# 阿里云 Web应用防火墙

统计分析

文档版本: 20200630

为了无法计算的价值 | [] 阿里云

### <u>法律声明</u>

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。

- 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。
- 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。
- 由于产品版本升级、调整或其他原因,本文档内容有可能变更。阿里云保留在没有任何通知或者 提示下对本文档的内容进行修改的权利,并在阿里云授权通道中不时发布更新后的用户文档。您 应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
- 4. 本文档仅作为用户使用阿里云产品及服务的参考性指引,阿里云以产品及服务的"现状"、"有缺陷"和"当前功能"的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引,但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的,阿里云不承担任何法律责任。在任何情况下,阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害,包括用户使用或信赖本文档而遭受的利润损失,承担责任(即使阿里云已被告知该等损失的可能性)。
- 5. 阿里云文档中所有内容,包括但不限于图片、架构设计、页面布局、文字描述,均由阿里云和/或 其关联公司依法拥有其知识产权,包括但不限于商标权、专利权、著作权、商业秘密等。非经阿 里云和/或其关联公司书面同意,任何人不得擅自使用、修改、复制、公开传播、改变、散布、发 行或公开发表阿里云网站、产品程序或内容。此外,未经阿里云事先书面同意,任何人不得为了 任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称(包括但不限于单独为或以组 合形式包含"阿里云"、"Aliyun"、"万网"等阿里云和/或其关联公司品牌,上述品牌的附属 标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识 或通过特定描述使第三方能够识别阿里云和/或其关联公司)。
- 6. 如若发现本文档存在任何错误,请与阿里云取得直接联系。

### 通用约定

格式	说明	样例
•	该类警示信息将导致系统重大变更甚至 故障,或者导致人身伤害等结果。	<b>一 禁止:</b> 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更 甚至故障,或者导致人身伤害等结果。	▲ 警告: 重启操作将导致业务中断,恢复业务 时间约十分钟。
!	用于警示信息、补充说明等,是用户必须了解的内容。	<b>注意:</b> 权重设置为0,该服务器不会再接受 新请求。
Ê	用于补充说明、最佳实践、窍门等,不 是用户必须了解的内容。	<b>说明:</b> 您也可以通过按Ctrl + A选中全部文 件。
>	多级菜单递进。	单击 <b>设置 &gt; 网络 &gt; 设置网络类型</b> 。
粗体	表示按键、菜单、页面名称等UI元素。	在 <b>结果确认</b> 页面,单击 <b>确定</b> 。
Courier字体	命令。	执行cd /d C:/window命令,进 入Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid
		Instance_ID
[]或者[alb]	表示可选项,至多选择一个。	ipconfig [-all -t]
{}或者{a b}	表示必选项,至多选择一个。	switch {active stand}

### 目录

法律声明	I
通用约定	I
1 查看总览信息	1
2 查看安全报表	9
3 数据大屏	

### 1 查看总览信息

Web应用防火墙(WAF)的总览页面展示了已接入WAF防护的所有网站的总体防护信息,包括攻击 事件和应急漏洞记录、防护统计数据、请求分析图表。您可以查看总览信息了解网站业务的安全状态 和做安全分析。

### 访问总览页面

- 1. 登录Web应用防火墙控制台。
- 2. 在顶部菜单栏,选择Web应用防火墙实例的资源组和地域(中国内地、)。
- **3.** 在左侧导航栏,单击。
- 在总览页面左侧列表上方,设置要查询的网站域名(全部域名或已接入防护的单个域名)和时间 段(实时、今天、7天、30天、自定义),查看对应的总览信息。

总览		
全部		$\sim$
实时 今天	7天 30天 自定义	
事件列表	应急漏洞	

### 

支持查看最近30天内的总览信息,使用自定义时间可以查看最近30天内指定时间段的数据。

### 总览信息解读

总览信息包括以下内容:

- 事件列表和应急漏洞记录(图示中①)
- 防护统计数据(图示中②)
- 请求分析图表(图示中③)



#### 事件列表和应急漏洞记录解读

默认展示**应急漏洞**信息,您可以查看Web应用防火墙针对最新披露的安全漏洞执行的防护规则更新。 在**应急漏洞**列表单击应急漏洞名称,可以展开**应急漏洞防护详情**页面,您可以查看0day高危漏洞等 应急漏洞的防护详情、对应的防护规则详情、漏洞影响的资产信息。单击**已防护资产数**,会跳转到**网** 站接入页面。

全部	1.800	应急漏洞防护详情 ×
实时 今天 7天 30天 自定义	1,300	
2020年5月26日 00:51	900	
2020年6月24日 00:51 箇	600	4 5
事件列表 应急漏洞	0 0 2020年5月26日 00-51 2020年5月29日 11-51 2020年6月1日 22-51 2020年6月5日 09-51 2020年6月8日 20-51 20	漏洞及防护规则详情
更新泛微ecology:超权遍历防护规则 更新时间: 2020年6月14日	- 金彩 - Web入惯的炉 - CC安全的炉 - 白脂的炉	应急开始时间 规则发布时间 2020年5月29日 11:24 2020年5月28日 11:24
更新用友NC反序列化远程代码执行助护规则 更新时间:2020年6月5日	Browser分布 UA Top URL请求次	選問名称 選問日 更新Fastjoon <= 12.68金版本這種代码执行防护规则 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
更新用友NC远程代码执行防护规则 更新时间: 2020年6月5日	wafwafqa3.c 1006.wafqa3	規則区称 期間D Fastjon <=1.2.68金版本运程代码执行 113311 
<b>更新fastjion &lt;= 12.68全版本选程代码执行</b> 防护规则 更新时间: 2020年5月28日	robot/spider 65.46%  1006.wafqa3  downloading tool 32.87%  1006.wafqa3	コロテロは
奥新FasterXML jackson-databind远程化码标 行動分规則(databind#2704) 思新世術前:2020年5月8日 更新FasterXML jackson-databind远程代码标	e drome 0.62% 9 368 0.05% 1000 wafqa3 gartner wafq	高齢(約約100-4-10日間) Lysticou <=TToo (回知(日ヤ ) F28(448で159(1) - H I In (ednest ∩H - H I In (ednest pool/機

切换到**事件列表**后,可以查看历史安全事件。为便于您快速了解网站遭受的攻击和威胁情况,WAF将 所拦截的攻击聚合成事件进行展示。

### 📙 说明:

如果您查询的是全部域名,则将显示全部域名遭受的攻击次数及聚合后的事件数量。您可以选择具体域名查看事件分布情况。

**Web应用防火墙按照攻击的类型、危险程度、频率与时间将攻击聚合成事件。**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。

⊕ 1168112235E	14 天前
(k) 5561500308	18 天前
⊕ 383102338	18 天前
<u>⊖</u> <u>69941</u> (2020)	18 天前
@ 6994120338	18 天順
<b>95380</b> /2000	18 天前
@ 97817/200m	19 天府

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方的专家防护建议,根据实际业务情况选择合适的防护方案。

2019年05月30日 10:49 → 2019年05月30	E 10:57		
資料公款 紅龍八数	Qualify		
157256 2 116811 2	391		
攻击未遂中		UserAgent	
116 .5/6	34920	ests/2.18.4	116
116	29580	<b>和元政治</b>	
57 BRMST	29286	\$07.039R	
222 2011 2011	28976	107.03H	
10: 澳大利亚	28969	報元政治	
Referer		URL	
	116811	<b>能无</b> 取错	
- 報元政県	0	<b>能无</b> 政结	
- 報元政府 報元政府	0	輸元約3月 輸元約3月	
- 報元政3県 報元政3県 報元政3県	0	報元80日 報元80日 報元80日	

#### 防护统计数据解读

展示网站域名收到的全部请求次数和触发不同防护模块的请求次数,包括Web入侵防护、CC安全防护、扫描防护、访问控制、Bot防护。

### 

Bot防护仅在新版防护引擎中支持,如果您使用旧版防护引擎,则不显示该记录。更多信息,请参见#unique\_4。

全部	Web入侵防护	CC安全防护	扫描防护	访问控制	Bot 防护
1,710次	95 <sub>次</sub>	33次	106 次	21次	<b>0</b> 次
	$\Box$		$\checkmark$		

单击不同防护模块下的请求次数,可以跳转到对应的**安全报表**页面,查看详细数据。更多信息,请参 见查看安全报表。

单击防护统计区域下方的展开按钮,显示对应数字的缩略趋势图。



如果您查询的是全部域名,展开后将额外显示数据大小排序Top 5的域名及对应的数据。

全部		Web入侵防护		CC安全防护		扫描防护		访问控制		Bot 防护	
1,710次		95次		33次		106次		21次		0 次	
	mille		سا				LL				
	1,198		80		18		72		15	暂无数据	0
	467		15	u u la	15		34		6	暂无数据	0
	29		0	暂无数据	0	暫无数据	0	暂无数据	0	暂无数据	0
	16	智无数据	0	智无数据	0	智无数据	0	智无数据	0	智无数据	0
- 智无数据	0	智无数据	0	暂无数据	0	暫无数据	0	暂无数据	0	智无数据	0
						^					

### 请求分析图表解读

• 业务趋势:展示指定时间段内的请求次数、QPS、带宽、响应码趋势(最细粒度达分钟级别)。



- 单击趋势图下方的图例,可以在图中取消或显示对应类型的记录。

- Bot防护仅在新版防护引擎中支持,如果您使用旧版防护引擎,则不显示该记录。更多信息,请参见#unique\_4。
- · **请求次数**:包含全部请求次数、Web入侵防护次数、CC安全防护次数、扫描防护次数、访问控制命中次数、Bot防护次数。



- **QPS**:包含全部请求QPS、Web入侵防护QPS、CC安全防护QPS、扫描防护QPS、访问控制QPS、Bot防护QPS。

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。

请求次数 QPS	带宽 响应码			
bps				
18,000				
15,000				
12,000				
9,000				
6,000				
3,000				
0 2020年1月28日 1	7:30 2020年2月4日 08:00	2020年2月10日 22:30	2020年2月17日 13:00	2020年2月24日 03:30
		📥 入带宽 📥 出带宽	<b>-</b>	

- 响应码:包含5xx、405、499、302、444等异常响应码的数量趋势。

道 说明:

单击趋势图右上角的**WAF返回客户端**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。



• 浏览器分布: 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: UA Top页签下展示收到的请求中UserAgent的排名情况和请求次数。

Browser分布 UA Top	
python-requests/2.18.4	14,548
curl/7.54.0	3,256
python-requests/2.22.0	1,008
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) App	322
PostmanRuntime/7.22.0	216
curl/7.64.1	172
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) App	77
curl/7.29.0	71
Mozilla/5.0 (iPhone; CPU iPhone OS 12_4_4 like Mac	69
SogoulMEMiniSetup_RandSkin	60

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

URL请求次数	Top IP	
	/collect/log	2,796
2 - 1	/mile-video-api/	1,562
	ı/api	866
	/loggw/logUpload.do	857
	/loggw/logConfig.do	805
-	/co-order-pull/order/pull	637
	/service/getlpInfo	532
	/mile-user-api/	459
1	/v1/lead/launch	454
	/mile-task-api/	425

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

URL请求次数 Top IP	
北京	9,440
北京	2,968
法国	2,657
澳大利亚	1,740
美国	438
澳大利亚	369
澳大利亚	369
澳大利亚	245
法国	242
北京	212

• 事件分布: **攻击分布**页签下展示将攻击聚合后的事件分布情况。



单击某个事件点,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。

### 2 查看安全报表

Web应用防火墙(WAF)安全报表向您展示WAF各个防护模块的防护记录。您可以使用安全报表查看WAF已防护域名的Web安全、Bot管理、访问控制/限流防护记录,进行业务安全分析。

### (!) 注意:

本文介绍的安全报表功能对应2020年1月发布的新版控制台界面,新版界面目前仅向中国内地地域 开放。如果您使用在此日期前开通的Web应用防火墙实例或海外地区服务,请参见#unique\_6。

### 前提条件

- 已开通Web应用防火墙实例。更多信息,请参见#unique\_7。
- 已完成网站接入。更多信息,请参见#unique\_8。
- 按量付费开通的Web应用防火墙实例,必须在中开启**提供业务分析报表**。更多信息,请参见#unique\_9。

#### 访问报表页面

- 1. 登录Web应用防火墙控制台。
- 2. 在顶部菜单栏,选择Web应用防火墙实例的资源组和地域(中国内地、)。
- 3. 在左侧导航栏,单击。
- 在安全报表页面,通过页签选择要查看的报表类型(Web安全、Bot管理、访问控制/限流),查 看对应报表。

#### Web安全报表解读

Web安全报表展示了Web入侵防护、防敏感信息泄露、账户安全和主动防御模块的防护记录。

• Web入侵防护:展示WAF阻断的所有Web应用攻击,分为攻击统计信息(图示中①)和攻击详情 记录(图示中②)。您可以使用域名、查询时间搜索某个域名在查询时间范围内的数据。

Web 安全 Bot 管理 访问控制/限流												
Web入侵防护	防敏感信息泄漏 則	印安全 主动防御										
全部	~ B	t天 今天 7天 S	80天 2020年	E4月21日 00:00 - 2	2020年5月21日 15:45	<b>崗</b> 搜索						
1 安全攻击类型分	布			攻击来源IP TOP5				攻击来源区	域 TOP5			
				;(北京)			28	澳大利亚				64
				?(澳大利亚)			24	北京				41
		webshell 00.38%		1(演大利亚)			21	陕西				1
		) 跨站脚本 0.94%					11	暂无数据				0
				■(澳大利亚)			8	暂无数据				0
正则防护	✓ 全部	~	攻击IP	搜索								
2 攻击IP	所属地区	攻击时间	攻击类型	攻击URL	请求方法	请求参数	规则录	加作	规则ID	攻击概率	操作	
2	中国 北京	2020年5月20日 13:37	其他		GET		阻断		200054		查看详情	
2	中国 北京	2020年5月20日 13:37	其他		GET		阻断		200054		查看详情	
?	中国 北京	2020年5月20日 13:37	其他		GET		阻断		200054		查看详情	
2	中国 北京	2020年5月20日 13:37	其他		GET		阻断		200054		查看详情	
2	中国 北京	2020年5月20日 13:37	其他		GET		阻断		200054		查看详情	
2	中国 北京	2020年5月20日 13:37	其他		GET		阻断		200054		查看详情	
2	中国 北京	2020年5月20日 13:37	其他		GET		阻断		200054		查看详情	
	演大利亚 演大利亚	2020年5月20日 12:02	webshell		GET		阻断		117028		查看详情	
	澳大利亚 澳大利亚	2020年5月20日 12:02	webshell		GET		阻断		117028		查看详情	
	演大利亚 演大利亚	2020年5月20日 12:02	webshell		GET		阻断		117028		查看详情	
	澳大利亚 澳大利亚	2020年5月20日 12:02	webshell		GET		阻断		117028		查看详情	
						共1	7 条,每页	10条 每页5	示 10   50	100 く 上一页	1 2 下-	页 >

- 攻击统计信息包括安全攻击类型分布、攻击来源IP TOP5和攻击来源区域 TOP5。

- 攻击详情记录展示Web攻击的详细信息,包括**攻击IP、所属地区、攻击时间、攻击类型、攻** 击URL、请求方法、请求参数、规则动作、规则ID、攻击概率。您可以使用防护模块(正则防 护、深度学习)、攻击类型(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、其他)或攻击IP筛选您关注的记录。

单击某个记录操作列下的**查看详情**,可以查看**攻击详情**。

攻击详情	
规则ID	200054
规则动作	阻断
攻击类型	其他
攻击IP	
所属地区	中国 北京
请求方法	GET
URL	/1.mdb
Trace Id	T0Tu01u10000000T0000T400u4144

关于Web入侵防护的设置方法,请参见以下文档:

- #unique\_10
- #unique\_11
- 防敏感信息泄露:展示触发了防敏感信息泄露规则的Web请求记录,包括攻击IP、所属地区、攻击时间、攻击URL、请求方法、请求参数、规则动作、规则ID、攻击概率。您可以使用域名、查询时间搜索某个域名在查询时间范围内的数据。

Web 安全	Bot 管理 访问控制	削/限流							
Web入侵防	护防敏感信息泄漏	账户安全 主动防御							
, and the	~	昨天 今天 7天 30	天 2020年4月21日 00:00	- 2020年	5月21日 16:09	<b>歯</b> 搜索			
攻击IP	所属地区	攻击时间	攻击URL	请求方法	请求参数	规则动作	规则ID	攻击概率	操作
					没有数据				

单击某个记录操作列下的**查看详情**,可以查看**攻击详情**。

关于防敏感信息泄露的设置方法,请参见#unique\_12。

账户安全:展示在账户安全中配置的防护接口上发生的风险事件记录,包括所属域名、接口、异常时间段、已拦截量/总请求量和告警原因。您可以使用域名、接口、查询时间搜索您关注的记录。

Web 安全	Bot 管理 访	问控制/限流						
Web入侵防护	防敏感信息泄漏	账户安全 主动防御						
	.com	∨ /ada	> 昨天	今天 7天	30天			报表解读   防护建议
所属域名		渡口		异常时间段		已拦截量 / 总请求量	告警原因	
					没有数据			

关于账户安全的设置方法,请参见#unique\_13。

主动防御:展示触发了主动防御自动生成的防护规则的Web应用攻击记录,包括攻击IP、所属地区、攻击时间、攻击URL、请求方法、规则动作、规则ID、攻击概率。您可以使用域名、查询时间搜索某个域名在查询时间范围内的数据。

Web 安全	Bot 管理 访	问控制/限流							
Web入侵防持	户 防敏感信息消	山漏 账户的	安全 主动防御						
_		~ 昨天	今天 7天 30天	2020年4月21日 00:00	- 2020年5月21日 16:24	<b>歯</b> 搜索			
攻击IP	所属	也区	攻击时间	攻击URL	请求方法	规则动作	规则ID	攻击概率	操作
					没有数据				

单击某个记录操作列下的查看详情,可以查看攻击详情。

关于主动防御的设置方法,请参见#unique\_14。

#### Bot管理报表解读

Bot管理报表展示网站业务的爬虫请求监控数据,包括**趋势数据**和近10分钟实时监控数据。您可以使 用域名、查询时间搜索某个域名在查询时间范围内的数据。

Web 安全	E Bot 管理	访问控	制/限流																
	com	~	昨天	今天	7天	30天	2020年3月2	日 00:00		- 2020	)年4月1日14	4:31	ė	搜索					
趋势数据																			
防护概	<b>览</b> 拦截分	析																	
(次/5分钟	中)																	统计信息	ĩ
	1																		
0.1	в																		
0.0	5																		
0.4	4																		
0.3	2																		
2020年3	3月2日 00:00	2020年	3月7日 0	4:00	202	0年3月	12日 08:00	2020年	E3月1	7日 12:00	2020	)年3月22	日 16:0	0 202	:0年3月27	日 20:00	)		
								━━ 请求量	-	拦截量									
近10分钟	的实时监控																		
城名	防护模块	策略名称	状态		14:31		14:30	14:29		14:28	14:27	14	26	14:25	14:	24	14:23	14:	22
	没有数据																		

- 趋势数据分为防护概览和拦截分析。防护概览展示了总请求量和触发了不同防护模块下策略的爬
  虫请求数量的趋势图。拦截分析展示了请求量和拦截量的相对趋势图。
- 近10分钟实时监控:展示近10分钟内触发了不同防护模块下策略的爬虫请求记录。

关于Bot管理的设置方法,请参见以下文档:

- #unique\_15
- #unique\_16
- #unique\_17

#### 访问控制/限流报表解读

访问控制/限流报表展示触发了CC安全防护、扫描防护和访问控制规则的Web请求记录。您可以使用 域名、查询时间搜索某个域名在查询时间范围内的数据。对于您关注的数据,也可以一键查询相关的 日志。

## • CC安全防护:展示CC防护趋势,包括总QPS、自定义CC告警、自定义CC拦截、CC系统拦截的数量趋势,和不同规则类型(包括自定义CC告警、自定义CC拦截、CC系统拦截)的匹配次数。



单击某个**规则类型的匹配次数**,将会跳转到**日志服务**页面,并自动输入与**CC安全防护**模块相关的 日志查询语句,方便您进一步查询相关日志。更多信息,请参见#unique\_18。

→
日志查询  日志分析
@ waf-logstore
<pre>v 1 matched_host:"</pre>

关于CC安全防护的设置方法,请参见#unique\_19。

关于自定义CC防护规则的设置方法,请参见#unique\_20。

扫描防护:展示扫描防护趋势,包括总QPS、目录遍历防护、协同防御、高频Web攻击、扫描工具封禁的数量趋势,和不同规则类型(包括目录遍历防护、协同防御、高频Web攻击、扫描工具封禁)的匹配次数。



## 单击某个规则类型的匹配次数,将会跳转到日志服务页面,并自动输入与扫描防护模块相关的日志查询语句,方便您进一步查询相关日志。更多信息,请参见#unique\_18。

.com	▶ 秋杰 🜑 该域名已开启日志服务状态,更多域名统一设置,在"网站配置"列表统一完成。
日志查询日志分析	
∅ waf-logstore	
✓ 1 matched_host	:" .com" and block_action: antiscan

关于扫描防护的设置方法,请参见#unique\_21。

 访问控制展示访问控制趋势,包括总QPS、ACL访问控制拦截、ACL访问控制告警、黑名单防护的 数量趋势,和自定义规则的匹配次数记录。



单击某个自定义规则的**规则ID**,将会打开**编辑规则**对话框,支持查看和修改当前自定义规则的配置。更多信息,请参见自定义规则参数描述。

编辑规则			×
规则名称			
<b>匹配条件</b> (条件之间为"且"关系)			
匹配字段 ?	逻辑符	匹配内容	
URL	∨ 包含	∼ acl	×
+ 新增条件 最多支持5个条件			
频率设置 🔵 执行并命中上述精	准条件后,启动频率设	置校验	
处置动作			
JS验证 V			
防护类型			
◎ CC攻击防护 ○ ACL访问控制			
			保存取消

单击某个自定义规则的**匹配次数**,将会跳转到**日志服务**页面,并自动输入与**访问控制**模块相关的 日志查询语句,方便您进一步查询相关日志。更多信息,请参见#unique\_18。

	✓ 状态 ● 该域名已开启日志服务状态,更多域名统一设置,在"网站配置"列	表统一完成。
日志查询日志分析		
𝔍 waf-logstore		
✓ 1 matched_host	and block_action: acl	

关于访问控制规则的设置方法,请参见#unique\_20。

关于IP黑名单的设置方法,请参见#unique\_22。

### 3 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。



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。



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。

展示项	描述
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。

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。

ഘ	
	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。



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



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。

可抑化大屈服条	不需要	单屈服备	多屈服备		
S Dardy Christop	T most		J 1111000		
	可视化大屏服务:提供M	站整体业务及安全状况的	的可视化大屏分析。	,里屏仅可选择1项,多屏不做限制,以条统支持的数量为准。	

- 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。

