。
ContinueBlockGeo	Integer	1	是否继续执行地区封禁，取值： • **0**：表示否。 • **1**：表示是。
ContinueCc	Integer	1	是否继续执行CC防护规则检测，取值： • **0**：表示否。 • **1**：表示是。
ContinueDataRiskControl	Integer	1	是否继续执行数据风控防护，取值： • **0**：表示否。 • **1**：表示是。
ContinueSA	Integer	1	是否继续执行智能防护引擎规则检测，取值： • **0**：表示否。 • **1**：表示是。
ContinueSdk	Integer	1	是否继续执行SDK防护，取值： • **0**：表示否 • **1**：表示是。

名称	类型	示例值	描述
ContinueWaf	Integer	1	是否继续执行Web攻击防护规则检测，取值： • **0**：表示否。 • **1**：表示是。
Id	Long	1111	ACL规则ID。
IsDefault	Integer	1	是否默认规则： • **0**：表示否。 • **1**：表示是。
Name	String	test	规则名称。
Order	Integer	1	规则顺序。 **说明：** 说明：该值越大，规则的优先级越高。
Total	Integer	1	规则总数。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeAclRules
&Domain=www.aliyun.com
&CurrentPage=1
&PageSize=50
&公共请求参数
```

正常返回示例

XML 格式

```
<DescribeAclRulesResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <AclRules>
            <AclRule>
                <IsDefault>1</IsDefault>
                <Order>0</Order>
                <ContinueBlockGeo>1</ContinueBlockGeo>
                <Action>1</Action>
                <ContinueWaf>1</ContinueWaf>
                <ContinueSdk>0</ContinueSdk>
```

```
                <Id>16572</Id>
                <ContinueCc>1</ContinueCc>
                <Conditions>
                    <condition>
                        <key>URL</key>
                        <contain>1</contain>
                        <value>asfas</value>
                    </condition>
                </Conditions>
                <Name>default</Name>
                <ContinueDataRiskControl>1</ContinueDataRiskControl>
                <ContinueSA>1</ContinueSA>
            </AclRule>
        </AclRules>
        <Total>1</Total>
    </Result>
</DescribeAclRulesResponse>
```

JSON 格式

```
{
 "Result":{
  "AclRules":{
   "AclRule":[
    {
     "Name":"default",
     "Conditions":{
      "condition":[
       {
        "contain":1,
        "value":"asfas",
        "key":"URL"
       }
      ]
     },
     "ContinueDataRiskControl":1,
     "Action":1,
     "ContinueSdk":0,
     "ContinueWaf":1,
     "IsDefault":1,
     "Order":0,
     "Id":16572,
     "ContinueCc":1,
     "ContinueSA":1,
     "ContinueBlockGeo":1
    }
   ]
  },
  "Total":1
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.1.8.2 CreateAclRule

调用CreateAclRule接口为指定域名添加精准访问控制规则。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateAclRule	要执行的操作。取值：**CreateAclRule**。
Domain	String	是	rstest.cdn.com	域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明:** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。

名称	类型	是否必选	示例值	描述
Rules	String	是	{"conditions":[{"key":"URL","contain":1,"value":"asfas"}],"continueComponent":{"post_action_cc":1,"post_action_waf":1,"post_action_sa":1,"post_action_block_geo":"0","post_action_data_risk_control":"1"},"action":"1","name":"lei123"}	精准访问控制规则详细信息，采用JSON格式的字符串表述，具体结构见下表。 • **Id**：Long类型，可选，规则ID。 • **Name**：String类型，必选，规则名称。 • **Action**：Integer类型，必选，规则的匹配动作，取值： - **0**：表示阻断，即命中该规则的匹配条件，则阻断该访问请求。 - **1**：表示放行，即命中该规则的匹配条件，则放行该访问请求。 - **2**：表示告警，即命中该规则的匹配条件，将放行该访问请求，但会记录该请求并告警。 • **ContinueComponent**：String类型，可选，是否继续执行其它WAF防护策略，采用JSON格式的字符串表述，具体结构见下表。 - **post_action_cc**，Integer类型，可选，是否继续执行CC防护规则检测，取值： ■ **0**：表示否。 ■ **1**：表示是。 - **post_action_waf**，Integer类型，可选，是否继续执行Web攻击防护规则检测，取值： ■ **0**：表示否。 ■ **1**：表示是。 - **post_action_sa**，Integer类型，可选，是否继续执行智能防护引擎规则检测，取值： ■ **0**：表示否。 ■ **1**：表示是。 - **post_action_block_geo**，Integer类型，可选，是否继续执行地区封禁，取值： ■ **0**：表示否。

名称	类型	是否必选	示例值	描述
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

匹配字段和逻辑符的映射关系

匹配字段	逻辑符
IP	属于、不属于
Referer	包含、不包含、等于、不等于、长度小于、长度等于、长度大于
User-Agent	包含、不包含、等于、不等于、长度小于、长度等于、长度大于
Param	包含、不包含、等于、不等于、长度小于、长度等于、长度大于
Cookie	包含、不包含、等于、不等于、长度小于、长度等于、长度大于、不存在
Content-Type	包含、不包含、等于、不等于、长度小于、长度等于、长度大于
X-Forwarded-For	包含、不包含、等于、不等于、长度小于、长度等于、长度大于、不存在
Content-Length	值小于、值等于、值大于
Post-Body	包含、不包含、等于、不等于
Http-Method	等于、不等于
Header	包含、不包含、等于、不等于、长度小于、长度等于、长度大于、不存在

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	该请求的ID。
Result			返回结果。
Status	Integer	2	请求执行状态： • **0**：表示该请求等待执行。 • **1**：表示该请求正在执行中。 • **2**：表示该请求已执行完成。
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	WAF的请求ID。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=CreateAclRule
&Domain=www.aliyun.com
&ServiceOn=1
&Rules={...}
&公共请求参数
```

正常返回示例

XML 格式

```
<CreateAclRuleResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</CreateAclRuleResponse>
```

JSON 格式

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
```

```
}
```

错误码

访问错误中心查看更多错误码。

5.1.8.3 ModifyAclRule

调用ModifyAclRule接口修改指定精准访问控制规则。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyAclRule	要执行的操作。取值：**ModifyAclRule**。
Domain	String	是	rstest.cdn.com	域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明:** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。

名称	类型	是否必选	示例值	描述
Rules	String	是	{"conditions":[{"key":"URL","contain":1,"value":"asfas"}],"continueComponent":{"post_action_cc":1,"post_action_waf":1,"post_action_sa":1,"post_action_block_geo":"0","post_action_data_risk_control":"1"},"action":"1","name":"lei123","id":65899}	精准访问控制规则详细信息，采用JSON格式的字符串表述，具体结构见下表。 • **Id**：Long类型，必选，规则ID。 • **Name**：String类型，必选，规则名称。 • **Action**：Integer类型，必选，规则的匹配动作，取值： - **0**：表示阻断，即命中该规则的匹配条件，则阻断该访问请求。 - **1**：表示放行，即命中该规则的匹配条件，则放行该访问请求。 - **2**：表示告警，即命中该规则的匹配条件，将放行该访问请求，但会记录该请求并告警。 • **ContinueComponent**：String类型，可选，是否继续执行其它WAF防护策略，采用JSON格式的字符串表述，具体结构见下表。 - **post_action_cc**，Integer类型，可选，是否继续执行CC防护规则检测，取值： ■ **0**：表示否。 ■ **1**：表示是。 - **post_action_waf**，Integer类型，可选，是否继续执行Web攻击防护规则检测，取值： ■ **0**：表示否。 ■ **1**：表示是。 - **post_action_sa**，Integer类型，可选，是否继续执行智能防护引擎规则检测，取值： ■ **0**：表示否。 ■ **1**：表示是。 - **post_action_block_geo**，Integer类型，可选，是否继续执行地区封禁，取值： ■ **0**：表示否。

名称	类型	是否必选	示例值	描述
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

匹配字段和逻辑符的映射关系

匹配字段	逻辑符
IP	属于、不属于
Referer	包含、不包含、等于、不等于、长度小于、长度等于、长度大于
User-Agent	包含、不包含、等于、不等于、长度小于、长度等于、长度大于
Param	包含、不包含、等于、不等于、长度小于、长度等于、长度大于
Cookie	包含、不包含、等于、不等于、长度小于、长度等于、长度大于、不存在
Content-Type	包含、不包含、等于、不等于、长度小于、长度等于、长度大于
X-Forwarded-For	包含、不包含、等于、不等于、长度小于、长度等于、长度大于、不存在
Content-Length	值小于、值等于、值大于
Post-Body	包含、不包含、等于、不等于
Http-Method	等于、不等于
Header	包含、不包含、等于、不等于、长度小于、长度等于、长度大于、不存在

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。
Result	Struct		返回结果。
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	WAF的请求ID。
Status	Integer	2	请求执行状态： • **0**：表示该请求等待执行。 • **1**：表示该请求正在执行中。 • **2**：表示该请求已执行完成。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=ModifyAclRule
&Domain=www.aliyun.com
&ServiceOn=1
&Rules={...}
&公共请求参数
```

正常返回示例

`XML` 格式

```
<ModifyAclRuleResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</ModifyAclRuleResponse>
```

`JSON` 格式

```
{
   "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
   "Result":{
      "Status":2,
      "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
   }
```

```
}
```

错误码

访问错误中心查看更多错误码。

5.1.8.4 DeleteAclRule

调用DeleteAclRule接口删除指定精准访问控制规则。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteAclRule	要执行的操作。取值：**DeleteAclRule**。
Domain	String	是	rstest.cdn.com	域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明：** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
RuleId	Long	是	65899	精准访问控制规则ID。
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。
Result			返回结果。

名称	类型	示例值	描述
Status	Integer	2	请求执行状态： • **0**：表示该请求等待执行。 • **1**：表示该请求正在执行中。 • **2**：表示该请求已执行完成。
WafTaskId	String	aliyun.waf.2018071221 4032277.qmxI9a	WAF的请求ID。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DeleteAclRule
&Domain=www.aliyun.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&RuleId=65899
&公共请求参数
```

正常返回示例

`XML` 格式

```
<DeleteAclRuleResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</DeleteAclRuleResponse>
```

`JSON` 格式

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.1.9 异步任务信息

查看WAF API任务执行状态。

5.1.9.1 DescribeAsyncTaskStatus

调用DescribeAsyncTaskStatus接口查询WAF任务执行状态。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeAsyncTaskStatus	要执行的操作。取值：**DescribeAsyncTaskStatus**。
InstanceId	String	是	waf_elasticity-cn-0xldbqtm005	WAF实例ID。 **说明：** 您可以通过调用DescribePayInfo接口查看您当前WAF实例ID。
WafRequestId	String	是	aliyun.waf.20180719140433783.SvaZeY	WAF任务ID。
Region	String	否	cn	WAF实例所在的地域。取值： • **cn**：表示中国大陆地区（默认） • **cn-hongkong**：表示海外地区

返回数据

名称	类型	示例值	描述
RequestId	String	12EF3845-CCEB-4B84-AE60-2B49B2FF1EE5	请求ID。
Result			返回结果
AsyncTaskStatus	String	2	异步任务执行状态： • **0**：表示该请求等待执行。 • **1**：表示该请求正在执行中。 • **2**：表示该请求已执行完成。

名称	类型	示例值	描述
Data	String	xx	异步任务需要返回的业务数据。
ErrCode	String	400	错误代码。 **说明:** 该参数仅在请求执行发生错误时返回。
ErrMsg	String	xx	错误信息描述。 **说明:** 该参数仅在请求执行发生错误时返回。
Progress	Integer	90	异步任务执行进度（百分比）。

示例

请求示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeAsyncTaskStatus
&InstanceId=waf_elasticity-cn-0xldbqtm005
&WafRequestId=aliyun.waf.20180719140433783.SvaZeY
&公共请求参数
```

正常返回示例

XML 格式

```
<DescribeAsyncTaskStatusResponse>
    <RequestId>12EF3845-CCEB-4B84-AE60-2B49B2FF1EE5</RequestId>
    <Result>
        <DomainConfig>
            <Progress>100</Progress>
            <AsyncTaskStatus>2</AsyncTaskStatus>
        </DomainConfig>
    </Result>
</DescribeAsyncTaskStatusResponse>
```

JSON 格式

```
{
 "Result":{
  "DomainConfig":{
   "AsyncTaskStatus":2,
   "Progress":100
  }
 },
 "RequestId":"12EF3845-CCEB-4B84-AE60-2B49B2FF1EE5"
```

```
}
```

错误码

访问错误中心查看更多错误码。