



Web应用防火墙 Web应用防火墙公共云合集

文档版本: 20210318



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。

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

通用约定

格式	说明	样例
⚠ 危险	该类警示信息将导致系统重大变更甚至故 障,或者导致人身伤害等结果。	介 危险 重置操作将丢失用户配置数据。
▲ 警告	该类警示信息可能会导致系统重大变更甚 至故障,或者导致人身伤害等结果。	會学者 重启操作将导致业务中断,恢复业务 时间约十分钟。
〔) 注意	用于警示信息、补充说明等,是用户必须 了解的内容。	大) 注意 权重设置为0,该服务器不会再接受新 请求。
? 说明	用于补充说明、最佳实践、窍门等 <i>,</i> 不是 用户必须了解的内容。	⑦ 说明 您也可以通过按Ctrl+A选中全部文 件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在 结果确认 页面,单击 确定 。
Courier字体	命令或代码。	执行 cd /d C:/window 命令,进入 Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid
[] 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 {act ive st and}

目录

1.查看WAF防护总览	05
2.WAF安全报表	12
3.资产识别	18
4.数据大屏	22
5.常见问题	27

1.查看WAF防护总览

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。

前提条件

- 已完成网站接入。更多信息,请参见网站接入。
- 已开启了WAF防护。

域名接入WAF后,WAF会自动为该域名开启**正则防护引擎**和CC**安全防护**模块,其他模块需要您手动开 启。更多信息,请参见概述。

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、海外地区)。
- 3. 在左侧导航栏,选择总览。
- 4. 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	~
实时 今天 7天 30天 自定义	
事件列表 应急漏洞	

⑦ 说明 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。

总览信息概述

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。在**应急漏洞防护详情**页面单击**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					
2020年5月26日 00:51				更新Fastjson <= 1.2.68全版本远程代码	执行防护规则
	900			已防护资产数 全部资产数	
2020年6月24日 00:51 📖				4 5	
事件列表 应急漏洞		A			
	2020年5月26日 00:51 2020年5月29日 11:51 20	2020年6月1日 22:51 2020年6月5日 09:51 2020年6月8日	3 20:51 20	漏洞及防护规则 详慎	
更新注意做ecology超权运力防护规则 更新时间: 2020年6月14日		💼 全部 🚃 Web入侵防护 🚃 CC安全防护		应急开始时间	规则发布时间
2011-11-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-				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防护规则	Browser分布 UA Top		URL请求次遵	漏洞名称	漏洞ID
更新时间: 2020年6月5日				更斯Fastjson <= 1.2.68金版本运程代码执行防护规则	#08/00
更新用友NC远程代码执行防护规则			wat.watqa3.cc	²⁰²⁰ Fastison <=1.2.68全版本远程代码执行	113311
更新时间: 2020年6月5日			1006.wafqa3.c	应用类型	防护英型
更新fastion <= 1.2.68全版本远程代码执行			1006.wafqa3.c	GENERAL	code_exec
的社会规则		orobot/spider 66.46%	1006.wafqa3.c	规则描述	
更新时间: 2020年5月28日		downloading tool 32.87%	1006.wafqa3.c	此规则阻止利用Fastjson <=1.2.68全版本远程代码执行,	攻击者可以构恶意请求对服务器进行远程代码执行攻击,
更新FasterXML jackson-databind远程代码执		chrome 0.62%	1006.wafga3.c	支配4月15月版44:20週: Pastjson <=1.2.08 位別仕以下近洋籠	E1247 : - HITP request UKI - HITP request bodym
行防护规则(databind#2704)		● 其他 0.05%	1006		
更新时间:2020年5月8日					
meriCaster/VML instrone databilite的平理伊拉拉			gartner.wafqa		

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。 ⑦ 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。

您可以单击聚合后的事件,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。

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。

⑦ 说明 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,请参见防护引擎全面升级。

0.07			100101004-04	Sala 200 Like alasi	
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
	\sim		\sim		

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WAF 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。

⑦ 说明 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	疠护	扫描防护		访问控制		Bot 防护	
1,710 次	95次	33次		106次		21次		0次	
M									
1,:	198	80	18		72		15	智无数据	0
	467	15	15		34		6	暂无数据	0
	29 智无数据	0 暫无数据	0	暂无数据	0	暂无数据	0	暂无数据	0
	16 暂无数据	0 暫无数据	0	暂无数据	0	暂无数据	0	暂无数据	0
- 暫无数据	0 暂无数据	0 暫无数据	0	暂无数据	0	暂无数据	0	暂无数据	0
L									

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)。

? 说明

- 。 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, 请参见防护引擎全面升级。

○ **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。

⑦ 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等异常响应码的数量趋势。

② 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。

防护总览

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	Тор ІР	
	/collect/log	2,796
	/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
	/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。

⑦ 说明 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.WAF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。

前提条件

- 已完成网站接入。更多信息,请参见网站接入。
- 已开启了WAF防护。

域名接入WAF后,WAF会自动为该域名开启**规则防护引擎**和CC**安全防护**模块,其他模块需要您手动开 启。更多信息,请参见概述。

如果您购买的是按量计费的WAF实例,则必须在功能与规格设置中开启提供业务分析报表,才能使用安全报表。更多信息,请参见功能与规格设置(按量付费模式)。

查看安全报表

- 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、海外地区)。
- 3. 在左侧导航栏,选择安全报表。
- 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。关于不同报表的具体说明,请分别参见以下内容:
 - o Web安全报表说明
 - o Bot管理报表说明
 - 访问控制/限流报表说明

Web安全报表说明

Web安全报表展示了Web入侵防护、防敏感信息泄露、账户安全、主动防御模块的防护记录,单击页签可以切换报表。

 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	防敏感信息泄露	容 账户安全 主	动防御					0			
全部		∨ 昨天 今天	5 7天 305	天 2021年2月16日 00:00	- 20	21年3月18日 11:00	Ē	搜索			
安全攻击势	类型分布			攻击来源IP TOP5				攻击来测	原区域 TOP5		
		● 其他 74.41%	6	3. 1(新加坡)		315	i,304	美国			463,018
		 SQL注入 13. webshell 6.1 	70% 14%	4. 1(美国)		171	,958	新加坡			360,128
		 远程文件包含 代码执行 01 	5.48%	6. 1(美国)		137	,888	乌克兰			24,142
		 本地文件包含 	0.11%	8. 1(美国)		75	i,985	中国(浙	I)		1,621
		 ● 跨站脚本 0.0 ● 定制规则 0.0 	16% 10%	121(美国)		46	6,327	未知			1,380
										•	
规则防护	~	全部	~	攻击IP	规则	ID		全部		✓ 搜索	
攻击IP	所属区域	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	操作
11. 3	美国 美国	2021年3月17日 22:18	webshell	ts25- wafq	GET		阻断	ŕ	117028		查看详情 误报屏蔽
113	美国 美国	2021年3月17日 22:18	webshell	ts25- .wafq	GET		阻断	ŕ	117028		查看详情 误报屏蔽

- 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、所属区域、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和攻击概率。

您可以使用以下字段筛选您关注的记录:

- 防护模块: 支持选择规则防护、深度学习。
- 攻击类型:支持选择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、定制规则、其他。
- 攻击IP
- 防护规则ID

您可以对攻击记录执行以下操作:

■ 单击攻击记录操作列下的**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	T0TL01LL+0000030T000CT+02.u+1+H

 如果您确认某条攻击记录是正常业务请求,后续不希望WAF阻断具有相同特征的请求,可以单击攻击 记录操作列下的误报屏蔽。

该操作将会根据当前攻击记录的特征,自动生成一条Web入侵防护白名单规则,使WAF后续不对具有 相同特征的请求执行对应的系统规则检测。在弹出的**新建规则**对话框,您只需为自动生成的规则设 置规则名称,并单击保存。

⑦ 说明 极少数情况下,一个请求可能因同时触发多个防护规则被阻断,而通过误报屏蔽生成的白名单规则仅不检测其中一个防护规则。这时,您可以手动修改白名单规则中的特定规则
 ID参数,将不需要检测的其他规则ID添加进来,并通过钉钉服务群或提交工单向我们反馈该误报记录。

新建规则							×
规则名称							
支持不超过50个英文字符,要	的学习汉字						
字段不能为空							
匹配条件 (条件之间为"目"关于	E)						
匹配字段 ②			逻辑符		匹配内容 ②		
URL		\sim	包含	~	/100		×
+ 新增条件最多支持5个条件							
不检测模块							
☑ 规则防护引擎 □ 深度学习	99]擎						
○ 全部规则							
● 特定規则ⅠD	200054 ×						
○ 特定规则类型			1				
L							
						保存	取満

成功创建规则后,规则自动启用。您可以在Web入侵防护-白名单页面,查询、编辑、删除已有规则。相关操作,请参见设置Web入侵防护白名单。

关于Web入侵防护的设置方法,请参见以下文档:

- o 设置规则防护引擎
- 设置大数据深度学习引擎
- 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和攻击概率。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。

您可以单击某个记录操作列下的查看详情,查看攻击详情。

关于防敏感信息泄露的设置方法,请参见设置防敏感信息泄露。

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。

关于账户安全的设置方法,请参见设置账户安全。

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和攻击概率。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。

您可以单击某个记录操作列下的查看详情,查看攻击详情。

关于主动防御的设置方法,请参见设置主动防御。

Bot管理报表说明

Bot管理报表展示了网站业务的爬虫请求监控数据和防爬规则的防护效果数据。您需要单击左上角防护域名 列表,选择要查看的域名,通过指定的查询时间,搜索某个域名在查询时间范围内的防护效果数据。WAF对 每个已配置的防爬场景化规则提供独立的防护效果报表。

- Bot管理报表分为防护效果总览和场景化防护效果两部分。防护效果总览展示了总请求量、Bot识别量 和触发了不同防护规则的爬虫请求数量的趋势图。
- Bot识别量:通过多维度的流量特征综合分析出的机器流量总和,可以辅助判断当前配置防爬规则的防护效果(如果实际拦截量远低于识别量,表示防护效果还可以进一步优化;如果实际拦截量接近识别量,表示防护效果良好)。
- 观察模式命中量:设置为观察模式的防爬规则命中的请求量。如果将观察模式改成防护模式,这部分流量将被拦截或挑战(如滑块校验)。
- 实际阻断量: 命中防爬规则中处置动作为拦截模式的请求量。

关于Bot管理的设置方法,请参见以下文档:

- 配置浏览器访问网页的防爬场景化规则
- 设置合法爬虫规则
- 设置爬虫威胁情报规则
- 设置App防护

访问控制/限流报表说明

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。

Web 安全	Bot 管理	访问控	淛/限流																			
CC安全防护	扫描防护	访问招	空制																			
全部		~	昨天	今天	7天	30天	2020年4月]21日 00:0	00	- 2020	年5月21	日 16:29	İ	搜索								
6 5 4 3 2 1 0 :020年4月21日 0	10:00 20)20年4月2	·5日 03:00	20	20年4月	29日 0	6:00	2020年5月 急QPS	■ 13日 09:00 自定义CC	20. 吉蓉	20年5月 自定义(7日 12:00	202 ■ CC系统	0年5月1 拦截	1日 15:00	2020	年5月15	日 18:00	20	20年5月	1 9⊟ 21:	00
规则类型										P	工配次数	τ										
自定义CC告答										C												
自定义CC拦截										C												
CC系统拦截										C												

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,请参见使用日志查询。

日志分析 ② waf-logstore ✓ 1 matched_host:" and block_action: tmd	, .com	/ 状态 ● 该城名已开启日志服务状态,更多城名统一设置,在"网站配置"列表统一完成。
Waf-logstore Imatched_host:"	日志查询 日志分析	
v 1 matched_host: " and block_action: tmd	∅ waf-logstore	
	✓ 1 matched_host:"	.com" and block_action: tmd

关于CC安全防护的设置方法,请参见设置CC安全防护。

关于自定义CC防护规则的设置方法,请参见设置自定义防护策略。

● 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,请参见使用日志查询。

.com	▶ 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	
∅ waf-logstore	
✓ 1 matched_host	:" .com" and block_action: antiscan

关于扫描防护的设置方法,请参见设置扫描防护。

 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			
匹配条件 (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	挂条件后, 启动频率设置	置校验	
处置动作			
JS验证 V			
防护类型			
◎ CC攻击防护			
			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,请参见使用日志查询。

	★本 ● 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:"J	and block_action: acl	

关于访问控制规则的设置方法,请参见设置自定义防护策略。

关于IP黑名单的设置方法,请参见设置IP黑名单。

3.资产识别

Web应用防火墙(WAF)提供资产识别功能。通过获取阿里云证书、云解析、Web应用防火墙、万网等产品的配置信息,结合大数据关联分析能力,主动发现云上与云下的域名资产,为您提供全局资产视角,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。

背景信息

⑦ 说明 资产识别模块支持检测的网站资源覆盖阿里云域名和非阿里云域名(非阿里云域名包括解析 至非阿里云服务器的域名和线下IDC机房使用的域名)。

网络应用资产是安全管理体系中最基础的载体,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。信息安全领域存在典型的木桶效应,即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。

资产识别模块基于阿里云默认Web攻击检测能力,结合威胁情报,计算出云上域名的安全分值,帮助您发现 被攻击者关注的域名,及时接入防护,避免遭受入侵。

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Web应用防火墙读取您云账号中相关云服务的网站信息和管理云解 析DNS服务的域名解析记录的权限。

↓ 注意 您只需在首次访问资产识别功能时进行授权。如果您已完成授权,则无需重复操作。

- 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、海外地区)。
- 3. 在左侧导航栏,选择资产中心 > 资产识别。
- 4. 在资产识别页面,单击立即授权。



一 说明 只有在您自人切问员**,以别**页面时,才会出现**立即投权**。如来您已经无规过投权,则 不会出现**立即授权**。

5. 在云资源访问授权页面,单击同意授权,授权Web应用防火墙访问您账号中相关云产品的资源。

云资源访问授权			
温馨提示:如素修改角色权限,请前往RAM控制台角色管理中设置,需要注意的是,错误的配置可能导致WAF无法获取到必要的权限。	×		
WAF请求获取访问您云资源的权限 下方是系统创建的可供WAF使用的角色,授权后,WAF拥有对您云资源相应的访问权限。			
✓ AliyunWAFAssetsManageRole 描述:云盾应用防火墙(WAF)默认使用此角色来访问您在其他云产品中的资源 权限描述:用于云盾应用防火墙(WAF)服务角色的授权策略			
同意授权取消			

授权完成后,Web应用防火墙将主动发现您云账号中的网络域名资产。

查看域名资产和添加防护

- 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、海外地区)。
- 3. 在左侧导航栏,选择资产中心 > 资产识别。
- 4. 在资产识别页面,查看Web应用防火墙主动发现的您账号中的所有域名资产。

资产中	心 / 资产识别							
资	产识别							
全部	刷状态	➤ 请输入关键字进行域名模糊查询 搜索						
	域名	服务器地址	第日号	协议	指纹信息	安全评分 🕑	防护状态 🕗	攝作
-	gft					78	未防护	添加网站
	cdr	47.74. 138.2	80	M http		32	未防护	添加网站
	*.gf	163.1				78	未防护	添加网站
	cdr	09b84				80	未防护	添加网站

Web应用防火墙提供的域名资产信息如下:

资产信息	描述
服务器地址	域名服务器的IP地址。
端口号	域名服务器的端口。
协议	服务器与该域名通信的网络协议,支持HTTP和HTTPS协议。
指纹信息	 服务器的指纹信息。包括以下内容: 开发语言,如JAVA、PHP、ASP等。 中间件,如Nginx、Apache、Tomcat等。 开源或商业应用,如wordpress、dedecms、discuz等。 开发框架,如ThinkPHP、Django等。 组件,如Apache Shiro、Apereo CAS等。
安全评分	安全评分基于云上近30天攻击趋势结合威胁情报数据加权计算。安全评分越低,表 示风险越高。建议您尽快接入Web应用防火墙防护,以免遭受入侵。

资产信息	描述
防护状态	表示网站是否已接入Web应用防火墙进行全面防护。包含以下状态: 未防护:网站未接入Web应用防火墙进行防护。 部分防护:该泛解析域名下有部分域名已接入了Web应用防火墙进行防护。建议您排查剩余未接入的域名,及时接入WAF。 防护中:网站已接入Web应用防火墙进行防护,Web应用防火墙检测到网站流量且提供全面防护。

Web应用防火墙根据一级域名将检测发现的域名资产进行聚合展示。您可以在**资产识别**页面进行以下操作:

• 在域名资产列表上方可以筛选域名的防护状态,快速定位到未防护的域名列表。

资产中心 / 资产识别				
资产识别				
全部状态	^	请输入关键字进行域名模糊查询	搜索	
未防护		服务器地址		端口号
部分防护防护				
全部状态	~	47.74.1	74.138.2	80

- 在域名资产列表上方的搜索框中输入域名关键字,单击搜索,查询域名。域名搜索支持模糊查询。
- 在域名资产列表中,单击某个域名左侧的+,可以展开该主域名下所有的子域名列表,查看具体的域 名资产信息。
- 在域名资产列表中,点击操作列的添加域名,可以将该域名一键接入到WAF防护中。

⑦ 说明 添加域名时,如果控制台提示泛域名已经被其他用户开通,表示该域名已被其他云 账号接入Web应用防火的防护中,您无需重复接入。

○ 查看已接入Web应用防火墙的域名的资产详情。

⑦ 说明 只有已接入Web应用防火墙的域名才会展示资产详情信息。

a. 在域名资产列表,定位到要操作的域名,单击其操作列下的资产详情。

b. 在站点树区域,查看域名资产聚合后的URL、参数名、参数值类型和近一天内URL的请求次数。

⑦ 说明 为了避免展示的URL数量过多,站点树中的URL仅展示到路径级别。默认展示最多 三级并按照URL的请求次数排序,优先展示重要的资产。

操作说明如下:

- 您可以通过选择URL查询或扩展名并输入关键字,搜索特定的URL情况。
- 在URL列中,对于带有文件夹图标的URL,您可以单击URL进行展开或折叠展示URL信息。
- 在参数名|值类型列中,您可以查看URL涉及的参数名和参数值类型。

⑦ 说明 与URL相同,所展示的参数信息也经过大数据归一化算法进行泛化聚合。默认展示三个聚合后的参数名和对应的值类型,您可以将鼠标移至其右下角的更多图标查看所有参数。

基本信息				
域名:	.com	协议类型:	http,https	
防护状态	防护中	服务器地址	35	
站点树 URL查询 ~	· 新和人 - 「新来			
URL 🕑		参数名 值类型 🚱		1天请求次数
🎦 /internal_ap	yi			5,095,739
🗂 /interna	I_api/client_authentication_with_userInfo	password => 数字+字母混合 auth_username => 其它变量 endpoint_id => 数值	Θ	2,070,534
🖻 /interna	I_api/thirdPlatformProductInfo			1,613,301
🗂 /inte	ernal_api/thirdPlatformProductInfo/getProductInfo	!! => 其它安量 appKey => 其它安量 appSecret => 其它安量 ····		1,613,301

Web应用防火墙通过采集到的域名访问流量大小和流量特征对已接入防护的域名进行URL站点树分析,识别URL类型并进行分类。同时,站点树使用大数据泛化聚合算法(归一化算法)对URL和参数进行聚合展示。例如,系统会将以下新闻站点的具体URL聚合为/{字符+数字}.html的URL形式:

- /news1234.html
- /oldnews1223.html
- /news1224.html
- /news124.html

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。

⑦ 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。

⑦ 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 T OP10	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。

② **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	下方的日期回	J选择展示指定	E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。

⑦ 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。

中国大地 🗸		
	2) 1) 1) 1) 1) 1) 1) 1) 1) 1) 1	

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

⑦ 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。

可视化大屏服务	不需要	单屏服务	多屏服务				
	可视化大屏服务:提供例	网站整体业务及安全状况的	的可视化大屏分析。	单屏仅可选择1项,	多屏不做限制,	以系统支持的数量为准	E,

- 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。

⑦ 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。

5.常见问题

本文列举了阿里云Web应用防火墙(WAF)相关的常见问题。

类型	问题列表		
类型	问题列表 • 售前咨询问题 • 非阿里云服务器能否使用WAF? • WAF支持云虚拟主机吗? • WAF支持云虚拟主机吗? • WAF是否支持助护HTTPS业务? • WAF是否支持助护HTTPS业务? • WAFE的QPS限制规格是针对整个WAF实例汇总的QPS,还是配置的单个域名的QPS 上限? • WAF的QPS限制规格是针对整个WAF实例汇总的QPS,还是配置的单个域名的QPS 上限? • WAF的QPS限制规格是针对整个WAF实例汇总的QPS,还是配置的单个域名的QPS 上限? • WAF的QPS限制规格是针对整个WAF实例汇总的QPS,还是配置的单个域名的QPS 上限? • WAF的QPS限制规格是针对整个WAF实例汇总的QPS,还是配置的单个域名的QPS 上限? • WAF的QPS限制规格是针对整个WAF实例汇总的QPS,还是配置的单个域名的QPS 上限? • WAF配要型数有关WS • WAF配互为规定、 • WAF更多支持接入采用NTLM协议认证的网站? • WAF包互助数 • 按量计费(旧版)常见问题 • 按量计费(目版)常见问题 • 按量计费(回版)常见问题 • 按量计费(回版)常见问题 • WAF配置PDL或量它与内间题 • WAF配置DL机构实际的网站? • WAF配置多个源达的如何负载? • WAF配置多个源达时问载案? • WAF配置多大资金结保持? • WAF配置的内载和阳器PR型和人安全组? • WAF配置PL是否能够防御DDOS政击? • WAF配强是否支持使用透明技入和CNAME接入两种模式? • WAF能和CDN或DDS高防一起接入吗? • WAF配要和是我的好更? • WAF配量可是否能够防御DDOS政击? • WAF配具否或并参照表入和LTAME接入两种模式? • WAF能和CDN或DDS高防一起接入吗? • WAF電表型使用式。按如或名型 • WAFL是否支持使用透明技入和CNAME接入两种模式? • 透明接入后、源站可以获取客户端的真实PMB? • MAFL是否支持使用透明发流和LTAME接入器和LMAME接入 使用 • 一个域名是否支持使用透明支入使其中		
	 ▲影响? ● 透明接入时为什么看不到我需要接入的七层SLB实例? 		
	■ 网站的扩配直回题		

类型	◎ WAF如何防御CC攻击? 问题列表 ◎ 在WAF管理控制台更改配置后大约需要多久生效?
	• WAF自定义防护策略(ACL访问控制)中的IP字段是否支持填写网段?
	● 为什么URL匹配字段包含双斜杠(//)的自定义防护策略规则不会生效?
	● 网站防护分析问题
	◎ WAF管理控制台中能查看CC攻击的攻击者IP吗?
	◎ 如何查询WAF使用的带宽流量?
	● 网站访问异常
	● HTTPS访问异常问题
网站访问专题	 SNI兼容性导致HTTPS访问异常(服务器证书不可信)
	• 已配置WAF防护的ECS源站遭受入侵的处理建议
	● WAF被黑洞怎么解决
	● 支持防护的域名后缀
	• 已接入网站的未配置端口是否会对源站带来安全风险?
产品配置	● Web应用防火墙流量访问示意图
	 ● CC攻击防护攻击紧急模式
	● 遇到405报错怎么解决?
	● 非标端口业务无法接入Web应用防火墙高级版
	● 上传HTTPS证书时提示"Https私钥格式错误"
故障分析	● Web应用防火墙拦截上传文件的请求
	● 登录状态丢失怎么解决?
	● 长连接超时问题
	● Web应用防火墙:产品经理、安全专家"面对面"
服夯奀	• 云解析版本产品规格
	● 営贝Web漏洞释义
知识点	● 为什么不能直接访问WAF生成的CNAME域名?