

产品文档



0

文档目录

产品简介

 \mathbf{i}

产品介绍

功能简介

主要功能

为何需要WAF

基础防御流程

产品优势

专业的网站防护能力

及时的补丁修复保障

稳定的高可用业务保障

ipv6安全防护

应用场景

政务网站防护

电商网站防护

金融网站防护

防数据泄密

操作指南

AI检测及管理

功能简介

注意事项

配置示例

CC 攻击防护设置

功能简介

配置示例

地域封禁设置

功能简介

配置说明

自定义策略防护设置

功能简介

注意事项

配置说明

IP黑白名单防护设置

功能简介

注意事项

配置示例

快速入门

一、添加域名

二、本地测试

常见问题

如何定位是否为龙御WAF拦截

如何分析拦截原因

日常运营中如何进行误拦截处置

如何进行AI引擎在线学习

如何添加自定义放行规则

CLB型WAF域名访问故障时如何应急

龙御WAF中各类自定义配置的优先级是什么

产品简介 产品介绍 功能简介

 \mathbf{i}

最近更新时间: 2023-02-09 14:48:23

Web应用防火墙(Web Application Firewall, WAF)基于AI+规则进行Web攻击识别,实时阻断SQL注入、XSS跨 站脚本、Webshell木马上传等常见的Web威胁攻击,并联动封禁产品进行恶意IP的封禁。 建行云为负载均衡WAF版本,通过域名与建行云七层负载均衡集群进行联动,对经过负载均衡的HTTP和HTTPS流 量进行威胁检测,并将检测结果发送给负载均衡,负载均衡根据检测结果直接拦截页面或者向后端云服务器转发, 实现业务转发和安全防护分离。

主要功能

C

最近更新时间: 2023-02-09 14:48:23

功能	简介
Al+Web应用防火墙	基于Al+规则的Web攻击识别,防绕过、低漏报、精准有效防御常见Web攻击,如SQL 注入、XSS跨站脚本、CSRF跨站请求伪造、web应用漏洞攻击,Webshell木马上传 等OWASP定义的十大Web安全威胁攻击
CC 攻击防御	多维度自定义精准访问控制、配合频率控制等对抗手段,高效控制访问频率及缓解 CC 攻击问题
IP黑白名单	可设置某个域名或者APPID下所有域名的IP黑/白名单规则,只支持IPV4地址,CC防 护命中的IP也在IP黑名单中查询到
自定义策略	自定义策略,根据租户需求可灵活配置,如对于来源ip、referer、请求路径、HTTP请 求方法等。动作可选择放行、阻断、人机识别、观察、重定向。
地域封禁	地域封禁,按照内置地址库对境外国家/地区以及中国各大省市自治区进行封禁,阻断 该区域的所有来源IP的访问,支持IPV4/IPV6地址
联动封禁	龙御waf对非自定义策略类拦截(自定义策略包括包括cc、ip黑名单、自定义阻断、地 域封禁)联动天幕进行封禁操作,减小攻击成功的可能性

为何需要WAF

最近更新时间: 2023-02-09 14:48:23

在以下场景中,使用 WAF 均可有效防御以及预防,保障企业网站的系统以及业务安全。

• 数据泄露(核心信息资产泄露)

Web 站点作为很多企业信息资产的入口,黑客可以通过 Web 入侵进行企业信息资产的盗取,对企业造成不可估量的损失。

• 恶意访问和数据抓取(无法正常服务,被商业竞争对手利用数据)

黑客控制肉鸡对 Web 站点发动 CC 攻击,资源耗尽而不能提供正常服务。恶意用户通过网络爬虫抓取网站的核 心内容(文学博客、招聘网 站、论坛网站、电商内的评论)电商网站被竞争对手刻意爬取商品详情进行研究。羊 毛党们试图搜寻低价商品信息或在营销大促前提前获取 情报寻找套利的可能。

• 网站被挂马被篡改(影响公信力和形象)

攻击者在获取 Web 站点或者服务器权限后,通过插入恶意代码来让用户执行恶意程序、赚取流量、盗取账号、 炫技等; 植入"黄、赌、非 法"链接; 篡改网页图片和文字; 对网站运行造成很大影响,损坏网站运营者的形象。 对外公信力和形象蒙受损失。

• 框架漏洞(补丁修复时段被攻击)

很多 Web 系统基于常见的开源框架如 Structs2、Spring、WordPress 等,这些框架常常爆出安全漏洞,但等待 安装补丁的维护时段,则是一段艰难和危险的过程,很多攻击会在漏洞公布之后一天内就遍地开花。

基础防御流程

最近更新时间: 2023-02-09 14:48:23

WAF 通过配置域名和建行云七层负载均衡(监听器)集群进行联动,对经过负载均衡的 HTTP/HTTPS 流量进行旁 路威胁检测和清洗,实现 业务转发和安全防护分离,最大限度减少安全防护对网站业务的影响,保护网站稳定运 行。



负载均衡型 WAF 提供两种流量处理模式:

镜像模式:通过域名进行关联,CLB 镜像流量到 WAF 集群,WAF 进行旁路检测和告警,不返回请求可信状态。



 清洗模式:通过域名进行关联,CLB 镜像流量到 WAF 集群,WAF 进行旁路检测和告警,同步请求可信状态, CLB 集群根据状态对请求 进行拦截或放行处理。



产品优势 专业的网站防护能力

最近更新时间: 2023-02-09 14:48:19

 云应用防火墙(龙御)拥有千余条防御规则结合AI模型检测全面防护各种Web入侵攻击、专业攻防团队迭代防护 系统,保障网站防御系统处于行业前沿。

及时的补丁修复保障

最近更新时间: 2023-02-09 14:48:19

• 可及时提供更新高危漏洞地补丁及常见通用型漏洞补丁服务。

稳定的高可用业务保障

最近更新时间: 2023-02-09 14:48:19

 \mathbf{O}

- 无感知接入, 毫秒级延迟, 域名接入 WAF 不需要调整现有的网络架构。
- 网站业务转发和安全防护分离,一键 bypass,保障网站业务安全、稳定可靠。

ipv6安全防护

最近更新时间: 2023-02-09 14:48:19

• 通过和建行云负载均衡进行联动,无缝处理 IPv4 和 IPv6 访问流量,使其具备同等安全防护能力,简单快捷。

应用场景 政务网站防护

最近更新时间: 2023-02-09 14:48:19

一键接入防御,轻松配置,隐藏并保护源站,保证网站内容不被黑客入侵篡改。保障网站信息正确,政府服务正常可用,民众访问满意畅通。

电商网站防护

最近更新时间: 2023-02-09 14:48:19

• 持续优化防护规则、精准拦截 Web 攻击,全面抵御 OWASP Top 10 Web 应用风险。在高并发抢购场景下,可 设定对于指定url的cc防护(基于ip或session),保障正常访问业务流畅。



金融网站防护

最近更新时间: 2023-02-09 14:48:19

一键接入防护,具备 Web 安全防护,可有效检测异常攻击行为,保护用户信息不外泄。云端资源优势,自动伸缩,轻松应对业务突发,大流量 CC 攻击。



防数据泄密

最近更新时间: 2023-02-09 14:48:19

• 避免因黑客的注入入侵攻击,导致网站核心数据被拖库泄露。 防 CC 攻击,防恶意 CC(HTTPFlood),通过在 七层阻断海量的恶意请求,保障网站可用性。

操作指南 AI检测及管理 功能简介

最近更新时间: 2023-02-09 15:07:37

AI引擎是云 Web 应用防火墙率先应用基于机器学习的 Web 攻击检测技术,通过 AI 引擎的检测模型及学习能力, 最大限度提高已知和未知 Web 威胁的检测率和捕获率,最大限度减少误报,并且灵活适应不断变化的 Web 应用。

注意事项

最近更新时间: 2023-02-09 15:07:37

添加AI漏报、误报后,AI模型会进行学习更新检测模型,请谨慎设置。

配置示例

最近更新时间: 2023-02-09 15:07:37

本章节将演示如何开启AI模型防护功能、对攻击负载进行AI模型的在线验证及误报的学习。

• 前置条件

相关测试域名已经配置了waf防护

• 示例

第一项:开启或关闭AI智能防护。

登陆租户控制台,进入云应用防火墙(龙御)界面下,选择相应域名点击防护配置,在基础防护下可以看到AI智能防 护功能(AI引擎具有三个选项:1、关闭,指关闭AI引擎防护功能;

2、观察,指AI引擎进行检测并记录相关日志但不进行拦截;3、拦截,指AI引擎既进行检测也进行拦截并记录拦截 日志)。

建行云	总览	云产品▼		zangchengj_ ▼ 费用 ▼ [⑦]
云应用防火墙	皆 (龙御) 《	🔶 防护设置	www.clbtest.com v	
概览		基础设置	自定义策略 CC防护设置2.0	
网站应用防火墙				0
防护设置				
规则引擎		WAF		
IP管理		1013	关闭WAF总开关后,所有的防护功能失效,WAF进入流量转发模式,不会拦截攻击行为也不会记录日志。	vieuzesaayy// XXX f==== 高级设置▼
日志服务		ter nu:	a100 843	Rhdomrifis
		「「「」「」「」「」「」「」「」「」「」「」「」「」「」「」「」「」」「」「」」「」」「」」「」」「」」「」」「」」」「」」「」」」「」」」「」」」「」」」「」」」「」」」」	apa www.clbtest.com	
		ID	waf-dNR36fvR In	AI引擎① 关闭 观察 <u>拦</u> 截
		(PTTTL)	PD 75	建议先开启观察模式一段时间(例如20天);在观察模式下,AI引擎后台会自动学习网站访问模式并进
		1(3±1)		行び404回臺塗,且較力量上型400%,均能会存在1000年的150%。这时以4号%中均186088223日451号进 行检测和学习,评估检测无误报后,建议开启拦截横式。如果其他缩问,请联系安全售后服务人员。
		绑定机		Lini-Britek
		流量相	葉式 ③ 特像模式 済況提式 ③	
		负载	均衡 - 监听器 の想はない (D) の想はないD 地町間	可以选择国内省份和海外地区进行封禁。了解更多
		武汉	以高記学習館 (10) 以高記学習館 (10) clbwafv4測読が完款(lb-10dv40 42.201.68.234 clbtest(HTTP:80) 102(HTTP:88)	已封禁地成 国内全部 国外全部

第二项:利用AI引擎验证攻击负载。

登陆租户控制台,进入云应用防火墙(龙御)界面下,选择Al引擎标签,点击Al在线验证,添加负载内容,点击立即 验证。如果验证为攻击,当请求内容中带有相关攻击负载会被Al引擎拦截并记录相关日志。

建行云	总览	云产品▼													zangchengj 🔻	裁用 ▼	1 0
云应用防火增	間 (龙御) 《	AI引擎															
概览		Ali具报处理	AI漏报处理	AI在线验	hiE												
网站应用防火墙			AP	(在线验证,提供)	了判定载荷是"正常"还是"	威胁数据" (SC	L注入、XSS	S、其他异常)的能	8方; 您可以根据	脸证结果,一個	對是交误报或漏报,然/	后在误报或漏报页面进行学习	. 了解更多 🖸		×		
防护设置																	
规则引擎																	
IP管理			1/51	inderit .	www.clbtest.com										0		
日志服务			12 12	(证参数*	参数类型			参数名称			参数值			操作			
					GET参数	Ŧ		请输入参数名称	\$r		a=alert(123)			删除			
											新增						
					A 072417												
					立的影響												
			验	证结果	一键添加误报												
			· 127	(证结果 (A)((本:+));===================================	威胁数据						处理时间	0.8ms					
			92	100-2011年11	AcomUCUL主人						攻击總数名称	/ 无					
			攻	击参数原始值	a=alert(123)												
			攻	法参数解码值	a=alert(123)												

第三项:对误报进行学习

登陆租户控制台,进入云应用防火墙(龙御)界面下,选择AI引擎标签,点击AI误报处理,手动添加负载内容(学习 内容为a=alert(123)),点击添加,然后选中添加内容点击学习。

建行云	总览	云产品▼							zangch	engj▼ 费用	• 🖻 0
云应用防火墙	(龙御) 《	AI引擎									
		Ali误报处理 Al漏拍	最处理 AI在线验证								
			您可以手动将误报的攻击	添加到此处,也可以在AI引擎检出的	攻击日志洋情中点	京击"误报"添加:添加之后,点击"学习",Al	引擎会根据误报信息更新模型	1. 优化算法,了解更多 🖸		×	
AI引擎			手动添加 删除	学习AI模型最后更新的	前司: 2022-09-15	10:19:17				Φ	
IP管理			序号 ID	载荷		来源	备注	创建时间 ↓	秋恋 ‡		
日志服务					添加误报		×				
					PayLoad *	a=alert(123)					
					备注	备注,非必填项					
						添加					
			共0项						每页显示行 20 * 📧 🕴 1/1 *		

建行云	总览	云产晶▼											zangchengj 🔻	裁用 ▼	0
云应用防火墙	(龙御) 《	AI引擎													
概览		Al误报处理	AI漏报	处理 A	AI在线	脸证									
网站应用防火墙				您可以手頭	动将误拍	灵的攻击添加到此处,也可以在Ali	目擊检出的攻击日志详情	青中点击"误报"添加;添加之后,点:	击"学习",AI引擎会根3	暑洪报信息更新模型、优化算法。了解更	\$ C		×		
AI引擎				手动添加		删除 学习 AI模型	最后更新时间: 2022-0	9-15 10:21:05					¢		
IP管理				序号	1	ID	载荷		来源	备注	创建时间 ↓	状态 ‡			
日志服务				1		63228bfdaaec5100eb48eae4	a=alert(123)		手动添加	无	2022-09-15 10:20:45	日学习			
				共1项							8	顾显示行 20 ▼ 🛛	< 1/1 ▼ > ×		

C

CC 攻击防护设置 功能简介

C

最近更新时间: 2023-02-09 16:55:56

CC策略是指攻击者通过工具,模拟多个用户不断向网站发送连接请求,导致用户业务不可用,添加 CC 防护规则,可以帮助用户防护针对页面请求的 CC 攻击。



配置示例

最近更新时间: 2023-02-09 16:55:56

本配置示例可实现,当单个源 IP 在 10 秒内访问/test.html超过 10 次,恶意访问惩罚功能将封禁此源 IP 30 分钟。

1、进入云应用防火墙(龙御) 主界面,单击【防护设置】,单击需要防护的站点域名,单击【CC防护设置】选项 卡进入恶意访问惩罚配置界

建行云 总览	云产品▼	✓ 删除成为I zangchengi *	费用▼ 1 1 0
云应用防火墙 (龙御) 《	← 防护设置 w	www.test.com *	CC助护设置操作指南 🖸
概览	基础设置 自定义	义策略 <u>CC防护设置2.0</u>	
网站应用防火墙 ~ 防护设置		CC 防护功能发持对公网用户访问将走 URL 的行为进行烦躁控制,人们识别,封禁恶孽幼能烦访问行为。了解更多 23 》	:
AI引擎		CECCIANIE	
規則引擎 IP管理 ~		定义SESSION, CO规则有启用SESSION, 则会基于SESSION维度进行统计和时指。	
日志服务			
		SESSION位型 未配置	
		匹徵機式 未 我還	
		会活际只 未產畫	
		规则名称 巴配条件 请求语径 访问频次 执行动作 启用SESSION 惩罚时长 优先缴 ↑ 规则开关 创建的词 ↓ 操作	
		· · · · · · · · · · · · · · · · · · ·	

2、单击【添加规则】,在规则名称输入框里面输入具体的规则名称、选择匹配条件(等于),具体的 URI(/test.html),以及访问频次(10次10秒),选择执行动作封禁访问(也可以选择人机识别,人机识别采用一 定的算法进行验证,如果验证失败后,将自动封禁访问),惩罚时长输入 10 分钟

云应用防火墙(龙	御) 《	添加CC防护	规则		×	
概览 网站应用防火墙		规则名称*	test			
		识别方式*				
AI引擎		匹配条件。	相等 🔻			
	÷.	URI路径*	/test.html			
		高级匹配 ▼ 🕄				
		访问频次*	10 次	10秒 - ③		
		执行动作*	拦截 マ	0		
		惩罚时长*	10 分钟	0		¢
		优先级	- 50 +			
			请输入1~100的整数,数字越小,	代表这条规则的执行优先级超高;相同优先级下,创建时间越晚,优先级超高		操作
				2530 RC36	2	8:21 编辑 删除

3、单击【添加】保存规则,此时规则将会生效,惩罚恶意访问行为。

云应用防火墙(龙御) «	设置时间	未配置									
 みらの 网站应用防火場 防护设置 AI引撃 	~	CC规则设置 添加规则	单个域名最多可以添加5:	条规则								¢
IP管理	~	规则名称	匹配条件	请求路径	访问频次	执行动作	启用SESSION	惩罚时长	优先级 ↑	规则开关	创建时间 ↓	操作
日志服务	~	test	相等	/test.html	10次/10秒	拦截	否	10分钟	50		2020-07-03 15:12:06	编辑删除
		共1项									每页显示行 10 -	H 4 1/1 ▼ → H

 \mathbf{i}

地域封禁设置 功能简介

 \bigcirc

最近更新时间: 2023-02-09 16:55:56

地域封禁指根据配置的地域(如北京),waf会根据配置的地域信息来拦截所在地域的ip地址的请求信息。目前支持 IPV4/IPV6地址。

配置说明

最近更新时间: 2023-02-09 16:55:56

1、登录控制台,单击【网站应用防火墙】>【防护设置】,选择需要防护的域名。

													-
建行云总宽	云产品▼									zangchengj 🔻 🛛	费用 ▼	⊠ 0	þ
云应用防火墙 (龙御) 《	^{负载均衡型} 防护设置										城名接入:	操作指南 🖸	*
网站应用防火墙 ~ 防护设置 A(引擎 规则引擎		域名列表 高加速名 开启 关闭 删除						支持城名、负载均衡名称	、监听器名称模糊搜索	Q			
IP管理 v		赋名/ID	流量模式①	区域	负载均衡 (ID)	负载均衡VIP()	监听器①	WAF开关 ▼	操作				
日志服务 ~		czh.com waf-87SmyfgG ⊘	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	test-czh(HTTP:8081)		删除 編輯 防护配置				
		d.com waf-qqAF2IGx ⊘	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置				
		C.com waf-PR8nE3i5 ⊘	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	test-hwl(HTTP:8001)		删除 编辑 防护配置				
		a.com waf-GcFCczsR 🥑	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	test-cry(HTTP:8002)		删除 编辑 防护配置				
		blj-1255000011.iss.com waf-j2MWecRc 🧭	清洗模式	武汉	堡垒机测试(lb-j8irt2vs)	2404:bc0:1:1400:0 253:b081:6139	0:9 堡垒机443(HTTPS:443)		删除 编辑 防护配置				
		www.cacc.com waf-PJQNvJ7z	清洗模式	武汉	新堡垒机测试(Ib-85disat8)	119.36.55.232	www.cscc.com(HTTP:90)		删除 編輯 防护配置				ł
		www.aaa.com waf-oAOtjjL9 🥥	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置				
		www.clbtest.com waf-dNB36fyB 🥥	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	clbtest(HTTP:80) 102(HTTP:88)		删除 编辑 防护配置				
		www.ccc.com waf-ofNr1HXX @	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置				

2、单击【基础设置】>【编辑封禁地区】,进入地域封禁配置界面。

建行云 总宽	云产品▼		切換封禁状态成功!		zangchengj マ 携用 マ 「 🗹 🕜
云应用防火墙 (龙御)	< 🧲 防护设置 www	clbtest.com v			
概览	基础设置 自定义策	踏 CC防护设置2.0			
网站应用防火墙					¢
防护设置					
AI引擎		WAF开关		WAF防护状态	
规则引擎		WAF状态 CO		Web基础防护 观察 拦战	
		关闭WAF总开关后,所有的防护功能失效,WAF进入流量转发模式,不会打	兰戴攻击行为也不会记录日志。	瀧级设置▼	
		基础配置	编辑	防护等级 宽松 正常 • 严格	规则管理
		城名 www.clbtest.com 后		AI智能防护	
		ID waf-dNB36fyB 🛅		A时学 ① 关闭 观察 益哉	
		代理協況 否		建议先开启观察模式一段时间(例如20天);在观察模式下,43引擎后台 行优化和调整;直接开启拦截模式,可能会存在低概率的误报。您可以#	a会自动学习网站访问模式并进 持续将可疑数据提交给AI引擎进
		御定状态 正常 ❷		行检测和学习,评估检测无误报后,建议开启拦截模式。如果其他疑问,	请联系安全售后服务人员。
		流星模式 ① 铜像模式 济济模式 ①		地域封禁	24
		合进均衡; 收邮架		封禁状态	
				可以选择国内省份和海外地区进行封禁。了解更多	
		武汉 clbwafv4测试·勿动(lb-10dv40 42.201.68.234 clbtest(HTTP:80) 102(HTTP:88)		已封禁地域 北京 国外全部	

3、勾选您要封禁的地区,单击【确定】。



4、此时,您选择封禁的地区将无法访问您的网站。以北京和国外为例,北京和国外被列入封禁地域后,以北京区域的IP 访问网站,云应用防火墙(龙御)会提示403 Forbidden。

403 Forbidden

自定义策略防护设置 功能简介

最近更新时间: 2023-02-09 16:55:56

 \bigcirc

自定义策略支持从HTTP报文的请求路径、GET参数、POST参数、Referer和User–Agent等多个特征进行组合,进 行特征匹配来对公网用户的访问进行管控。面对来自互联网上的各种攻击行为,用户可以利用自定义策略灵活应 对,组合出有针对性的规则来阻断各类攻击行为。

注意事项

 \bigcirc

最近更新时间: 2023-02-09 16:55:56

- 每个自定义策略最多可以设置5个条件进行特征控制。
- 每个自定义策略中的多个条件之间是"与"的关系,也就是所有条件全部匹配策略才生效。
- 每个自定义策略匹配之后可以配置多种动作: 放行、阻断、人机识别、观察、重定向。
- 如果选择放行模式,应尽量勾选继续执行其他防护,以减小白名单放行带来的风险。
- 如果是临时申请加白策略尽量指定截止时间。
- 自定义放行策略优于自定义阻断策略。



 \mathbf{i}

最近更新时间: 2023-02-09 16:55:56

• 案例一:禁止特定 IP 地址访问指定站点

1、登录控制台 , 单击【网站应用防火墙】>【防护设置】,选择需要防护的站点域名,单击【自定义策略】进入 自定义策略配置界面。

建行云总题	云产品▼				② 删除成功!					zangchengj 🔻 🛛	裁用 ▼	
云应用防火墙 (龙御)	≪ ← 防护设置 ***	w.test.com	•								自定义	規則操作指南 🖸
概范	基础设置 自定义	策略(CC防护设置2.0									
网站应用防火墙 ~		自定义的	策略支持从 HTTP 报文的请求路径、GE	T 参数、 POST 参数、 Referer 和 User-Agent f	等多个特征进行组合,进行特征匹配来对公网月	用户的访问进行管控	了解更多已			×		
AI引擎		添加规则	3 单个域名最多可以添加10条规则	9					请输入规则名称或匹配条件	Q Ø		
规则引擎		序号	规则名称	匹配条件	执行动作 ▼	创建时间	优先级 🛈	过期时间	规则开关	操作		
日志服务					记录为空							
		共0项							每页显示行 10 🔻 🖂	< 1/1 ▼ → H		

2、单击【添加规则】,输入规则名称(如 001),在匹配字段中选择一个字段(如来源 IP),逻辑符号选择匹配,匹配内容填入需要禁止访问的来源 IP(如117.136.0.211),选择执行(如阻断)。

建行云 总范	云产品,												zangchengj 🔻	2月 1 ⑦ 1 ⑦
云应用防火墙 (龙御) 。	← 防护设置	www.test.com		Ŧ										自定文規則操作指南已
概范 网站应用防火墙 ~	基础设置	定义策略 CCD 自定义策略	5护设置2.0										×	
MIPIE			添加规则								×			
规则引擎		10203	规则名称	001								加制人规则省称组织自动并		
■P管理 ~ 日志服会 ~		640	匹配条件 •	匹配字段		匹配參數	逻辑符号		匹配内容	操作		MANTA	DR11-	
H-0/80/03 *			(来源P	Ŧ	此字假不支持参数选择	匹配	Ŧ	17.136.0.211	删除				
							<mark>源加</mark> 还可以添加	4条,最多5条						
			执行动作。	阻断	*									
			截止时间 •	永久生效	٣									
			优先级。	- 100	+									
		12.015		调输入1~100的	整改,数字越小	, 代表这条规则的执行优先级越	高.					10 ▼ 16 1	1/1 - 3	
		700%					海加	i						

3、 同时, 云应用防火墙(龙御)的自定义策略支持使用掩码来控制某一网段的 源 IP 的访问请求。我们可以在 匹配内容中输入特定网段(如10.10.10.10/24)。

建行云 总宽			
云应用防火墙 (龙御)	★ 防护设置 www.test.com	•	自定义规则操作描意
概范 网站应用防火端 ~	基础设置 自定义策略 CC	55PQEE2.0	×
		添加規則 ×	
规则引擎	汤血用巴利	规则名称* 002	Q Q
IP管理 v	座号		操作
日志服务 🗸	90327		li Ble
		● 東原P ▼ 此方位不反片参数近降 正配 ▼ 10.10.10.10/24 割除	
		清加 还可以添加4条。最多5条	
		94(530)) * RBM *	
		截止22回。 参久生效 *	
		(税把限* - 100 +	
	共1项	清编入1~100的组织,数字接小,代表这些规则的执行优先家族驾。 第页显示行 10 + K < 1	/1 + → H
		减加 和2H	



建行云	总览	云产品▼									zangchengj 🔻 🛛	费用 ▼	⊠ ।	0
云应用防火堆	青 (龙御) 🔹	← 防护设置 🗤	w.test.com	Ŧ								自定义	规则操作的	a 🖻
概范		基础设置 自定义	(策略 C	C防护设置2.0										
网站应用防火增 防护设置			自定义务	發略支持从 HTTP 报文的请求路径、GET 参数、 POS	ST 参数、 Referer 和 User-Agent 等多个特征进行组	合,进行特征匹配来对公	☆网用户的访问进行管控。	了解更多 🗹			×			
AI引擎 规则引擎			添加规则	单个域名最多可以添加10条规则						请输入规则名称或匹配条件	Q Ø			
IP管理			序号	规则名称	匹配条件	执行动作 🔻	创建时间	优先级 ①	过期时间	规则开关	操作			
日志服务			90327	001	来源IP 匹配 117.136.0.211	阻断	2022-09-15 14:46:53	100	永不过期		编辑 删除			
			90328	002	来遯IP 匹配 10.10.10.10/24	阻断	2022-09-15 14:47:38	100	永不过期		编辑删除			
			共2项							每页显示行 10 * 14	∈ 1/1 × ⊨ ⊨			

• 案例二:禁止公网用户访问特定的Web资源

1、当网站管理员不希望公网用户访问某些特定的 Web 资源时(如管理后台/admin.html),可以在匹配字段中 选择请求路径,选择逻辑符号等于,匹配内容输入/admin.html ,执行选择阻断进行配置。

云应用防火墙(龙御)	«	泰加规则							×	É	自定义规则操作指	南 🖸
概览												
网站应用防火墙 ~	规	见则名称 *	test2						- 8			
防护设置 A121整	2	正配条件 •	匹配字段	匹配参数	逻辑符号		匹配内容	操作				~
IP管理 v	(Ð	请求路径 🔻	此字段不支持参数选择	等于	•	/admin.html	删除	±		Q. 操作	Ģ
日志服务 ~					添加 还可以添加4条	- 最多5条					2011	
									_ /		3編4群 前引称	
	ŧ	机行动作 *	阻断 ▼									
	樹	ى⊥时间 *	永久生效 🛛 🔻									
	Ø	尤先级 *	- 100 + 请输入1~100的整数,数字越小,	代表这条规则的执行优先级越	100 g							
					添加取消							
	共11	项						每页显	示行 10 ▼	H A	1/1 🔻 🕨	H

• 案例三:禁止某个外部站点盗链获取资源

1、当网站管理员需要阻断外部站点(如www.test.com)的盗链行为时,可以利用自定义策略对盗链请求的 Referer 特征进行捕获和阻断。 在匹配字段中选择 Referer ,选择逻辑符号包含,匹配内容输入



www.test.com, 执行选择阻断进行配置。

云应用防火墙(龙	卸)《	添加规则								×		自定义规则操作指南	新 (2)
网站应用防火墙	~	规则名称*	test3										
防护设置 AI引擎		匹配条件 *	匹配字段	匹配參数	逻	建辑符号		匹配内容	操作			Q	^
IP管理	×	Ū	Referer v	此字段不支持参数选择		包含 🔻		www.test.com	删除		*	播作	
日志服务	Ť				添加] 还可以添加4条,最	多5条)	编辑删除	
		执行动作・	阳断 👻)	编辑删除	
		截止时间 *	永久生效 🔻										
		优先级 *	- 100 + 请输入1~100的整数,数字越小,作	代表这条规则的执行优先级越高。									
				3	添加	取消							
		共2项							每页显	显示行 10	D 🖛 🖂	< 1/1 → →	М

IP黑白名单防护设置 功能简介

最近更新时间: 2023-02-09 16:58:56

C

IP黑白名单管理,可设置某个域名或者APPID下所有域名的IP黑/白名单规则,只支持IPV4地址。CC防护命中的IP也在IP黑名单中查询到。



注意事项

最近更新时间: 2023-02-09 16:58:56

- 添加IP白名单后,此IP的任何访问都不会被阻断,请谨慎设置。
- IP黑白名单功能不支持添加网段。

配置示例

最近更新时间: 2023-02-09 16:58:56

• 添加网站黑名单

1、登录控制台,单击【网站应用防火墙】>【IP管理】>【IP黑白名单】,选择需要防护的站点域名(如 www.test.com),单击【添加黑白名单】进入配置界面。

建行云	总览	云产品▼															zangchengj 🔻	费用 ▼	⊠ 0
云应用防火墙	(龙御) 《	IP黑白名单	www.test.c	om		Ŧ													操作指南 🖸
概览 网站应用防火增				在这里,您可 IP黑白名单优	「以将一个雪 洗級:全局	或多个IP加) 局白名单 > 対	、黑/白名单,实 《名白名单 > 城谷	现稿/推的访问排 呂黑名单 > 全局	控制。需要注意: ■黑名单[2]	的是:黑白名单的	的优先级仅低于W	AF自定义放行策略,高	新于其他检测逻辑	4編。			×		
IP查询 IP重询 IP黑白名单 IP封堵状态				类别: 黑名 查询	单	• *	源: 全部	Ŧ	输入IP		高级饰选	•							
日志服务				添加黑白名单		批量删除	导入数据	ŝ									导出全部筛选结果		
				序号	来)	源	IP地址		类别	更新时间	1 +	截止时间 ‡ 没有记录	备注	Ì			操作		
				共0項											每页显示行 20	▼ [4] 4	1/1 *		



建行云 总览	云产品。		zangshengj*	悪用▼ 四 ⑦
云应用防火墙 (龙御) 《	IP黑白名单 www.tes	st.com 👻		操作指南 🖸
概览 网站应用防火墙 >		在这里,您可以将一个或多个IP加入黑/白名单,实现解 IP黑白名单优先级:全局白名单 > 城名白名单 > 城名黑	和動的印刷控制,等要主要的是:蛋白高单的优先级仅低于WAF自定义的行業者,而于其他检测逻辑。	
 P査询 P罵白名单 P封塔状态 		発明: 王公単 ・ 未通: 全部 査知	添加黑白IP ×	
日志服労 >		添加照白名单 批量额除 导入数据	#30 ● 素名单 ○ 素名单 1P85± 1.1.1.1 ● 4.45% (\$	
		■ 序号 来源 IP地址		
			 戦止対向・ 202209-22 前 23:59:59 輸注 串心協規, 200个字符以内 	
			76.00 ROM	
		共0项	每页显示行 20 ▼ K ≤ 1/1 ▼ ≯ H	

3、单击【添加】保存规则,此时规则将会生效。此IP访问防护的站点域名(如 www.test.com)的任何页面都会被 阻断,提示403 Forbidden。

建行云 总宽	云产品▼	⊘ 液如成功	zangchengj 💌	裁用▼	⊠ 0
云应用防火墙 (龙御)	《 IP黑白名单 www.tee	test.com v			操作指南 🖸
概览 网站应用防火墙 ~ IP管理 ~		在这里,您可以将一个成多个小如人裹/白名单,实现陈幸的访问拉利,等要主要的是:黑白名单的优先欲仅低于WAF自定又妨行策略,落于其他检测逻辑。 IP黑白名单优先级:全局白名单,域名白名单,域名黑名单。全有黑名单 2	×		
IP查询 IP黑白名单 IP封堵状态		英部: 黑公单 ▼ 末语: 全部 ▼ 総入IP 業務保護 ▼			
日志服务		高加馬台名巻 和品目的 母人政策	导出全部演选结果		
		序号 来源 IP地址 类别 更新时间↓ 截止时间↓ 备注	操作		
		1 自定义 1.1.1.1 黑名单 2022-09-15 15-20:19 2022-09-22 23:59:59 无	编辑加白删除		
		邦 政 梅 双显示	47 20 ▼ <u>μ < 1/1 ▼</u> <u>μ</u>		

快速入门 一、添加域名

最近更新时间: 2023-02-09 14:48:19

为了能够让云应用防火墙(龙御)识别需要防护的域名,您需要先在云应用防火墙(龙御)添加域名。下面以防护 www.clbtest.com 为例说明域名添加的步骤。

1、登录控制台,单击导航条【云应用防火墙(龙御)】选项卡,进入云应用防火墙(龙御)控制台。在左侧导航窗 格中,单击【防护设置】,进入防护设置页面。

											_	_	
建行云 总览	云产品▼									zangchengj 🔻	费用 ▼		3
云应用防火墙 (龙御) 《 ^{概览}	_{负载均衡型} 防护设置										域名接入	操作指南 🖸	-
网站应用防火墙 ~ 防护设置 AI引擎 相则回导		域名列表 高加坡名 开启 关闭 副绘						支持域名。负载均衡名称。	监听器名称模糊搜索	Q			
IP管理 v		i 域名/ID	流星模式(j)	区域	负载均衡 (ID)	负载均衡VIP③	监听器()	WAF开关 ▼	操作				
日志服务 🗸 🗸		czh.com waf-87SmyfgG ⊘	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40.	. 42.201.68.234	test-czh(HTTP:8081)		删除 编辑 防护配置	ŧ			
		d.com waf-qqAF2IGx ⊘	清洗模式	武汉	clbwafv4测试-勿勍(lb-10dv40.	. 42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置	ł			
		c.com waf-PR8nE3i5 ⊘	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40.	. 42.201.68.234	test-hwl(HTTP:8001)		删除 编辑 防护配置	Ł			
		a.com waf-GcFCczsR ⊘	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40.	_ 42.201.68.234	test-ory(HTTP:8002)		删除 编辑 防护配置	È			
		blj-1255000011.iss.com waf-j2MWecRc 🧭	清洗模式	武汉	堡垒机测试(lb-j8irt2vs)	2404:bc0:1:1400:0 253:b081:6139	9 堡垒机443(HTTPS:443)		删除 编辑 防护配置	i			
		www.cscc.com waf-PJQNvJ7z	清洗模式	武汉	新堡垒机测试(lb-85dlsat8)	119.36.55.232	www.cscc.com(HTTP:90)		删除 编辑 防护配置	ł			ł
		www.aaa.com waf-oA0tjjL9 🥑	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40.	. 42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置	ł			
		www.clbtest.com waf-dNB36fyB	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40.	42.201.68.234	clbtest(HTTP:80) 102(HTTP:88)		删除 编辑 防护配置	E			
		www.ccc.com waf-ofNr1HXX 🔗	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40.	. 42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置	i			

2、单击【添加域名】按钮,弹出添加域名窗口,输入要添加的域名,根据实际情况下选择是否已使用了CDN、高防、云加速等代理(代理模式选择"是",WAF将通过XFF字段获取客户真实IP作为源地址),点击【下一步】验证 域名是否已存在。

建行云	总览	云产品▼			zangchengj 👻 🛛	裁用 ▼		0
云应用防火	増 (龙御)	🗧 🗧 添加域名				城名	渡入操作	指南 🖸
概览	e		1 输入增资	> (2) 務認能評論				
防护设置								
AI引擎 规则引擎			城名 🚯	www.olbtest.com				
IP管理			代理情况	● 音 ○ 量 品目已使用了高約、CDN、云加速等代置?				
日志服务								

3、再次点击【下一步】按钮,弹出选择监听器界面(注:监听器配置的域名必须与waf添加的域名一致),选中监 听器点击【确定】按钮。

建行云 总览 云产品 ▼			zangchengj_ * 圓用 * 🖸 ⑦
云应用防火墙 (龙御) < 🗲 添加域名			域名接入操作指南区
 転記 「利益目前5大集」 「利益目前5大集」 「利益用第二 「利益用第二 「利益用第二 「利益用第二 「日志都好」 	● 広ん成名 25月2日 日日 10月9日日日日 26月2日日日日 10月1日日日 26月2日日日日 10月1日日 26月2日日日 10月1日日 26月2日日日 10月1日日 26月2日日 10月1日日 26月2日日 10月1日日 26月2日日 10月1日日 26月2日日 11月1日日 26月2日日 11日日 26月2日日 11日日 26月2日 11日 26月2日 1	EBI#O) A http://www.clitest.com.90 × ↔	
	<u>1-5</u> %		

4、点击【完成】按钮



5、此时域名 www.clbtest.com 添加完成

建行云 总览	云产品▼								zangchengj 🔻	#用▼
云应用防火墙 (龙御) 《	负载均衡型									▲ 域名接入操作指南 🖸
概范	防护设置									
网站应用防火墙 防护设置 A引擎								古法被な 布括内面な8		
規则引擎 IP管理 ∨		100,000 21 11 21 12 21 22 22 22 22 22 22 22 22	流星模式①	区域	负载均衡 (ID)	负载均衡VIP()	监听器①	жағ开关 ▼	操作	
日志服务 🗸 🗸		www.clbtest.com waf-Bda2nzBU 📀	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置	
		www.test.com waf-vMOYNUjx 🥑	清洗模式	无	未配置	未配置	未配置		删除 编辑 防护配置	
		czh.com waf-87SmyfgG ⊘	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	test-czh(HTTP:8081)		删除 編輯 防护配置	
		d.com waf-qqAF2IGx 🥥	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置	
		c.com waf-PR8nE3I5 ⊘	清洗欄式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	test-hwl(HTTP:8001)		删除 编辑 防护配置	
		a.com waf-GcFCczsR 🥥	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	test-cry(HTTP:8002)		删除 编辑 防护配置	
		blj-1255000011.iss.com waf-j2MWecRc 🥥	清洗模式	武汉	堡垒机测试(Ib-j8irt2vs)	2404:bc0:1:1400:0 253:b081:6139):9 堡垒机443(HTTPS:443)		删除 编辑 防护配置	
		www.cscc.com waf-PJQNvJ7z	清洗模式	武汉	新堡垒机测试(lb-85disat8)	119.36.55.232	www.cscc.com(HTTP:90)		删除 编辑 防护配置	
		www.aaa.com waf-oA0tjjL9 🥑	清洗模式	武汉	clbwafv4测试-勿动(lb-10dv40	42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置	

6、点击【防护配置】按钮,进行waf防护配置。【流量模式】选择为"清洗模式",【Web基础防护】选择为"拦 截",高级设置下的【恶意文件检测】设定为"否",【防护等级】选择为"严格",【Al引擎】选择为"观察"(在观



察期间,持续对AI告警日志进行分析和学习,评估无误报后,开启拦截模式)

建行云 ^{总宽}	云产品 ▼	✓ 切換對葉状态成功!	zangchengj▼	38月▼ 🖸 ⑦
云应用防火墙(龙御)《	← 防护设置 www.clbtest.com ▼			
概览 网站应用防火增 > 防护设置	基础设置 自定义策略 CC防护设置2.0		¢	
AI引擎 規则引擎 IP管理 →	WAF开关 WAF状态	WAF95ታታዊ Web35840000	な 2 双条 <u> </u>	
日志服务 >	大利WAF おけたら、所有的DF-UBEため、	WAH进入高量转发物式,不管打制权制行力也不管过度日本。 编辑 防护等级 AIRECTION	====================================	
	iD wef8da2x8U 的 代理版符 音	- A的庫 ① - A的庫 ①	大石 死業 王美 建议先手回顾课程式一段时间(例2020天): 石观景様広下, ARI型版台会自动学习网站协同模式并进 行死化和周期, 直接开码巨氟模式, 可能会存在低氟率的风极。忽可以持续将可凝放强度炎给ARI原进	
	(第三次応 正常 ②) (注意) (注意)<	地域对萘	行性的科学,评估性的方法形成局,建议打烊在制度式。如果外区规则,读集会交生管由部分人员。	
	负载约衡:监听器 区域 负载均衡(ID) 负载均衡VIF 武汉 clovaf+4期试-参词(b=10d+40 42.201.68.2	p 盒所面 34 olbtest(HTTP-80)	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
		C33m64		

二、本地测试

Ĉ

最近更新时间: 2023-02-09 14:48:19

本地机器访问网站测试经过waf防护后正常请求页面是否返回正常及攻击请求是否拦截。

一、正确请求测试,通过浏览器访问域名 http://www.clbtest.com

 	~ - ¤ ×
← → C 🛕 不安全 dbtest.com 😢 ☆	* 🛛 😩 更新 🗄
😵 百度 👶 苏宁易购 🚱 🤣 www.clbclbwaf.com 😧 搜索 関 淘宝 🗾 京东 🔇 天猫 🔇 https://download 🕥 未命名文件 - Proc 🖏 python中open与w 🛂 未命名表单-迅捷画 🖏 centos7安装mysql	>>
2022/9/15 下午4:13:37	





二、攻击请求测试,通过浏览器访问域名 http://www.clbtest.com/?Cmd=alert(1111)



常见问题 如何定位是否为龙御WAF拦截

最近更新时间: 2023-02-09 14:52:48

页面内容为"403 Forbidden""、页面标题为"访问拦截",页面的源代码包含"waf-empty" 注:客户端请求被拦截后,状态码返回200(CLB型WAF) 如使用CDN的业务,可能会缓存WAF的拦截页面。



如何分析拦截原因

 \bigcirc

最近更新时间: 2023-02-09 14:52:48

提供信息:域名、客户端IP、故障时间、URL、返回的页面内容 1、登录租户控制台,选择云产品-云应用防火墙(龙御)-日志服务-攻击日志 2、选择域名、时间段,输入客户端IP,点击查询 3、查看是否存在执行动作为拦截的攻击日志,根据具体的攻击类型+策略ID+策略名称分析具体原因 攻击类型为自定义策略(规则ID非0)、地域封禁拦截、IP黑白名单、CC策略拦截,则租户自行分析判断 攻击类型为AI引擎检出,租户需与安全处一起分析判断是否进行在线学习 其他攻击类型,租户需与安全处一起分析判断是否为正常拦截,是否可以添加白名单规则

建行云	总览	≂,7°∺ *	liukehan@ 🔻 费用 🔻 🤐 🕐
云应用防火墙(龙御)《	攻击日志	
概览		日志查询	
网站应用防火墙			
IP管理		a.com v 近1小时 近6小时 今天 昨天 近7天 2021-06-15 15:48:50 至 2021-06-15 23:59:59 自	
日志服务		全部风险等级 ▼ 全部块行动作 ▼ 全部攻击类型 ▼ 输入策略D 输入文击那P 會資	
攻击日志			
		总数量: 0项	¢
			执行动作 风险等级 操作
		没有记录	



最近更新时间: 2023-02-09 14:52:48

1、排查客户IP地址是否已触发天幕联动封禁,如需解封客户IP可联系一线值班处理;

2、确认WAF拦截的告警类型,告警日志中的攻击类型字段包含规则引擎17种告警类型、AI引擎拦截、自定义策略、 IP黑名单和CC拦截,对于不同类型告警需做不同处置;

3、对于规则引擎拦截,应急处置可通过告警日志获取触发的规则编号,关闭该条规则开关;后续根据规则编号查看 规则内容及CVE信息等,根据攻击内容判断属于开发不合规问题还是误报,对于不合规情形需应用整改,对于误报 可设置规则白名单;

4、对于AI引擎拦截,应急处置可将AI引擎切换为观察模式;分析引擎拦截原因,进行应用改造或AI模型学习或设置 自定义放行策略不再勾选"继续执行AI引擎防护"等后续处置;

5、对于其他自定义类型拦截,需根据自身配置规则进行排查,关闭、删除或修改配置规则。

如何进行AI引擎在线学习

最近更新时间: 2023-02-09 14:52:48

 \bigcirc

注: AI在线学习分误报和漏报处理,请勿将带有攻击特征的报文添加到误报学习中,否则可能会影响检测的准确性 1、在攻击日志中找到AI拦截的攻击内容,将攻击内容在AI在线验证界面进行验证。验证为威胁数据后,将威胁数据 人工拆分成几段,分别验证,直到找打最小的威胁数据。

2、点击AI误报学习,手动添加威胁数据。

3、选中误报数据,点击学习。学习后再次进行AI在线验证,验证正常。

建行云	总览	云产品▼						zangcheng.	▼ │ 费用 ▼ │	⊠ ∣ Ø
		请求方法	POST	风险等级	局危	运营商	联通	纬度	39.938884	A
云应用防火墙	(北側)	攻击时间	2021-06-15 16:49:08	匹配来源	其他					
概览		请求UUID	1c58388288142dc27772a4387d04e8a6-21cd641cd	187 执行动作	拦截					
网站应用防火墙			0d4c3eeb6efc1880cfb22							
IP管理		请求URI	/operator/server/checkrule							
		攻击内容	#!/bin/bash\n\n##################################	****		###				
日心版穷			######################################	n\n#email:wen.lu@ten	dcloud.com\n\n##################################					
攻击日志			*****		######################################	Cdr				
			om_name_dir Ks_name_dir Tmp_dir Mount_dir\n\n	\n\nauto_cd()\n\n\n	Cdrom_name_dir=/home/remotecard/RHEL6.4_X86_64	_Au				
			toInstall_DVD_`date +'%Y%m%d'`.iso\n\n Source_	file=/home/remotecard	/rhel-server-6.4-x86_64-dvd.iso\n\n Ks_name_dir=ks.cfg	\n\n				
			Tmp_dir=/tmp/rhel6.4\n\n Label=RHEL6.4_X86_64	_AutoInstall_DVD\n\n	Mount_dir=/mnt\n\n if [-d \${Tmp_dir}]\n\n then\n\n echo	"Т				
			mp_dir is exits"\n\n else\n\n mkdir \${Tmp_dir} &> /o	lev/null\n\n fi\n\n moun	t \${Source_file} -o loop \${Mount_dir} &> /dev/null\n\n cp	-a				
			\${Mount_dir}/. \${Tmp_dir}\n\n###create file isolinux	.cfg\n\n mv \${Tmp_dir	/isolinux/isolinux.cfg /isolinux.cfg.bak &> /dev/null\n\nca	t <<				
			EOF >> \${Tmp_dir}/isolinux/isolinux.cfg\n\ndefault	install\n\nprompt 1\n\n	#timeout 600\n\ntimeout 30\n\n\n\ndisplay boot.msg\n\n	1 Б				
			oot.msg\n\nF2 options.msg\n\nF3 general.msg\n\n	F4 param.msg\n\nF5 re	escue.msg\n\nlabel install \n\n kernel vmlinuz\n\n appen	d ks				
			=cdrom:/ks.cfg initrd=initrd.img\n\nlabel linux\n\n m	enu label ^Install or up	grade an existing system\n\n menu default\n\n kernel vn	nlinu				
			z∖n∖n append initrd≕initrd.img∖n∖nlabel vesa∖n∖n mei	nu label Install system	with ^basic video driver\n\n kernel vmlinuz\n\n append ir	nitrd				
			=initrd.img xdriver=vesa nomodeset\n\nlabel rescu	e\n\n menu label ^Reso	cue installed system\n\n kernel vmlinuz\n\n append initro	l=ini				
			trd.img rescue\n\nlabel local\n\n menu label Boot fr	om ^local drive\n\n loc	alboot 0xffff\n\nlabel memtest86\n\n menu label ^Memor	y te				
			st\n\n kernel memtest\n\n append -\n\nEOF\n\n um	ount \${Mount_dir}\n\n	cp \${Ks_name_dir} \${Tmp_dir}\n\n cd \${Tmp_dir}\n\n fin	d -ty				
			pe f -name "TRANS TBL" lxargs rm -f\n\n rm -rf iso	linux/boot.cat\n\n chmo	od +w isolinux/* &> /dev/null\n\n In					
		添加误报	添加误报							

如何添加自定义放行规则

最近更新时间: 2023-02-09 14:55:27

 \mathbf{i}

1、登录租户控制台,选择云产品--云应用防火墙(龙御)--防护设置,点击域名,选择"防护配置"

2、选择自定义规则,点击"添加规则",输入匹配条件,执行动作选择放行,并勾选继续执行剩余的检测防护,设置 截止时间

添加规则					×					
规则名称*	请输入名称,最长50个雪	字符								
匹配条件 *	匹配字段	匹配参数	逻辑符号	匹配内容	操作					
(j)	来源IP ▼	此字段不支持参数选择	匹配 🔹	1.1.1.1	删除					
		添加 还可以添加4条,最多5条								
执行动作 *	放行 💌	汝行规则优先于其他匹配操作执行								
	✔ 继续执行地域封禁	防护 🔽 继续执行CC策略防护	✓ 继续执行WEB应用防护	✓ 继续执行AI引擎防护	✔ 继续执行信息防泄漏防护					
截止时间*	限定日期 🔻	2021-06-15 🟥 🚯								
优先级 *	- 100 +									
	请输入1~100的整数,数号	字越小,代表这条规则的执行优先级越行	<u>言</u> 同 。							
			添加取消							

CLB型WAF域名访问故障时如何应急

最近更新时间: 2023-02-09 14:55:27

- 1、关闭部分防护功能,包含AI引擎防护、WEB基础防护、恶意文件检测、流量模式
- 2、切换流量模式为镜像模式
- 3、关闭WAF防护

C

4、删除CLB型WAF的防护配置(应急后需恢复)

防护设置	www.d1.com	*				
基础设置	自定义策略 CC防护设置2.0					
						¢
WAF开关			W	AF院护护?	**	
WAF状态			We	p基础防护	2 观察 拦截	
关闭	WAF总开关后,所有的防护功能失效,WAF	进入流量转发模式,不会拦截攻击行为也不会	记录日志。		高级设置▲	
基础配置			编辑		恶意文件检测 💿 否 🗌 是	
域名 4	www.d1.com		防护	护等级	○ 宽松 ○ 正常 ○ 严格	規則管理
ID V	waf-ZxtlDhvk 🕞		Al	智能防护		
10-99-09-09	-		Alē	引擎 🛈	关闭 观察 拦截	
代理情况	8			l	建议先开启观察模式一段时间(例如20天);在观察模式下,AI引擎后台会自	动学习网站访问模式并进
绑定状态	正常 🥥				行检测和学习,评估检测无误报后,建议开启拦截模式。如果其他疑问,请联	系安全售后服务人员。
流量模式 ()	镜像模式 清洗模式 ()					
负载均衡 - 监叭	斤器		地	域封禁	_	编辑
区域 负载均	街 (ID) 负载均衡VIP	监听器 1000HTTP:100	203	祭状态	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
JEUX CIDWar	v4//3 ta// in/(in-100v4 42.201.00.234	100(1111.100)			יין איז ארגעא אין איז	
			E	封禁地域	国内全部 国外全部	



龙御WAF中各类自定义配置的优先级是什么

最近更新时间: 2023-02-09 14:55:27

全局IP白名单>域名IP白名单>域名IP黑名单>全局IP黑名单>自定义策略放行规则>CC策略>地域封禁>自定义策略拦截规则