阿里云
Web应用防火墙

用户指南

文档版本：20190909

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
	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，恢复业务所需时间约10分钟。
	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。	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。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *`{stand | slave}`*

目录

法律声明.....I
通用约定.....I
1 WAF功能使用概览..... 1
2 使用透明代理模式接入WAF.....7
3 使用DNS配置模式接入WAF..... 11
3.1 网站配置.....11
3.2 业务接入WAF配置.....18
3.3 放行WAF回源IP段.....23
3.4 本地验证.....24
3.5 更新HTTPS证书..... 26
3.6 HTTPS高级配置..... 29
3.7 非标端口支持.....31
3.8 标记WAF回源流量.....32
3.9 WAF源站负载均衡.....33
3.10 同时部署WAF和DDoS高防.....34
3.11 同时部署WAF和CDN..... 36
4 资产管理.....40
5 防护配置.....43
5.1 IPv6环境防护支持..... 43
5.2 Web应用攻击防护..... 44
5.3 大数据深度学习引擎.....45
5.4 CC安全防护.....47
5.5 自定义CC防护.....49
5.6 精准访问控制.....52
5.7 封禁地区.....60
5.8 IP黑白名单配置.....61
5.9 数据风控.....64
5.10 网站防篡改..... 72
5.11 防敏感信息泄露..... 74
5.12 高频Web攻击IP自动封禁..... 79
5.13 目录遍历防护..... 81
5.14 扫描威胁情报..... 83
5.15 主动防御..... 84
6 防护统计.....88
6.1 业务总览.....88
6.2 安全报表.....96
6.3 全量日志查询.....98
6.4 数据大屏..... 104

7 设置.....110
7.1 功能与规格配置（按量付费模式）..... 110
7.2 查看产品信息..... 114
7.3 自定义规则组..... 117
7.4 配置WAF告警..... 122
7.5 关闭WAF..... 124
8 日志实时查询分析.....126
8.1 WAF日志实时分析简介..... 126
8.2 计费方式..... 133
8.3 配置WAF日志服务..... 135
8.4 日志采集..... 136
8.5 日志分析..... 139
8.6 日志报表..... 155
8.7 日志字段说明..... 163
8.8 高级管理..... 166
8.9 导出日志..... 167
8.10 为子账号授予日志查询分析权限.....169
8.11 日志存储空间管理.....171
9 安全服务.....173
9.1 开通WAF安全服务授权..... 173
9.2 查看安全专家操作日志..... 175
9.3 取消WAF安全服务授权..... 176
10 WAF产品托管服务..... 178

1 WAF功能使用概览

本文介绍在开通和使用阿里云Web应用防火墙（WAF）过程中遇到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、旗舰版三种订阅规格。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。我们结和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国内省份或海外地区的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。

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

通过WAF最佳实践，更好地应用和管理WAF。

操作导航

- 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。

有问题，找专家

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:**
> 请参考钉钉官网，下载并安装钉钉聊天软件。

2 使用透明代理模式接入WAF

WAF透明代理模式向您提供一种简便的接入阿里云Web应用防火墙（WAF）的方法。本文介绍了使用透明代理模式接入WAF的具体操作。

前提条件

只有满足以下条件才能使用WAF透明代理模式：

- 您的WAF实例为包年包月模式。
- 源站服务器部署在阿里云ECS，且ECS实例所在地域为华北2（北京）。
- 源站ECS实例拥有公网IP或已绑定弹性公网IP（EIP）。

> 说明：
> WAF透明代理接入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

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。具体操作见本文操作步骤。
- 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控制台添加一个网站配置并更新域名的DNS设置。具体操作请参见网站配置、业务接入WAF配置。

透明代理模式优势

- 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。
- 自动透明的流量迁移，无需修改域名DNS记录，避免对业务造成影响。

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。
3. 选择透明代理模式。

4. （可选） 单击立即授权。

> **说明:**
> 首次使用透明代理时，您需要授权阿里云Web应用防火墙访问您的ECS实例信息。若已完成过授权，请直接执行步骤6。

5. （可选） 在云资源访问授权页面，单击同意授权。

完成授权后直接跳转到添加域名页面，请直接执行步骤7。

6. （可选） 单击添加域名。
7. 在添加域名页面，输入要防护的域名，并从左侧WAF读取到的当前云账号中符合前提条件的ECS服务器IP中，选择域名对应的源站IP地址。

> **说明:**

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WAF进行分析、处理；WAF将根据为该域名所配置的防护策略检测访问请求，并将处理后的请求回注到源站服务器。

8. 确认其他配置，并单击确认，完成域名添加。

添加域名后自动触发流量牵引，您可以在服务器IP管理中查看已配置IP的牵引状态。

流量牵引状态包括：

- 已牵引：表示该服务器IP 80端口接收到的所有HTTP协议流量都将自动牵引至WAF进行监控。

- 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。

对于不再需要流量牵引的服务器IP，您可以在服务器IP管理中删除对应记录。

> **说明:**
> 在删除网站配置时，对应的服务器IP流量牵引不会随之删除，您需要在服务器IP管理中执行删除操作。

后续步骤

使用透明代理模式成功接入WAF后，请参见WAF防护配置，为域名配置防护策略。

3 使用DNS配置模式接入WAF

3.1 网站配置

网站配置指在Web应用防火墙（WAF）控制台上配置启用WAF防护的网站的转发信息。本文介绍了通过DNS配置模式接入WAF时，如何添加和管理网站配置。

背景信息

> **说明:**
> 如果您通过包年包月方式开通WAF，且您的源站服务器部署在阿里云ECS（华北2地域），同时ECS实例拥有公网IP或已绑定弹性公网IP（EIP），则您可以使用透明代理模式接入WAF。
>
> - 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。具体操作请参见使用透明代理模式接入WAF。
> - 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并更新域名的DNS设置。

使用DNS配置模式接入WAF时，您可以选择自动添加网站配置或手动添加网站配置。

- 自动添加网站配置。添加网站配置时，WAF可以自动读取阿里云云解析DNS控制台中的解析A记录，获取网站域名和源站服务器IP地址，帮助您自动添加网站配置。自动添加网站配置后，WAF也会自动更新域名的解析记录，完成网站接入。
- 手动添加网站配置。如果域名的DNS解析没有托管在阿里云云解析DNS上，您只能手动添加网站配置，并在域名的DNS服务商处手动修改DNS解析，将网站收到的Web请求转发至WAF进行监控，完成网站接入。

  关于手动修改DNS解析的方法，请参见#unique_53。

> **说明:**
> 允许添加的网站配置数量由WAF实例规格和扩展域名包数量决定，具体请参见扩展域名包。

如果网站配置中的源站服务器地址、服务协议、端口等信息发生变化，或者您需要调整HTTPS高级设置功能，您可以编辑网站配置。

对于不再需要WAF防护的域名，您可以在恢复其DNS解析后，删除网站配置。

自动添加网站配置

前提条件

- 要防护的网站的DNS解析托管在阿里云云解析DNS，且其解析记录中存在至少一条生效的A记录。

  推荐您使用阿里云云解析DNS，相关操作请参见设置域名解析。

  如果您暂时无法使用阿里云云解析DNS，建议您参见网站配置，手动添加网站配置。
- （仅针对中国大陆地域）网站已经通过中华人民共和国工业和信息化部ICP备案。

  推荐您使用阿里云备案服务，相关操作请参见备案导航。

  > 注意:
  > 如果您添加的网站域名尚未通过工信部域名备案，请务必尽快完成备案。WAF将不定期自动释放未通过备案的域名配置记录。
- （仅针对支持HTTPS协议的网站）获取网站的HTTPS证书和私钥文件，或者已将证书托管在阿里云证书服务。

  推荐您使用阿里云SSL证书服务对云上证书进行统一管理，相关操作请参见证书服务快速入门。

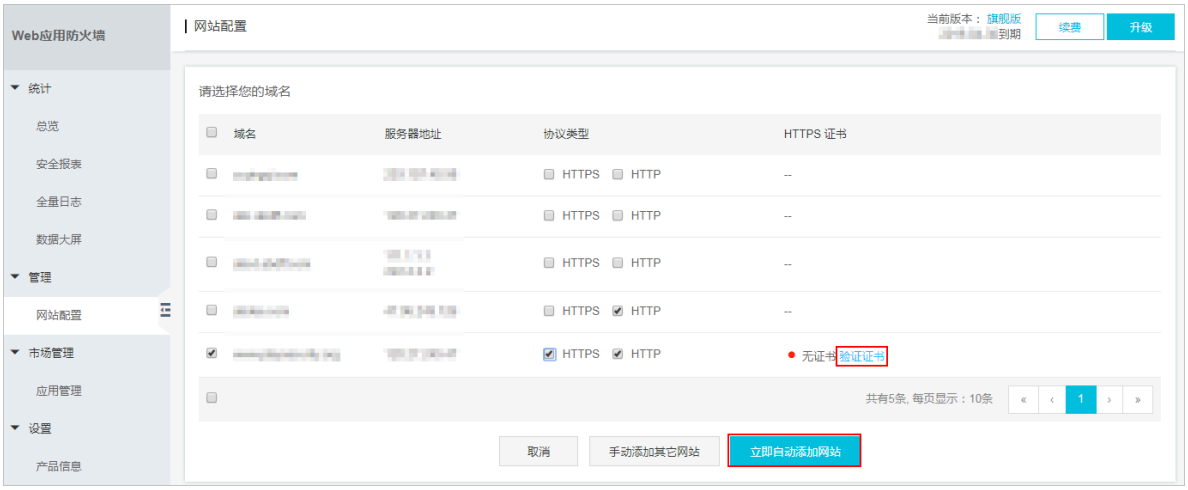
操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆、海外地区。
3. 前往管理 > 网站配置页面，选择DNS配置模式。

4. 单击添加网站。

   WAF自动罗列出当前阿里云账号在云解析DNS中已添加过解析A记录的域名。如果云解析DNS中无任何解析A记录，则不会出现请选择您的域名页面，建议您参见网站配置，手动添加网站配置。

   > 说明:
   > 如果您添加的网站域名尚未通过工信部域名备案，请务必尽快完成备案。WAF将不定期自动释放未通过备案的域名配置记录。



5. 在请选择您的域名页面勾选要防护的域名及协议类型。

6. （可选） 如果协议类型包括HTTPS，您必须先完成证书验证，才能添加网站。

   > 说明:
   > 您也可以先不勾选HTTPS，在完成网站配置后，参见更新HTTPS证书上传证书。

   a) 单击验证证书。

   b) 在验证证书对话框中上传证书和私钥文件。

   - 如果您已将网站的证书托管在阿里云证书服务控制台，则可以在验证证书对话框中单击选择已有证书，并选择一个与要防护的域名绑定的证书。
   - 手动上传证书。单击手动上传，填写证书名称，并将该域名所绑定的证书文件和私钥文件中的文本内容分别复制粘贴到证书文件和私钥文件文本框中。

     更多信息，请参见更新HTTPS证书。

   c) 单击验证，完成证书验证。

7. 单击立即自动添加网站。

   自动添加网站后，WAF将自动为您更新该域名的DNS CNAME解析记录，将网站Web请求转发到WAF进行监控。一键添加及解析的过程一般需要10-15分钟。

   > 说明:
   > 如果您收到提示，需要手动更新DNS解析记录，请参见步骤2：修改DNS解析完成WAF接入。

8. 在管理 > 网站配置页面查看新添加的域名及其DNS解析状态。

   - DNS解析状态正常表示该网站已正常接入WAF。您可以参见步骤3：配置WAF防护策略，完成后续任务。
   - 刚添加完网站配置后，该域名的DNS解析状态也可能显示为异常。建议您稍等一会儿再来查看，或者在DNS供应商处检查域名的DNS设置。

     如果DNS设置不正确，请参见步骤2：修改DNS解析。关于DNS解析状态的判断标准，请参见DNS解析状态说明。

手动添加网站配置

前提条件

- 获取要防护的网站的域名。
- 获取网站的源站服务器地址。
- 确认网站是否已接入或需要接入CDN、高防IP等其它代理型系统。
- （仅针对中国大陆地域）网站已经通过中华人民共和国工业和信息化部ICP备案。

  推荐您使用阿里云备案服务，相关操作请参见备案导航。
- （仅针对网站支持HTTPS协议）获取网站的HTTPS证书和私钥文件，或者已将证书托管在阿里云证书服务。

  推荐您使用阿里云SSL证书服务对云上证书进行统一管理，相关操作请参见证书服务快速入门。

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，并在页面上方选择地域：中国大陆、海外地区。

3. （可选）如果在地域选项后有配置模式选项，请选择DNS配置模式，否则直接前往下一步。

4. 单击添加网站。

   WAF自动罗列出当前阿里云账号在云解析DNS中已添加过解析A记录的域名。如果云解析DNS中无任何解析A记录，则请选择您的域名页面不会出现。

5. （可选）在请选择您的域名页面，单击手动添加其它网站。

6. 在填写网站信息任务中，完成以下配置。

配置项	配置说明
域名	填写要防护的域名。 **说明:** · 支持填写泛域名，如`*.aliyun.com`。WAF将自动匹配该泛域名对应的子域名。 · 如果同时存在泛域名和精确域名配置（如`*.aliyun.com`和`www.aliyun.com`），WAF优先使用精确域名所配置的转发规则和防护策略。 · 暂不支持添加.edu域名。如果您需要添加.edu域名，请提交工单联系售后技术支持。
协议类型	勾选网站支持的协议类型，可选值：HTTP、HTTPS、HTTP2.0。 **说明:** · 如果网站支持HTTPS加密认证，请勾选HTTPS，并在添加网站后参见更新HTTPS证书上传证书和私钥文件。 · 勾选HTTPS后，可使用高级设置实现HTTP强制跳转和HTTP回源等功能，保证访问平滑。更多信息，请参见HTTPS高级配置。 · 使用HTTP2.0协议，需要符合以下要求： - 您的WAF实例已升级至企业版或旗舰版。 - 您已勾选HTTPS协议。

配置项	配置说明
服务器地址	填写网站的源站服务器地址，支持IP地址和其它地址格式。网站接入WAF后，WAF将过滤后的访问请求转发至该地址。 · （推荐）勾选IP，并填写源站服务器的公网IP地址（如云服务器ECS实例的IP、负载均衡SLB实例的IP等）。 说明: - 多个地址间以逗号分隔。最多支持添加20个源站IP。 - 如果配置多个IP地址，WAF将在这些地址间自动进行健康检查和负载均衡。更多信息，请参见源站负载均衡。 · 勾选其它地址，填写服务器回源域名（如对象存储OSS的CNAME等）。 说明: - 服务器回源域名不应和要防护的网站域名相同。 - 如果您的源站服务器地址为OSS域名，在WAF控制台中完成域名接入配置后，需要在OSS控制台中为该OSS域名绑定自定义域名，具体操作请参见管理域名。
服务器端口	配置网站的协议端口。网站接入WAF后，WAF将过滤后的访问请求转发至该端口。 注意: 配置的协议和端口必须与您所接入的网站业务源站IP（在WAF中配置的服务器IP地址）的协议和端口（在WAF中配置的服务器端口）一致，不支持端口转换功能。 · 勾选HTTP协议后，默认HTTP端口为80。 · 参见勾选HTTPS协议后，默认HTTPS端口为443。 · 如果要使用其它端口，单击自定义进行添加。 说明: 关于WAF支持的非标准端口说明，请参见非标端口支持。 · HTTP2.0协议的端口与HTTPS端口保持一致。
WAF前是否有七层代理（高防/CDN等）	根据该网站业务的实际情况勾选。如果在WAF前需要配置其它七层代理进行转发，请务必勾选是，否则WAF将无法获取访问该网站的客户端真实IP。
负载均衡算法	如果配置了多个源站IP，勾选IP hash或轮询。WAF将根据所选择的方式在多个源站IP间分发访问请求，实现负载均衡。

配置项	配置说明
流量标记	填写一个空闲的Header字段名称和自定义Header字段值，用来标识经过WAF转发到源站的Web请求。流量经过WAF后，WAF在请求中添加此处指定的字段，方便您的后端服务统计信息。 说明: 如果Web请求中本身包含此处定义的头部字段，WAF将用此处的设定值覆盖原Web请求中对应字段的内容。

7. 完成配置后，单击下一步，成功添加网站配置。

   成功添加网站配置后，您可以选择执行以下任务：

   - 根据页面提示，完成修改DNS解析任务。具体操作请参见#unique_53。
   - （已勾选HTTPS协议）上传网站HTTPS证书和私钥。具体操作请参见更新HTTPS证书。
   - 回到管理 > 网站配置页面，查看新添加的网站配置，根据需要进行编辑或删除。

   注意:
   如果您添加的网站域名尚未通过工信部域名备案，请务必尽快完成备案。WAF将不定期自动释放未通过备案的域名配置记录。

编辑网站配置

已添加的网站配置若发生变化，例如源站服务器地址、协议类型（高级HTTPS功能）、监听端口等变化，您可以编辑网站配置。

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆、海外地区。
3. 前往管理 > 网站配置页面，在DNS配置模式下，选择要操作的网站配置，单击其操作列下的编辑。
4. 在编辑页面，参见手动添加网站步骤6，修改相应配置。

   说明:
   域名不支持调整。若要防护其他域名，建议您新增一个网站配置，并删除不需要的网站配置。

5. 单击确定，成功编辑网站配置。

删除网站配置

若网站不再需要WAF防护，您可以先恢复其DNS解析（即将DNS指回服务器源站IP），然后删除网站配置。

1. 登录云盾Web应用防火墙控制台。

2. 在页面上方选择地域：中国大陆、海外地区。
3. 前往管理 > 网站配置页面，在DNS配置模式下，选择要删除的网站配置，单击其操作列下的删除。

> 说明:
> 确认删除前，请先恢复网站DNS解析；否则在删除配置后，该域名的流量将无法正常转发。

4. 在提示信息对话框中，单击确定，成功删除网站配置。

跨账号网站配置迁移说明

为了防止网站配置迁移误操作导致业务流量转发出现问题，在您删除网站配置后，有一段时间的域名保护期。如果您需要将WAF的网站配置迁移到另一个账号下，在原账号中删除网站配置后，您需要等待30分钟后才能在另一个账号的WAF实例中添加该域名的网站配置。

如果您需要快速添加该网站配置，请提交工单或在钉钉服务群中申请解除该域名的保护期。待保护期解除后，您就可以在新的账号中添加该域名的网站配置。

3.2 业务接入WAF配置

本文介绍通过DNS配置模式接入WAF时，如何在已添加网站配置后，配置域名解析，实现业务接入。

背景信息

> 说明:
> 如果您通过包年包月方式开通WAF，且您的源站服务器部署在阿里云ECS（华北2地域），同时ECS实例拥有公网IP或已绑定弹性公网IP（EIP），则您可以使用透明代理模式接入WAF。
>
> - 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。具体操作请参见使用透明代理模式接入WAF。
> - 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并更新域名的DNS设置。

通过DNS配置模式接入WAF时，您需要先添加网站配置；成功添加网站配置后，您可以选择通过（推荐）CNAME接入和A记录接入的方式更新域名DNS解析，将网站访问流量转发到WAF进行监控。

说明:

推荐您采用CNAME接入。在某些极端情况下（如节点故障、机房故障等），通过CNAME解析方式接入WAF，可以实现自动切换节点IP甚至直接将解析切回源站，从而最大程度保证业务的稳定运行，提供高可用性和灾备能力。

下文内容适用于为网站单独开启WAF防护，即该网站不接入CDN、DDoS高防等其它代理型服务。如果您需要将WAF与其它代理型服务结合部署，请参见以下文档：

- 同时部署WAF和CDN：介绍同时为网站部署CDN和Web应用防火墙的配置方法。
- 同时部署WAF和DDoS高防：介绍同时为网站部署DDoS高防和Web应用防火墙的配置方法。

（推荐）CNAME接入

前提条件

- 已添加网站配置。具体请参见网站配置。
- 获取WAF CNAME地址。
  1. 登录云盾Web应用防火墙控制台。
  2. 在页面上方选择地域：中国大陆、海外地区。
  3. 前往管理 > 网站配置页面，在DNS配置模式下，选择已添加的网站配置，将鼠标放置在域名上，即可出现复制CName按钮。

  4. 单击复制CName，将该CNAME复制到剪贴板中。
- 具有在域名的DNS服务商处更新DNS记录的权限。
- （可选）放行WAF回源段IP。源站服务器上已启用非阿里云安全软件（如安全狗、云锁）时，您需要在这些软件上设置放行WAF回源段IP，防止由WAF转发到源站的正常业务流量被拦截。具体请参见放行WAF回源段IP。

- （可选）进行本地验证。通过本地验证确保WAF转发规则配置正常后，再修改网站域名的DNS解析记录，防止因配置错误导致业务中断。具体请参见本地验证。

操作步骤

以下操作以阿里云云解析DNS为例介绍修改域名CNAME解析记录的方法。如果您的域名的DNS解析托管在阿里云云解析DNS上，您可以直接参照以下步骤进行操作；若您使用阿里云以外的DNS服务，请参见以下步骤在域名的DNS服务商的系统上进行类似配置。

下文也提供了花生壳配置示例，介绍在花生壳修改域名解析的方法。

1. 登录云解析DNS控制台。
2. 选择要操作的域名，单击其操作列下的解析设置。

3. 选择要操作的主机记录，单击其操作列下的修改。

关于域名的主机记录，以域名abc.com为例：

- www：用于精确匹配www开头的域名，如www.abc.com。
- @：用于匹配根域名abc.com。
- *：用于匹配泛域名，包括根域名和所有子域名，如blog.abc.com、www.abc.com、abc.com等。

4. 在修改记录对话框中，完成以下操作：

   - 记录类型：修改为CNAME。
   - 记录值：修改为已复制的WAF CNAME地址。
   - 其他设置保持不变。TTL值一般建议设置为10分钟。TTL值越大，则DNS记录的同步和更新越慢。

   关于修改解析记录：

   - 对于同一个主机记录，CNAME解析记录值只能填写一个，您需要将其修改为WAF CNAME地址。
   - 不同DNS解析记录类型间存在冲突。例如，对于同一个主机记录，CNAME记录与A记录、MX记录、TXT记录等其他记录互相冲突。在无法直接修改记录类型的情况下，您可以先删除存在冲突的其他记录，再添加一条新的CNAME记录。

     > 说明：
     > 删除其他解析记录并新增CNAME解析记录的过程应尽可能在短时间内完成。如果删除A记录后长时间没有添加CNAME解析记录，可能导致域名无法正常解析。

     关于DNS解析记录互斥的详细说明，请参见解析记录冲突的规则。
   - 如果必须保留MX记录（邮件服务器记录），您可以参见#unique_53，使用A记录解析的方式将域名解析到WAF IP。

5. 单击确定，完成DNS配置，等待DNS解析记录生效。
6. 验证DNS配置。您可以Ping网站域名或使用17ce等工具验证DNS解析是否生效。

   > 说明：
   > 由于DNS解析记录生效需要一定时间，如果验证失败，您可以等待10分钟后重新检查。

7. 查看DNS解析状态。

a) 登录云盾Web应用防火墙控制台。

b) 前往管理 > 网站配置页面，在DNS配置模式下，查看域名的DNS解析状态。

- 正常：表示网站已成功接入WAF，网站访问流量由WAF监控。
- 异常：如果DNS解析状态为异常，且收到未检测到CNAME接入、无流量、检测失败等提示，说明网站未正确接入WAF。

  如果您确认已将网站域名解析到WAF CNAME地址，可在一小时后再次查看DNS解析状态或者参见DNS解析状态异常排查异常原因。

> **说明:**
> 该提示仅说明网站是否正确接入WAF，不代表您的网站访问异常。

花生壳配置示例

如果您的域名DNS托管在花生壳，您可以参照下图修改DNS解析设置。

启用源站保护

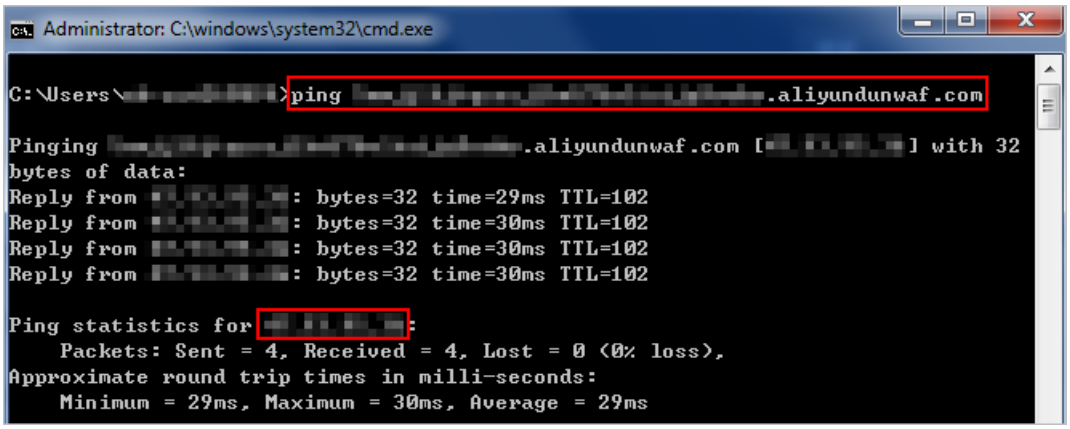
启用源站保护可以防止攻击者在获取源站服务器的真实IP后，绕过WAF直接攻击您的源站。建议您通过配置源站ECS的安全组或源站SLB的白名单，防止恶意攻击者直接攻击您的源站。具体请参见源站保护配置。

A记录接入

A记录接入和CNAME接入的流程大体相同，区别在于以下两点：

- 前提条件：获取WAF CNAME后，执行以下步骤，获取WAF IP地址。

  1. 在Windows操作系统中，打开cmd命令行工具。
  2. 执行以下命令：`ping "已复制的WAF Cname地址"`。



  3. 在返回结果中，记录WAF IP地址。

- 操作步骤：在步骤4修改记录时，执行以下操作，修改记录类型和记录值。
  - 记录类型：修改为A。
  - 记录值：修改为已获得的WAF IP地址。
  - 其他设置保持不变。

3.3 放行WAF回源IP段

网站成功接入WAF后，所有网站访问请求将先流转到WAF进行监控，经WAF实例过滤后再返回到源站服务器。流量经WAF实例返回源站的过程称为回源。

WAF实例的IP数量有限，且源站服务器收到的所有请求都来自这些IP。在源站服务器上的安全软件（如安全狗、云锁）看来，这种行为很可疑，有可能触发屏蔽WAF回源IP的操作。因此，在接入WAF防护后，您需要在源站服务器的安全软件上设置放行所有WAF回源IP。

说明:

强烈推荐您在接入WAF防护后，卸载源站服务器上的其他安全软件。

操作步骤

WAF控制台提供了最新的回源IP段列表，您可以参照以下步骤进行操作：

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方，选择地域：中国大陆、海外地区。
3. 前往设置 > 产品信息页面。

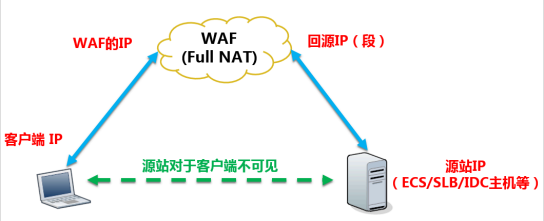
4. 在产品信息页面底部，查看和复制所有WAF回源IP段。

5. 打开源站服务器上的安全软件，将复制的IP段添加到白名单。

常见问题

什么是回源IP?

回源IP是WAF用来代理客户端请求服务器时用的源IP，在服务器看来，接入WAF后所有源IP都会变成WAF的回源IP，而真实的客户端地址会被加在HTTP头部的XFF字段中。



为何要放行回源IP段?

由于来源的IP变得更加集中，频率会变得更快，服务器上的防火墙或安全软件很容易认为这些IP在发起攻击，从而将其拉黑。一旦拉黑，WAF的请求将无法得到源站的正常响应。因此，在接入WAF后，您应确保源站已将WAF的全部回源IP放行（加入白名单），不然可能会出现网站打不开或打开极其缓慢等情况。

建议在部署WAF后，您在源站上只允许来自WAF的访问请求，这样既可保证访问不受影响，又能防止源站IP暴露后被黑客直接攻击。更多信息，请参考源站保护。

3.4 本地验证

在把业务流量切到WAF之前，建议您先通过本地验证确保一切配置正常，WAF转发正常。本地验证需要在本地模拟接入WAF，然后访问被防护网站，验证WAF正常转发。

本地接入WAF

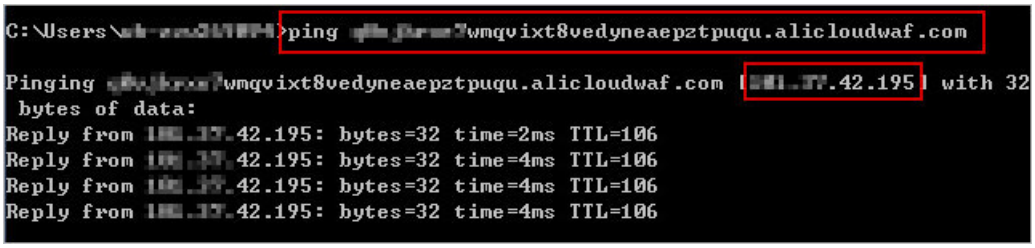
通过修改本地`hosts`文件（什么是hosts文件）模拟接入WAF，将从本地访问被防护站点的请求导向WAF。以Windows操作系统为例，

1. 用记事本或notepad++等文本编辑器打开`hosts`文件，`hosts`文件一般位于`C:\Windows\System32\drivers\etc\hosts`路径。

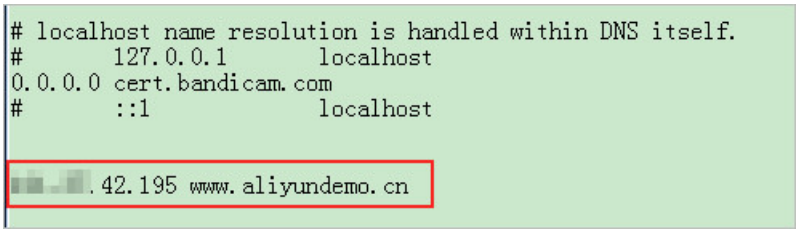
2. 在最后一行添加如下内容：`WAF的IP 被防护的域名`。

   以域名`www.aliyundemo.cn`为例，该域名已添加到WAF的网站配置中，且WAF为其分配了以下CNAME值：`xxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com`

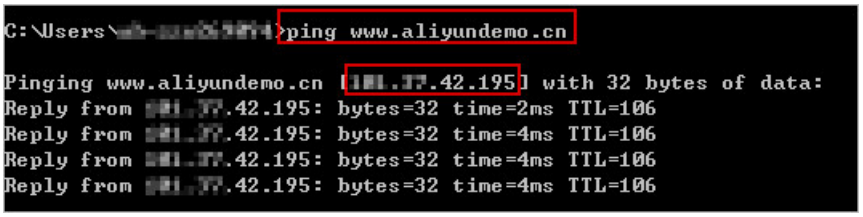
   a. 在Windows中打开cmd命令行工具，运行`ping xxxxxxxxxwmqvixt8vedyneaepztpuqu.alicloudwaf.com`获取WAF IP。如下图所示，在响应结果中可以看到用来防护您的域名的WAF IP。

   b. 在`hosts`文件添加如下内容，前面的IP地址即上一步获取的WAF IP地址，后面的域名即被防护的域名。

3. 修改`hosts`文件后保存。然后本地ping一下被防护的域名。

   预期此时解析到的IP地址应该是刚才绑定的WAF IP地址。如果依然是源站地址，可尝试刷新本地的DNS缓存（Windows的cmd下可以使用`ipconfig/flushdns`命令）。

验证WAF转发正常

确认hosts绑定已经生效（域名已经本地解析为WAF IP）后，打开浏览器，输入该域名进行访问，如果WAF的配置正确，预期网站能够正常打开。

同时也可以尝试手动模拟一些简单的web攻击命令。例如，您可以在URL后面加`/alert(xss)`（这是一个用作测试的Web攻击请求），访问`www.aliyundemo.cn/alert(xss)`。

预期WAF会弹出如下阻拦页面。

3.5 更新HTTPS证书

要使Web应用防护墙（WAF）帮助您监控HTTPS业务流量，您必须在网站配置中勾选HTTPS协议，并上传HTTPS证书，保证HTTPS协议状态正常。如果证书发生变化，您也要在WAF控制台及时更新证书。

背景信息

如果您已将证书文件上传到云盾SSL证书服务进行统一管理，那么在以下步骤中，您可以选择一个已有证书进行更新。

否则，您需要准备好网站的证书和私钥文件，以完成以下操作。

一般情况下，您所需准备的证书相关内容包括：

- *.crt（公钥文件）或*.pem（证书文件）
- *.key（私钥文件）

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆、海外地区。
3. 在管理 > 网站配置页面，选择要操作的域名，单击其HTTPS协议状态右侧的上传按钮（）。

4. 在更新证书对话框中，选择上传方式并上传证书。

- 如果该域名所绑定的HTTPS证书已添加至云盾SSL证书服务进行管理，您可以单击选择已有证书，直接选择想要上传的证书。

- 手动上传证书。单击手动上传，填写证书名称，并将该域名所绑定的证书文件和私钥文件中的文本内容分别复制粘贴到证书文件和私钥文件文本框中。

> **说明:**
>
> - 对于.pem、.cer、.crt格式的证书，您可以使用文本编辑器直接打开证书文件，并复制其中的文本内容；对于其他格式（如.pfx、.p7b等）的证书，则需要将证书文件转换成.pem格式后，才能用文本编辑器打开并复制其中的文本内容。
>
>   关于证书格式的转换方式，请参考HTTPS证书转换成PEM格式。
> - 如果该HTTPS证书有多个证书文件（如证书链），需要将证书文件中的文本内容拼接合并后粘贴至证书文件文本框中。

证书文件文本内容样例：

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx8ixZJ4krc+1M+
j2kcubVpsE2
cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOk
jgvhlqt9vc
65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9
nIrHsPl8YKk
vRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

私钥文件文本内容样例：

```
-----BEGIN RSA PRIVATE KEY-----
DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThL
yvsmLQKBgQ
```

```
Cr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJ
aiygoIYo
aMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDz
FdZ9Zujxvuh9o
4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

5. 单击保存，成功上传证书和私钥文件。

预期结果

HTTPS协议状态显示为正常。

3.6 HTTPS高级配置

WAF提供灵活的HTTPS配置功能，帮助您在不改造源站的情况下，一键实现全站HTTPS和强制客户端使用HTTPS连接。

背景信息

如果您使用按量付费模式WAF，您必须在功能与规格中勾选支持HTTPS相关业务，才能使用HTTPS高级配置。具体操作，请参考功能与规格配置。

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆、海外地区。
3. 在管理 > 网站配置页面，选择要操作的域名，单击其操作列下的编辑。
4. 在协议类型下勾选HTTPS，并单击打开高级设置菜单。

- 开启HTTP回源

  如果您的网站不支持HTTPS回源，请开启HTTP回源（默认回源端口是80端口），通过WAF实现HTTPS访问。使用该设置后，客户端可以通过HTTP和HTTPS方式访问站点。

  
  说明:

使用HTTP回源，可以无需在源站服务器上做任何改动，也不需要配置HTTPS。但是，该配置的前提是在WAF上传正确的证书和私钥（证书可以在阿里云证书免费申请）。

- 开启HTTPS的强制跳转

  如果您需要强制客户端使用HTTPS来访问（从安全性考虑，推荐这样做），您可以开启HTTPS的强制跳转。

  说明:
  开启HTTPS强制跳转前必须先取消HTTP协议。

  选择开启HTTPS的强制跳转后，部分浏览器将被缓存设置为使用HTTPS请求访问网站，请确保您的网站支持HTTPS业务。

  开启HTTPS强制跳转后，HTTP请求将显示为HTTPS，默认跳转到443端口。

3.7 非标端口支持

WAF默认支持以下端口：80/8080（HTTP）和443/8443（HTTPS）。企业版和旗舰版WAF实例支持更多的非标端口，且对被防护域名使用的不同端口的总数有相应限制。

如果您使用按量付费模式WAF，您必须在功能与规格中勾选支持非标端口业务防护，才能使用非标端口接入WAF。具体操作请参见功能与规格配置。

不同端口总数限制

针对每个阿里云账号（即每个WAF实例），由WAF防护的全部域名所使用的不同端口的总数有以下限制：

- 每个企业版用户支持最多10个不同的端口（包含80/8080/443/8443端口）
- 每个旗舰版用户支持最多50个不同的端口（包含80/8080/443/8443端口）
- 按量付费开通的WAF支持最多50个不同的端口（包含80/8080/443/8443端口）

支持的端口

说明:

WAF仅防护支持的端口，对于不支持的端口WAF既不会防护，也不会转发。例如，4444端口的业务请求到达WAF后，请求会被直接丢弃。

- 在企业版和旗舰版WAF中，HTTP协议支持以下端口：

  80、81、82、83、84、86、87、88、89、97、800、808、1000、1090、3333、3501、3601、5000、5222、6001、6666、7000、7001、7002、7003、7004、7005、7006、7009、7010、7011、7012、7013、7014、7015、7016、7018、7019、7020、7021、7022、7023、7024、7025、7026、7070、7081、7082、7083、7088、7097、7510、7777、7800、8000、8001、8002、8003、8008、8009、8020、8021、8022、8025、8026、8077、8078、8080、8081、8082、8083、8084、8085、8086、8087、8088、8089、8090、8091、8106、8181、8334、8336、8686、8800、8888、8889、8999、9000、9001、9002、9003、9021、9023、9027、9037、9080、9081、9082、9180、9200、9201、9205、9207、9208、9209、9210、9211、9212、9213、9898、9908、9916、9918、9919、9928、9929、9939、9999、10000、10001、10080、12601、28080、33702、48800

- 在企业版和旗舰版WAF中，HTTPS协议支持以下端口：

  443、4443、5443、6443、7443、8443、8553、8663、9443、9553、9663、18980
- 按量付费的WAF实例在开启支持非标端口业务防护后，支持上述HTTP和HTTPS端口。

3.8 标记WAF回源流量

在将网站域名接入Web应用防火墙进行防护时，您可以为网站域名设置流量标记。当该网站域名的流量经过WAF时，WAF将在请求中添加对应的流量标记，便于后端的源站服务器统计相关信息。

根据您在流量标记中设置的HTTP Header字段名称和字段值，当流量经过WAF时，WAF将在所有请求头中添加对应的字段和字段值。通过设置流量标记的方式，方便地标识经过WAF转发的流量，从而实现精准的源站保护（访问控制）、防护效果分析等。

> 说明：
> 如果所设置的HTTP自定义头部字段已存在，WAF仍将用您设置的流量标记字段值覆盖该请求中的原本存在的字段值。

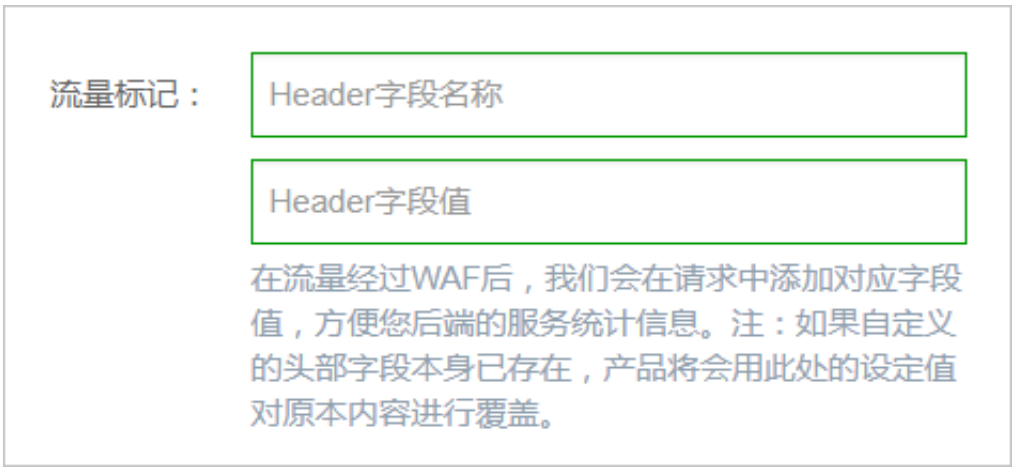
操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆、海外地区。
3. 前往管理 > 网站配置页面，选择域名配置记录，单击编辑。

   > 说明：
   > 您也可以在添加网站域名配置时，设置流量标记。
4. 在流量标记配置项中，填写Header字段名称和字段值。

   > 说明：

请勿填写已经被使用的自定义Header字段，否则请求中该字段的值将被WAF的流量标记字段值所覆盖。



5. 单击确定。配置生效后，WAF将在转发该网站域名的请求时添加对应的HTTP Header字段和字段值。

3.9 WAF源站负载均衡

如果您的源站有多个服务器，在将域名接入WAF时，您可以配置多个源站IP。WAF支持最多20个源站IP。

如果您配置了多个源站IP，WAF在将过滤后的访问请求回源时，将按照IP Hash或轮询的方式去做负载均衡。同时，WAF也会对多个源站进行健康检查，对所有回源IP进行接入状态检测，如果某个回源IP没有响应，将不再将请求转发到这个回源IP，直到其接入状态回复正常。

假设源站IP有3个（1.1.1.1、2.2.2.2、3.3.3.3），您可以按照下图所示进行配置。

说明:
如果WAF前面有接高防、CDN等七层代理，务必勾选是否已使用高防、CDN、云加速等代理下的是。

添加源站IP后，您需要指定负载均衡算法：IP hash、轮询。

说明:

使用IP HASH时，如果源IP不够分散，可能会出现负载不均。

3.10 同时部署WAF和DDoS高防

Web应用防火墙（WAF）与DDoS高防完全兼容。您可以参照以下架构为源站同时部署WAF和DDoS高防：DDoS高防IP（入口层，实现DDoS防护）> Web应用防火墙（中间层，实现应用层防护）> 源站。

操作步骤

1. 在Web应用防火墙中添加网站配置。

   · 服务器地址：勾选IP并填写ECS公网IP、SLB公网IP，或云外机房服务器的IP。

   · WAF前是否有七层代理（高防/CDN等）：勾选是。

   具体操作请参考网站配置。

2. 在高防IP中添加网站配置。操作步骤如下：

   a. 在接入 > 网站页面，单击添加域名。

   b. 在填写域名信息任务中， 完成以下配置：

      · 防护网站：填写被防护网站的域名。

      · 协议类型：勾选源站支持的协议类型。

      · 源站IP/域名：勾选源站域名并填写Web应用防火墙生成的CNAME地址。

      说明:

      关于如何查看WAF生成的CNAME地址，请参考WAF接入指南。

   c. 单击下一步。

   d. 完成任务选择实例与线路。

3. 变更域名的DNS解析。登录域名的DNS系统，添加一条CNAME记录，将网站域名的解析地址指向DDoS高防生成的CNAME地址。

   具体操作请参考DDoS高防CNAME接入流程。

预期结果

完成上述配置后，网站流量先经过DDoS高防，再转发到Web应用防火墙。

3.11 同时部署WAF和CDN

云盾Web应用防火墙（WAF）可以与CDN（如网宿、加速乐、七牛、又拍、阿里云CDN等）结合使用，为开启内容加速的域名提供Web攻击防御。

背景信息

您可以参照以下架构为源站同时部署WAF和CDN：CDN（入口层，内容加速）> Web应用防火墙（中间层，实现应用层防护）> 源站。

使用阿里云CDN

1. 参见CDN快速入门，将要防护的域名（即加速域名）接入CDN。
2. 在Web应用防火墙中创建网站配置。
   - 域名：填写要防护的域名。
   - 服务器地址：填写SLB公网IP、ECS公网IP，或云外机房服务器的IP。
   - WAF前是否有七层代理（高防/CDN等）：勾选是。

   具体操作请参见网站配置。

3. 成功创建网站配置后，Web应用防火墙为该域名生成一个专用的CNAME地址。

说明:

关于如何查看WAF生成的CNAME地址，请参见WAF接入指南。

4. 将CDN配置中的源站修改为Web应用防火墙分配的CNAME地址。

   a) 登录阿里云CDN控制台。

   b) 在域名管理页面，选择要操作的域名，单击管理。

   c) 在源站信息下，单击修改配置。

   d) 修改源站信息。

   - 类型：选择源站域名。
   - 域名：填写WAF生成的CNAME地址。
   - 端口：选择80端口。

   e) 前往回源配置页面，在回源配置页签下，确认回源HOST未开启。

完成上述配置后，流量经过CDN，其中动态内容将继续通过Web应用防火墙进行安全检测防护。

使用非阿里云CDN

1. 配置CDN，将域名接入CDN。
2. 在Web应用防火墙中创建网站配置。具体请参见使用阿里云CDN步骤2。
3. 查看WAF CNAME地址。具体请参见使用阿里云CDN步骤3。
4. 将CDN配置的源站改为WAF CNAME地址。

4 资产管理

Web应用防火墙提供资产管理功能，通过获取阿里云平台上的SSL证书、云解析DNS、Web应用防火墙等云产品的配置信息和站点通信流量中的网站信息，主动发现您云平台上的网络资产，同时提供一键接入防护功能帮助您的企业实现全面的网络资产管理和安全防护。

背景信息

网络应用资产是安全管理体系中最基础最重要的载体，同时也是业务系统中最基本的组成单元。随着企业业务的高速发展，各类业务系统平台逐年增多，同时也存在着员工私建站点、测试环境未及时回收等情况，可能产生大量“僵尸”资产。信息安全是很典型的木桶效应，安全防护的水位由企业最薄弱的一环决定。由于无人管理，“僵尸”资产往往使用了低版本的开源系统、组件、Web框架等，导致一些薄弱环节暴露在攻击者的视野下，攻击者可以利用这些站点作为“跳板”绕过企业的网络边界防护，进而使得整个企业内网沦陷。

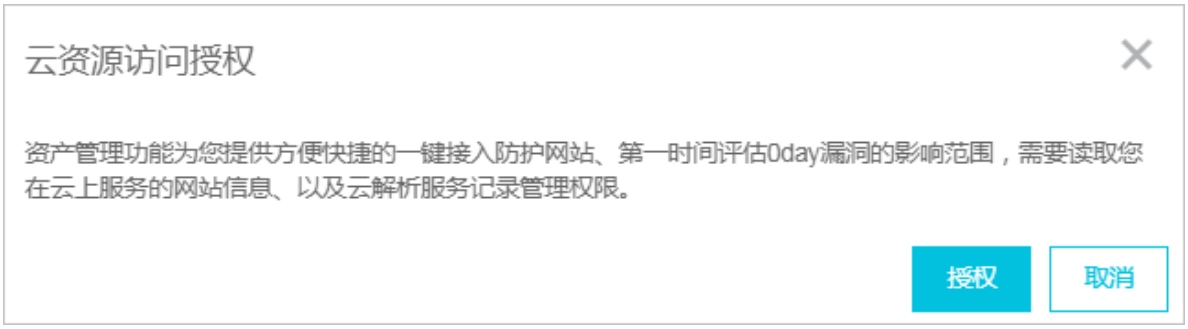
Web应用防火墙（WAF）的资产管理功能旨在协助您发现阿里云上的应用资产、监控资产变化，避免在安全防护中出现资产遗漏， 提高整体安全防护水位线。资产管理为您提供云上资产识别、一键自动接入防护、0day漏洞影响范围评估等功能，为企业网络域名资产的安全管理决策提供事实依据以及将网络资产快速接入安全防护的能力，全面保障企业云上网络资产的安全。

在得到您的授权后，WAF将基于所获取的您阿里云账号中的SSL证书、云解析DNS、Web应用防火墙等云产品的配置信息和阿里云上站点通信流量中的网站（Host）信息，综合发现您在阿里云平台中的所有域名资产信息，包括域名和子域名信息、服务器IP地址、端口、协议、Web防护状态等。

授权WAF访问云资源

为实现网络资产的主动发现，您需要授予WAF读取您云账号中相关云服务的网站信息和管理云解析服务的域名解析记录的权限。

1. 登录云盾Web应用防火墙控制台，定位到资产管理页面，您将收到云资源访问授权提示。



2. 单击授权，前往访问控制平台授权页面。

3. 单击同意授权，授权WAF访问您账号中相关云产品服务的资源。

授权完成后，WAF将主动发现您云账号中的网络域名资产。

查看域名资产

您可以在WAF控制台的资产管理页面，查看WAF主动发现的您账号中的所有域名资产。

1. 登录云盾Web应用防火墙控制台，在页面上方选择WAF实例所在地区（中国大陆、海外地区）。
2. 定位到资产管理页面，查看您的域名资产。

   WAF根据一级域名将所发现的域名资产进行聚合展示，您可以展开指定一级域名查看所发现的具体的域名资产信息，包括服务器地址、端口号、访问协议、防护状态等信息。

   说明:

   - 资产管理页面仅展示近期有流量的云上域名资产。
   - 如果域名资产的服务器地址、端口号、协议等信息未显示，表示该IP资产不属于当前的阿里云账号。

   其中，防护状态表示是否已接入WAF进行全面防护：

   - 未防护：网站资产未接入WAF防护
   - 已添加未防护：已在WAF中添加网站资产接入配置，但WAF未检测到网站流量
   - 已防护：网站资产已接入WAF防护，检测到网站流量，提供全面防护

   说明:

对于尚未接入WAF的域名资产（防护状态为未防护），建议您通过#unique_79/unique_79_Connect_42_auto-website-configuration一键接入WAF进行防护，实现域名资产的全面防护。

您也可以在域名资产列表上方的搜索框中输入任意关键字，单击搜索查找指定域名资产。

5 防护配置

5.1 IPv6环境防护支持

Web应用防火墙支持一键防护IPv6环境下发起的攻击，帮助您的源站实现对IPv6流量的安全防护。

随着IPv6协议的迅速普及，新的网络环境以及新兴领域均面临着新的安全挑战，阿里云Web应用防火墙的IPv6防护功能帮助您轻松构建覆盖全球的安全防护体系。

说明:
目前，仅中国大陆地区的企业版或旗舰版WAF实例支持IPv6安全防护功能。

开启IPv6安全防护

注意:
为指定网站配置开启IPv6安全防护前，请务必在源站服务器的安全软件上设置放行以下WAF回源IP段：

- 39.96.158.0/24
- 47.110.182.0/24
- 120.77.139.0/25
- 47.102.187.0/25

将您的网站域名接入WAF防护后，您只需在云盾Web应用防火墙控制台的网站配置页面中，选择已添加的网站配置记录，单击IPv6状态开关即可一键开启IPv6安全防护。

说明:
关于如何将网站域名接入WAF防护，请参见#unique_82。

IPv6安全防护功能开启后，WAF自动生成的CNAME地址将实现双路解析。其中，A记录（IPv4客户端发起的解析请求）解析到一个IPv4地址的防护集群，而4A记录（IPv6客户端发起的解析请求）则解析到一个IPv6地址的防护集群，从而实现对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。其中，IPv6流量将自动转换为IPv4流量转发回源站服务器。

5.2 Web应用攻击防护

Web应用攻击防护可防护SQL注入、XSS跨站等常见Web应用攻击，且提供不同规格的防护策略：宽松、正常、严格。

背景信息

将网站接入WAF后，您可以为其开启Web应用攻击防护，并根据实际需求调整相应防护策略。Web应用防护开启后实时生效；如果您不想使用该功能，可将其关闭。

执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参见CNAME接入指南。

操作步骤

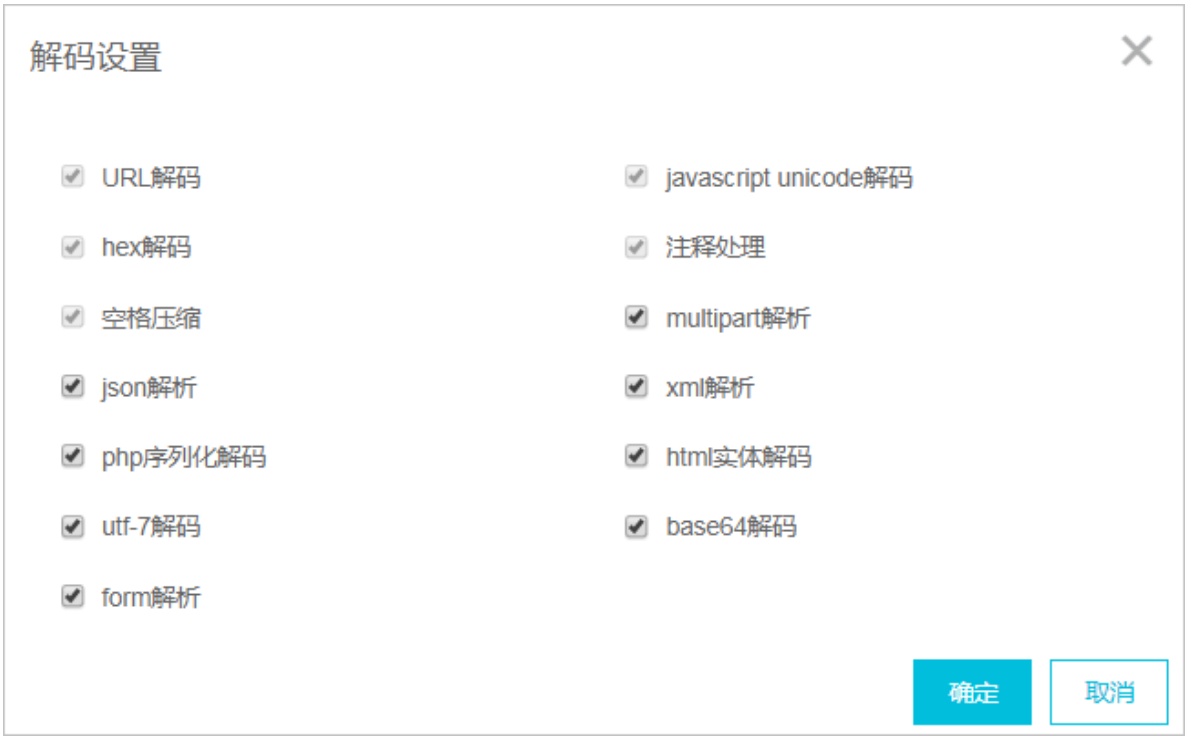
1. 登录云盾Web应用防火墙控制台。
2. 前往管理 > 网站配置页面，并在页面上方选择WAF所在地区（中国大陆、海外地区）。
3. 选择要操作的域名，单击其操作列下的防护配置。
4. 在Web应用攻击防护功能项，开启防护开关，并选择防护模式：

> **说明:**
> 如果您不想使用该功能，可在此处关闭防护。

- 防护：发现攻击后直接阻断。
- 预警：发现攻击后只告警，不阻断。

5. 在防护规则策略下拉框中，选择合适的防护策略：
   - 默认使用正常模式规则。
   - 当您发现在正常模式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），建议您选择宽松模式。
   - 当您需要更严格地防护路径穿越、SQL注入、命令执行时，建议您选择严格模式。
6. 单击解码设置右侧的前去配置，可在解码设置对话框中勾选需要Web应用攻击防护功能模块解码分析的格式。如果您发现WAF的Web应用攻击防护功能模块经常对您业务中包含指定格式内容的请求造成误拦截，您可以在解码设置对话框中取消该格式的解码的勾选并单击确定来针对性地降低误杀率。

> **说明:**
> 为保证防护效果，默认对请求中所有格式类型的内容进行解码分析。其中，URL解码、JavaScript Unicode解码、hex解码、注释处理、空格压缩类型的解码设置无法被取消。



5.3 大数据深度学习引擎

通过有监督学习的方式，Web应用防火墙的大数据深度学习引擎依托于阿里云强大的算法团队构建的神经网络系统，对阿里云上每日亿级的攻击数据进行分类训练，最终通过模型实时地对未知风险请求进行在线检测拦截，弥补其它防御引擎对未知0day漏洞风险检测的不足。

前提条件

已将网站接入WAF进行防护。具体操作请参见CNAME接入指南。

背景信息

> 说明:
> 包年包月模式的WAF实例均支持大数据深度学习引擎。按量付费的WAF实例必须在功能与规格中为Web攻击防护启用高级防护，才能使用新智能防护引擎。具体操作，请参见功能与规格配置。

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。

大数据深度学习引擎基于对业务正常模型的不断学习和建模，实时识别并预警异常风险行为，为用户提供最快、最全面的防护能力。

> 说明:
> 大数据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，建议您启用大数据深度学习引擎功能。

大数据深度学习引擎的主要特性如下：

- 语义化：新智能防护引擎归并同类攻击行为的行为特征，并以攻击行为的多个行为特征组成的排列组合来表示同一类攻击，从而实现攻击行为的语义化，即用自然语言的语义来理解并描述同一类攻击。
- 异常攻击集：基于阿里云云盾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，然后从繁多的Web应用攻击中提炼出异常攻击模型，从而形成异常攻击集。

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WAF所在地区（中国大陆、海外地区）。
3. 选择要操作的域名，单击其操作列下的防护配置。

4. 在大数据深度学习引擎下，开启防护开关，并选择防护模式。

- 预警：发现攻击后只告警，不阻断。
- 防护：发现攻击后直接阻断。

> 说明:
> 如果您不想使用大数据深度学习引擎，您可以在此页面关闭防护。

5.4 CC安全防护

CC安全防护帮助您防护针对页面请求的CC攻击。

功能描述

CC安全防护可以拦截机器恶意CC攻击，并提供不同模式的防护策略：正常、攻击紧急。将网站接入WAF后，您可以为其开启CC安全防护，并根据实际需求调整相应防护策略。当您为网站开启CC防护后，WAF将以关闭连接的方式帮您阻断检测出的CC攻击请求。

企业版和旗舰版WAF支持更高级的CC防护功能，具体请参考CC防护规格。

> 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（会造成大量误杀）；对于后者，建议您将WAF升级到企业版或旗舰版，并使用自定义CC防护。

> 说明:
> 如果您使用按量付费的WAF实例，您可以在功能与规格中为缓解CC攻击启用高级防护，这样可以自定义CC防护。具体操作，请参考功能与规格配置。

操作步骤

参照以下步骤，配置CC安全防护模式：

说明:

执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考业务接入WAF配置。

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WAF所在地区（中国大陆、海外地区）。
3. 选择要操作的域名，单击其操作列下的防护配置。
4. 在CC安全防护下，开启防护，并选择相应防护模式：

- 正常：默认使用正常模式。此模式误杀较少，只针对特别异常的请求进行拦截。建议您在网站无明显流量异常时采用此模式，避免误杀。
- 攻击紧急：当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，可以选择攻击紧急模式。此模式拦截CC攻击效果较强，但可能会造成较多误杀。

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。具体操作请参考自定义CC防护。
- 旗舰版：专家定制防护规则，保障防护效果。

规格详情请参照Web应用防火墙价格详情页。

关于如何升级WAF规格，请参考续费与升级。

> **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。

5.5 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。例如，您可以配置如下规则：当单个源IP在10秒内访问 *www.yourdomain.com/login.html* 超过20次时，封禁该IP一小时。

背景信息

对于WAF高级版，您必须升级到企业版或旗舰版，才能使用自定义CC防护功能。具体操作请参考续费与升级。

对于按量付费的WAF实例，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，才能使用自定义CC防护功能。具体操作，请参考功能与规格配置。

执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考CNAME接入指南。

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WAF所在地区（中国大陆、海外地区）。
3. 选择要操作的域名，单击其操作列下的防护配置。

4. 在CC安全防护下，选择正常防护模式，并单击前去配置配置自定义规则。

5. 单击新增规则，添加一条规则。参数描述如下：

配置	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*。
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。

配置	说明
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（WAF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WAF拦截，只有被识别为合法才会放行。

以图中的配置为例，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。

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。

预期结果

规则添加成功后即时生效，您可以选择编辑或者删除规则。

5.6 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

已将网站接入WAF进行防护。具体操作请参见CNAME接入指南。

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WAF所在地区（中国大陆、海外地区）。
3. 选择要操作的域名，单击其操作列下的防护配置。
4. 在精准访问控制下，开启防护，并单击前去配置。

5. 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。

6. 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。
- 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。

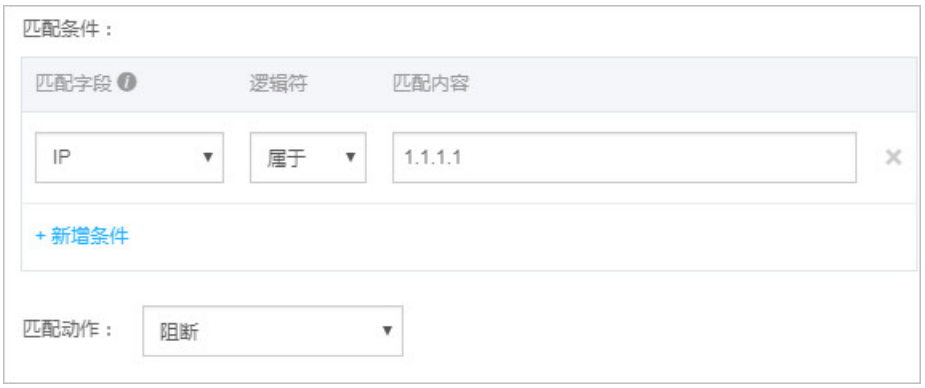
配置示例

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。

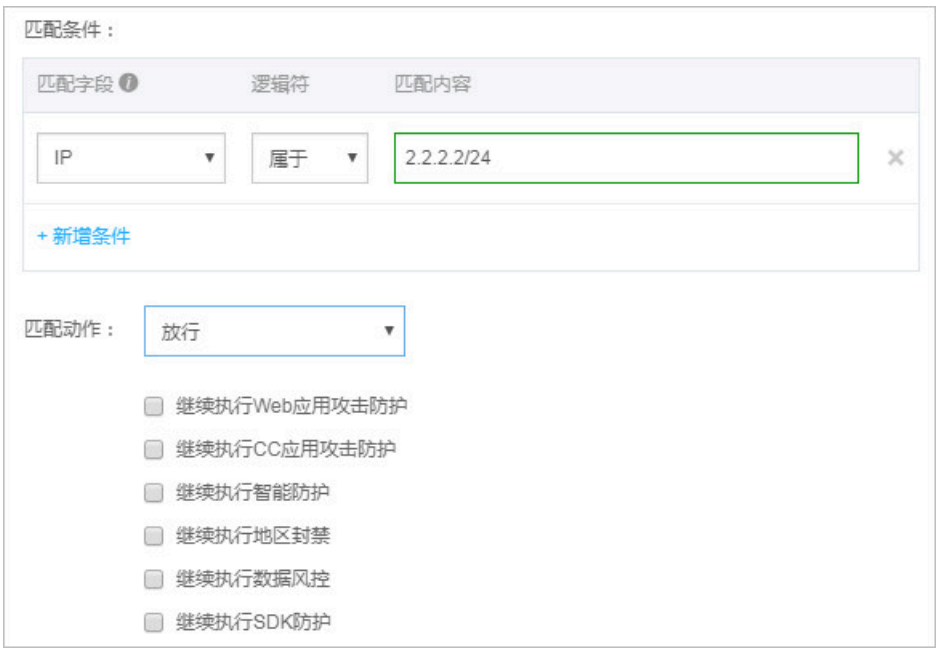
以下罗列了一些常用的精确访问控制配置示例，供您参考。

- 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。

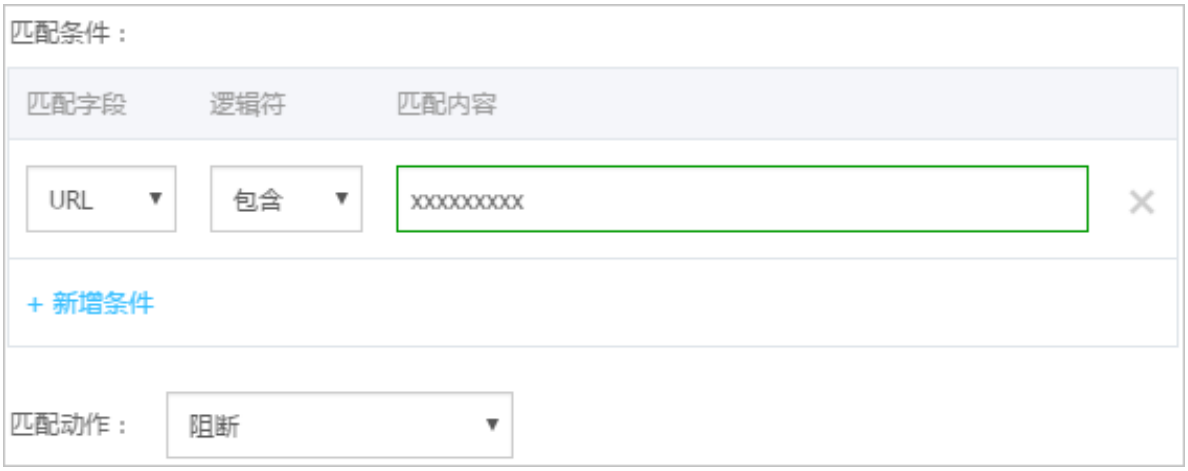
UA
WordPress/4.2.10; http://ascsolutions.vn; verifying pingback from 191.96.249.54
WordPress/4.0.1; http://146.148.63.90; verifying pingback from 191.96.249.54
WordPress/4.6.1; https://www.nokhostinsabt.com; verifying pingback from 191.96.249.54
WordPress/4.5.3; http://eadastage.lib.umd.edu; verifying 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。

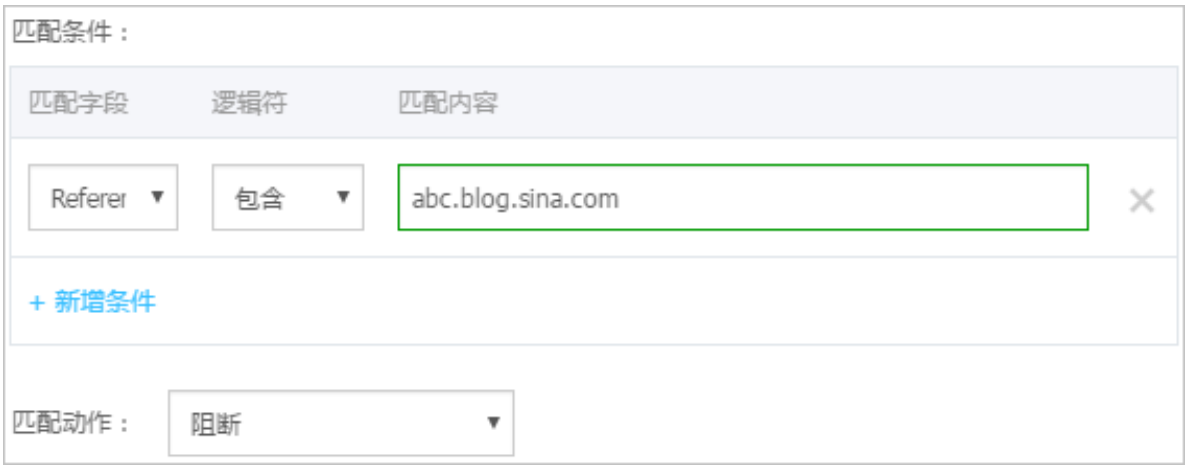
- 封禁特定的URL

  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

5.7 封禁地区

使用封禁地区可以对指定的中国大陆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。

前提条件

已将网站接入WAF进行防护。具体操作请参见CNAME接入指南。

背景信息

对于WAF高级版，您必须升级到企业版或旗舰版，才能使用封禁地区功能。具体操作，请参见续费与升级。

> 说明:
> 海外地域WAF实例必须升级至旗舰版。

对于按量付费的WAF实例，您必须在功能与规格中勾选支持基于地理位置的区域封禁，才能使用该功能。具体操作，请参见功能与规格配置。

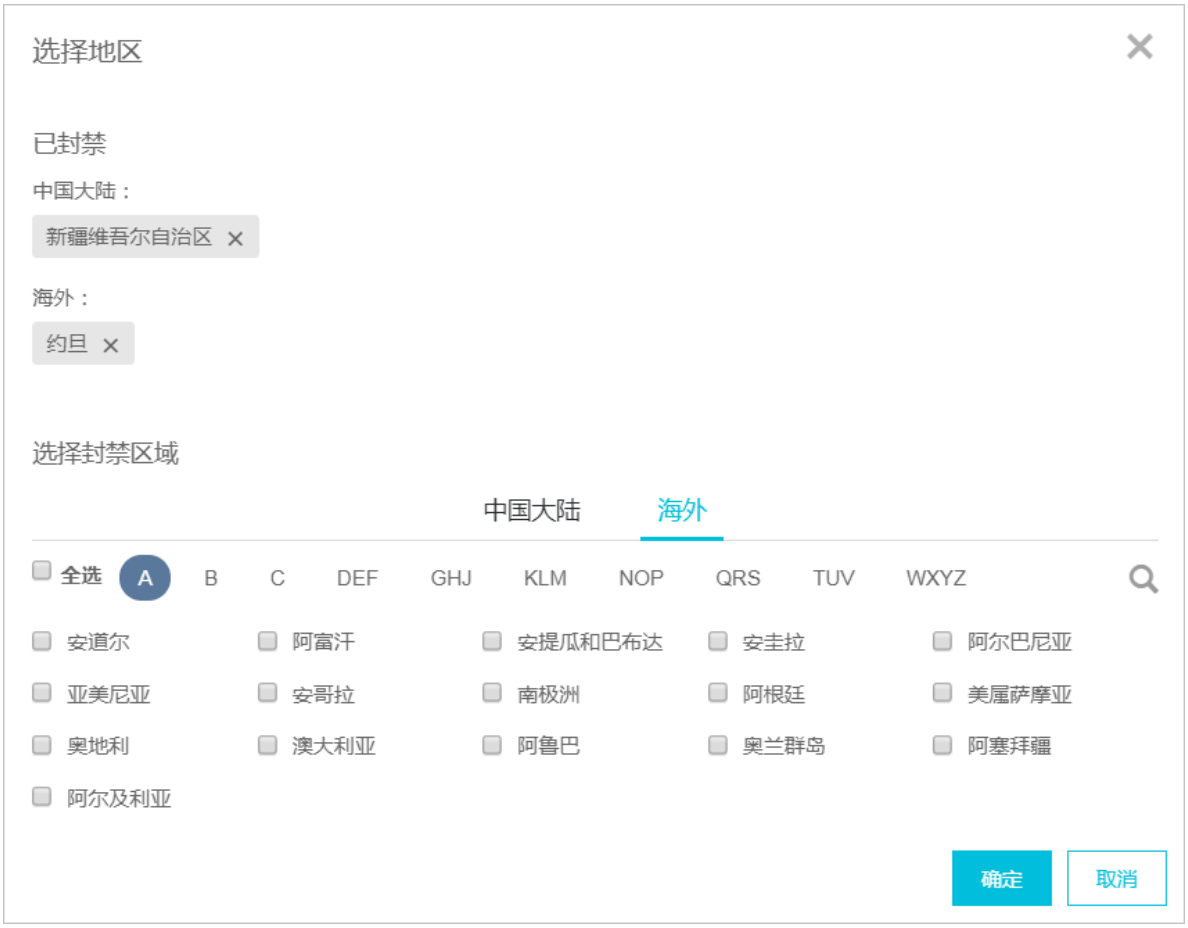
操作步骤

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WAF所在地区（中国大陆、海外地区）。
3. 选择要操作的域名，单击其操作列下的防护配置。
4. 在封禁地区下，启用防护。

> 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。

5. 单击设置，选择中国大陆或海外范围并勾选需要封禁的地区，完成后单击确定。

> **说明:**
> 选择海外范围时，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。

5.8 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

已将网站接入WAF进行防护。具体操作请参见CNAME接入指南。

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WAF所在地区（中国大陆、海外地区）。
3. 选择要操作的域名，单击其操作列下的防护配置。
4. 在精确访问控制下，开启防护，并单击前去配置。

5. 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。

5.9 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。

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，仅中国大陆地域的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：

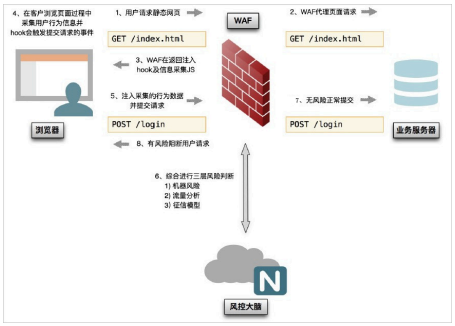
- 垃圾注册
- 短信验证码滥刷
- 撞库、暴力破解
- 恶意抢购、秒杀、薅羊毛、抢红包
- 机器人抢票、刷票、恶意投票

- 垃圾消息

> 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实时日志分析服务进行兼容性和效果测试。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。
>
> 原生App业务防护请使用爬虫风险管理提供的App增强防护SDK方案。

功能原理

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。

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大陆地域。
3. 选择要操作的域名，单击其操作列下的防护配置。
4. 打开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：

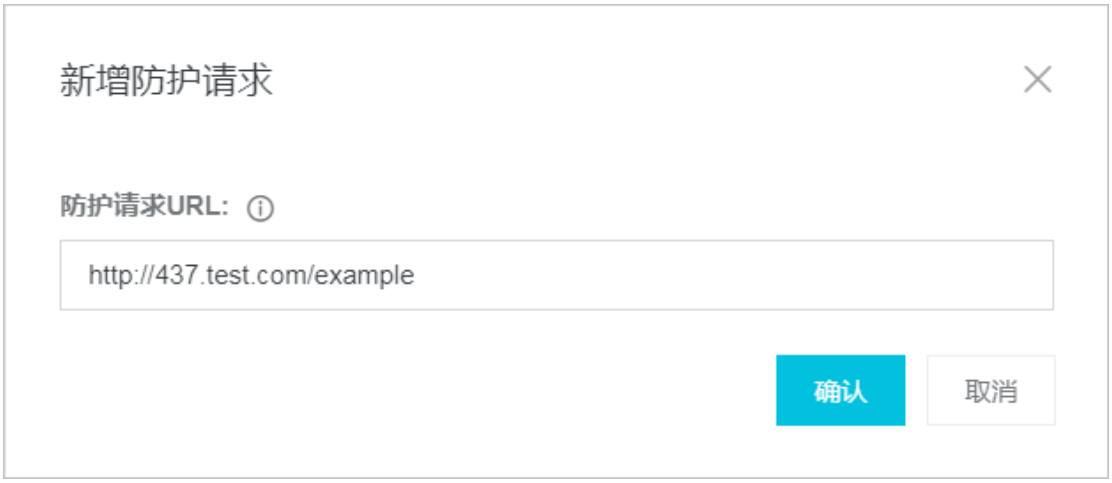
默认使用预警模式，数据风控不会对任何请求进行拦截，但依然会在静态页面中插入JS脚本分析客户端行为。

6. 单击前去配置，添加防护请求或指定JS插入页面。

- 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。

· 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。

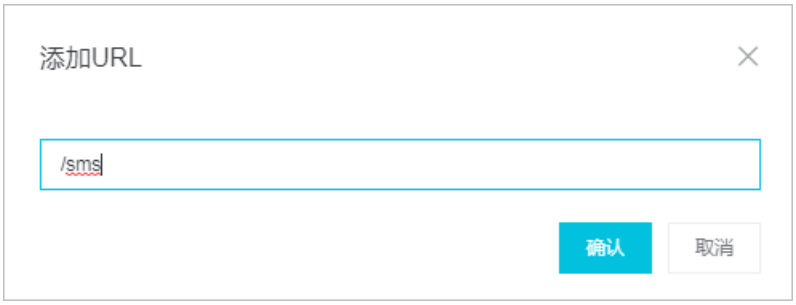
a. 在JS插入页面页签下，单击指定页面插入JS。

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。

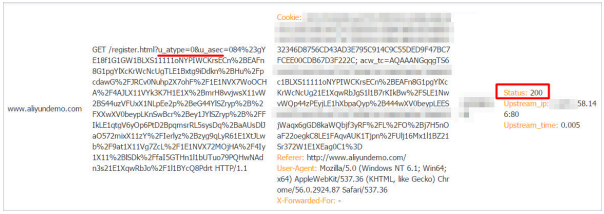
    - 如果通过滑块验证方式可疑（例如，使用脚本模仿真人滑动过程等），数据风控将继续通过其它方式再次进行验证，直到验证通过且通过方式可信。
    - 如果无法通过验证，数据风控将阻断该请求。
  - 如果基于之前的行为，数据风控判断该请求来自正常用户，则该用户在注册过程中将无任何感知。

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

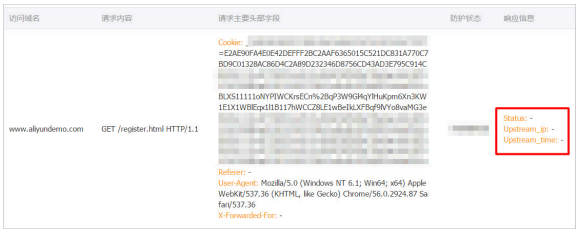
您可以使用WAF的全量日志查询功能来排查数据风控的监控和拦截情况。

- 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。

5.10 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。

背景信息

对于按量付费的WAF实例，您必须在功能与规格中启用网页防篡改、敏感信息防泄露，才能使用该功能。具体操作，请参考功能与规格配置。

参照以下步骤，启用并配置网站防篡改：

> **说明:**
> 执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考CNAME接入指南。

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WAF所在地区（中国大陆、海外地区）。

3. 选择要操作的域名，单击其操作列下的防护配置。
4. 在网站防篡改下，启用防护，并单击前去配置。

说明:

如果您不想使用网站防篡改，您可以在该页面关闭防护。

5. 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。

6. 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。

7. 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。

5.11 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。

功能描述

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。

对于按量付费的WAF实例，您必须在功能与规格中启用网页防篡改、敏感信息防泄露，才能使用该功能。具体操作，请参考功能与规格配置。

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。

工作原理

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

参照以下步骤，启用并配置防敏感信息泄露：

> 说明：
> 执行以下操作前，请确保已将网站接入WAF进行防护。具体操作请参考CNAME接入指南。

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WAF所在地区（中国大陆、海外地区）。
3. 选择要操作的域名，单击其操作列下的防护配置。
4. 在防敏感信息泄露下，启用防护，单击前去配置。

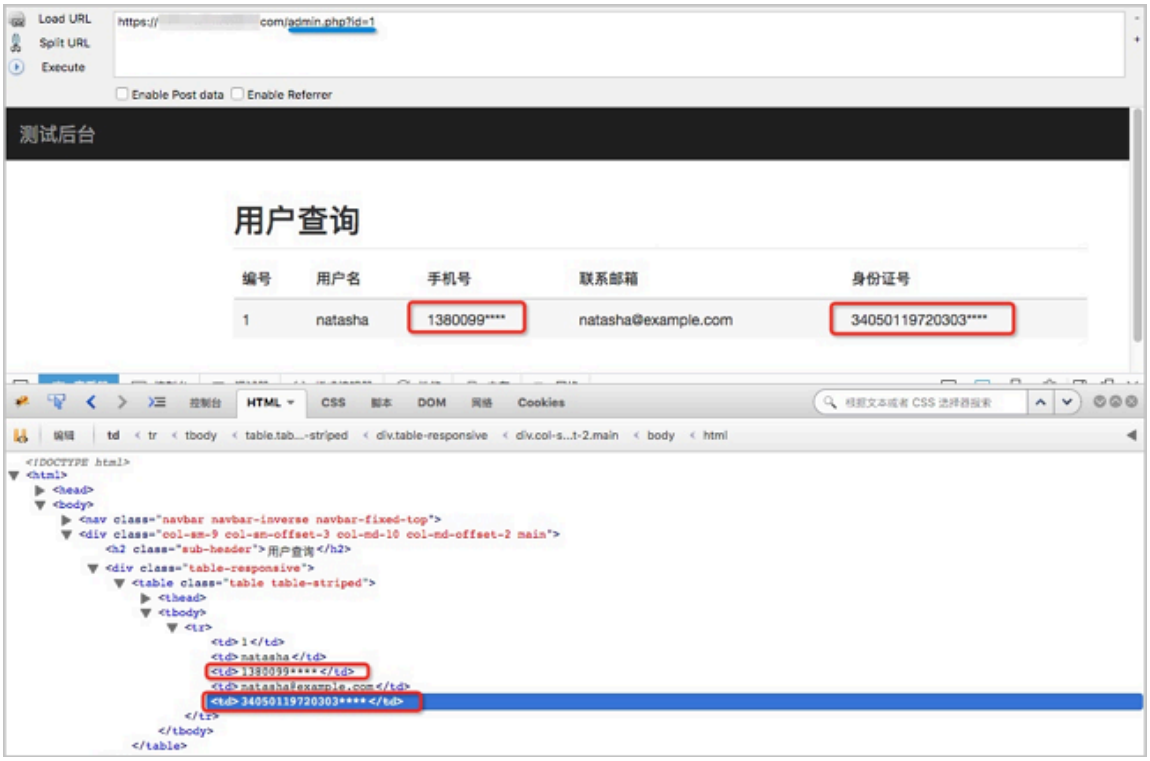
5. 单击新增规则，添加敏感信息防护规则。

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。

6. 成功添加规则后，您可以编辑或删除规则。

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。

5.12 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

只有同时满足以下条件时，才能开启高频Web攻击IP自动封禁：

- 使用包年包月模式开通Web应用防火墙（WAF），或者使用按量付费模式开通Web应用防火墙并且开启Web攻击防护高级防护。具体请参考开通Web应用防火墙、功能与规格配置（按量付费模式）。
- 网站已接入WAF进行防护。具体请参考WAF功能使用概览接入WAF部分。
- 已开启Web应用攻击防护和CC安全防护功能。具体请参考Web应用攻击防护和CC安全防护。

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WAF所在地区（中国大陆、海外地区）。
3. 选择要操作的域名，单击其操作列下的防护配置。
4. 在高频Web攻击IP自动封禁下，开启防护。

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。

5. （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。

> 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。

配置	描述
检测时间范围	设置检测时间间隔，单位为秒。
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。

配置	描述
封禁IP	设置触发封禁时，封禁客户端IP多长时间，单位为秒。

c) 单击确定。

6. （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。

5.13 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

只有同时满足以下条件时，才能开启目录遍历防护：

- 使用包年包月模式开通Web应用防火墙（WAF），或者使用按量付费模式开通Web应用防火墙并且开启Web攻击防护高级防护。具体请参考开通Web应用防火墙、功能与规格配置（按量付费模式）。
- 网站已接入WAF进行防护。具体请参考WAF功能使用概览接入WAF部分。
- 已开启Web应用攻击防护和CC安全防护功能。具体请参考Web应用攻击防护和CC安全防护。

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WAF所在地区（中国大陆、海外地区）。
3. 选择要操作的域名，单击其操作列下的防护配置。
4. 在目录遍历防护下，开启防护。

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。

5. （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。

> 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。

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	

配置	描述
封禁IP	设置触发封禁时，封禁客户端IP多长时间，单位为秒。

c) 单击确定。

6. （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。

5.14 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

只有同时满足以下条件时，才能开启扫描威胁情报：

- 使用包年包月模式开通Web应用防火墙（WAF），或者使用按量付费模式开通Web应用防火墙并且开启Web攻击防护高级防护。具体请参考开通Web应用防火墙、功能与规格配置（按量付费模式）。
- 网站已接入WAF进行防护。具体请参考WAF功能使用概览接入WAF部分。
- 已开启Web应用攻击防护和CC安全防护功能。具体请参考Web应用攻击防护和CC安全防护。

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WAF所在地区（中国大陆、海外地区）。
3. 选择要操作的域名，单击其操作列下的防护配置。
4. 在扫描威胁情报下，根据实际需求开启防护功能。

   可开启的防护功能包括：

   - 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。

5.15 主动防御

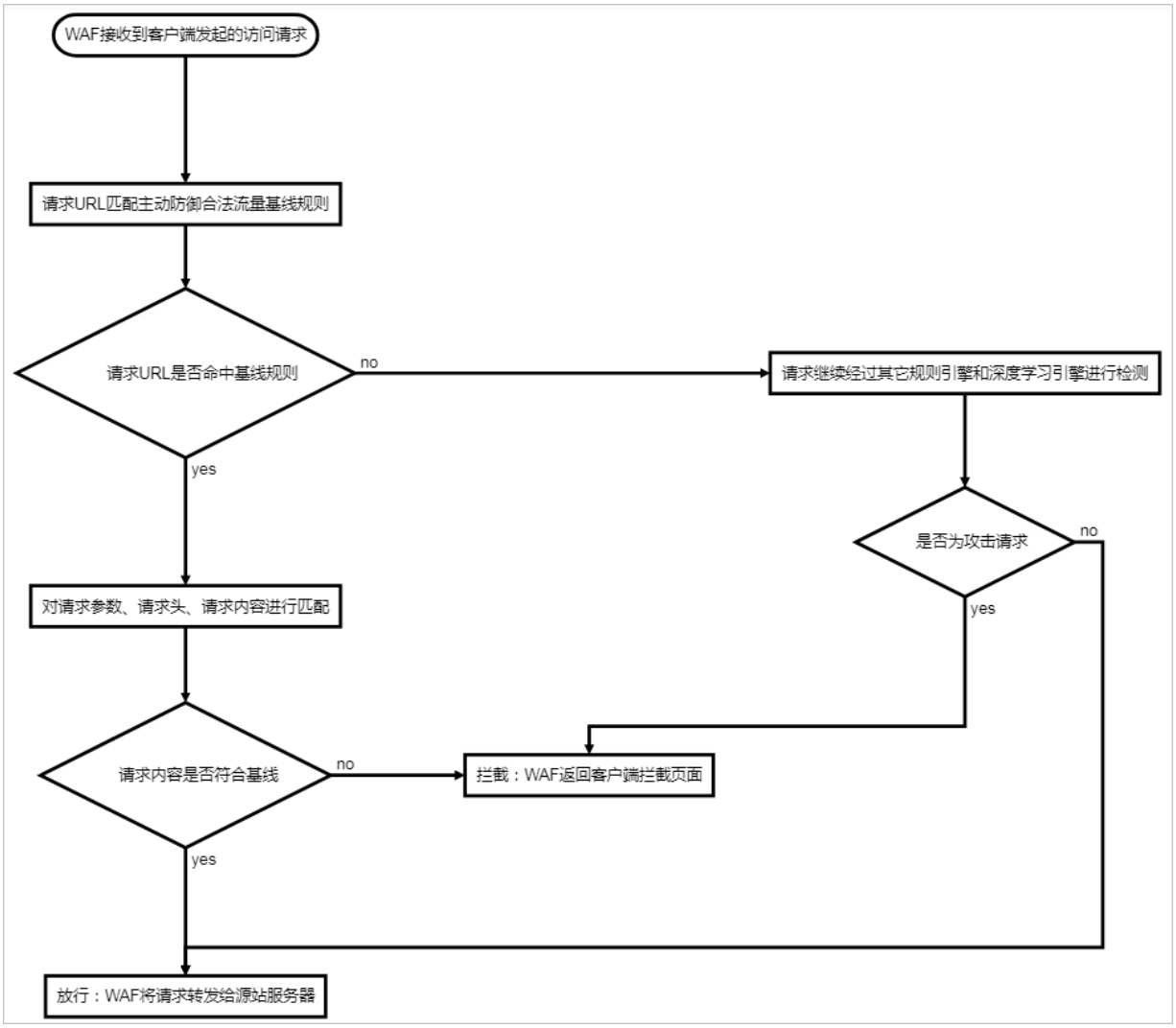
主动防御功能采用阿里云自研的机器学习算法自动学习域名的合法流量，从而为域名自动生成定制化的安全策略，防护未知攻击。

前提条件

- 网站已接入WAF进行防护。具体请参见WAF功能使用概览接入WAF部分。
- 对于WAF高级版或企业版实例，您必须升级至旗舰版，才能使用主动防御功能。具体操作，请参见续费与升级。

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WAF所在地区（中国大陆、海外地区）。**
3. **选择要操作的域名，单击其操作列下的防护配置。**

4. 定位到主动防御区域，打开主动防御功能开关。

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。

5. 当主动防御的算法模型完成对域名的流量学习后，单击主动防御区域的前去配置可查看主动防御功能为该域名自动生成的安全规则。

说明:

默认情况下，主动防御功能采用预警模式。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，再将其设置为防护模式。

只有当主动防御功能的模式设置为防护时，被设置为防护模式的安全规则才会对业务流量产生影响。当主动防御功能的模式为预警时，即使部分安全规则的防护模式为防护，这些安全规则也不会对命中规则的请求进行拦截。

6. （可选）在安全规则列表中，单击操作栏中的编辑，修改主动防御功能自动生成的规则的防护模式。您也可以单击删除来删除指定安全规则。

说明:

为保证主动防御的防护效果，通常情况下建议您不要随意删除算法模型自动生成的安全规则。您可以先使用预警模式并通过#unique_104观察该规则的执行情况，完全确认规则效果后再将防护模式设置为防护使其真实生效。

主动防御规则说明

 说明:
目前，在编辑安全规则时，您只能修改主动防御规则的防护模式字段。

字段	说明
规则名称	主动防御规则的名称。
模式	用于定义HTTP请求中的URL（不包含参数）。例如，对于`/index.php?a=122`，其模式表示为`/index.php`。系统自动生成的安全规则通常使用正则表达式来描述。
方法	定义该URL支持的HTTP请求方法，支持选择多个方法。
参数	定义该URL中的参数。例如，对于`/index.php?a=122`，其参数名称为a，参数值为122。系统自动生成的安全规则通常使用正则表达式来描述。
防护模式	规则的防护生效模式，包括： · 防护：当域名配置的主动防御功能启用防护模式时，该规则将真实生效，对命中规则条件的业务流量产生影响。 · 预警：命中该规则条件的请求将上报至安全报表，但不会被拦截。  说明: 建议您在规则学习完成后，先将其设置为预警模式观察一段时间，确认规则没有出现误拦截的情况后，再将其设置为防护模式使其真实生效。

6 防护统计

6.1 业务总览

云盾Web应用防火墙总览页面展示您已接入WAF的所有网站的总体威胁情况，包括攻击防护和威胁概述、以及业务、攻击、威胁的详细分析。

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 前往统计 > 总览页面，在页面上方选择WAF所在地区（中国大陆、海外地区）。
3. 选择要查看的网站域名（可以是一个具体的域名或全部域名）和要查看的历史时间段（实时、1天、7天、30天、自定义）。

   说明:
   支持查看最近30天内的业务总览信息，使用自定义可以查看最近30天内指定时间段的信息。

4. 根据所选择的网站域名和时间范围，在总览页面您可以通过以下图表查看符合过滤条件的网站的业务、攻击防护、威胁信息。

   · 总体情况：展示网站域名收到的全部请求次数、Web攻击次数、CC攻击次数、访问控制拦截次数、区域封禁拦截次数。同时，单击该图表区域下部的展开按钮，将显示对应数字的缩略趋势图。

   说明:

如果您选择的是全部网站域名资产，展开后将额外显示Top 5的域名及其对应的请求次数、Web攻击次数、CC攻击次数、访问控制拦截次数、区域封禁拦截次数。

- 攻击与事件：为便于您快速了解网站遭受的攻击和威胁情况，在筛选设置下方，WAF将所拦截的攻击聚合成事件进行展示。

说明:

如果您选择的是全部网站域名资产，将显示网站域名遭受的攻击次数及聚合后的事件数量。您可以单击选择具体网站域名查看事件分布情况。

WAF按照攻击的类型、危险程度、频率与时间等因素将攻击聚合成事件。目前，主要包含业务请求异常、CC攻击拦截、Web攻击拦截、精准访问控制拦截、区域封禁拦截、持续攻击拦截等事件类型。

您可以单击聚合后的事件，进一步查看该事件的具体信息及该事件类型相关数据的分布情况。例如，对于CC攻击拦截事件，将展示Top 5的攻击来源IP、请求UserAgent、请

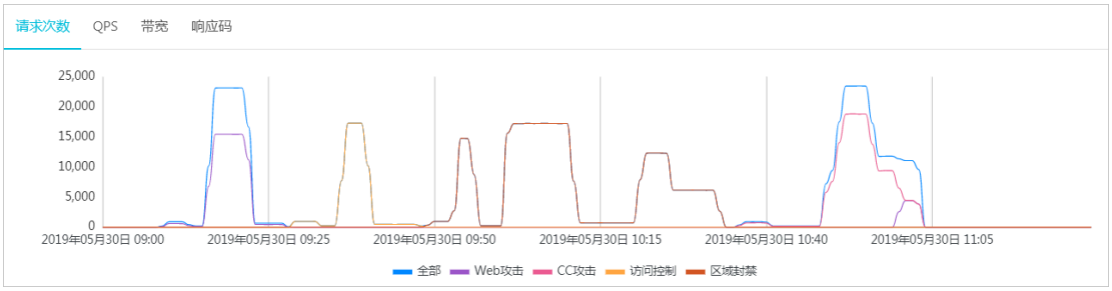
求Referer、目标URL和对应的拦截次数。同时，您可以参考事件详情页面下部的专家防护建议，根据实际业务情况选择合适的防护方案。

- 业务趋势情况：展示所选择的时间段内的请求次数、QPS、带宽、响应码的时间分布情况（最细粒度达分钟级别）。

说明:

单击趋势图下方的图例，可以在图中取消/显示对应类型的记录。

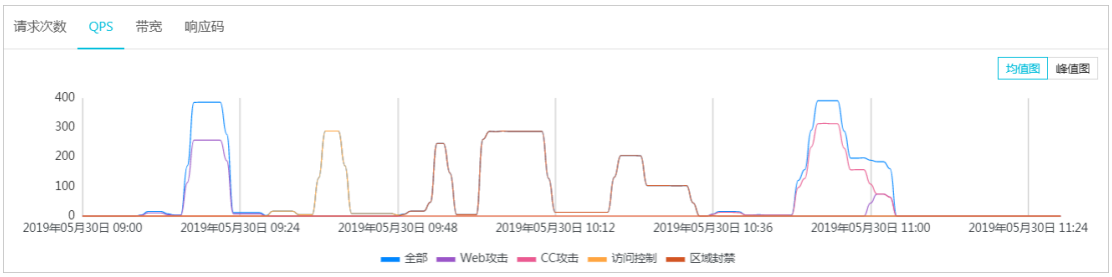
- 请求次数：包含全部请求次数、Web攻击拦截次数、CC攻击拦截次数、精准访问控制拦截次数、区域封禁拦截次数。



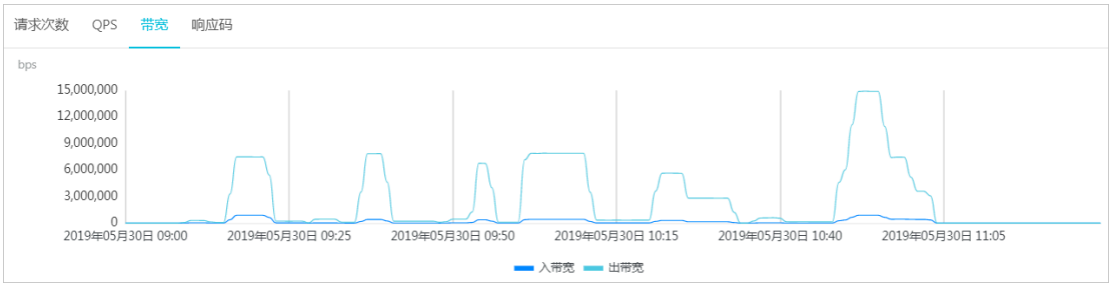
- QPS：包含全部请求QPS、Web攻击拦截QPS、CC攻击拦截QPS、精准访问控制拦截QPS、区域封禁拦截QPS。

说明:

单击趋势图右上角的均值图和峰值图，可以选择显示QPS均值或QPS峰值。



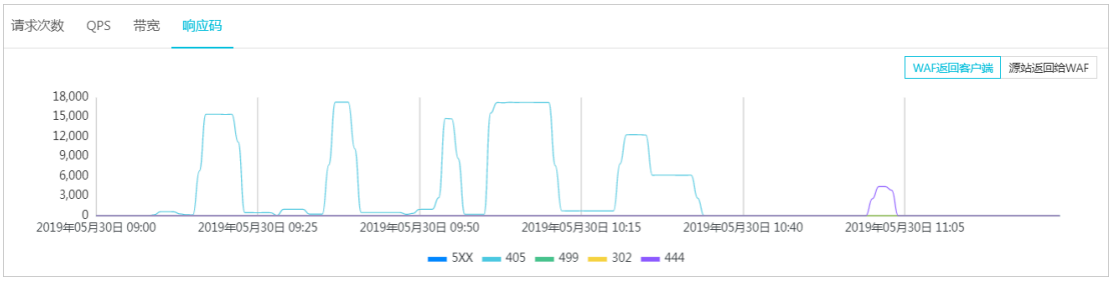
- 带宽：包含入方向带宽和出方向带宽（单位：bps）。



- 响应码：包含5xx、405、499、302、444等异常响应码。

说明:

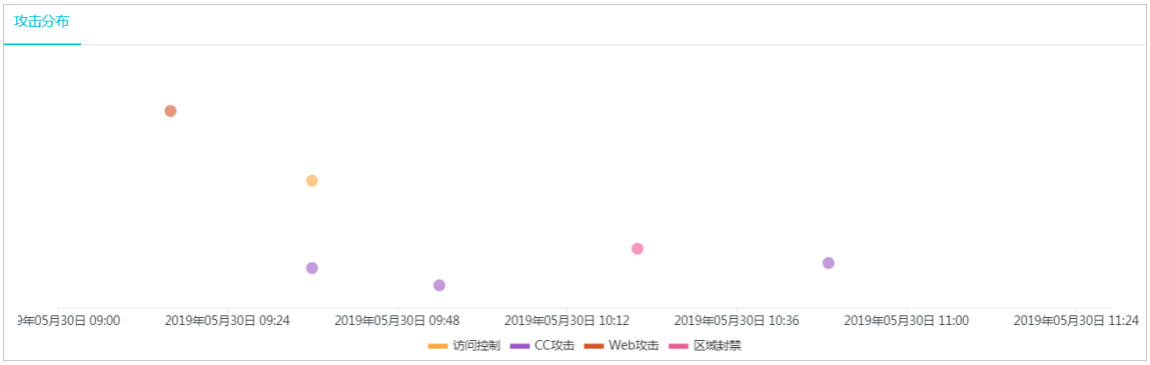
单击趋势图右上角的WAF返回给客户端和源站返回给WAF，可以选择查看WAF返回给客户端或源站服务器返回给WAF的响应码的时间分布情况。



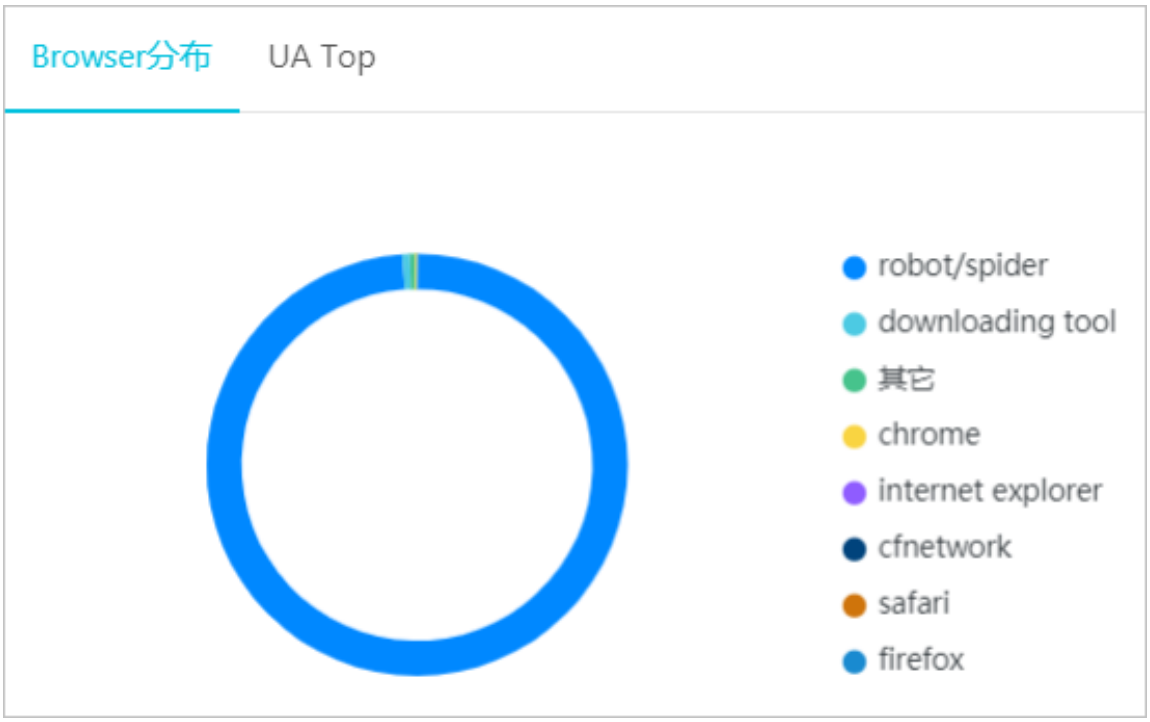
- **事件分布情况：攻击分布页签下展示将攻击聚合后的事件分布情况。**

说明:

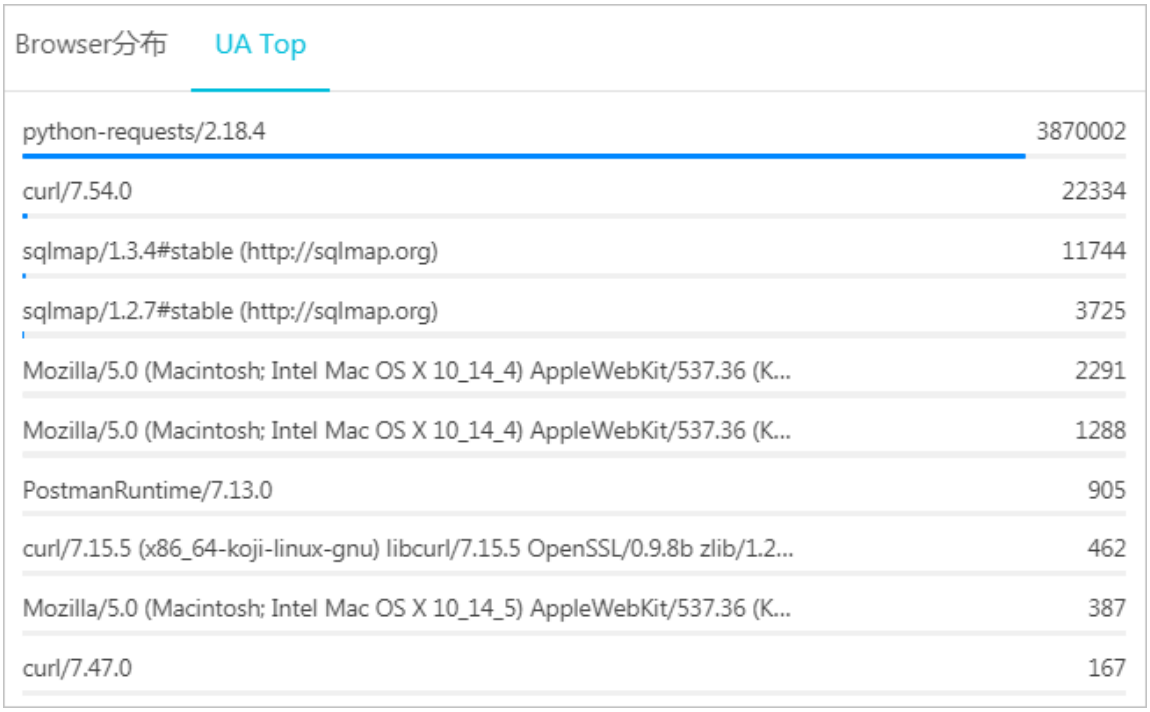
单击事件点，可以进一步查看该事件的具体信息及该事件类型相关数据的分布情况。



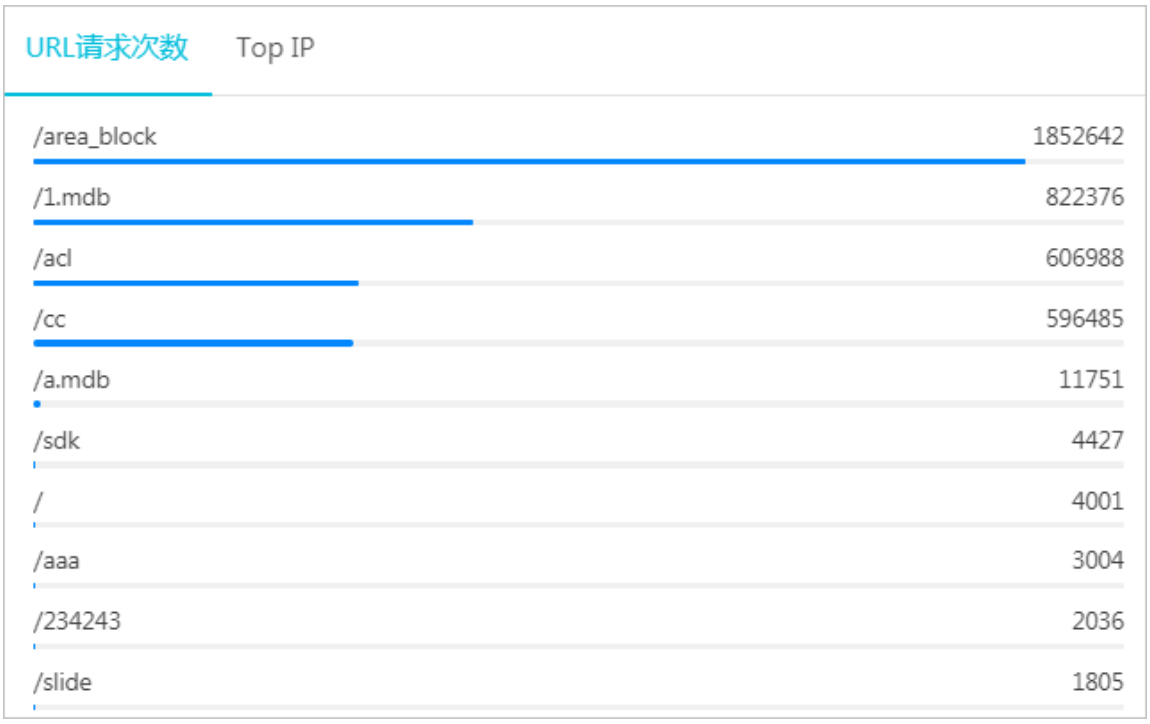
- **浏览器分布情况：Browser分布页签下以饼状图展示访问源的浏览器类型分布情况。**



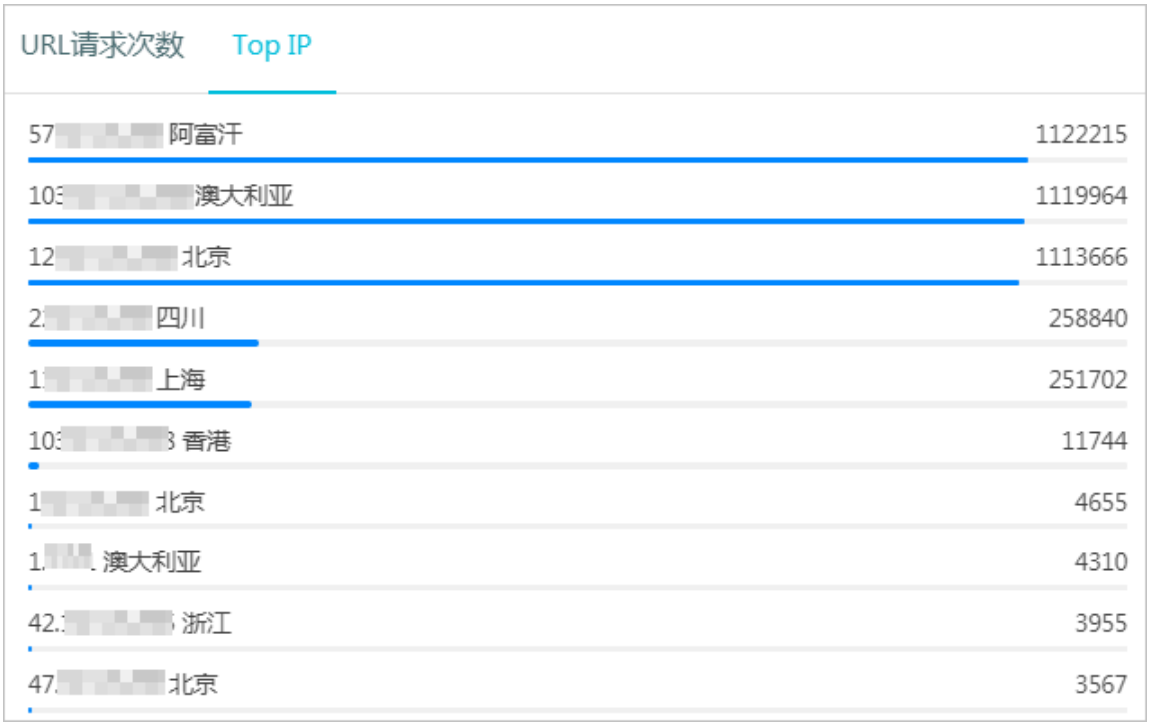
- **请求UserAgent排名情况：UA Top页签下展示收到的请求中UserAgent的排名情况和请求次数。**



- **被请求URL排名情况：URL请求次数页签下展示被请求URL的排名情况和请求次数。**



- **访问来源IP排名情况：Top IP页签下展示访问来源IP的排名情况和访问次数。**



6.2 安全报表

WAF提供安全报表帮助您了解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:

对于按量付费的WAF实例，您必须在功能与规格中勾选提供业务分析报表，才能使用该功能。具体操作，请参考功能与规格配置。

背景信息

WAF提供安全报表，供您查看和了解WAF的所有防护动作。攻击防护安全报表集中展示Web应用攻击、CC攻击的防护记录和访问控制事件。

操作步骤

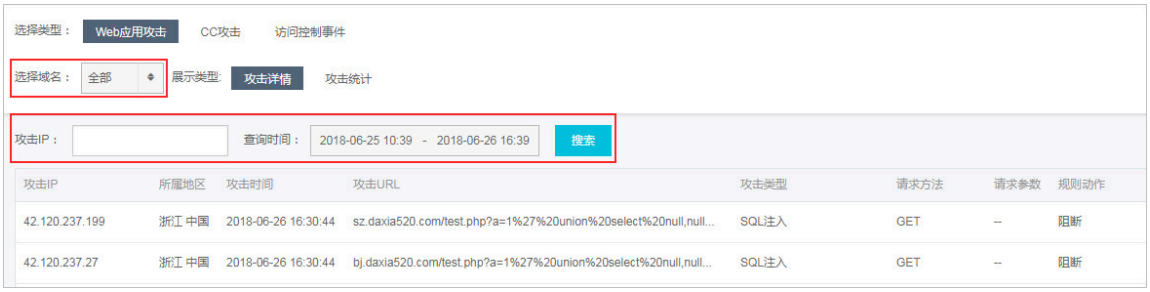
参照以下步骤，查看WAF安全报表：

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。

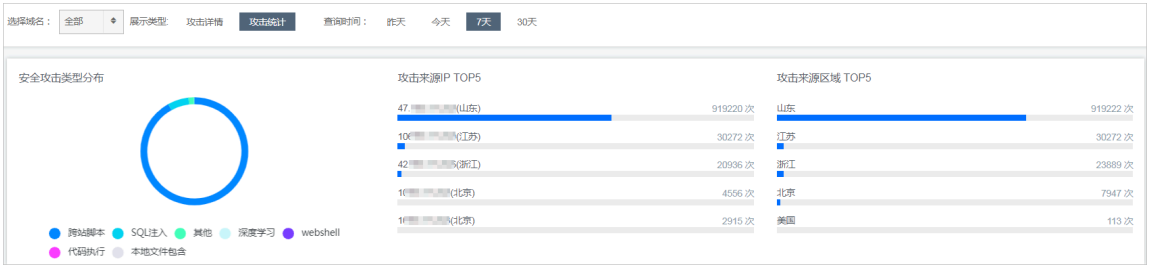
- Web应用攻击：展示WAF阻断的所有Web攻击记录。您可以使用域名、攻击IP、和攻击时间来筛选您关注的记录。

> 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。

6.3 全量日志查询

启用全量日志功能后，WAF将记录您网站的所有访问请求日志，您可以通过一键智能搜索快速定位请求记录，满足运维、安全方面的管理需求。

背景信息

对于WAF高级版，您必须升级到企业版或旗舰版，才能使用全量日志查询。具体操作请参考续费与升级。

> 说明:
> 海外地域的WAF必须升级到旗舰版才可使用全量日志查询功能。

对于按量付费的WAF实例，您必须在功能与规格中勾选全量日志查询，才能使用该功能。具体操作，请参考功能与规格配置。

通过全量日志功能，您可以轻松地完成以下运维工作：

- 确认某个具体请求是否被WAF拦截或放行。
- 确认某个具体拦截是由Web攻击、CC攻击防护或是自定义的访问控制规则触发。
- 查询源站对于某个具体请求的响应时间，观察是否超时等。
- 通过源IP、URL关键字、cookie、referer、user-agent、X-forwarded-for、服务器响应状态码等条件组合查询具体的请求。

> 说明:
> 启用全量日志查询功能，即表示您允许阿里云记录您全部经过WAF的Web请求（POST数据不会被记录）。

使用日志检索功能前，需要在网站配置页面为指定的网站域名开启日志检索功能。只有开启日志检索功能后，WAF才会开始记录该网站的访问日志。为网站域名开启日志检索功能后，您就可以在全量日志页面查询该网站的访问日志。

> 说明:
> WAF最多支持查看100个域名的全量日志。

操作步骤

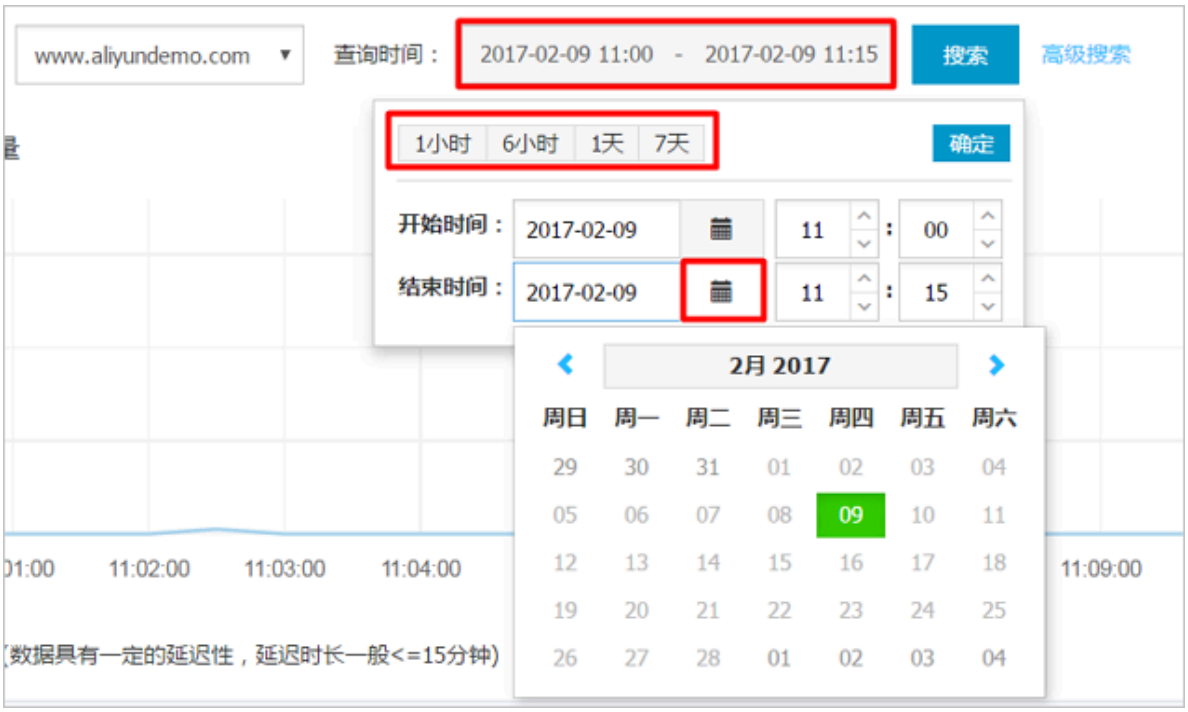
1. 登录云盾Web应用防火墙控制台。
2. 前往管理 > 网站配置页面，并在页面上方选择WAF所在地区（中国大陆、海外地区）。
3. 选择已添加的网站域名，在日志检索栏，单击开启日志检索功能。

> 说明:

您也可以在此页面停用日志检索。如果您停用日志检索功能，则停用期间的访问请求日志不会被记录；即使重新开启日志检索功能，您也无法查询到停用期间的访问请求日志。

4. 前往统计 > 全量日志页面。
5. 选择域名，设置查询时间，单击搜索。

说明:
全量日志功能最多记录最近一个月内的访问日志。



您也可以单击高级搜索，设置更详细的检索条件。

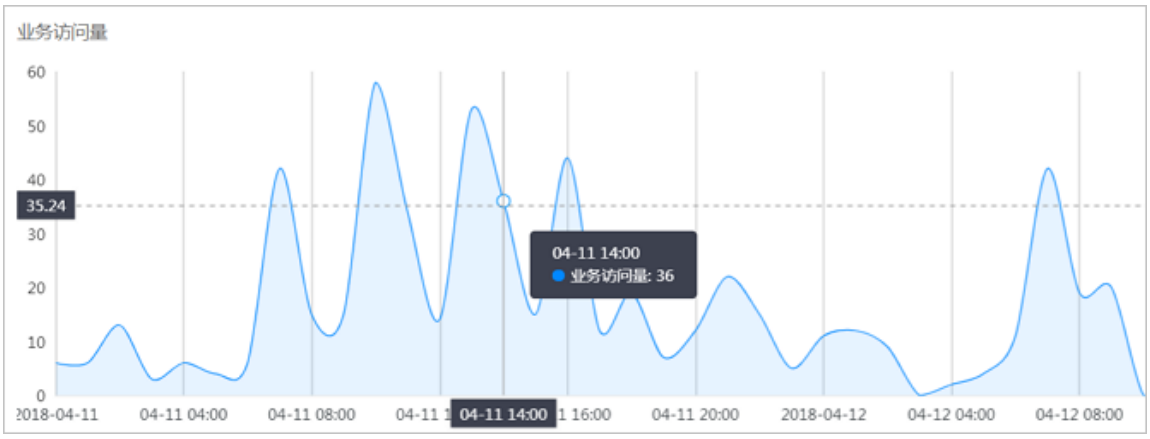
表 6-1: 高级搜索条件

字段	描述
源IP	访问的客户端来源IP。

字段	描述
URL关键字	访问请求URL。  说明: 所填写的URL关键字支持包含“/”符号。例如，您可以填写/ntis/cashier。
Cookie	访问请求头部中带有的访问来源客户端Cookie信息。
Referer	访问请求头部中带有的访问请求的来源URL信息。
User-Agent	访问请求头部中带有的访问来源客户端浏览器标识、操作系统标识等信息。
X-Forwarded-For	访问请求头部中带有的XFF头信息。
服务器响应状态码	源站服务器返回给WAF的响应状态信息。 状态码支持填写最多三位数字，且支持模糊搜索。例如，输入4*进行搜索，将查找所有以4开头的状态码。  说明: · *可以匹配0或多位数字，但不能以*开头。 · 支持填写-符号，查找无状态信息的访问请求。
WAF返回客户端响应码	WAF返回给客户端的响应状态信息。 响应码支持填写最多三位数字，且支持模糊搜索。例如，输入4*进行搜索，将查找所有以4开头的响应码。  说明: · *可以匹配0或多位数字，但不能以*开头。 · 支持填写-符号，查找无状态信息的访问请求。
请求唯一ID标识	指定访问请求。如果存在访问请求被拦截，可以填写拦截页面中的该请求的ID进行搜索。
访问域名	当您对泛域名启用全量日志功能，可以利用该字段对一级子域名进行搜索。
防护规则	选择命中的防护规则类型，包括Web攻击防护、CC防护策略、访问控制策略、区域封禁、数据风控。

6. 查看日志检索结果。

   · 在业务访问量区域，查看检索时间范围内的访问请求量趋势图。



   · 在访问日志列表中，查看符合检索条件的访问请求记录。例如，被CC攻击防护规则拦截的访问请求记录如下图所示。

   关于源站响应信息中的参数含义说明

   - Status：指WAF返回给客户端的响应状态信息。
   - Upstream_Status：指源站返回给WAF的响应状态信息。如果返回“-”，表示没有响应（例如该请求被WAF拦截或源站响应超时）。
   - Upstream_ip：指该请求所对应的源站IP。例如，WAF回源到ECS的情况，该参数即返回源站ECS的IP。
   - Upstream_time：指源站响应WAF请求的时间。如果返回“-”，代表响应超时。

7. 单击全量日志页面右上方的日志下载可为当前检索到的日志结果生成下载任务。下载任务生成完成后，在查看下载文件页签中即可将相应格式的日志文件下载到本地。

   说明:

单次最多支持导出2000万条日志。如果您需要导出的日志超过2000万条以上，建议您分多次任务进行导出。

日志文件字段说明

字段	字段名称	描述
Time	访问时间	访问请求的发生时间，在所下载的日志文件中以UTC时间记录。
Domain	访问域名	访问请求的域名。
Source_IP	来源IP	访问的客户端来源IP。
IP_City	来源IP所属地区	访问来源IP所属地区，中国大陆地区可精确到市级。
IP_Country	来源IP所属国家	访问来源IP所属国家。
Method	访问请求方法	访问的请求行中的请求类型。
URL	访问请求URL	访问请求行中的所访问的服务器资源。
Https	访问请求协议	访问请求行中的请求所使用的协议。
Referer	HTTP Referer字段	访问请求头部中带有的访问请求的来源URL信息。
User-Agent	HTTP User-Agent字段	访问请求头部中带有的访问来源客户端浏览器标识、操作系统标识等信息。
X-Forwarded-For	HTTP X-Forwarded-For字段	访问请求头部中带有的XFF头信息，用于识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址。
Cookie	HTTP Cookie字段	访问请求头部中带有的访问来源客户端Cookie信息。

字段	字段名称	描述
Attack_Type	防护状态	WAF对该访问请求的处理结果： · 0：表示未发现攻击 · 1：表示触发Web应用攻击防护规则 · 2：表示触发CC安全防护规则 · 3：表示触发精准访问控制规则 · 4：表示触发地区封禁防护策略 · 5：表示触发数据风控防护策略 · 6：表示触发高频扫描攻击封禁规则 · 7：表示触发目录遍历扫描防护规则 · 8：表示触发协同防护策略 · 9：表示触发扫描工具封禁规则
Status	响应状态码	指WAF返回给客户端的响应状态信息。
Upstream_Status	源站响应状态码	源站返回给WAF的响应状态。如果返回“-”，表示没有响应（例如该请求被WAF拦截或源站响应超时）。
Upstream_IP	源站响应IP	访问请求所对应的源站IP。例如，WAF回源到ECS的情况，该参数即返回源站ECS的IP。
Upstream_Time	源站响应时间	源站响应WAF请求的时间。如果返回“-”，代表响应超时。

6.4 数据大屏

依托接入WAF后的网站业务详细日志，WAF提供数据大屏服务，通过将数据转化为直观的可视化大屏，对您网站的实时攻防态势进行监控和告警，为您提供可视化、透明化的数据分析和决策能力，让安全攻防一目了然。

背景信息

目前，WAF数据大屏开放WAF实时攻防态势大屏和WAF安全数据平台大屏。由于大屏的特殊性，目前数据大屏仅支持谷歌Chrome浏览器56及以上版本。

说明：

更多WAF数据大屏即将开放，敬请期待。

WAF实时攻防态势大屏

WAF实时攻防态势大屏以秒级数据维度实时更新，展示所有已接入WAF防护的网站业务当日的业务访问情况及整体拦截情况，集中体现业务运行的稳定性及网络质量。

说明:

数据统计范围为当日零点至当前时分。

展示项	描述
In带宽	入方向业务带宽流量（单位：bps）。
Out带宽	出方向业务带宽流量（单位：bps）。
QPS	当前业务访问量（单位：QPS）。
拦截比例	WAF拦截次数占总访问请求量的百分比值。
今日拦截次数	WAF拦截的恶意请求次数。
移动端OS分布	移动端访问请求来源OS分布情况。
PC端浏览器分布	PC端访问请求来源浏览器分布情况。
访问来源IP TOP10	访问次数排名前十的访问来源IP及其访问次数。
访问URL次数 TOP5	访问次数排名前五的被访问URL。
异常监控	访问请求返回的异常HTTP响应状态码及其出现次数。
访问统计（中国）	访问统计热点图，展示近一小时内访问请求来源的热力分布情况。
业务请求	访问请求QPS趋势图。同时，图中展示WAF所拦截的请求次数趋势，包括访问控制拦截、数据风控拦截、Web攻击拦截、CC攻击拦截。
带宽	入方向带宽与出方向带宽趋势图。

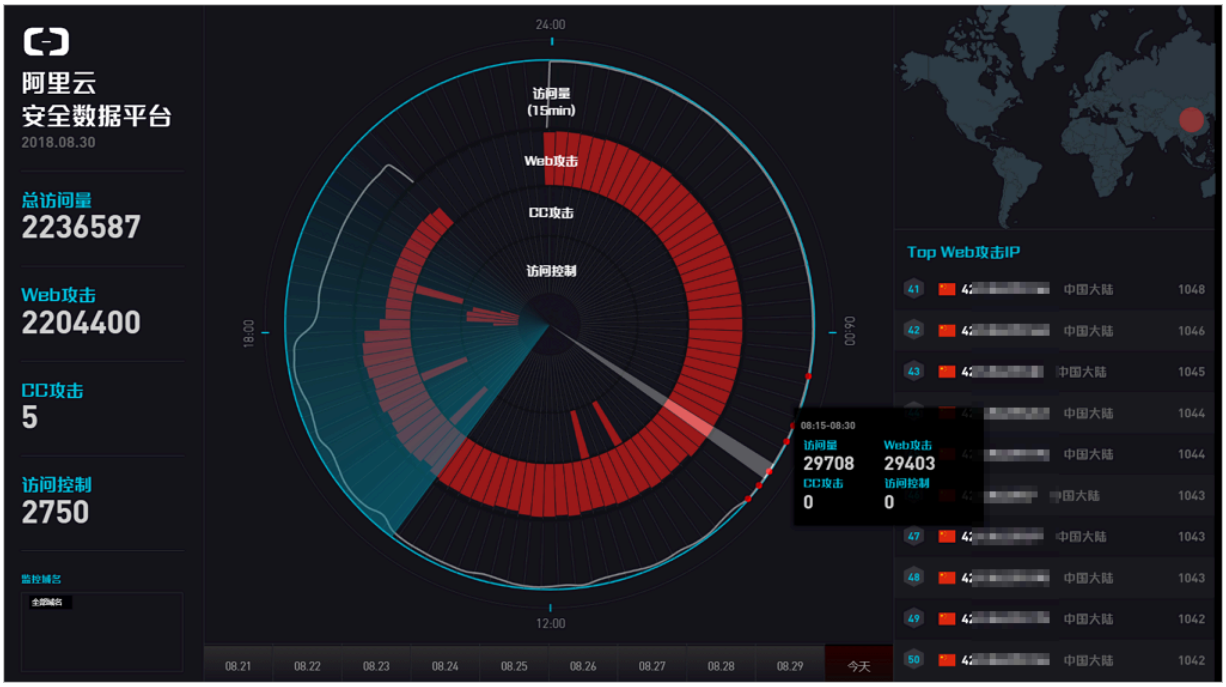
其中，WAF实时攻防态势大屏正中间的地球上白色的点和闪烁的虚线代表WAF机房。

WAF安全数据平台大屏

WAF安全数据平台大屏，展示Web攻击、CC攻击、访问控制拦截等安全数据信息。

> **说明:**
> 单击大屏左下角的监控域名区域，您可以选择需要展示安全数据的域名，您也可以选择监控所有域名。

展示项	描述
总访问量	所选择域名的当日总访问量。
Web攻击	所选择域名当日WAF所拦截的Web攻击次数。
CC攻击	所选择域名当日WAF所拦截的CC攻击次数。
访问控制	所选择域名当日WAF的精准访问控制规则的拦截次数。
Top Web攻击IP	展示TOP攻击来源IP、所属地域及攻击次数。同时，将鼠标移至该TOP攻击来源IP可查看Web攻击类型及该IP的属性。
地域热力图	右上角的地域热力图展示攻击来源所属地域的热力分布情况。

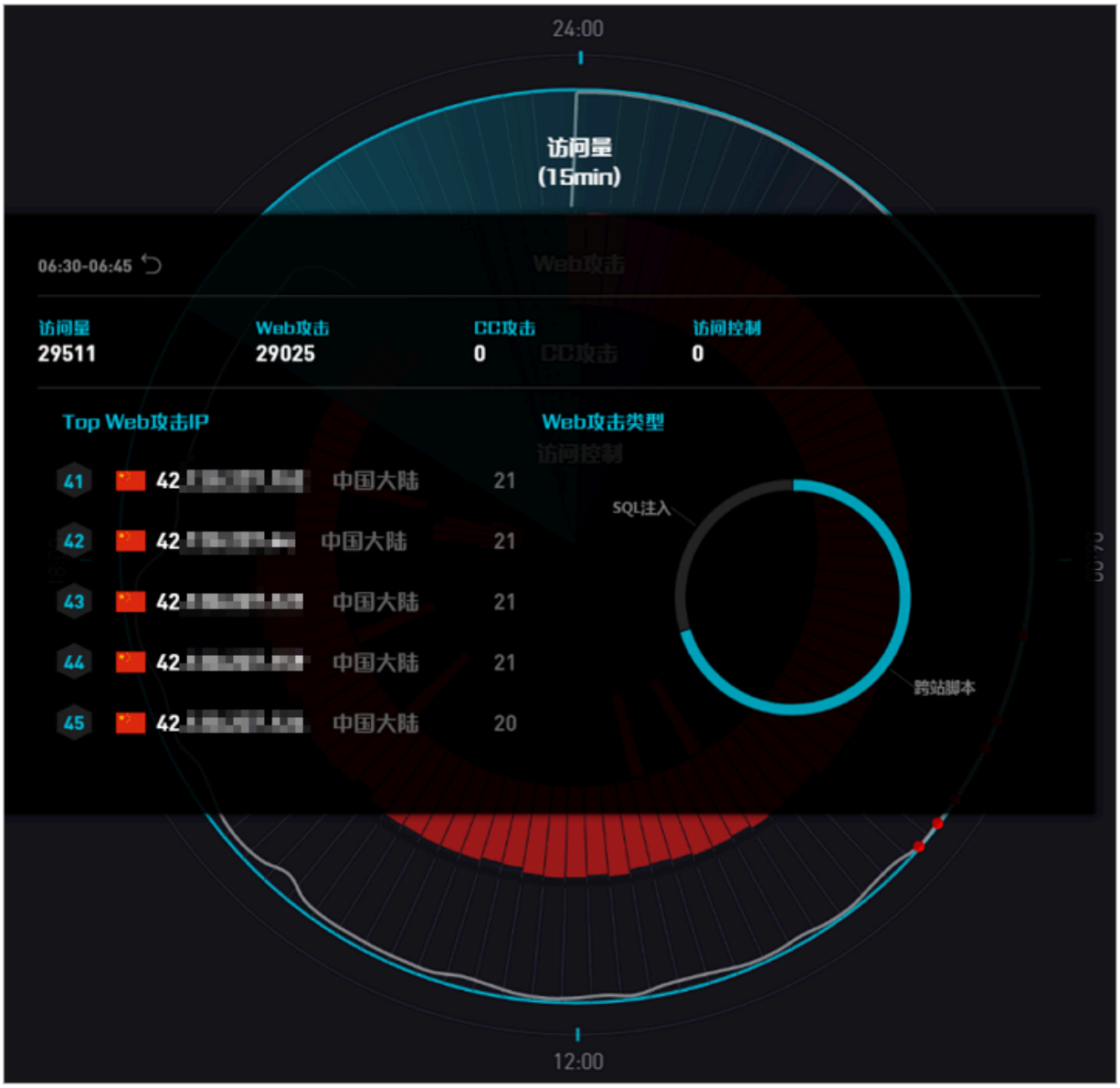


WAF安全数据平台大屏正中间的雷达图以每15分钟作为区间展示该时间段内的访问QPS、Web攻击拦截、CC攻击拦截、访问控制拦截情况。同时，选择雷达图中的时间段，单击悬浮窗口将展示该时间段内的详细安全数据信息。

说明:

单击大屏最下方的日期可选择展示指定日期的安全数据。

展示项	描述
访问量	业务访问量（单位：QPS）。
Web攻击	WAF所拦截的Web攻击次数。
CC攻击	WAF所拦截的Web攻击次数。
访问控制	WAF的精准访问控制规则的拦截次数。
Top Web攻击IP	展示TOP攻击来源IP、所属地域及攻击次数。同时，将鼠标移至该TOP攻击来源IP可查看Web攻击类型及该IP的属性。
Web攻击类型	所拦截的Web攻击类型分布情况。
Top攻击地区	TOP5攻击来源地区。
Top命中规则	命中触发次数TOP5的WAF防护规则。



开通大屏

1. 登录云盾Web应用防火墙控制台。
2. 定位到统计 > 数据大屏页面，选择您的WAF实例所属地域，单击立刻购买。

> **说明:**

如果WAF实例的地域为海外，您必须升级到企业版或旗舰版，才能开通数据大屏服务。

3. 在WAF实例配置变更页面的可视化大屏服务配置项，选择单屏服务或多屏服务。

选项	描述	定价
单屏服务	仅支持选择开通一块数据大屏。	1,000 元/月
多屏服务	支持开通所有WAF提供的数据大屏。	2,000 元/月

说明:

数据大屏服务将沿用您当前WAF实例的到期时间，系统将根据您选择的服务和当前WAF实例的到期时间，自动计算您所需支付的款项金额。开通数据大屏服务后，暂不支持仅续费WAF实例，您必须同时续费已开通的数据大屏服务。

4. 勾选《Web应用防火墙（包月）服务协议》，单击去支付完成付款。
5. 在数据大屏页面，单击您想要展示的大屏即可享受WAF数据大屏服务。

说明:

如果您购买的是单屏服务，选择您想要开通的大屏，单击立刻开通并确认。

7 设置

7.1 功能与规格配置（按量付费模式）

以按量付费模式开通WAF后，您可以实时调整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。

背景信息

调整WAF的功能规格后，WAF的计费会发生变化。关于按量付费WAF的计费方式，请参见产品价格页。WAF控制台也提供了基于当前配置的价格预估功能，具体请参见查询价格预估。

支持调整的功能

名称	描述
Web攻击防护	抵御各类Web应用攻击，如SQL注入、命令执行、XSS等。
CC安全防护	独家算法防护引擎、结合大数据、秒级拦截机器恶意CC攻击。
精准访问控制（黑白名单）	针对性地拦截或放行某次访问。
高频Web攻击IP自动封禁	自动封禁在短时间内进行多次Web攻击的客户端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。
扫描威胁情报	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。
新智能防护引擎	发现SQL注入和XSS高危风险，降低误报率。
数据风控	防止垃圾注册、账号被盗、活动作弊、垃圾消息等欺诈威胁。
网页防篡改	防止指定网站目录页面被篡改。
敏感信息防泄露	避免身份证、银行卡、电话号码等敏感数据泄露；针对服务器返回的异常页面或关键字做信息保护。
封禁地区	针对指定的国内省份或海外地区的来源IP进行一键黑名单封禁。
独享IP	可针对域名开启，使其不受针对其他域名的DDoS攻击的影响。
扩展域名包	购买后支持接入更多域名进行防护。

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 前往设置 > 功能与规格页面。

3. 根据需要，在功能与规格设置下调整相应设置。

- Web攻击防护：提供基础防护和高级防护两种规格。
  - 默认使用基础防护，该规格支持预警和拦截模式，以及宽松、正常、严格三种防护策略。关于防护策略的调整方法，请参见Web应用攻击防护。
  - 高级防护在基础防护的基础上，提供高频Web攻击IP自动封禁、目录遍历防护、扫描威胁情报和新智能防护引擎功能。关于新增功能的操作，请分别参见高频Web攻击IP自动封禁、目录遍历防护、扫描威胁情报和新智能防护引擎。
- 缓解CC攻击：提供基础防护和高级防护两种规格。
  - 默认使用基础防护，该规格依据独家算法引擎，支持秒级拦截恶意CC攻击，并提供正常和攻击紧急两种拦截模式。关于拦截模式的调整方法，请参见CC安全防护。
  - 高级防护在基础防护的基础上，提供基于URL设定IP访问频率的功能，即自定义CC防护规格，每个域名可设置50条规则。更多信息，请参见自定义CC防护。
- 精准访问控制（黑白名单）：提供基础防护和高级防护两种规格。
  - 基础防护提供基于IP和URL的黑白名单功能，每个域名可设置10条规则。更多信息，请参见IP黑白名单配置。
  - 高级防护提供基于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。关于精准访问控制的具体操作，请参见精准访问控制。
- 数据风控：开启后可以配置防护规则，防止恶意短信注册、恶意登录、活动作弊等机器威胁。更多信息，请参见数据风控。

- 网页防篡改、敏感信息防泄漏：开启后支持网站防篡改和防敏感信息泄露功能，具体请分别参见网站防篡改和防敏感信息泄露。

- 支持HTTPS业务：勾选后，可以设置网站一键HTTPS（仅需上传证书私钥，无需变更源站）和设置HTTP回源，降低网站负载损耗。更多信息，请参见HTTPS高级配置。
- 全量日志查询：勾选后，WAF会记录网站上所有访问请求日志，并提供一键智能搜索，快速定位请求，方便运维、安全相关管理。更多信息，请参见全量日志查询。
- 支持非标端口业务防护：勾选后，可以使用默认端口（HTTP：80、8080；HTTPS：443、8443）以外的非标端口接入WAF。关于WAF支持的非标端口，请参见非标端口支持。

说明:

开启非标端口支持后，不支持关闭。

- 支持基于地理位置的区域封禁：勾选后，可以针对指定国内省份或海外地区的来源IP进行一键黑名单封禁。更多信息，请参见封禁地区。
- 提供业务分析报表：勾选后，可以查看安全报表，包括访问次数、访问IP个数、访问源IP和区域的Top排行，以及响应时间和响应状态码的分布等信息。更多信息，请参见#unique_104。

- 扩展域名包：支持根据需求增加扩展域名包的数量。一个WAF实例默认支持接入10个域名（仅限在1个一级域名下）；每增加1个域名包，则可以多使用一个不同的一级域名，且支持多接入10个域名。最多可增加1000个扩展域名包。更多信息，请参见#unique_114。

  说明:
  增加扩展域名包数量后，不支持减小。

- 独享IP：支持增加独享IP的数量。每30天内只允许做1次调整。最多可增加10个独享IP。更多信息，请参见独享IP包说明。

  说明:
  增加独享IP数量后，不支持减少。

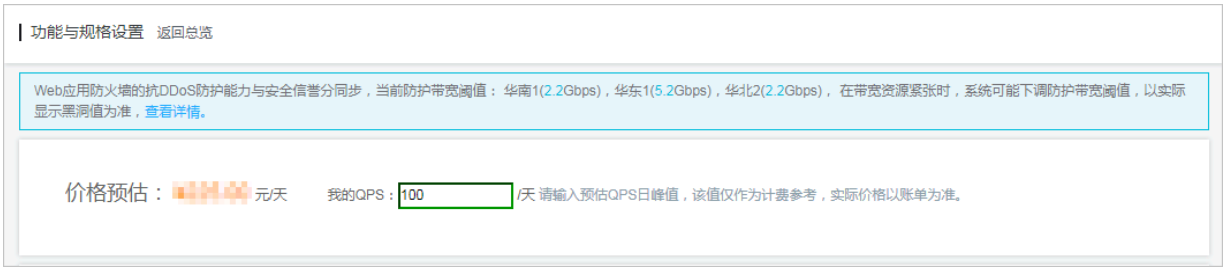
4. 调整完功能规格后，单击页面下方的保存设置，使设置生效。

查询价格预估

针对当前功能与规格配置，WAF支持预估按量付费的日结费用。

登录云盾Web应用防火墙控制台，前往设置 > 功能与规格页面，在价格预估下设置被防护网站的QPS日峰值，左侧即显示出当前配置下WAF实例的价格，单位：元/天。

说明:
预估价格仅作为计费参考，实际价格以账单为准。



7.2 查看产品信息

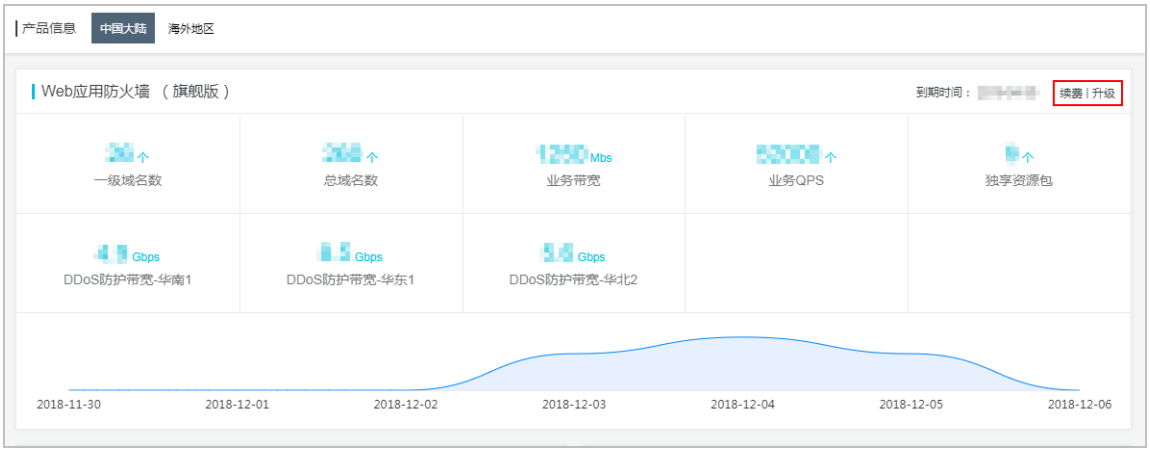
产品信息页向您展示当前Web应用防火墙（WAF）实例的资源详情、WAF的防护规则更新通知、功能更新通知和WAF的回源IP段。

操作步骤

1. **登录云盾Web应用防火墙控制台。**
2. **在页面上方选择地域：中国大陆、海外地区。**

3. 前往设置 > 产品信息页，查看以下信息。

- WAF资源详情
  - 当前WAF版本及到期时间（支持执行续费和升级操作）
  - 支持接入防护的一级域名数
  - 支持接入防护的总域名数
  - 所有接入业务的最大业务带宽
  - 所有接入业务的最大业务QPS
  - 已购买的独享资源包数量
  - 额外获得的DDoS防护带宽（根据业务区域分布）
  - 最近7日内的业务QPS曲线图



- 规则更新通知

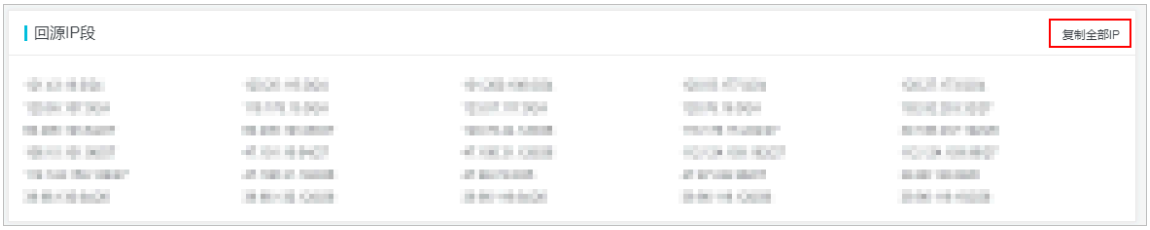
  展示WAF内置防护规则的最新更新记录，单击记录可查看详情。

- **功能更新公告**

  展示WAF功能调整的最新记录，单击记录可查看详情。

- **回源IP段**

  展示WAF的所有回源IP地址，单击复制全部IP可直接复制。



7.3 自定义规则组

通过自定义规则组，您可以查看并自由组合Web应用防火墙（WAF）的内置防护规则，生成有针对性的防护策略（规则组），并在相应防护功能中应用该策略。

说明:

该功能仅支持企业版或旗舰版的包年包月WAF实例（对于海外地域的WAF实例，仅支持旗舰版）。目前，仅支持自定义Web应用攻击防护的防护策略。关于Web应用攻击防护的默认策略，请参考Web应用攻击防护。

查看内置规则集

在使用自定义规则组前，建议您查看并熟悉Web应用防火墙的内置防护规则集。

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆或海外地区。
3. 在设置 > 自定义规则组页面，选择要操作的防护功能页签（目前仅支持Web攻击防护）。
4. 单击内置规则集页签，查看WAF所有内置的Web攻击防护规则。每条规则包含以下信息：
   - 规则：该规则的名称。
   - 规则ID：该规则的唯一标识ID。
   - 危险等级：该规则防御的Web攻击的危险等级，包括高危、中危、低危。
   - 应用类型：该规则防护的Web应用类型，包括通用、Wordpress、Discuz、Tomcat、phpMyAdmin等。
   - 防护类型：该规则防御的Web攻击类型，包括SQL注入、跨站脚本、代码执行、CRLF、本地文件包含、远程文件包含、webshell、CSRF、其它。

     说明:

     关于具体的Web攻击的含义，请参考常见通用漏洞。
   - 规则描述：该规则防御的Web攻击的信息、要检测的命令，以及在哪些选择器上执行检测等。

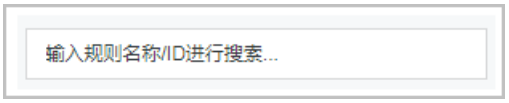
     说明:

将鼠标悬停在一个规则描述上可以看到完整的描述信息。

5. （可选）使用筛选和搜索功能定位到指定的规则。

   - 支持通过防护类型、应用类型、危险等级筛选规则。

   - 支持通过规则名称/ID搜索规则。



添加自定义规则组

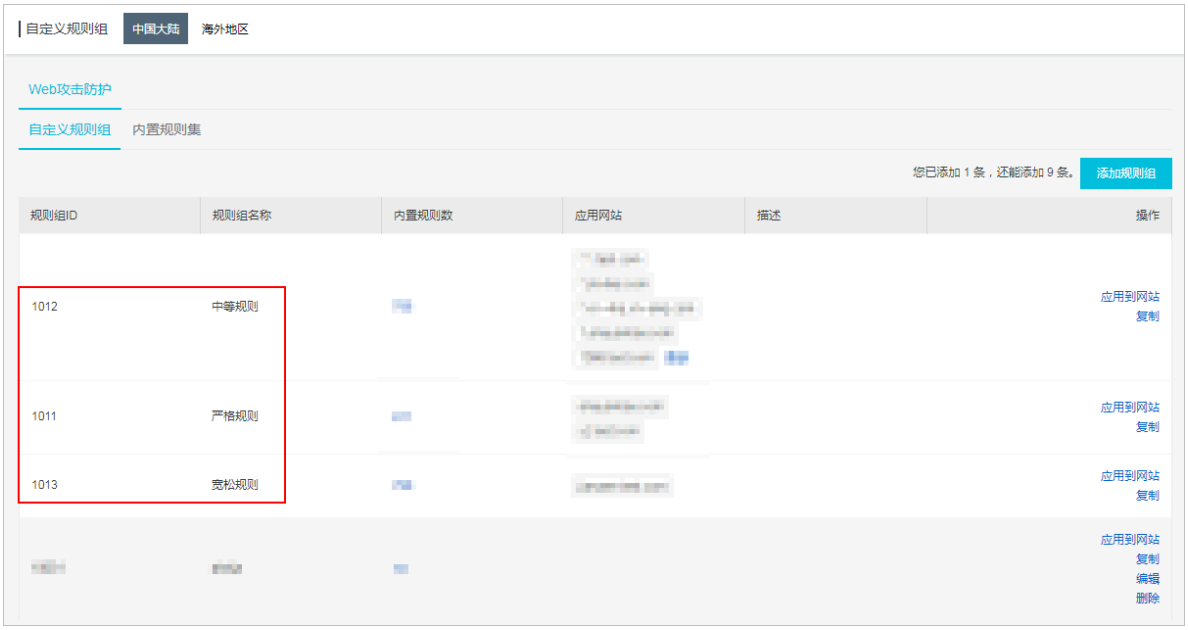
您可以为指定防护功能添加自定义防护规则组。添加自定义规则组时，您为该规则组自由搭配WAF支持的内置防护规则，形成有针对性的防护策略。

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆或海外地区。

3. 在设置 > 自定义规则组页面，选择要添加自定义规则组的防护功能页签（目前仅支持Web攻击防护）。

   自定义规则组页签下罗列了所有Web攻击防护规则组，其中规则组ID 1012、1011、1013为默认的Web攻击防护策略。



4. 新建一个规则组，或者复制已有规则组生成一个新的规则组。

   说明:

您最多可以添加10条自定义Web攻击防护规则组。

- 新建规则组

  a. 单击添加规则组。

  b. 在添加规则组页面，完成以下配置。

  - 规则组名称：必填，该名称会显示在防护策略配置下拉框中。建议您使用有明确含义的名称。
  - 规则描述：选填，添加关于该规则的说明。
  - 规则：从左侧所有Web攻击防护规则集中选择要添加到右侧该规则组中的规则。

    关于规则信息的含义，请参考查看内置规则集步骤4。您也可以使用筛选和搜索功能定位到指定的规则，具体请参考查看内置规则集步骤5。

  c. 单击确定，完成规则组添加。

  自定义规则组中出现新添加的规则组，系统已为其分配唯一的规则组ID。

- 复制已有规则组

  a. 定位到要复制的规则组，单击其操作列下的复制。

  b. 在添加规则组页面，重新设置一个规则组名称，并确认规则组信息（不支持调整规则组内的规则）。

  c. 单击确认，完成复制添加。

  自定义规则组中出现复制添加的规则组，系统已为其分配唯一的规则组ID。您可以参照编辑自定义规则组，进一步调整规则组内的规则。

应用自定义规则组

已添加自定义规则组后，您可以在具体网站的防护配置中应用/解除应用自定义规则组，或者在自定义规则组页面批量对网站应用自定义规则组。

操作步骤

以Web攻击防护为例，参照以下步骤，在网站配置中应用/解除应用自定义规则组：

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆或海外地区。
3. 在管理 > 网站配置页面，选择要操作的域名，并单击其操作列下的防护配置。
4. 在Web应用攻击防护下，开启防护。

5. 打开防护规则策略下拉框，根据规则名称选择新添加的自定义规则（本示例中为custom）。

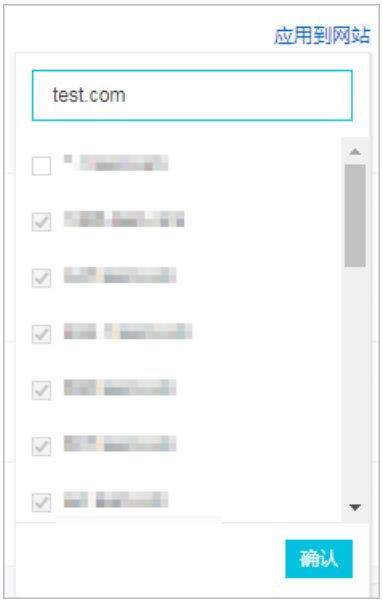
   如果您希望解除应用自定义规则组，只需在防护规则策略下拉框中选择一个默认策略（宽松规则、中等规则、严格规则）。

以Web攻击防护为例，参照以下步骤，批量应用自定义规则组：

说明:
如果需要解除应用自定义规则组，建议您到具体网站的防护配置页面进行操作。

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆或海外地区。
3. 在设置 > 自定义规则组页面，选择要操作的防护功能页签（目前仅支持Web攻击防护）。
4. 在自定义规则组页签下，选择要操作的自定义规则组，单击其操作列下的应用到网站。
5. 勾选需要应用该规则组的网站，单击确认，完成配置。

   支持搜索指定域名。



编辑自定义规则组

已添加自定义规则组后，您可以调整其包含的规则以及规则组名称和描述信息。默认规则组不支持编辑。

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆或海外地区。
3. 在设置 > 自定义规则组页面，选择要操作的防护功能页签（目前仅支持Web攻击防护）。
4. 选择要操作的规则组，单击其操作列下的编辑。
5. 在编辑规则组页面，调整规则配置信息。具体请参考新建规则组。
6. 单击确认，完成编辑。

删除自定义规则组

对于不再需要的自定义规则组，您可以将其删除。删除自定义规则组前，应确保该规则组未被应用到网站上。默认规则不支持删除。

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆或海外地区。
3. 在设置 > 自定义规则组页面，选择要操作的防护功能页签（目前仅支持Web攻击防护）。
4. 选择要删除的规则组，单击其操作列下的删除。
5. 在提示对话框中，单击确认，完成删除。

> 说明:
> 如果该规则组被应用到网站上，您必须先解除应用，才能删除该规则组。具体操作请参考应用自定义规则组。

7.4 配置WAF告警

WAF可以通过短信或邮件向您推送安全事件和系统告警。

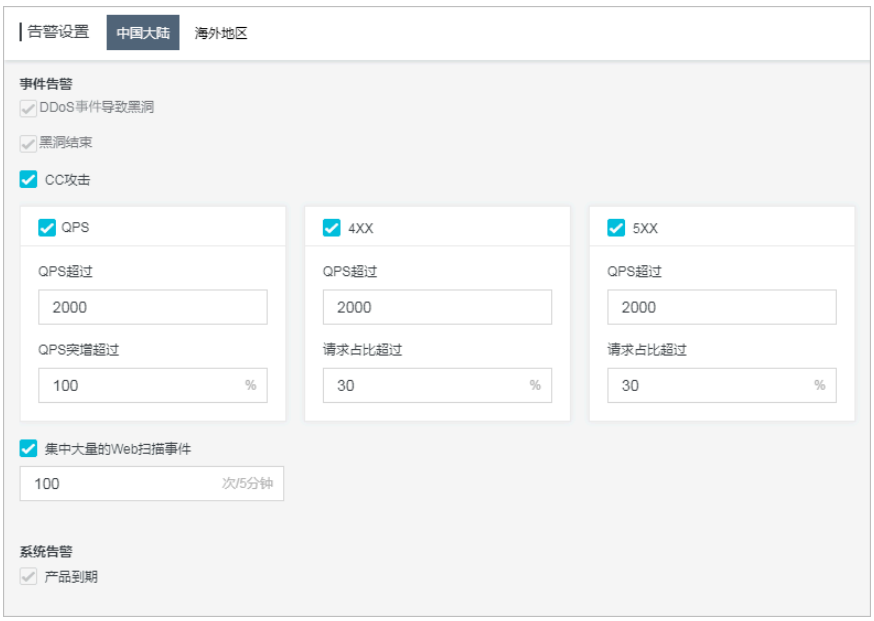
背景信息

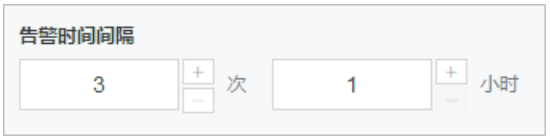
通过配置告警策略，您可以设置告警触发方式、告警周期、以及告警信息接收方式。

操作步骤

1. 登录云盾Web应用防火墙控制台。
2. 在页面上方选择地域：中国大陆或海外地区。

3. 前往设置 > 告警设置页面，完成以下告警配置。

配置项	描述
告警触发方式	指定由哪些事件告警和系统告警触发告警。 说明: 默认告警不可取消，且不支持自定义告警方式和告警周期。 · 事件告警 - DDoS事件导致黑洞（默认） - 黑洞结束（默认） - CC攻击 必须指定CC攻击判断阈值，支持以下三种方式： ■ QPS值（0至10,000,000间整数）和QPS突增百分比（0至1,000间整数） ■ 4xx页面的QPS值（0至10,000,000间整数）和请求占比（0至1,000间整数） ■ 5xx页面的QPS值（0至10,000,000间整数）和请求占比（0至1,000间整数） - 集中大量的Web扫描事件 必须指定Web扫描次数阈值，即多少次/5分钟。 · 系统告警：产品到期（默认） 

配置项	描述
告警方式	指定通过短信/邮件方式告警，并添加收信号码和邮箱地址。 说明: 最多支持添加3个收信号码和3个邮箱地址。 
告警时间间隔	指定每xx（0至24）小时告警xx（0至10）次。 

4. 单击保存设置。

7.5 关闭WAF

如果您决定不再继续使用按量计费模式的WAF实例，您可以关闭WAF，确保不再产生任何费用。

包年包月模式的WAF实例到期后，您也可以通过关闭WAF来释放该实例。

背景信息

在满足以下条件时，您可以选择变更WAF的计费方式。

- 从按量付费模式变更为包年包月模式：必须先关闭当前按量付费模式的WAF实例。
- 从包年包月模式变更为按量付费模式：必须先释放已到期的包年包月模式的WAF实例。

只有在满足以下条件时，您才能够关闭或释放WAF实例。

- 包年包月模式： WAF实例已经到期。
- 按量付费模式： 近两日内仅有少量或没有请求到达WAF实例。

说明:

关闭WAF实例前，请确认当前配置的网站域名DNS已解析回源站。关闭或释放WAF实例后，所有网站域名配置信息将被清空。如果仍有请求到达WAF实例，其将无法被正常转发，导致网站无法正常访问。

操作步骤

1. 登录云盾Web应用防火墙控制台，选择地域。
2. 在页面右上角，单击关闭实例。

   说明:
   包年包月模式的WAF只有在实例到期后，才会出现该按钮。

3. 确认当前配置的网站域名解析已切换回到源站，单击确定，即可关闭WAF。

8 日志实时查询分析

8.1 WAF日志实时分析简介

阿里云Web应用防火墙（WAF）与日志服务打通，对外开放Web访问与攻击日志，提供WAF日志实时分析服务。

WAF日志实时分析可以近实时地收集并存储网站访问日志，并基于日志服务，输出查询分析、报表、报警、下游计算对接与投递等能力，帮助您专注于分析，远离琐碎的查询和整理工作。

通过以下视频介绍，快速学习了解WAF日志实时分析的功能和操作。

适用用户

- 对云上资产的主机、网络以及安全日志有存储合规需求的大型企业与机构，如金融公司、政府类机构等。
- 拥有自己的安全运营中心（SOC），需要收集安全告警等日志进行中央运营管理的企业，如大型地产、电商、金融公司、政府类机构等。
- 拥有较强技术能力，需要基于云上资产的日志进行深度分析，对告警进行自动化处理的企业，如IT、游戏、金融公司等。
- 对云上业务安全事件有溯源需求，需要定期输出安全周报、月报和年报，或者拥有三级以上等保合规需求的所有用户。

功能优势

WAF日志实时查询分析服务具有以下功能优势：

- 等保合规：存储网站六个月以上的访问日志，助力网站符合等保合规要求。

- 配置灵活：轻松配置即可实现Web访问与攻击日志的实时采集。同时，支持自定义日志存储的时长和容量，自由选择日志采集的网站。您还可以根据自己的业务需求修改或者重新自定义符合自己业务或安全需求的报表模板，帮助您快速感知网站业务和安全状态。
- 实时分析：依托日志服务产品，提供实时日志分析能力、开箱即用的报表中心与交互挖掘支持，从传统几十分钟级别到秒级别，让您对网站业务的各种Web攻击状况以及客户访问细节了如指掌。
- 实时告警：支持基于特定指标定制准实时的监测与告警，确保在关键业务发生异常时能第一时间响应。
- 生态体系：支持对接其他生态如实时计算、云存储、可视化等方案，进一步挖掘数据价值。

使用说明

要使用WAF日志实时分析，必须满足以下前提条件：

- 开通阿里云日志服务。
- 开通阿里云Web应用防火墙（中国大陆任意版本或者海外地区企业版和旗舰版），并购买日志分析模块。

> 说明:
> 按量付费模式不支持该功能。

WAF所存储的日志库属于专属日志库，有如下特性：

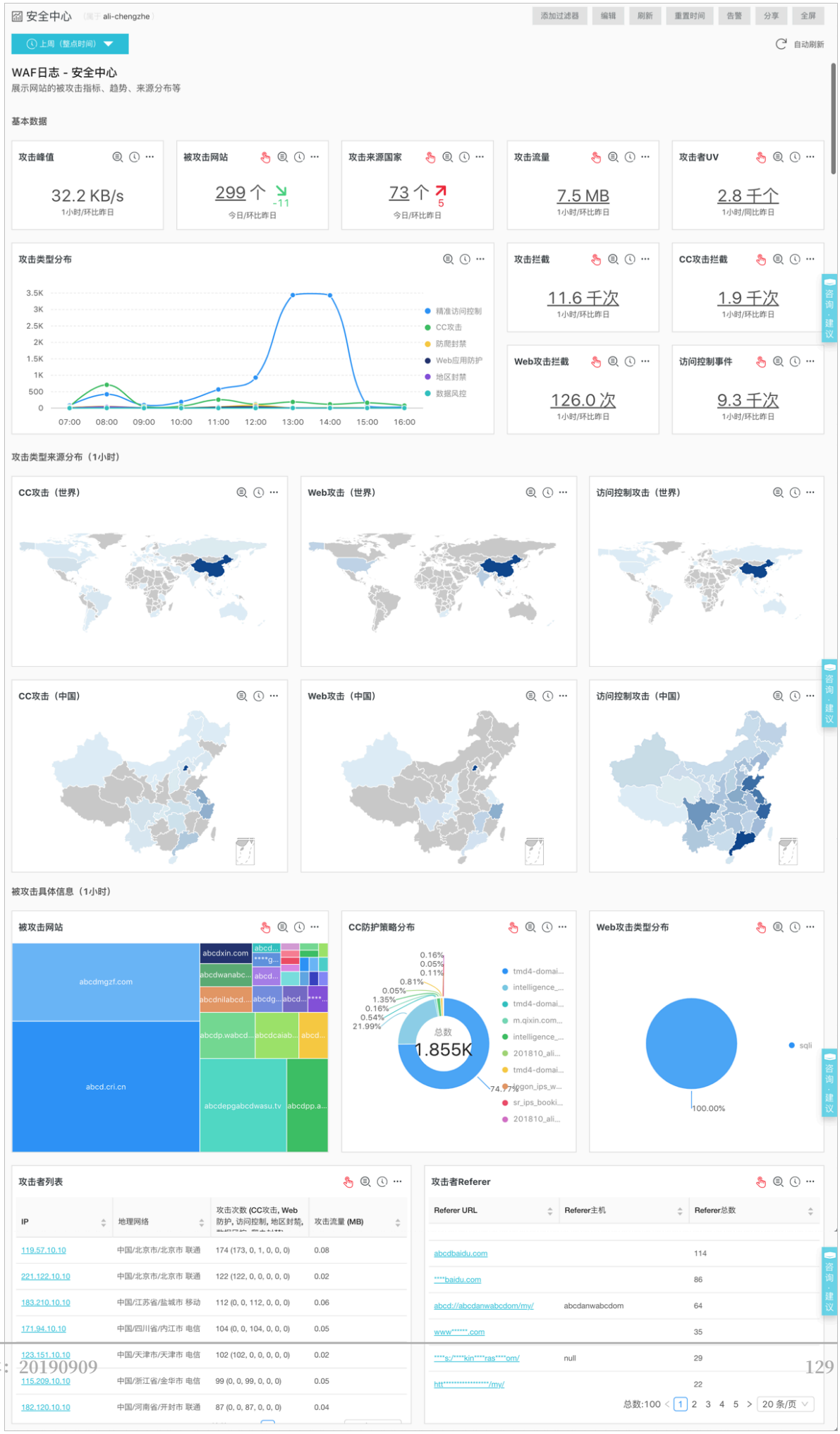
- 用户无法通过API/SDK等方式写入数据，或者修改日志库的属性（例如存储周期等）。

> 说明:
> 支持其他日志库功能（例如查询、统计、报警、流式消费等），且与一般日志库无差别。

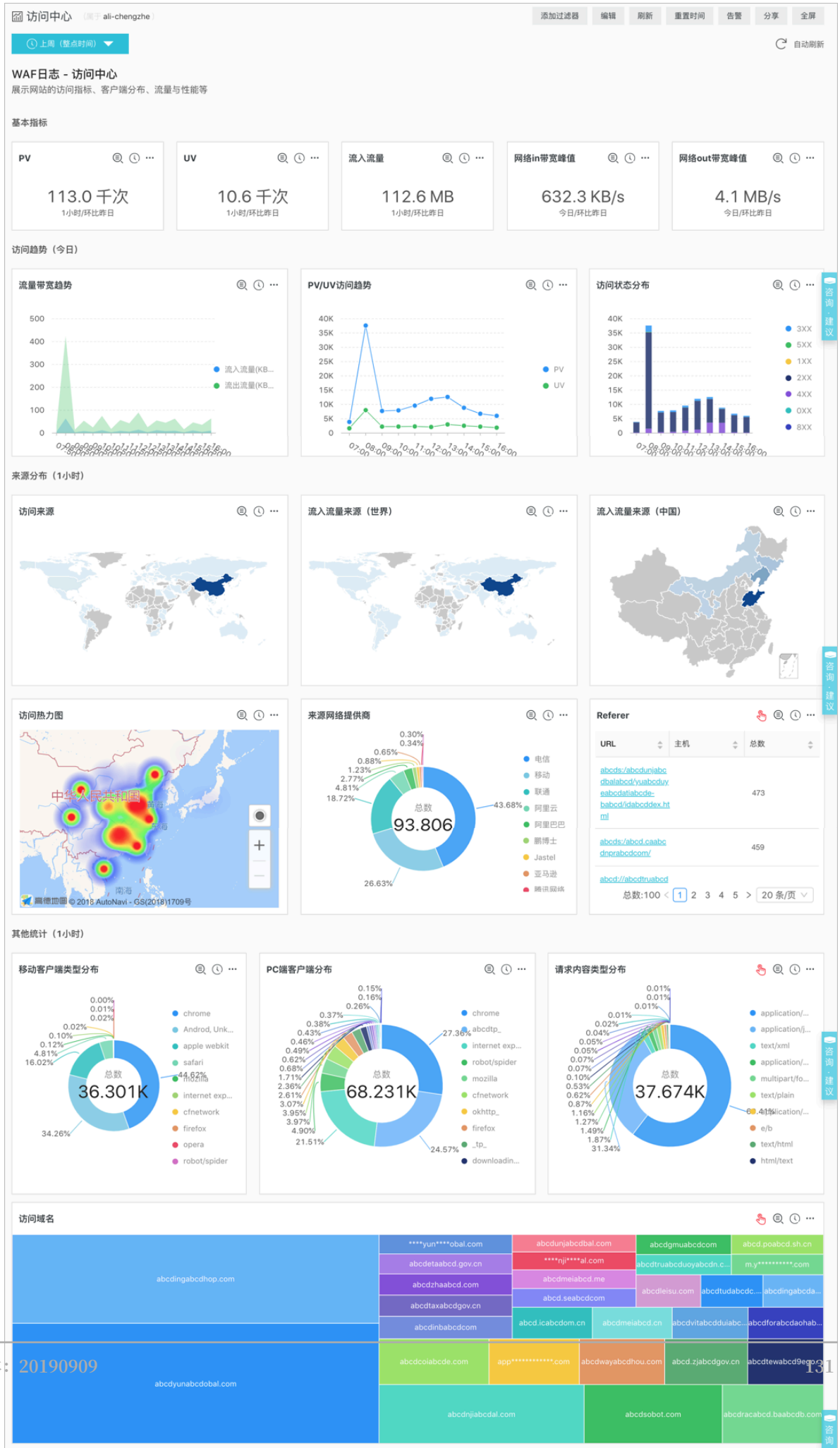
- 日志服务不对专属日志库计费，但日志服务本身需处于可用状态（不超期欠费）。
- 内置报表样式可能会发生更新和升级。

应用场景

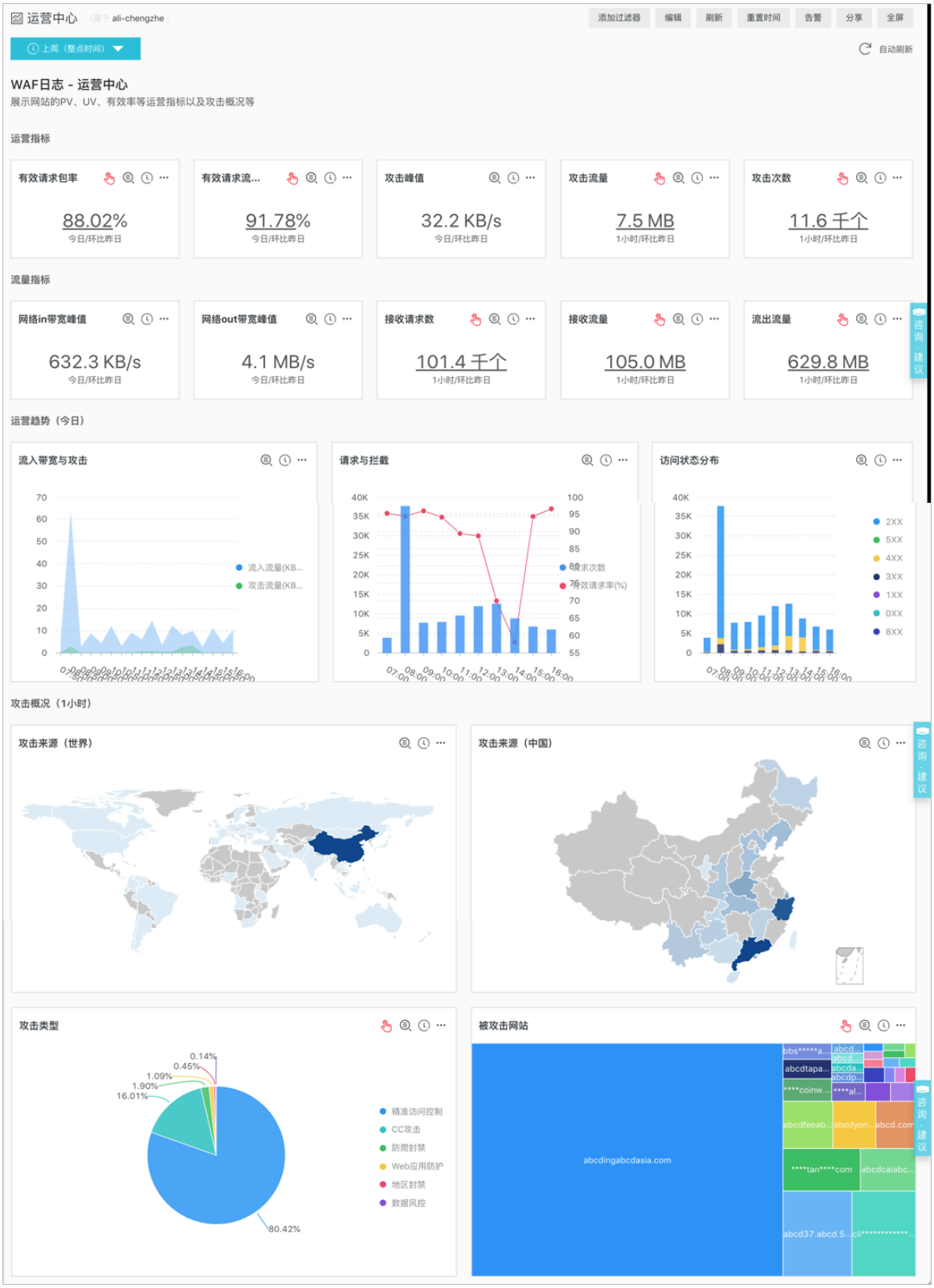
- **追踪Web攻击日志，溯源安全威胁。**


安全中心
添加过滤器
编辑
刷新
重置时间
告警
分享
全屏
上周（整点时间）
自动刷新
WAF日志 - 安全中心
展示网站的被攻击指标、趋势、来源分布等
基本数据
攻击峰值
32.2 KB/s
1小时/环比昨日
被攻击网站
299 个
-11
今日/环比昨日
攻击来源国家
73 个
5
今日/环比昨日
攻击流量
7.5 MB
1小时/环比昨日
攻击者UV
2.8 千个
1小时/同比昨日
攻击类型分布
精准访问控制
CC攻击
防爬封禁
Web应用防护
地区封禁
数据风控
攻击拦截
11.6 千次
1小时/环比昨日
CC攻击拦截
1.9 千次
1小时/环比昨日
Web攻击拦截
126.0 次
1小时/环比昨日
访问控制事件
9.3 千次
1小时/环比昨日
攻击类型来源分布（1小时）
CC攻击（世界）
Web攻击（世界）
访问控制攻击（世界）
CC攻击（中国）
Web攻击（中国）
访问控制攻击（中国）
被攻击具体信息（1小时）
被攻击网站
abcdmgzf.com
abcdxin.com
abcd.cri.cn
abcdepgabcdwasu.tv
abcdpp.a...
CC防护策略分布
总数
1.855K
0.16%
0.05%
0.11%
0.81%
0.05%
1.35%
0.16%
0.54%
21.99%
74.77%
Web攻击类型分布
sqli
100.00%
攻击者列表
IP
地理网络
攻击流量 (MB)
119.57.10.10
221.122.10.10
183.210.10.10
171.94.10.10
123.151.10.10
115.209.10.10
182.120.10.10
攻击者Referer
Referer URL
Referer主机
Referer总数
abcdbaidu.com
114
****baidu.com
86
abcd://abcdanwabcdom/my/
abcdanwabcdom
64
www******.com
35
****s:/****kin****ras****om/
null
29
htt**********/my/
22
总数:100
20 条/页
咨询·建议

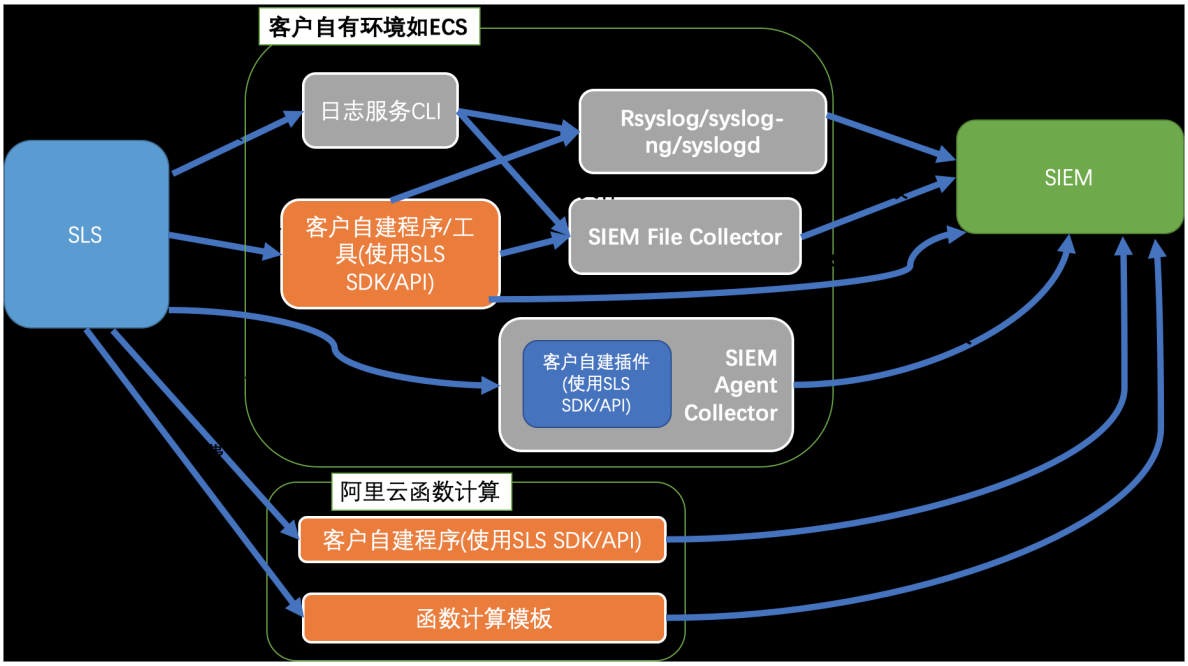
- **实时查看Web请求活动，洞察状态与趋势。**


访问中心
添加过滤器
编辑
刷新
重置时间
告警
分享
全屏
上周（整点时间）
自动刷新
WAF日志 - 访问中心
展示网站的访问指标、客户端分布、流量与性能等
基本指标
PV
113.0 千次
1小时/环比昨日
UV
10.6 千次
1小时/环比昨日
流入流量
112.6 MB
1小时/环比昨日
网络in带宽峰值
632.3 KB/s
今日/环比昨日
网络out带宽峰值
4.1 MB/s
今日/环比昨日
访问趋势（今日）
流量带宽趋势
PV/UV访问趋势
访问状态分布
来源分布（1小时）
访问来源
流入流量来源（世界）
流入流量来源（中国）
访问热力图
来源网络提供商
Referer
URL
主机
总数
其他统计（1小时）
移动客户端类型分布
PC端客户端分布
请求内容类型分布
访问域名

- **快速了解安全运营效率，及时反馈处理。**



· 输出安全网络日志到自建数据与计算中心。



8.2 计费方式

WAF日志服务根据您选择的日志存储时长和日志存储容量进行计费。

WAF日志服务采用预付费（包年包月）方式。

> 说明:
> WAF日志服务目前仅支持Web应用防火墙包年包月实例开通使用。

您在Web应用防火墙购买页面中，选择开通日志服务，并根据实际需要选择日志存储时长和日志存储容量的规格，系统将自动根据您选定的日志存储规格和WAF实例的购买时长计算费用。

日志存储规格

WAF日志服务各日志存储规格的详细定价如下表所示：

日志存储时长	日志存储容量	推荐场景	中国大陆地域实例		海外地区实例	
			包月费用	包年费用	包月费用	包年费用
180天	3TB	适合日均QPS不高于80的业务场景	1,500	18,000	3,000	36,000
	5TB	适合日均QPS不高于120的业务场景	2,500	30,000	5,000	60,000
	10TB	适合日均QPS不高于260的业务场景	5,000	60,000	10,000	120,000

日志存储时长	日志存储容量	推荐场景	中国大陆地域实例		海外地区实例	
			包月费用	包年费用	包月费用	包年费用
	20TB	适合日均QPS不高于500的业务场景	10,000	120,000	20,000	240,000
	50TB	适合日均QPS不高于1,200的业务场景	25,000	300,000	50,000	600,000
	100TB	适合日均QPS不高于2,600的业务场景	50,000	600,000	100,000	1,200,000
360天	5TB	适合日均QPS不高于60的业务场景	2,500	30,000	5,000	60,000
	10TB	适合日均QPS不高于120的业务场景	5,000	60,000	10,000	120,000
	20TB	适合日均QPS不高于260的业务场景	10,000	120,000	20,000	240,000
	50TB	适合日均QPS不高于600的业务场景	25,000	300,000	50,000	600,000
	100TB	适合日均QPS不高于1,200的业务场景	50,000	600,000	100,000	1,200,000

日志存储容量满额说明

如果您已购买的日志存储容量已经满额，系统将自动提醒您升级容量。您可以随时通过升级日志存储容量规格的方式进行扩容。

注意:
如果日志存储容量已满，且您未及时升级容量，WAF将停止向日志服务的专属日志库写入新的日志数据。日志库中已存储的日志数据将保留，直到该日志数据超出所选择的日志存储时长。或者，您所购买的WAF日志服务到期7天后未续费，日志库中的所有日志数据将自动释放。

购买时长

WAF日志服务的购买时长与您购买的WAF包年包月实例绑定。

- 新购：您在新购WAF包年包月实例时，系统将根据您选择的实例购买时长计算日志服务的费用。

- 升级：您通过升级已购买的WAF包年包月实例开通日志服务时，系统将根据您现有的WAF实例的剩余时长（精确到分钟级别）计算日志服务的费用。

服务到期说明

当您购买的WAF实例服务到期，WAF日志服务将同时到期。

- 服务到期后，WAF将停止向日志服务的专属日志库写入日志数据。
- 服务到期后，WAF日志服务中的日志数据将为您保留7天。如果7天内您完成续费则可以继续使用WAF日志服务功能；如果未能及时完成续费，所有已存储的WAF日志将被清空。

8.3 配置WAF日志服务

购买Web应用防火墙（WAF）服务后，如果您的网站业务需要详细的实时日志查询和分析服务，您可以在控制台的应用管理中开通日志实时查询分析服务。

背景信息

WAF日志服务通过日志服务（SLS）的功能实时采集已接入WAF防护的网站业务的各类日志，并对采集到的日志数据进行实时检索与分析，以丰富的仪表盘形式展示查询结果。WAF日志服务完全满足等保合规要求和您网站业务防护和运营需求，您可以在开通WAF日志服务时根据实际需要，选择存储时长和存储容量大小。

说明:

WAF日志服务目前仅对Web应用防火墙包年包月实例开通，包括高级版、企业版、旗舰版。

操作步骤

1. 登录Web应用防火墙管理控制台。
2. 定位到市场管理 > 应用管理页面，选择您的WAF实例所在地域。
3. 单击日志实时查询分析服务区域中的升级。

4. 在Web应用防火墙购买页面，勾选日志服务，根据您的业务需要选择日志存储时长和存储容量，单击去支付并完成支付。

> **说明:**
> 关于WAF日志服务收费标准，请参见WAF日志服务计费方式。

5. 回到Web应用防火墙的市场管理 > 应用管理页面，在日志实时查询分析服务区域单击授权。
6. 单击同意授权，授权WAF将日志存储至您的专属日志库中。

至此，您已完成WAF日志服务的开通与授权。

7. 回到Web应用防火墙的市场管理 > 应用管理页面，在日志实时查询分析服务区域单击配置。
8. 在日志服务页面，选择已接入WAF防护的网站域名，单击域名右侧的状态开关，为该网站域名开启WAF日志服务。

预期结果

日志服务将实时采集WAF记录到的该网站域名的所有日志，并根据采集到的日志数据进行实时检索与分析。

8.4 日志采集

您可以在Web应用防火墙管理控制台为指定网站域名开启WAF日志采集功能。

前提条件

- 已购买开通Web应用防火墙，并且已将您的网站域名接入WAF进行防护。

- 已开通日志服务产品。

背景信息

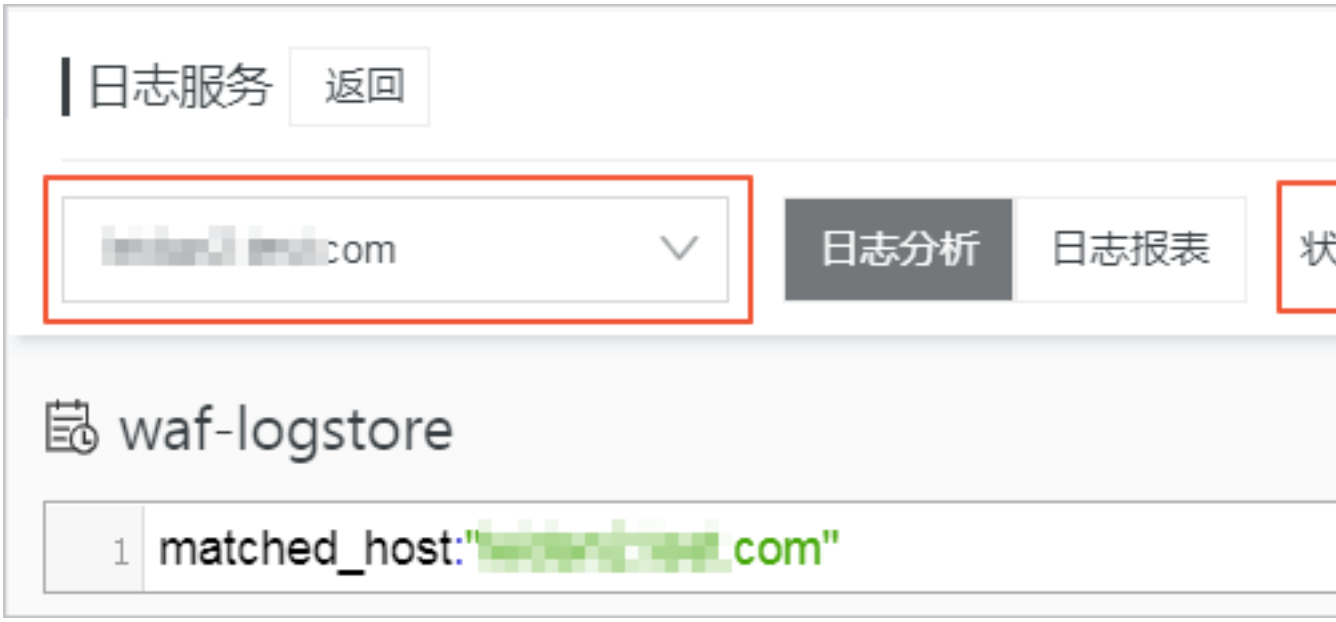
日志服务支持实时采集阿里云Web应用防火墙已防护的网站访问日志、攻击防护日志，并支持对采集到的日志数据进行实时检索与分析，以仪表盘形式展示查询结果。您可以通过日志对网站的访问和攻击行为进行即时分析研究、协助安全管理人员制定防护策略。

操作步骤

1. 登录Web应用防火墙管理控制台。
2. 定位到市场管理 > 应用管理，单击日志服务实时查询分析。

说明:
如果您是第一次配置WAF日志采集功能，单击授权，根据页面提示完成授权操作，授权WAF将所有记录的日志分发到您专属的Logstore中。

3. 选择您需要开启WAF日志采集功能的网站域名，单击右侧的状态开启日志采集功能。



至此，您已成功为该网站域名开启WAF日志采集功能。日志服务会在您的账号下自动创建一个专属日志库和专属Logstore，WAF自动将所有开启日志采集功能的网站域名的日志实时导入该专属日志库中。专属日志库和专属Logstore等默认配置如默认配置所示。

表 8-1: 默认配置

默认配置项	配置内容
Project	默认为您创建Project。Project名称由您的WAF实例的地域决定。 · 大陆地域的WAF实例：`waf-project-#####ID-cn-hangzhou` · 其他地域的WAF实例：`waf-project-#####ID-ap-southeast-1`
Logstore	默认为您创建Logstore，`waf-logstore`。 WAF日志采集功能产生的所有日志都将保存到该Logstore中。
地域	· WAF实例地域为中国大陆地区的，默认Project保存在杭州地域。 · WAF实例地域为其他地区的，默认Project保存在新加坡地域。
Shard	默认为您创建2个Shard，并开启自动分裂Shard 功能。

默认配置项	配置内容
仪表盘	默认为您创建三个仪表盘，分别为： · 访问中心 · 运营中心 · 安全中心 关于仪表盘的更多信息，请参见WAF日志服务-日志报表。

限制与说明

· 专属日志库不支持写入其他数据。

WAF日志将被存放在专属日志库中，该日志库不支持通过API、SDK等任何方式写入其他数据。

说明：
专属日志库在查询、统计、报警、流式消费等功能上均无特殊限制。

· 不支持修改专属日志库的存储周期等基本设置。
· 专属日志库不另行收费。

日志服务对专属日志库不进行任何收费，但您账号中的日志服务产品需处于正常使用状态。

说明：
当您的日志服务产品出现欠费时，WAF日志采集功能将暂停工作，及时补缴欠款后采集功能自动恢复。

· 请勿随意删除或修改日志服务为您创建的默认Project、Logstore、索引和仪表盘设置。日志服务将不定期更新、升级WAF日志查询与分析功能，专属日志库中的索引与默认报表也会自动更新。
· 如果您的子账号需要使用WAF日志查询分析功能，需要为其授予日志服务相关权限。具体操作方式，请参见为子账号授予日志服务日志查询分析功能权限。

8.5 日志分析

Web应用防火墙管理控制台的日志服务实时查询分析功能页面集成日志服务的日志分析和日志报表功能。您为指定网站域名开通WAF日志采集功能后，即可在日志服务实时查询分析功能页面对采集到的日志数据进行实时查询与分析、查看或编辑仪表盘、设置监控告警等操作。

操作步骤

1. 登录Web应用防火墙管理控制台，定位到市场管理 > 应用管理页面。

2. 单击日志服务查询分析区域，打开日志服务页面。
3. 选择网站域名，确认右侧的状态开关为开启。
4. 单击日志分析。

   当前页面集成日志服务产品的查询分析页面，系统将自动为您输入查询语句。例如，`matched_host: "www.aliyun.com"`，查看您选定网站域名的所有日志数据。

5. 输入您的查询分析语句，选择日志时间范围后单击查询/分析。

更多操作说明

在日志分析页面，您还可以对查询到的日志数据进行以下操作：

- 自定义查询与分析

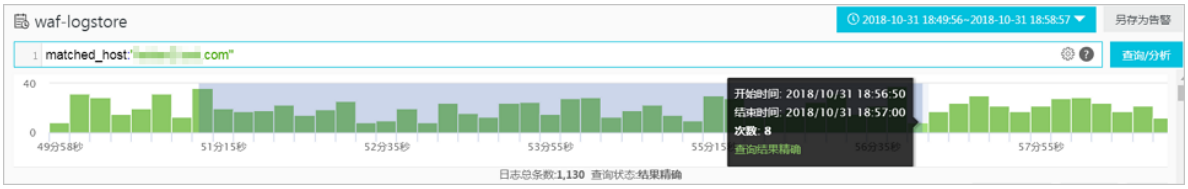
  日志服务定义了一系列查询语法和分析语法，支持多种复杂场景下的日志查询。更多详细介绍，参考自定义查询与分析。

- 查看日志的时间分布

  搜索框下方展示了符合查询时间和查询语句的日志的时间分布情况，以时间为横轴、数量为纵轴的柱状图形式展示。并显示查询到的日志总数。

说明：

您可以在柱状图上按住鼠标左键拖拽选择更小范围的时间区域，时间选择器将自动更新为选择的时间范围，并展示该所选择时间范围内的结果。

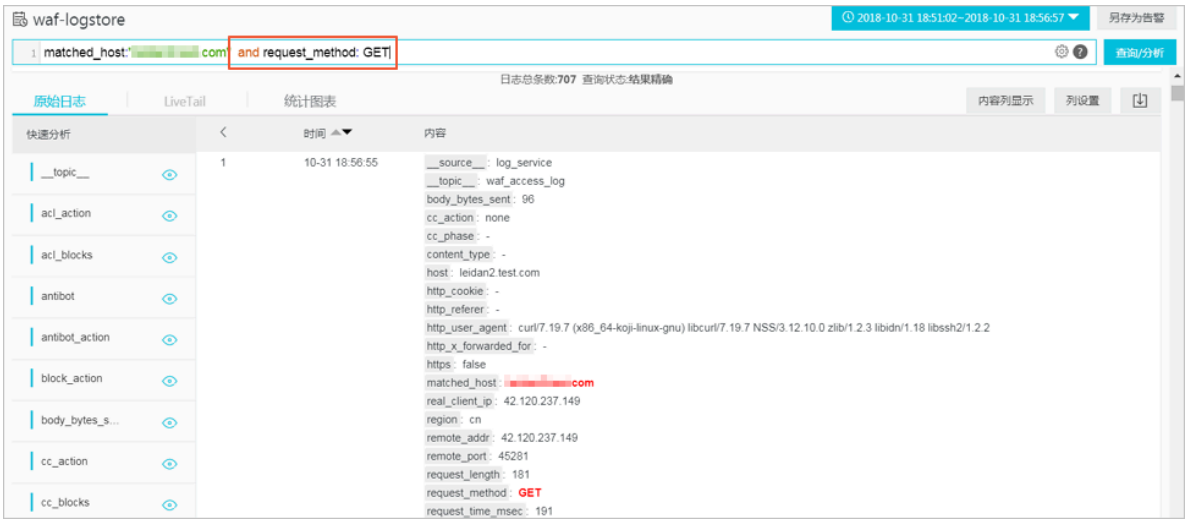


- 查看原始日志

在原始日志页签中，以分页的形式展示每一条日志的详细内容，包括时间、内容以及其中的各个字段。您可以单击内容列显示设置内容列中长字符的显示效果（整行或换行）、单击列设置选择特定的字段进行展示、或单击日志下载按钮将当前查询结果下载至本地。

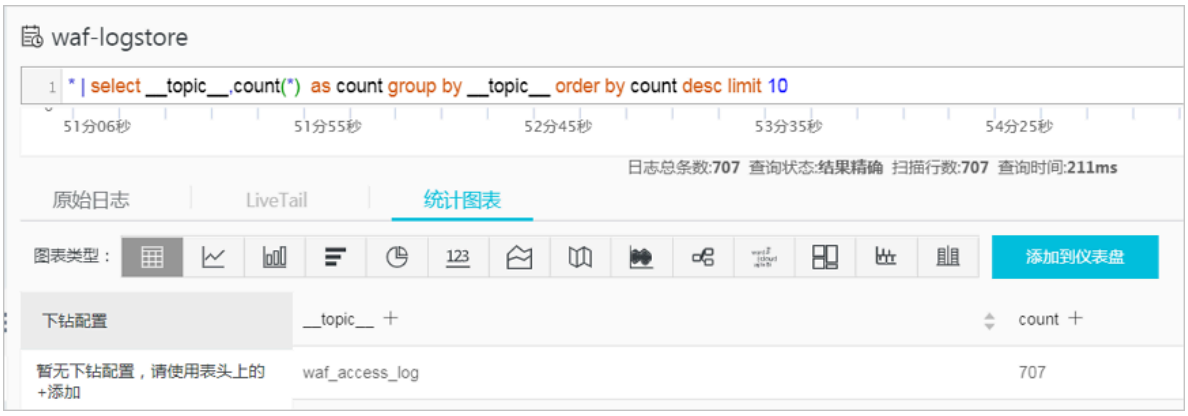
同时，在内容列中单击相应字段的值或分词，搜索框中将自动增加相应的搜索条件。例如，单击`request_method: GET`中的值`GET`，搜索框中将自动增加更新为以下查询语句，并展示相应的查询结果：

原来的搜索语句 `and request_method: GET`



- 查看分析图表

  日志服务支持以图表形式展示分析结果，您可以在统计图表页面根据需要选择不同的图表类型。更多详细介绍，参考分析图表。



- 快速分析

  原始日志页签中的快速分析功能为您提供一键交互式查询体验，帮助您快速分析某一字段在一段时间内的分布情况，减少索引关键数据的时间成本。更多详细介绍，参考快速分析。

自定义查询分析

日志查询语句由查询语法（Search）和分析语法（Analytics）两个部分组成，中间通过|进行分割：

```
$Search | $Analytics
```

类型	说明
查询（Search）	查询条件，由关键词、模糊、数值、区间范围和组合条件等产生。如果为空或*，则代表查询所有数据。
分析（Analytics）	对查询结果或全量数据进行计算和统计。

 说明：

查询和分析两部分均为可选。

- 当Search部分为空时，代表针对该时间段所有数据不进行任何过滤，直接对结果进行统计。
- 当Analysis部分为空时，代表只返回查询结果，不进行统计。

查询语法

日志服务查询语法支持全文查询和字段查询，查询框支持换行显示、语法高亮等功能。

- 全文查询

  无需指定字段，直接输入关键字进行全文查询。您可以用双引号（""）包裹关键字查询包含该完整关键字的日志，也可以用空格或and分割查询多个关键字。

  示例

  - 多关键字查询

    搜索包含所有www.aliyun.com和error的日志。

    www.aliyun.com error或者www.aliyun.com and error

  - 条件查询

    搜索所有包含www.aliyun.com，并且包含error或者404的日志。

    ```
    www.aliyun.com and (error or 404)
    ```

  - 前缀查询

    搜索所有包含www.aliyun.com，并且以failed_开头的日志。

    ```
    www.aliyun.com and failed_*
    ```

     说明:
    查询中只支持后缀添加*，但不支持以*作为前缀（如*_error）。

- 字段查询

  基于字段进行更精准的查询。

  字段查询支持数值类型字段的比较查询，格式为字段：值或字段 >= 值。同时，通过and、or等可进行组合查询，并支持与全文搜索组合使用。

   说明:

WAF日志服务中网站域名的访问、运营、攻击日志同样支持基于字段查询。关于日志中各个字段的含义、类型、格式等信息，查看WAF日志字段说明。

示例

- 查询多字段

  搜索所有被WAF拦截的针对www.aliyun.com网站域名的CC攻击的日志。

  ```
  matched_host: www.aliyun.com and cc_blocks: 1
  ```

  如果要搜索指定客户端1.2.3.4访问www.aliyun.com网站的所有404错误的访问日志，您可以设置以下查询条件。

  ```
  real_client_ip: 1.2.3.4 and matched_host: www.aliyun.com and
  status: 404
  ```

  说明:

  本示例中的matched_host、cc_blocks、real_client_ip和status字段都是WAF记录的日志字段。

- 查询数值字段

  搜索所有响应时间超过5秒的慢请求日志。

  ```
  request_time_msec > 5000
  ```

  同时，也支持区间查询。例如，查询响应时间大于5秒且小于等于10秒的日志。

  ```
  request_time_msec in (5000 10000]
  ```

  说明:

您也可以通过以下查询语句获得同样的查询结果：

```
request_time_msec > 5000 and request_time_msec <= 10000
```

- 查询字段是否存在

  查询指定字段是否存在：

  ■ 查询存在ua_browser字段的日志。

  ```
  ua_browser: *
  ```

  ■ 查询不存在ua_browser字段的日志。

  ```
  not ua_browser: *
  ```

关于日志服务支持的查询语法完整说明，参考索引与查询。

分析语法

您可以使用SQL/92语法对日志数据进行分析与统计。

关于日志服务支持的语法与函数说明，参考实时分析。

说明：

- 分析语句中可以省略SQL标准语法中的from 表格名语句，即from log语句。
- 日志数据默认返回前100条，您可以通过LIMIT语法修改返回范围。

查询分析示例

基于日志时间的查询分析

每一条WAF记录的日志都存在time字段，用于表示日志的时间，格式为年-月-日T时:分:秒+时区。例如，2018-05-31T20:11:58+08:00，其中时区为UTC+8区，即北京时间。

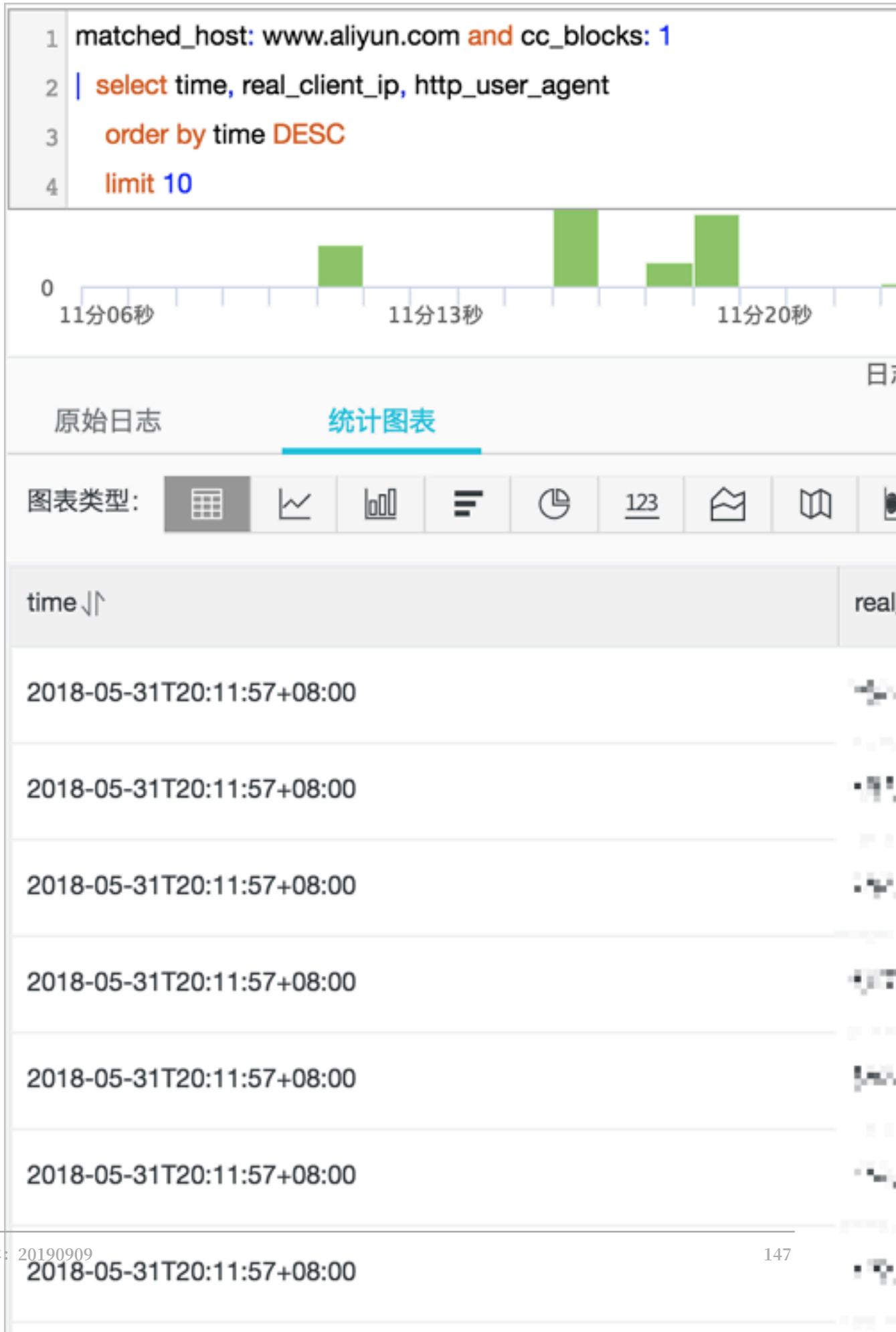
同时，每条日志都拥有一个内置字段，__time__。该字段也表示该条日志的时间，以便在统计时进行基于时间的计算，其格式为Unix时间戳，其本质是一个自从1970-1-1 0:0:0 UTC时间开始的累计经过的秒数。因此在实际使用时，经过可选的计算后，需要经过格式化才能进行展示。

- 选择并展示时间

  使用time字段展示日志的时间信息。例如，在特定时间范围内，查询被WAF拦截的针对www.aliyun.com网站域名的最近10条CC攻击日志，展示日志中的时间、来源IP以及访问客户端字段。

  ```
  matched_host: www.aliyun.com and cc_blocks: 1
  |  select time, real_client_ip, http_user_agent
      order by time desc
  ```

```
limit 10
```


1 matched_host: www.aliyun.com and cc_blocks: 1
2 | select time, real_client_ip, http_user_agent
3 order by time DESC
4 limit 10
0
11分06秒
11分13秒
11分20秒
原始日志
统计图表
图表类型:
123
time
2018-05-31T20:11:57+08:00
2018-05-31T20:11:57+08:00
2018-05-31T20:11:57+08:00
2018-05-31T20:11:57+08:00
2018-05-31T20:11:57+08:00
2018-05-31T20:11:57+08:00
2018-05-31T20:11:57+08:00

- 计算时间

使用__time__字段进行时间的计算。例如，查询遭受CC攻击后经过的天数。

```
matched_host: www.aliyun.com  and cc_blocks: 1
|  select time, round((to_unixtime(now()) - __time__)/86400, 1) as "
days_passed", real_client_ip, http_user_agent
      order by time desc
      limit 10
```

说明:

本示例中，使用round((to_unixtime(now()) - __time__)/86400, 1)计算遭受CC攻击后经过的天数。首先，用to_unixtime将now()获取到的当前时间转化为Unix时间戳；再将该时间与内置时间字段__time__相减，得到已经过的时间秒数；最后，将该值除以86400（即一天的总秒数），再使用函数round(data, 1)取整为小数点后1位数的值。最终，得到每条攻击日志产生的时间距离现在已经过的天数。

time	days_passed	real_client_ip	http_user_agent
2018-05-31T20:11:57+08:00	26.6	[illegible]	Mozilla/5.5 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
2018-05-31T20:11:57+08:00	26.6	[illegible]	Mozilla/5.5 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
2018-05-31T20:11:57+08:00	26.6	[illegible]	Mozilla/5.5 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
2018-05-31T20:11:57+08:00	26.6	[illegible]	Mozilla/5.5 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
2018-05-31T20:11:57+08:00	26.6	[illegible]	Mozilla/5.5 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)

- 基于特定时间分组统计

查询指定时间范围内，某网站域名每天遭受的CC攻击趋势。

```
matched_host: www.aliyun.com  and cc_blocks: 1
| select date_trunc('day', __time__) as dt, count(1) as PV
      group by dt
   order by dt
```

说明:

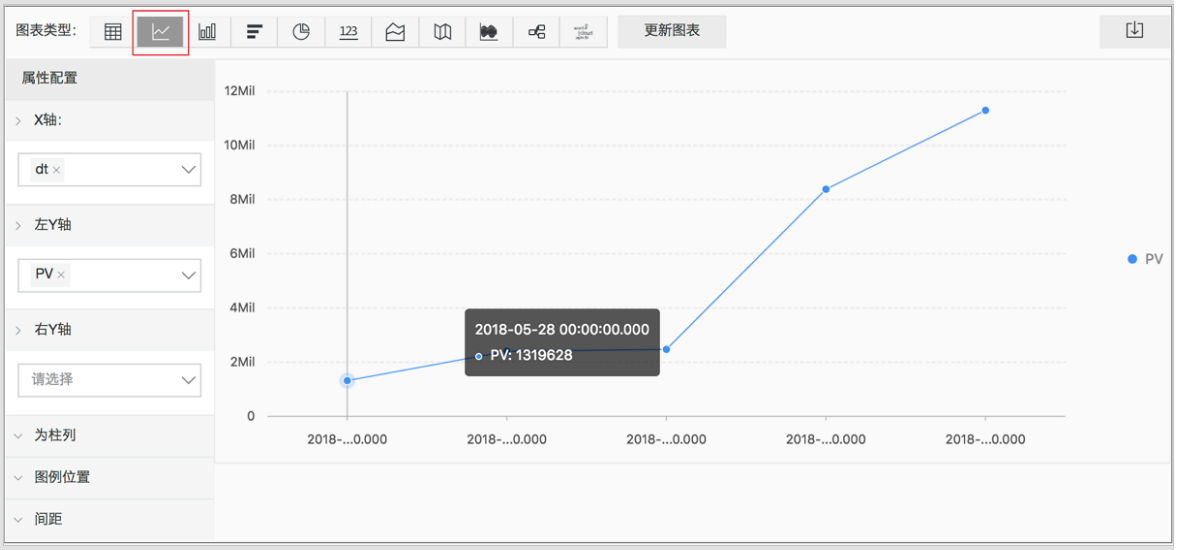
本示例中，使用内置时间字段__time__，供date_trunc('day', ..)函数进行时间按天对齐分组处理，将每条日志分组至其所属的天的分组中统计总次数（count(1)），并按照所分的时间组进行排序。其中，date_trunc函数中的第一个参数支持使用其他时间单位进行对

齐，包括second、minute、hour、week、month、year等。关于该函数的详细说明，参考日期和时间函数。

dt	PV
2018-05-28 00:00:00.000	1319628
2018-05-29 00:00:00.000	2402020
2018-05-30 00:00:00.000	2473332
2018-05-31 00:00:00.000	8381076
2018-06-01 00:00:00.000	11293642

说明:

您也可以使用折线图方式进行展示。



- 基于时间分组统计

如果需要分析更灵活的分组情况下的时间规律，例如指定网站每5分钟遭受CC攻击的趋势，可以通过进一步的数学计算实现。

```
matched_host: www.aliyun.com  and cc_blocks: 1
| select from_unixtime(__time__ - __time__% 300) as dt,
         count(1) as PV
      group by dt
   order by dt
   limit 1000
```

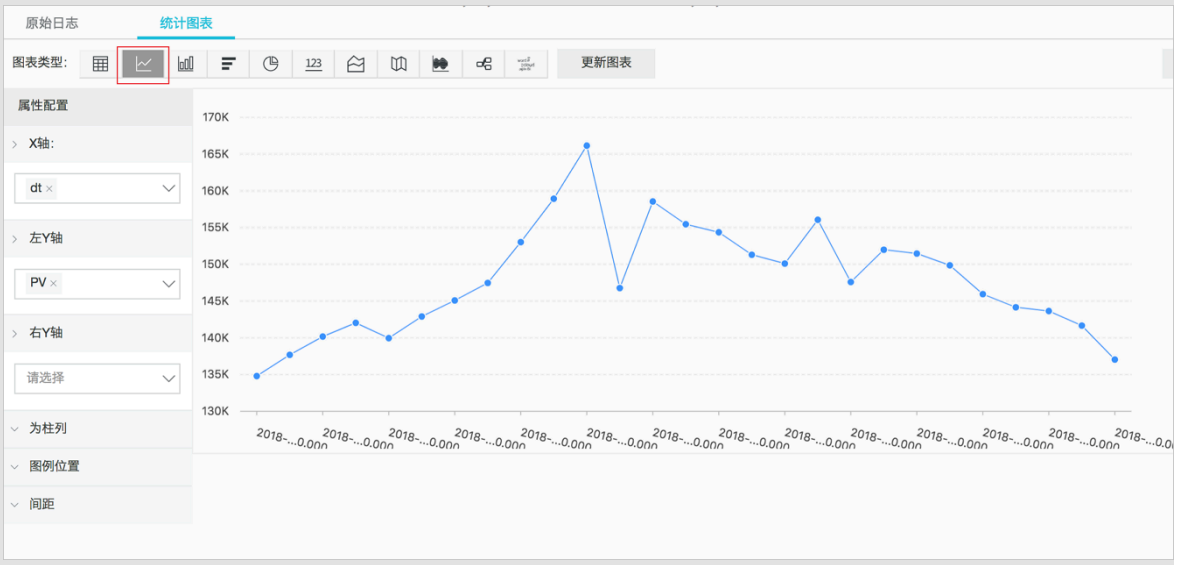
说明:

本示例中，使用内置时间字段计算__time__ - __time__% 300，并使用from_unixtime函数对计算结果进行格式化，将每条日志分到一个5分钟（300秒）的分组区间中统计总次数（count(1)）。最终，将查询结果按照所分的时间区间排序，返回前1,000条结果，即相当于所选择时间范围内前83小时的统计结果。

dt	PV
2018-05-31 21:30:00.000	134795
2018-05-31 21:35:00.000	137691
2018-05-31 21:40:00.000	140171
2018-05-31 21:45:00.000	142037
2018-05-31 21:50:00.000	139958
2018-05-31 21:55:00.000	142906
2018-05-31 22:00:00.000	145093
2018-05-31 22:05:00.000	147474

说明:

您也可以使用折线图方式进行展示。



更多关于时间解析的函数，例如将一个时间格式转化为另外一个格式，需要使用date_parse与date_format函数，相关具体说明，参考日期和时间函数。

基于客户端IP的查询分析

WAF日志中包含反映真实客户端IP的字段real_client_ip。如果由于用户通过代理服务器访问或请求头中IP字段有误等原因无法获得用户真实IP时，也可以直接使用直连客户端IP的字段remote_addr来获取客户端真实IP。

- 攻击者国家分布

  查询指定网站遭受的CC攻击的来源国家分布情况。

```
matched_host: www.aliyun.com  and cc_blocks: 1
| SELECT ip_to_country(if(real_client_ip='-', remote_addr,
real_client_ip)) as country,
         count(1) as "攻击次数"
   group by country
```

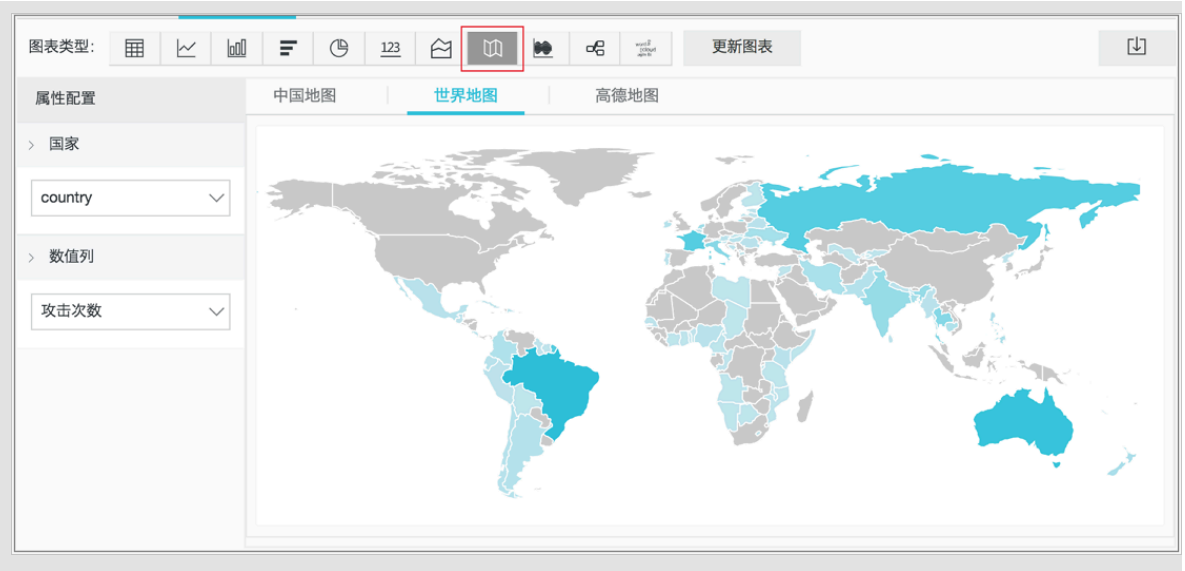
说明:

本示例中，使用函数if(condition, option1, option2)来选取real_client_ip字段或者remote_addr字段（当real_client_ip字段为-时）作为客户端真实IP。然后，使用ip_to_country函数获得客户端IP所对应的国家信息。

country	攻击次数
菲律宾	6321
斯洛文尼亚	521
吉布提	91
多哥	9
印度	14436
爱沙尼亚	65
莱索托	12

说明:

您也可以使用世界地图方式进行展示。



- **访问者省份分布**

  如果您希望进一步查询基于省份的分布情况，可以使用`ip_to_province`函数获得IP对应的省份信息。

```
matched_host: www.aliyun.com  and cc_blocks: 1
| SELECT ip_to_province(if(real_client_ip='-', remote_addr,
real_client_ip)) as province,
         count(1) as "攻击次数"
   group by province
```

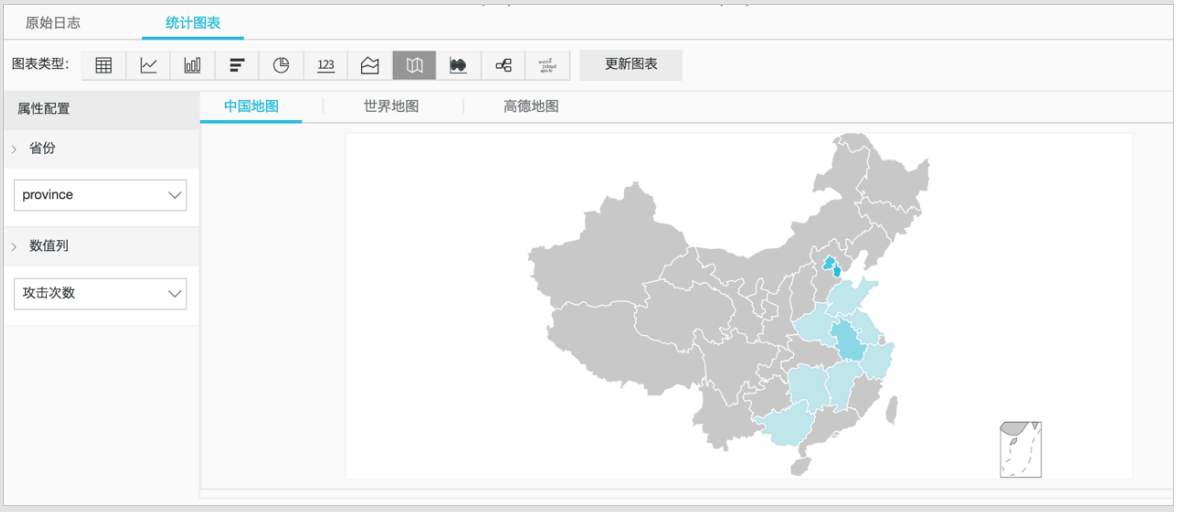
说明:

本示例中，使用ip_to_province函数获取客户端真实IP对应的省份信息。如果该IP是中国大陆地区以外的IP，函数依然会尝试获取其国家的省份（州）信息，但您在使用中国地图进行展示时，将无法展示大陆地区以外的IP。

province	攻击次数
江苏省	53
湖南省	2
北京市	509026
河南省	1411
安徽省	205629
广西壮族自治区	503
天津市	723121
浙江省	318

说明:

您也可以使用中国地图方式进行展示。



- 攻击者热力分布

  如果您想要获得攻击者的热力分布情况，可以使用ip_to_geo函数获得客户端真实IP对应的经纬度信息。

```
matched_host: www.aliyun.com  and cc_blocks: 1
| SELECT ip_to_geo(if(real_client_ip='-', remote_addr, real_clien
t_ip)) as geo,
         count(1) as "攻击次数"
```

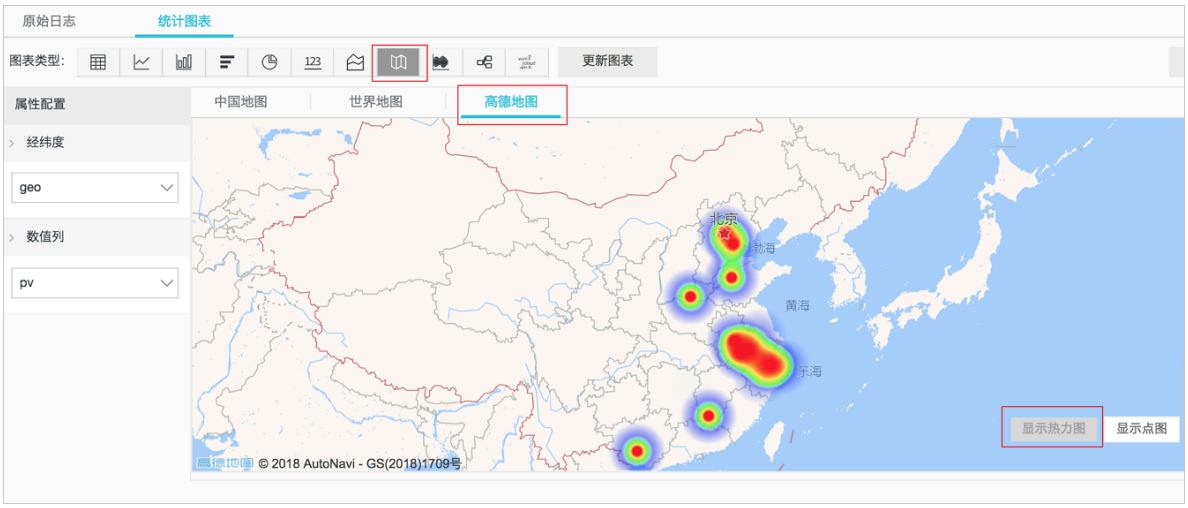
```
group by geo
limit 10000
```

说明：

本示例中，使用ip_to_geo函数获取客户端真实IP对应位置的经纬度，并返回前10,000条查询结果。

geo	pv
31.8639,117.281	81378
36.6683,116.997	656
30.0135,120.288660	72
39.1422,117.177	723121
31.1461,118.571	124143
22.8167,108.316670	503
25.85,114.933	673
32.2109,119.455	53

选择高德地图方式，并单击显示热力图。



基于IP的更多解析函数，例如获得IP所属运营商ip_to_provider、判断IP是内网还是外网ip_to_domain等函数的详细说明，参考IP地理函数。

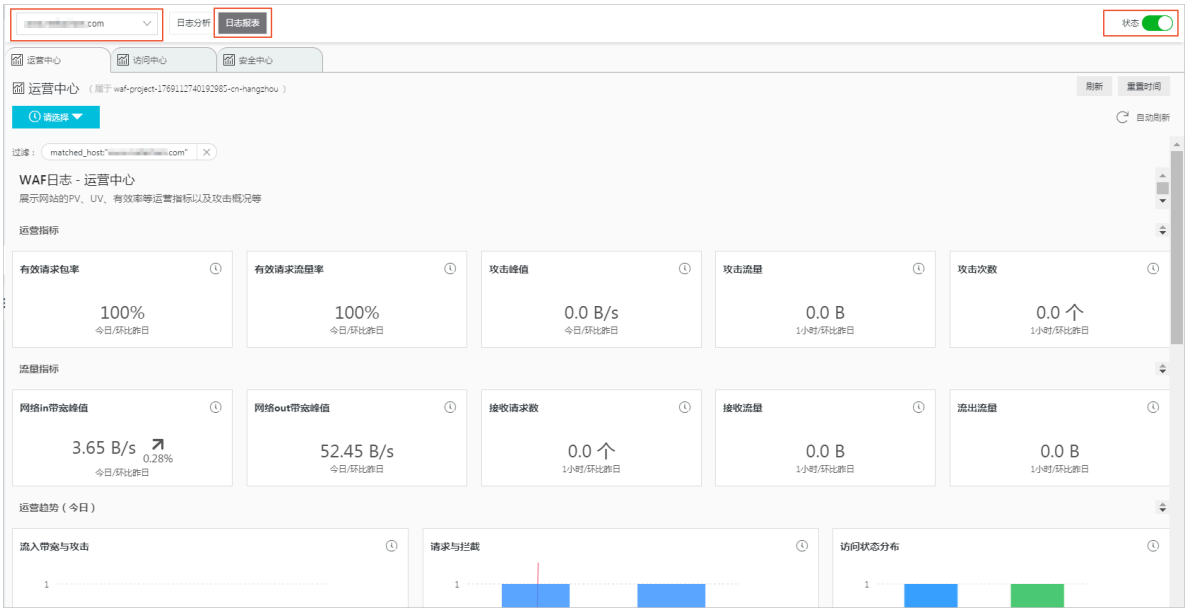
8.6 日志报表

日志报表页面集成日志服务的仪表盘页面，为您展示默认仪表盘。您可以通过修改时间范围、添加过滤条件等操作，在仪表盘中快速查询您关心的网站业务和安全数据。

查看报表

1. 登录Web应用防火墙管理控制台，定位到市场管理 > 应用管理页面。
2. 单击日志服务查询分析区域，打开日志服务页面。
3. 选择网站域名，确认右侧的状态开关为开启。
4. 单击日志报表。

   当前页面集成日志服务产品的仪表盘页面，系统将根据您选择的网站域名自动添加过滤条件，例如`matched_host: www.aliyun.com`，展示该网站的日志报表数据。



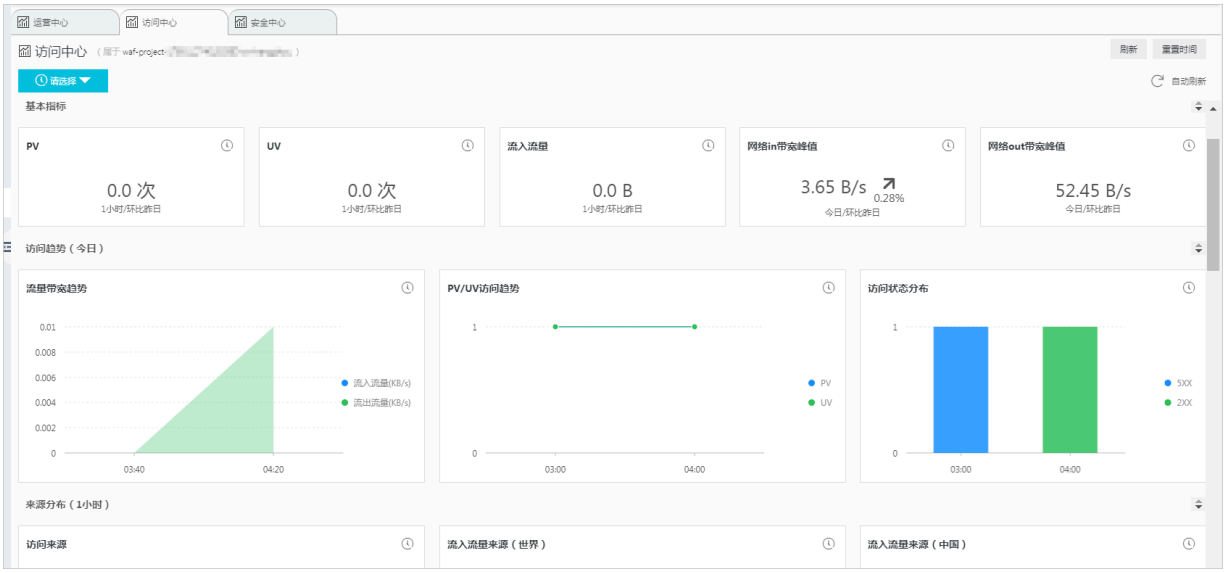
为网站域名开启WAF日志采集功能后，日志服务将自动创建三个默认的仪表盘，即运营中心、访问中心和安全中心。

说明:

关于默认仪表盘的详细说明，查看默认仪表盘。

仪表盘	说明
运营中心	展示网站业务的有效率、攻击情况等运营指标，网络In/Out带宽峰值、请求数等流量指标，运营趋势及攻击概况等信息。
访问中心	展示网站业务的PV、UV等基本访问指标，访问趋势、访问来源分布等信息。

仪表盘	说明
安全中心	展示网站业务遭受攻击的基本指标、攻击类型、攻击趋势、来源分布等信息。



说明:

WAF日志仪表盘展示区域按照预定义的布局展示多个报表，包含以下多种类型。关于日志服务提供的更多图表类型说明，参考图表说明。

图表类型	说明
数字	用于展示重要指标。例如，有效请求率、攻击峰值等。
线/面积图	用于展示重要指标在特定时间单元内的趋势信息。例如，流入带宽趋势、攻击拦截趋势等。
地图	用于展示访问者、攻击者的地理分布。例如，攻击来源国家分布、访问热点分布等。
饼图	用于展示分布占比情况。例如，被攻击网站、客户端类型分布等。
表格	用于展示攻击者列表信息等。

时间选择器

仪表盘页面的所有图表都是基于不同时间段的数据展示统计结果。如果您想要设置当前页面的所有图表均按照同样的时间范围显示统计结果，您可以通过设置时间选择器来实现。

1. 在日志报表页面，单击请选择。
2. 在弹出的时间设置框中选择时间范围。您可以选择相对时间、整点时间或设置自定义时间范围。

说明:

- 设置指定时间范围后，所有图表的时间都将更新为该时间范围。
- 时间选择器仅在当前页面提供临时的图表查看方式，无法保存该设置。您下次查看报表时，系统仍将为您展示默认的时间范围。
- 如果您希望只修改仪表盘中某个图表的时间范围，单击该图表右上角的 按钮，设置时间范围。

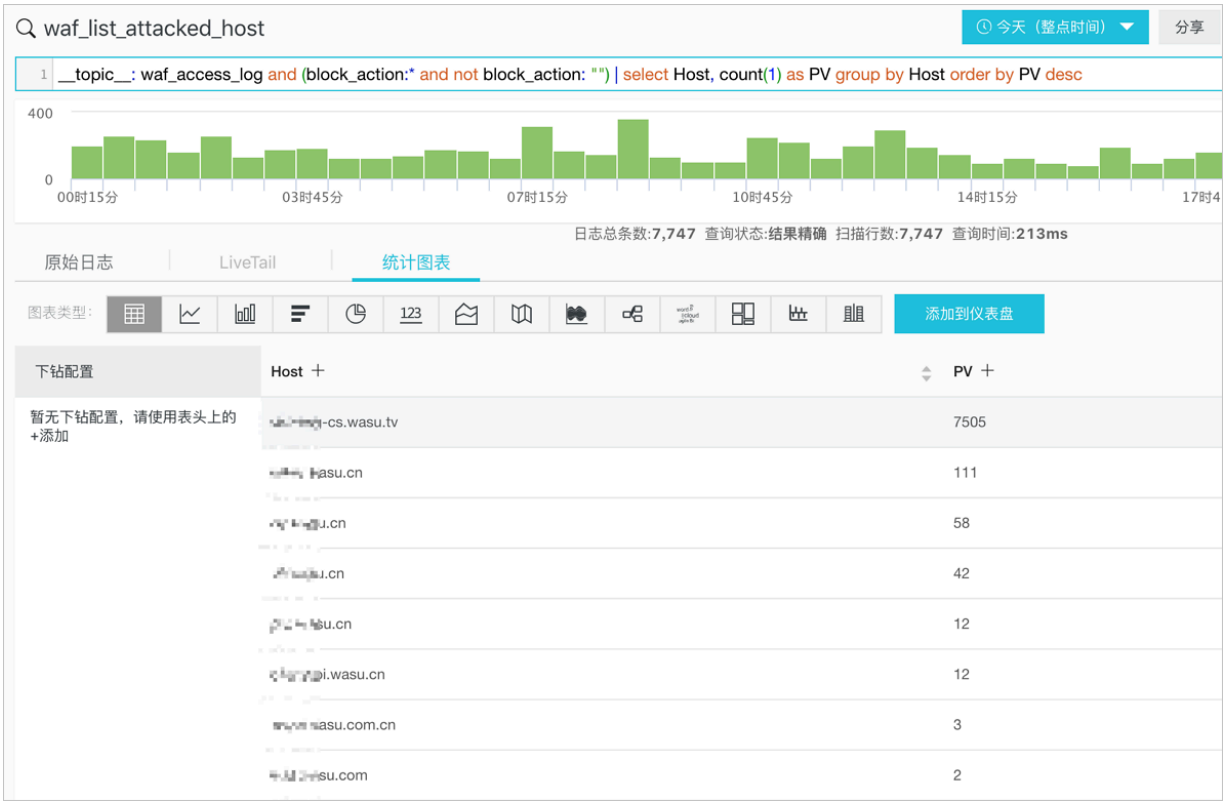
图表数据下钻

仪表盘页面中部分图表默认配置数据下钻，帮助您从统计数据快速探索到底层的详细数据。

如果图表右上方存在  图标，表示该图表已默认配置数据下钻操作。您可以单击带有下划线的数字，查看该数字底层更详细的数据。例如，单击安全中心报表的被攻击网站图表中的数字，您可以快速查看到被攻击的具体网站域名和遭受的攻击次数。

说明:

您也可以切换到原始日志页签，查看相关的原始日志。



默认仪表盘数值说明

- 运营中心：展示网站业务的有效率、攻击情况等运营指标，网络In/Out带宽峰值、请求数等流量指标，运营趋势及攻击概况等信息。

图表	类型	默认时间范围	描述	样例
有效请求包率	单值	今天（整点时间）	有效请求（即非攻击请求或返回400错误的请求）数量在所有请求总数的占比值。	95%
有效请求流量率	单值	今天（整点时间）	有效请求在所有请求总流量的占比。	95%
攻击峰值	单值	今天（整点时间）	遭受的攻击流量峰值，单位：Bps。	100 B/s

图表	类型	默认时间范围	描述	样例
攻击流量	单值	1小时（相对）	攻击请求流量总和，单位：B。	30 B
攻击次数	单值	1小时（相对）	攻击请求总次数。	100 个
网络in带宽峰值	单值	今日（整点时间）	网站业务流入方向流量速率的最高峰值，单位：KB/s。	100 KB/s
网络out带宽峰值	单值	今日（整点时间）	网站业务流出方向流量速率的最高峰值，单位：KB/s。	100 KB/s
接收请求数	单值	1小时（相对）	有效请求总数。	7.8 千个
接收流量	单值	1小时（相对）	有效请求的流入方向流量总和，单位：MB。	1.4 MB
流出流量	单值	1小时（相对）	有效请求的流出方向流量总和，单位：MB。	3.8 MB
流入带宽与攻击趋势	面积图	今天（整点时间）	有效请求和攻击请求的带宽流量趋势图，单位：KB/s。	-
请求与拦截趋势	线图	今天（整点时间）	每小时的有效请求和被拦截请求总数的趋势图，单位：个/小时。	-
访问状态分布趋势	流图	今天（整点时间）	每小时访问请求响应状态（400、304、20等状态码）的趋势图，单位：个/小时。	-
攻击来源分布（世界）	世界地图	1小时（相对）	攻击请求的来源国家分布。	-
攻击来源分布（中国）	中国地图	1小时（相对）	攻击请求的来源省份（中国）分布。	-
攻击类型	饼图	1小时（相对）	攻击请求的攻击类型分布。	-
被攻击网站	矩形树图	1小时（相对）	遭受攻击最多的网站排名。	-

- 访问中心：展示网站业务的PV、UV等基本访问指标，访问趋势、访问来源分布等信息。

图表	类型	默认时间范围	描述	样例
PV	单值	1小时（相对）	请求总数。	100 千次

图表	类型	默认时间范围	描述	样例
UV	单值	1小时（相对）	独立的访问客户端总数。	100 次
流入流量	单值	1小时（相对）	网站的流入方向流量总和，单位：MB。	300 MB
网络in带宽峰值	单值	今天（整点时间）	网站请求的流入方向流量速率的最高峰值，单位：KB/s。	0.5 KB/s
网络out带宽峰值	单值	今天（整点时间）	网站请求的流出方向流量速率的最高峰值，单位：KB/s。	1.3 KB/s
流量带宽趋势	面积图	今天（整点时间）	网站流入、流出方向流量趋势图，单位：KB/S。	-
PV/UV访问趋势	线图	今天（整点时间）	每小时PV、UV趋势图，单位：次。	-
访问状态分布	流图	今天（整点时间）	每小时访问请求响应状态（400、304、20等状态码）的趋势图，单位：个/小时。	-
访问来源分布（世界）	世界地图	1小时（相对）	访问请求的来源国家分布。	-
流入流量来源分布（世界）	世界地图	1小时（相对）	访问请求的流入方向流量来源国家分布。	-
流入流量来源分布（中国）	中国地图	1小时（相对）	访问请求的流入方向流量来源省份（中国）分布。	-
访问热力图	高德地图	1小时（相对）	访问请求来源在地理位置上的访问热力图。	-
来源网络提供商	饼图	1小时（相对）	访问请求来源的网络服务提供商分布情况，例如电信、联通、移动、教育网等。	-
Referer	表格	1小时（相对）	前100个最多的跳转Referer URL、主机及出现次数信息。	-
移动客户端类型分布	饼图	1小时（相对）	来自移动客户端请求的客户端类型分布情况。	-

图表	类型	默认时间范围	描述	样例
PC端客户端类型分布	饼图	1小时（相对）	来自PC客户端请求的客户端类型分布情况。	-
请求内容类型分布	饼图	1小时（相对）	请求内容类型分布，例如HTML、Form、JSON、流数据等。	-
访问域名	矩形树图	1小时（相对）	前30个被访问最多的网站域名。	-
访问最多的客户端	表格	1小时（相对）	前100个访问最多的客户端信息，包括客户端IP、地域城市、网络、请求方法分布、流入流量、错误访问次数、攻击次数等。	-
响应最慢的URL	表格	1小时（相对）	前100个响应时间最长的URL信息，包括网站域名、URL、平均响应时间、访问次数等。	-

- 安全中心：展示网站业务遭受攻击的基本指标、攻击类型、攻击趋势、来源分布等信息。

图表	类型	默认时间范围	描述	样例
攻击峰值	单值	1小时（相对）	遭受的攻击流量峰值，单位：Bps。	100 B/s
被攻击网站个数	单值	今天（整点时间）	遭受攻击的网站个数。	3 个
攻击来源国家	单值	今天（整点时间）	攻击请求来源国家个数。	2 个
攻击流量	单值	1小时（相对）	攻击请求流量总和，单位：B。	1 B
攻击者UV	单值	1小时（相对）	攻击请求来源的独立客户端个数。	40 个
攻击类型分布	流图	今天（整点时间）	攻击请求的攻击类型分布。	-
攻击拦截	单值	1小时（相对）	WAF拦截的攻击请求总次数。	100 次
CC攻击拦截	单值	1小时（相对）	WAF拦截的CC攻击请求次数。	10 次

图表	类型	默认时间范围	描述	样例
Web攻击拦截	单值	1小时（相对）	WAF拦截的Web应用攻击请求次数。	80 次
访问控制事件	单值	1小时（相对）	被WAF的精准访问控制规则拦截的请求次数。	10 次
CC攻击来源分布（世界）	世界地图	1小时（相对）	CC攻击请求的来源国家分布。	-
CC攻击来源分布（中国）	中国地图	1小时（相对）	CC攻击请求的来源省份（中国）分布。	-
Web攻击来源分布（世界）	世界地图	1小时（相对）	Web应用攻击请求的来源国家分布。	-
Web攻击来源分布（中国）	中国地图	1小时（相对）	Web应用攻击请求的来源省份（中国）分布。	-
访问控制攻击来源分布（世界）	世界地图	1小时（相对）	WAF精准访问控制规则拦截的攻击请求的来源国家分布。	-
访问控制攻击来源分布（中国）	中国地图	1小时（相对）	WAF精准访问控制规则拦截的攻击请求的来源省份（中国）分布。	-
被攻击网站	矩形树图	1小时（相对）	遭受攻击最多的网站排名。	-
CC防护策略分布	饼图	1小时（相对）	触发的CC防护策略分布情况。	-
Web攻击类型分布	饼图	1小时（相对）	遭受的Web攻击类型分布情况。	-
攻击者列表	表格	1小时（相对）	前100位攻击者的IP、所在省份、网络运营商信息，以及发起的各类攻击次数和攻击流量。	-
攻击者Referer	表格	1小时（相对）	攻击请求的Referer统计信息，包括Referer URL、Referer主机、出现次数。	-

8.7 日志字段说明

WAF详细记录网站域名的访问、攻防日志。日志中包含数十个字段，您可以根据不同需要选取特定的日志字段进行查询分析。

字段	说明	示例
__topic__	日志主题（Topic），该字段值固定为waf_access_log。	waf_access_log
acl_action	WAF精准访问控制规则行为，例如pass、drop、captcha等。  说明: 其中，空值或-值也表示pass，即放行。	pass
acl_blocks	是否被精准访问控制规则拦截，其中： · 1：表示拦截。 · 其他值均表示通过。	1
antibot	触发的爬虫风险管理防护策略类型，包括： · ratelimit：频次控制 · sdk：APP端增强防护 · algorithm：算法模型 · intelligence：爬虫情报 · acl：精准访问控制 · blacklist：黑名单	ratelimit
antibot_action	爬虫风险管理防护策略执行的操作，包括： · challenge：嵌入JS进行验证 · drop：拦截 · report：记录 · captcha：滑块验证	challenge

字段	说明	示例
block_action	触发拦截的WAF防护类型，包括： · tmd：CC攻击防护 · waf：Web应用攻击防护 · acl：精准访问控制 · geo：地区封禁 · antifraud：数据风控 · antibot：防爬封禁	tmd
body_bytes_sent	发送给客户端的HTTP Body的字节数。	2
cc_action	CC防护策略行为，例如none、challenge、pass、close、captcha、wait、login、n等。	close
cc_blocks	是否被CC防护功能拦截，其中： · 1：表示拦截。 · 其他值均表示通过。	1
cc_phase	触发的CC防护策略，包括seccookie、server_ip_blacklist、static_whitelist、 server_header_blacklist、server_cookie_blacklist、server_args_blacklist、qps_overmax等。	server_ip_blacklist
content_type	访问请求内容类型。	application/x-www-form-urlencoded
host	源网站。	api.aliyun.com
http_cookie	访问请求头部中带有的访问来源客户端Cookie信息。	k1=v1;k2=v2
http_referer	访问请求头部中带有的访问请求的来源URL信息。若无来源URL信息，则显示-。	http://xyz.com
http_user_agent	访问请求头部中的User Agent字段，一般包含来源客户端浏览器标识、操作系统标识等信息。	Dalvik/2.1.0 (Linux; U; Android 7.0; EDI-AL10 Build/HUAWEIEDISON-AL10)

字段	说明	示例
http_x_forwarded_for	访问请求头部中带有的XFF头信息，用于识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址。	-
https	访问请求是否为HTTPS请求，其中： · true：HTTPS请求。 · false：HTTP请求。	true
matched_host	匹配到的已接入WAF防护配置的域名，可能是泛域名。若无法匹配到相关域名配置，则显示-。	*.aliyun.com
querystring	请求中的查询字符串。	title=tm_content%3Darticle&pid=123
real_client_ip	访问的客户端的真实IP。若无法获取到，则显示-。	1.2.3.4
region	WAF实例地域信息。	cn
remote_addr	访问请求的客户端IP。	1.2.3.4
remote_port	访问请求的客户端端口。	3242
request_length	访问请求长度，单位字节。	123
request_method	访问请求的HTTP请求方法。	GET
request_path	请求的相对路径（不包含查询字符串）。	/news/search.php
request_time_msec	访问请求时间，单位为毫秒。	44
request_traceid	WAF记录的访问请求唯一ID标识。	7837b117154103869434037009ea1f0
server_protocol	源站服务器响应的协议及版本号。	HTTP/1.1
status	WAF返回给客户端的HTTP响应状态信息。	200
time	访问请求的发生时间。	2018-05-02T16:03:59+08:00
ua_browser	访问请求来源的浏览器信息。	ie9
ua_browser_family	访问请求来源所属浏览器系列。	internet explorer
ua_browser_type	访问请求来源的浏览器类型。	web_browser
ua_browser_version	访问请求来源的浏览器版本。	9.0
ua_device_type	访问请求来源客户端的设备类型。	computer

字段	说明	示例
ua_os	访问请求来源客户端的操作系统信息。	windows_7
ua_os_family	访问请求来源客户端所属操作系统系列。	windows
upstream_addr	WAF使用的回源地址列表，格式为`IP:Port`，多个地址用逗号分隔。	1.2.3.4:443
upstream_ip	访问请求所对应的源站IP。例如，WAF回源到ECS的情况，该参数即返回源站ECS的IP。	1.2.3.4
upstream_response_time	源站响应WAF请求的时间，单位秒。如果返回“-”，代表响应超时。	0.044
upstream_status	源站返回给WAF的响应状态。如果返回“-”，表示没有响应（例如该请求被WAF拦截或源站响应超时）。	200
user_id	阿里云账号AliUID。	12345678
waf_action	Web攻击防护策略行为，包括： · block：表示拦截 · bypass或其它值均表示放行	block
web_attack_type	Web攻击类型，例如xss、code_exec、webshell、sqli、lfilei、rfilei、other等。	xss
waf_rule_id	匹配的WAF的相关规则ID。	100

8.8 高级管理

WAF日志查询分析服务提供高级管理功能，您可使用高级管理功能跳转至日志服务管理控制台进行告警与通知、实时订阅与消费、数据投递和对接其他可视化等高级操作。

操作步骤

1. 登录云盾Web应用防火墙管理控制台，定位到市场管理 > 应用管理页面。
2. 单击日志服务查询分析区域，打开日志服务页面。
3. 单击右上角的高级管理。
4. 在弹出的对话框中，单击前往打开日志服务管理控制台。

5. 在日志服务管理控制台，您可以对WAF专属的日志Project和Logstore进行以下高级管理操作：
   - 设置告警与通知
   - 设置日志实时订阅与消费
   - 将日志数据实时投递至其它阿里云存储类产品
   - 对接其它可视化产品进行展示

8.9 导出日志

WAF日志查询分析服务支持将日志查询结果导出到本地。

操作步骤

1. 登录云盾Web应用防火墙管理控制台，定位到市场管理 > 应用管理页面。
2. 单击日志服务查询分析区域，打开日志服务页面。
3. 在日志分析页面的原始日志页签中，单击右侧的日志下载按钮  。

> **说明：**
> 如果当前查询未返回任何结果，将不会显示日志下载按钮。

4. 在日志下载对话框中，选择下载本页日志或通过命令行工具下载所有日志。

   · 下载本页日志：单击确定，将当前页面查询到的原始日志以CSV格式导出至本地。

   · 通过命令行工具下载所有日志

     a. 参见命令行工具CLI用户手册，安装命令行工具。

     b. 单击安全信息管理页面链接查看并记录当前用户的秘钥ID和Key信息。

     c. 单击复制命令行，将该命令行复制到CLI命令行工具中并根据当前用户的秘钥ID和Key信息替换命令行中【步骤2中的秘钥ID】和【步骤2中的秘钥Key】部分后，执行该命令。

命令执行完成后，WAF记录的所有原始日志将自动下载并保存至运行该命令的当前目录下的*download_data.txt*文件中。

8.10 为子账号授予日志查询分析权限

如果子账号需要使用WAF日志查询分析服务，需要由主账号为其进行授权操作。

背景信息

开通和使用WAF日志查询分析服务，具体涉及以下权限：

操作类型	支持的操作账号类型
开通日志服务（全局一次性操作）	主账号
授权WAF实时写入日志数据到日志服务的专属日志库（全局一次性操作）	· 主账号 · 具备AliyunLogFullAccess权限的子账号 · 具备指定权限的子账号
使用日志查询分析功能	· 主账号 · 具备AliyunLogFullAccess权限的子账号 · 具备指定权限的子账号

您也可以根据实际需求为子账号授予相关权限。

授权场景	授予权限	操作步骤
为子账号授予日志服务产品的所有操作权限。	授予日志服务全部管理权限AliyunLogFullAccess	具体操作步骤，请参见RAM用户管理。
主账号开通WAF日志查询分析服务并完成授权操作后，为子账号授予日志查看权限。	授予只读权限AliyunLogReadOnlyAccess	具体操作步骤，请参见RAM用户管理。
仅为子账号授予开通和使用WAF日志查询分析服务的权限，不授予日志服务产品的其他管理权限。	创建自定义授权策略，并为子账号授予该自定义授权策略。	具体操作步骤，请参见本文操作步骤章节。

操作步骤

1. 登录 RAM控制台。
2. 在左侧导航栏的权限管理菜单下，单击权限策略管理。
3. 单击新建权限策略。
4. 填写策略名称和备注。

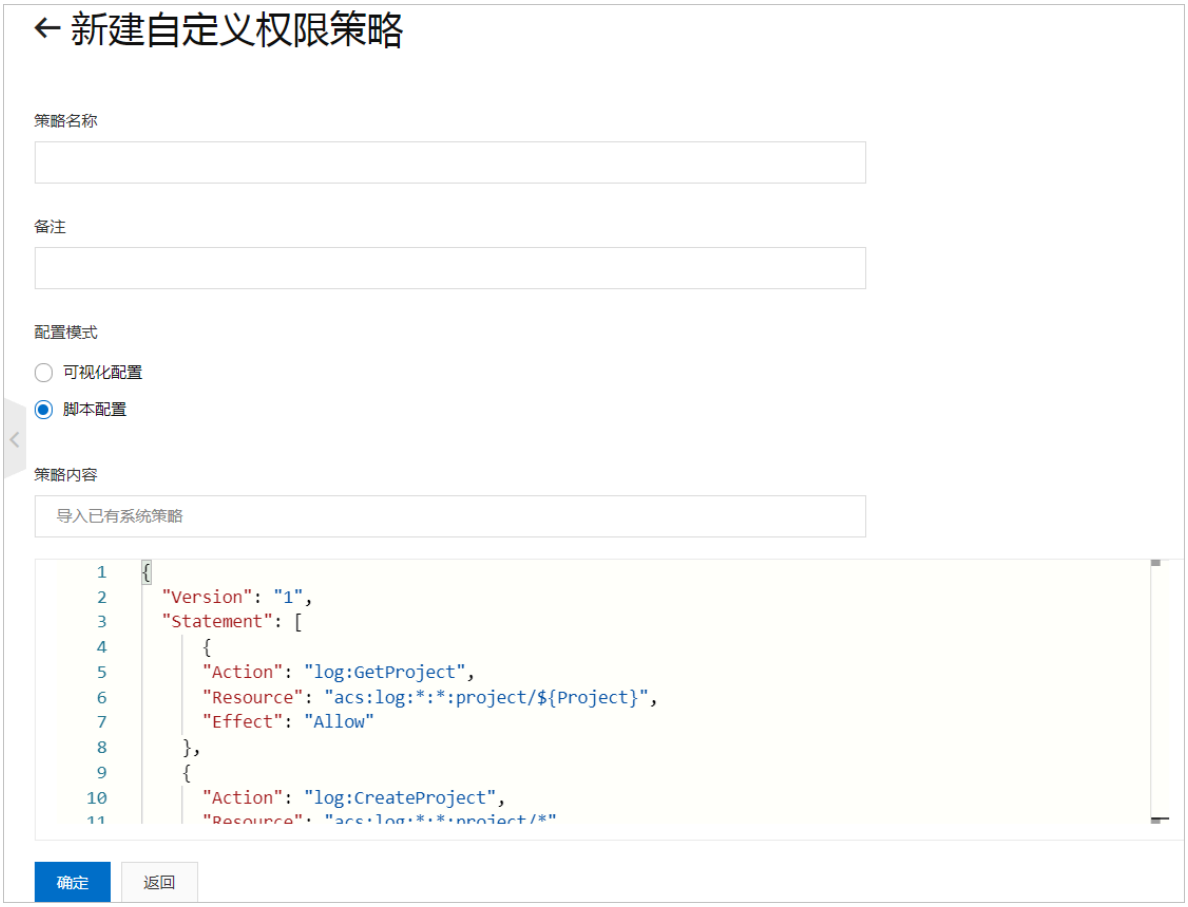
5. 选择脚本配置模式，输入以下策略内容。

说明:

将以下策略内容中的${Project}与${Logstore}分别替换为您的WAF日志服务专属Project和Logstore的名称。

```
{
  "Version": "1",
  "Statement": [
      {
      "Action": "log:GetProject",
      "Resource": "acs:log:*:*:project/${Project}",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateProject",
      "Resource": "acs:log:*:*:project/*",
      "Effect": "Allow"
    },
    {
      "Action": "log:ListLogStores",
      "Resource": "acs:log:*:*:project/${Project}/logstore/*",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateLogStore",
      "Resource": "acs:log:*:*:project/${Project}/logstore/*",
      "Effect": "Allow"
    },
    {
      "Action": "log:GetIndex",
      "Resource": "acs:log:*:*:project/${Project}/logstore/${
Logstore}",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateIndex",
      "Resource": "acs:log:*:*:project/${Project}/logstore/${
Logstore}",
      "Effect": "Allow"
    },
    {
      "Action": "log:UpdateIndex",
      "Resource": "acs:log:*:*:project/${Project}/logstore/${
Logstore}",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateDashboard",
      "Resource": "acs:log:*:*:project/${Project}/dashboard/*",
      "Effect": "Allow"
    },
    {
      "Action": "log:UpdateDashboard",
      "Resource": "acs:log:*:*:project/${Project}/dashboard/*",
      "Effect": "Allow"
    },
    {
      "Action": "log:CreateSavedSearch",
      "Resource": "acs:log:*:*:project/${Project}/savedsearch/*",
```

```
      "Effect": "Allow"
    },
    {
      "Action": "log:UpdateSavedSearch",
      "Resource": "acs:log:*:*:project/${Project}/savedsearch/*",
      "Effect": "Allow"
    }
  ]
}
```



6. 单击确定。
7. 定位到人员管理 > 用户页面，找到需要授权的子账号并单击对应的添加权限。
8. 选择您所创建的自定义授权策略，单击确定。

   被授权的子账号即可以开通和使用WAF日志查询分析服务，但无法对日志服务产品的其它功能进行操作。

8.11 日志存储空间管理

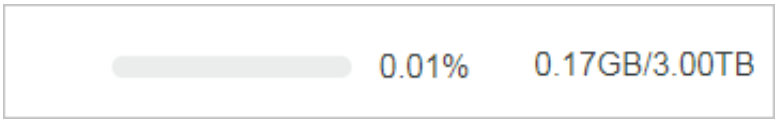
开通WAF日志服务后，系统将根据您所选择的日志存储规格分配日志存储空间，您可以在Web应用防火墙管理控制台的日志服务页面查看日志存储空间的使用情况。

查看日志存储空间使用情况

您可以随时查看您WAF日志查询分析服务的日志存储空间用量。

> 说明:
> 控制台中显示的日志存储空间用量并非实时更新，与实际使用情况存在两个小时的延迟。因此，当日志存储空间即将占满时，请提前升级容量。

1. 登录Web应用防火墙管理控制台。
2. 定位到市场管理 > 应用管理页面，选择您的WAF实例所在地域，单击日志服务实时查询分析。
3. 在日志服务页面上方，查看日志存储空间用量。



升级日志存储空间容量

如果您发现日志存储空间即将占满，您可以单击日志服务页面上方的升级容量，选择更大的日志存储容量规格，并支付相应的扩容费用。

> 说明:
> 为避免因日志存储空间容量占满，新的日志数据无法写入专属日志库，而造成日志数据不完整的情况，请您及时升级日志存储空间容量。

清空日志存储空间

根据业务需要，您可以清空当前日志存储空间中的所有日志数据。例如，清空测试阶段产生的日志数据，从而充分利用日志存储空间记录有意义的生产数据。

> 说明:
> 清空日志存储空间功能存在使用次数限制。

单击日志服务页面上方的清空，并确认清空您日志存储空间中的全部日志。

> 注意:
> 日志清空后将无法复原，请务必谨慎使用清空功能。

9 安全服务

9.1 开通WAF安全服务授权

通过WAF安全专家服务，您将获得阿里云安全服务专家和第三方安全专家为您提供的针对您业务场景的WAF产品安全服务，帮助您基于业务实际情况更好地使用WAF产品功能，保障您业务的网络应用安全。

背景信息

安全专家可以为您提供WAF中的域名接入咨询服务，同时通过对您的业务日志数据进行深度分析，有针对性地为您提供WAF防护配置的相关建议。

购买WAF产品安全服务后，您需要开通服务授权，阿里云安全服务专家和第三方安全专家才能通过阿里云安全服务平台为您提供产品服务。

> **说明:**
> 您必须已购买或开通云盾Web应用防火墙产品，才能享受WAF安全专家服务。

操作步骤

1. 登录云盾先知（安全情报）管理控制台。
2. 定位到服务授权页面，您可以查看到您的WAF产品安全服务订单的授权情况。

> **说明:**
> 一般情况下，新创建的安全服务订单状态为未授权。

3. 单击查看授权协议，确认并同意授权书内容后单击确定。

4. 单击授权，跳转至服务订单所对应的云资源RAM角色授权页面，单击同意授权。

说明:

为了确保与安全专家的交流，确认您已申请并开通与安全专家的专属钉钉服务群。

授权完成后，在云盾先知（安全情报）管理控制台的服务授权页面，该服务订单的状态显示为已授权，您可以随时单击查看授权协议查看授权书。

同时，您的专属安全专家将可以通过阿里云安全服务平台直接查看您的WAF中相应的业务数据及配置数据，为您的业务提供专属的安全策略和建议。

说明:
安全专家通过阿里云安全服务平台查看您WAF控制台进行的所有操作都将产生相应的操作日志，您可以随时登录阿里云控制台查看安全专家操作记录。

9.2 查看安全专家操作日志

安全专家通过阿里云安全服务平台查看您在WAF控制台上进行的所有操作都将产生相应的操作日志，您可以随时登录阿里云操作审计控制台查看相关操作记录，审计安全专家的操作行为。

操作步骤

1. 登录操作审计管理控制台，并选择华东1（杭州）地域。

   说明:
   目前，所有WAF安全服务的操作日志记录均存储在华东1（杭州）地域的操作审计服务中。

2. 定位到历史事件查询页面，设置以下查询条件，并单击搜索，查询您的专属安全专家在WAF控制台中的操作记录日志。

   - 资源名称：aliyunmsspaccessingwafrole
   - 事件类型：所有类型

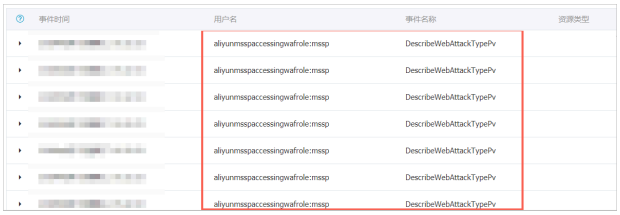
   说明:

目前，WAF安全服务仅授权安全专家查看您WAF控制台中的数据，不具备更改配置等权限。因此，您也可以将事件类型条件设置为读类型，查询到的事件记录与选择所有事件类型得到的查询结果一致。

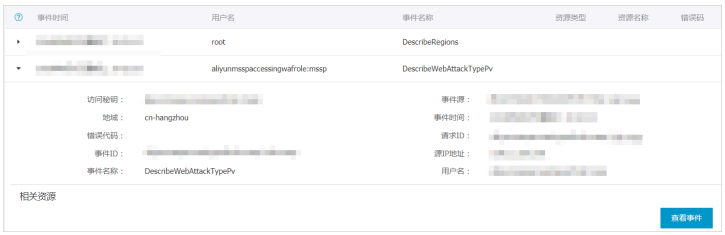
- 时间：选择您想查询的时间范围。

> **说明:**
> 历史事件查询支持查看最近30天内的操作记录。

查询结果如下图所示。



3. 在事件列表中，单击操作记录可展开查看事件详情。



4. 单击查看事件可查看该事件的详细参数。

9.3 取消WAF安全服务授权

WAF安全服务授权开通后，您可以随时在访问控制（RAM）控制台中删除WAF安全服务的授权角色，取消WAF安全服务授权。

操作步骤

1. 登录RAM控制台。
2. 定位到RAM角色管理页面，找到授权服务订单时生成的MSSP安全产品服务的授权角色（AliyunMSSPAccessingWAFRole），单击删除。
3. 在删除RAM角色对话框中，单击确认。

4. 获取并输入手机验证码，单击确定，通过手机验证。

   授权角色删除成功后，在云盾先知（安全情报）管理控制台的服务授权页面中相应服务订单的状态将变更为未授权。

10 WAF产品托管服务

云盾Web应用防火墙（WAF）支持产品托管服务。开通WAF产品托管后，您可以在阿里云安全产品专家的帮助下完成WAF接入配置、防护策略优化，并享有安全事件响应、安全咨询、安全培训与案例分享、安全报告分析等服务。

概述

WAF产品托管由阿里云原厂安全服务团队提供技术支持，面向云盾WAF用户提供产品托管服务。WAF产品托管帮助您更有效地使用WAF保护Web资产、降低业务安全风险、减少运维人力投入。

WAF产品托管适用于已开通阿里云Web应用防火墙，但缺乏业务持续监控能力和缺少可应对安全漏洞风险的安全工程师的业务场景。该服务适合需要外包专业人员协助来进行安全产品服务运营的用户。

服务内容

WAF安全托管为您提供完整的WAF接入和使用支持，下表描述了具体的服务内容。

表 10-1: WAF安全托管服务服务内容

服务类型	描述
接入配置	· 在WAF上配置保护对象的域名策略 · 协助用户配置和上传HTTPS证书（用户可自行上传） · 协助用户配置ECS和SLB的源站保护策略 · 产品适配和访问测试验证 · 用户保护域名变化时，调整相关配置
防护策略优化	· 在WAF上的业务出现异常时，提供诊断和排错服务 · 基于攻防日志，优化用户安全防护策略和配置 · 安全事件响应时，调整防护策略和提供方案，帮助用户缓解事件影响 · 提供故障处理、CC防护规则、精准访问控制规则、数据风控等WAF防护配置建议
监控和预警	· 系统自动化监控WAF集群可用性故障 · 系统自动化监控安全高危事件和攻击导致的异常事件 · 人工在线判断和过滤监控事件预警
安全报告	· 根据用户要求提供定制化安全报告内容 · 提供服务日报和服务月报，其中日报包括当天操作信息，月报包括操作数据和攻防数据分析

安全事件响应时间

开通WAF安全托管后，当您遇到安全事件需要紧急协助时，服务团队响应您的时间遵循下表描述。

表 10-2: 安全事件响应时间

序号	优先级	定义	响应时间
1	危险	用户核心业务严重受损或完全不可用	15分钟
2	紧急	用户核心业务出现非全局异常	30分钟
3	高	用户非核心业务严重受损或不可用	2小时
4	中	用户非核心业务出现非全局异常	4小时
5	低	用户日常技术咨询	8小时

服务交付方式

下表描述了WAF产品托管的服务交付方式。

表 10-3: 服务交付方式

类别	描述
服务交付方式	远程在线服务
服务语言	中文和英语
服务周期	与用户购买周期一致
支持的服务渠道	· 电子邮件 · 钉钉 · 电话

定价和售卖方式

WAF产品托管服务支持通过预付费方式开通，并且可按月或者按年续费。购买WAF产品托管服务，请前往WAF产品托管服务售卖页。

注意:

由于服务支持系统和服务人力资源投入的特殊性，WAF产品托管服务在支付购买后暂不支持退款。