

# Web 应用防火墙

# 实践教程







#### 【版权声明】

#### ©2013-2025 腾讯云版权所有

本文档(含所有文字、数据、图片等内容)完整的著作权归腾讯云计算(北京)有限责任公司单独所有,未经腾讯云事先明确书面许可,任何主体不得以任何形式 复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯,腾讯云将依法采取措施追究法律责任。

【商标声明】

## 🕗 腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标,依法由权利人所有。未经腾讯云及有关 权利人书面许可,任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为,否则将构成对腾讯云及有关权利人商标权的侵犯,腾讯云将依 法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况,部分产品、服务的内容可能不时有所调整。 您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则,腾讯云对本文档内容不做任何明示或默示的承 诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务,及相应的技术售后服务,任何问题请联系 4009100100或95716。



## 文档目录

实践教程 WAF 等保测评解读 BOT 管理相关 BOT 场景化实践教程 API 安全相关 API 安全实践教程 API 容量保护 API 数据防护与加固 WAF 结合 API 网关提供安全防护 API 行为管控 API 暴露面管理 接入相关 WAF 与 DDoS 高防包结合应用 WAF 与 CDN 联动使用实践教程 HTTPS 免费证书申请和应用 WAF 一键开启 IPv6功能 如何获取客户端真实 IP 如何更换证书 防护与配置相关 如何设置 CC 防护 前后端分离站点接入 WAF 验证码 使用 TCOP 设置 WAF 异常告警

## 实践教程 WAF 等保测评解读

🔗 腾讯云

最近更新时间: 2025-04-11 14:24:52

腾讯云 Web 应用防火墙(Web Application Firewall, WAF)符合等级保护2.0标准体系主要标准。根据《网络安全等级保护基本要求》(GB/T 22239−2019),腾讯云 Web 应用防火墙满足第三级安全要求。

序 号	等保标准章节	等保标准序号	等保标准内容	对应功能描述
1	访问控制	8.1.3.2 e)	应对进出网络的数据流实现基于应用协议和应 用内容的访问控制	配置应用层的访问控制策略,对进出网络的数据流实现 基于应用协议和应用内容的访问控制
2	入侵防范	8.1.3.3 a)	应在关键网络节点处检测、防止或限制从外部 发起的网络攻击行为	边界区域部署 WAF,能对各种攻击和扫描行为进行检 测和报警
3	入侵防范	8.1.3.3 c)	应采取技术措施对网络行为进行分析,实现对 网络攻击特别是新型网络攻击行为的分析	WAF 支持对 Web 流量进行实时检测和阻断,支持 Al+ 规则双引擎防护,可阻断 0day 攻击和其他新型未 知攻击
4	入侵防范	8.1.3.3 d )	当检测到攻击行为时,记录攻击源IP,攻击类 型、攻击目的、攻击事件,在发生严重入侵事 件时应提供报警	WAF 支持 HTTP 和 HTTPS 流量攻击检测和防御, 记录攻击类型、攻击 URL、攻击内容、攻击源 IP、命 中规则名称和 ID、风险等级、攻击时间、目的 host、 执行动作等信息
5	恶意代码防范	8.1.3.4 a)	应在关键网络节点处对恶意代码进行检测和清 除,并维护恶意代码防护机制的升级和更新	WAF 基础安全和规则引擎模块可以实现该功能
6	安全审计	8.1.3.5 a )	应在网络边界、重要网络节点进行安全审计, 审计覆盖到每个用户,对重要的用户行为和重 要安全事件进行审计	在边界处对入侵事件进行审计
7	安全审计	8.1.3.5 c)	应对审计记录进行保护,定期备份,避免受到 未预期的删除、修改或覆盖等	日志存储至少6个月,租户不能删除、篡改

## BOT 管理相关 BOT 场景化实践教程

最近更新时间: 2025-06-18 14:23:01

## 功能介绍

う 腾讯云

通过 BOT 与业务安全,用户可以在 BOT 管理中开启并配置对应模块内容,并结合 BOT 流量分析与访问日志进行观察和分析。根据流量分析提供的会话状态信 息进行精细化策略设置,保护网站核心接口和业务免受 BOT 侵害。

BOT 管理设置支持配置 BOT 场景类型、客户端风险识别(前端对抗)、威胁情报、AI 策略、智能统计、动作分数、自定义规则、会话管理、合法爬虫模块,通 过配置这些模块,实现对 BOT 的精细化管理。BOT 实践教程流程图如下所示:



## 前提条件

- BOT 流量管理需要购买 WAF 对应实例的 BOT 流量管理功能。
- 已在 BOT 与业务安全页面,选择需要防护的域名,并开启 BOT 流量开关。

BOT与业务安全 · · · · · · · · · · · · · · · · · · ·							(2) RW809
807篇度 Saust 出版全地展示:+**【IT 附 全局设置 以下模块设置线带会面符于面和结构下的全部块展 条人机环的设置 有性容量						Am 人机识别设置 前往设置	
0011178 2822	±∞## 7 ↑	<sup>还要急数</sup> 9 条	(	Riteauni O ș. Riteaun	智能分析 ① 33条 前往配置	会過普理 <b>1</b> 条 前往配置	合法观虫 2 条 前往配置

## 创建 BOT 场景

该功能依托腾讯多年 BOT 治理的专家经验,针对 BOT 中常见的秒杀、爬价格/爬内容和登录等场景,从客户端风险识别(前端对抗)、威胁情报、AI 策略、智 能分析、动作得分、会话管理、合法爬虫和自定义规则等维度基于专家经验进行设置,解决客户配置难的问题,简单易用,轻松上手。

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择**配置中心 > BOT 与业务安全**。
- 2. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。
- 3. 在 BOT 管理的 BOT 防护页面,单击新建场景。
- 4. 在新建场景弹窗中,配置相关参数,单击**立即创建**。

#### ▲ 注意:

- 选中秒杀、登录和爬文案/爬内容中的任意一个场景与自定义场景互斥。
- 选择对应场景后,将为您自动生成防护对应业务场景的自定义规则,规则默认为"观察"模式,您可以观察命中流量后调整为拦截模式。



#### 参数说明:

- 场景名称: 描述场景的名称,不可超过50个字符。
- **业务场景类型**:支持多选,可选择秒杀、登录、爬文案/爬内容和自定义场景。
- **客户端类型:**访问防护目标的客户端类型。
- 优先级: 该场景的执行优先级,输入范围为1-100的整数,数字越小,优先级越高。
- 生效范围: 该场景在该域名下的生效范围,支持全部范围和自定义范围。
- 5. 场景化管理列表中,将出现创建完成的场景卡片数据,即可进一步对其进行配置。

#### 会话管理

用户可通过配置该功能,配置会话 Token 所在的位置,实现在同一 IP 下区分识别不同用户的访问行为,实现不影响其他用户的情况下,精准处置存在异常访问 行为的用户。

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择**配置中心 > BOT 与业务安全**。
- 2. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。

BOT与业务安全 · · · · · · · · · · · · · · · · · · ·	•					③ 解助说明
BOT放在 San 52 出版企业和推动 小叶和丁酮 全局设置 以下模块设置领带会由用于由前域名下的全部体质 经全部设置 即计设置						
807管理 查看说是 【 【 【 】	<sup>生效场最</sup> 7 ↑	场景总数 9 条	前端9抗 ① ● 条 前社記園	智能分析 ③ 33 条 前住記載	会活管理 <b>1</b> 条 前往配置	合法原生 2 条 前1185版

3. 在 BOT 管理页面,在全局设置中,单击会话管理模块的前往配置。



<b>全局设置</b> 以下模块设置项将会应用于	于当前域名下的全部场景		是 人机识别设置 前往设置
前端对抗 🛈	智能分析 🛈	会话管理	合法爬虫
<b>O</b> <sub>条</sub>	<b>33</b> <sub>条</sub>	<b>1</b> <sub>条</sub>	<b>2</b> <sub>条</sub>
前往配置	前往配置	前往配置	前往配置

#### 4. 在会话管理页面,单击添加配置,配置相关参数,单击确定。

## 🕛 说明:

会话标识应为可持续性记录 tokenid ,例如登录后的 set-cookies 的值。

新增会话标识	
*会话标识名称	自定义标识名称,最多128个字符
会话标识描述	自定义描述文案,最多128个字符
*会话标识位置 🛈	
*会话标识参数 访	请输入会话标识,64个字符以内
*规则开关	
⑦ 高级设置▲	
*应用场景	<ul><li>● 全部场景</li><li>● 部分场景</li><li>请选择一个或多个场景</li><li>▼</li></ul>
*优先级	- 1 +
	请输入1-100的整数,数字越小优先级越高,优先匹配对应设置的会话标识
	确定 返回

字段名称	说明
会话标识位置	指定识别特定位置(QUERY、BODY、COOKIE 或 HEADERS)的参数名作为会话标识,以该参数名对应的值作为 会话 ID 。
会话标识参数	取值标识,以.字符区隔各个层级的参数,示例如下: • test: 识别 JSON 字符串中 test 参数的值为会话 ID。 • test1.test2: 识别 JSON 字符串中 test1包含的 test2参数的值为会话 ID。 • 除了 HEADERS 以外,其余配置均需要区分字母大小写。
高级设置	支持单击 <b>展开高级设置并</b> 配置,不特殊设置的情况下默认应用于全部场景,优先级为1。 ● 应用场景:支持选择全部场景或指定场景,对选中场景生效。 ● 优先级:支持输入1−100的整数,数字越小优先级越高,优先匹配对应设置的会话标识。优先级相同时,更新时间越近 越优先。

## 客户端风险识别(前端对抗)

客户端风险识别功能通过客户端动态安全验证技术,对业务请求的每个客户端生成唯一 ID,检测客户端对 Web 或 H5页面访问中可能存在机器人和恶意爬虫行 为,保护网站业务安全。

#### 🕛 说明

•本功能不支持 CLB-WAF,泛域名,App/小程序,只适用于 Web 或 H5页面,如果有非动态认证,自动化接口脚本需要优先加入白名单。



● 基于对抗功能设计,开启前端对抗功能开关后会在 Response 中插入 JS ,可能导致 WAF 到源站带宽略有增加。

## 添加白名单

添加白名单主要用于对不需要进行设置的接口放行处理。

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择配置中心 > BOT 与业务安全。
- 2. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。

BOT与业务安全     11								
BOT概算 Saast			全局设置 以下概块设置项将合应用于当前域名下的全部场景			A. 人机识别设置 前往设置		
±20182 ±22.8 € 107872 ±22.8 128.	活要总数 <b>9</b> 条		前端对抗 ① 〇 条 前社紀派	智能分析 ③ 33条 前往配置	会话管理 1 条 前往配置	合油原虫 2 余 前11起面		

- 3. 在 BOT 管理页面,在全局设置中,单击前端对抗模块的前往配置。
- 4. 在前端对抗页面,单击添加规则,弹出添加白名单规则窗口。

前端对抗							×
() 这是一个	全局策略,对前端对抗的	)修改将会对到当前域名	下的全部场景生效			不再提醒	×
验育防护 🛈 🤇	编辑 自动	化工具识别	页面防调试				
1名单策略							
添加规则				请输.	入规则ID	(	φ

5. 在添加白名单规则窗口中,配置相关参数,单击确定即可。

添加白名单规则	
类型	<ul> <li>○请求白名单</li> <li>○响应白名单</li> <li>加白防护路径下不需要进行动态安全检测的请求路径或URL</li> </ul>
匹配条件	路径后缀名匹配
匹配内容	请输入文件后缀名,使用英文逗号隔开,128个字符以内
	ico.gif,bmp,htc.jpg.jpeg,png,tiff,swf,js,css,rm,rmvb,wmv,avi,mkv,mp3,mp4,ogg,wma,zip,exe,rar,eot,woff,woff2,ttf,sv g <b>ြ</b>
规则描述 (选埴)	请输入规则,最长256个字符
规则开关	
	确定 返回

## 案例一: 大量机器自动化脚本请求服务

有大量机器自动化脚本请求服务,禁止类似 CURL,SOAPUI、JMETER、POSTMAN 访问请求。

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择**配置中心 > BOT 与业务安全**。
- 2. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。



807与业务安全 (」,								
BOT概范 SaaS型	BOT義王 5xx5월 최종승규제 제품 ··································							
BOT管理 查看完量	±338∰ 7 ↑	场景总数 9 条		前端时抗 ① 〇 条 前柱配置	智能分析 ① 33 条 前注意度	会运管理 1 条 前住配置	合法更生 2 <sub>条</sub> 新社記堂	

#### 3. 在 BOT 管理页面,在全局设置中,单击前端对抗模块的**前往配置**。

4. 单击自动化工具识别的 (),确认白名单。

前端对抗		×
这是一个全局策略,对前端对抗的修改将会对到当前域名下的全部场景生效	不再提醒	×
自动化工具识别 页面防调试 〇〇		

#### 5. 在场景化管理中,选择目标场景,单击右侧的查看配置。

BOT防护	BOT白名单							
场景化管理								
新建场景	新建场器         全部场景类型         ▼         【 仅重看主效场景 【 仅重看主效场景 【 仅重看款从场景 ①							
优先级: 1								
	场展名称	→ 请求路径 ●	动作策	自定义规	生效状	+ 7 5 7		
2	te	O 2022-11-21	略	则	态	三百印度		
	场展id: 3	📑 前端对抗 🚺 威胁情报 📀 AI策略 📀 智能分析 📀	1	9		3時734~2382		
	登录 浏览器/H5 小程序		▲条	<b>3</b> 条		012H3T-9/03HR		

6. 在场景详情页面,单击该场景下前端对抗模块的 , 防护模式选择 拦截,开启该前端对抗功能。

场景配置	
前端对抗 第一道拦截 ① 建议敏感目录下开启此功能	查看文档 [2
检测客户端对Web取H5页面访问中可能存在机器人和思想爬虫行为,保护网站业务安全。 开关防护模式 监控 重定向 人机识别 拦截	

7. 使用 CURL、SELENIUM、POSTMAN 请求结果分别如下所示:



<pre>\$1f.length;_\$uD++){\$1f[_\$uD]^=_\$2_[Math.abs(_\$uD)%16];}}return;}}else if(_\$WA*122&gt;1830&amp;&amp;32\$WA&gt;0}{if(-106&lt;_\$WA-123&amp;&amp;_\$ WA*122&lt;3416){if(150===126+_\$WA){\$hL+=7;}else if(92*_\$WA==2300}{\$hL+=-13;}else if(-24===_\$WA-50}{\$uD.push("MT7Fp9Dreu0 OxmJnUWnNuL");}else{var _\$wr=_\$mt[19];}else if(16===_\$WA-60}{\$12=_\$vc&amp;&amp;_\$vc[_\$88(_\$mt[31)];}else{\$12=_\$1t[_\$88(_\$mt[61)](_\$88(_\$mt[61)](_\$88(_\$mt[61)](_\$88(_\$mt[61)](_\$vc);}else if(16===_\$WA-61){\$uD.push(4};}else _\$mt[0]);}else if(15=_\$WA&lt;08&amp;20&gt;_\$WA){if(43===27+_\$WA}{\$12=_\$vc&amp;&amp;_\$vc[_\$88(_\$mt[31)][\$88(_\$mt[29])](_\$vc);}else if(16*==1682){\$322} =_\$1t[_\$88(_\$mt[41)];}else if(-63===_\$WA-61){\$uD.push(4};}else{\$\$12[_\$vc];}else{\$1f(91===63+_\$WA){\$uD.push(4});}else{\$1f(2*_\$WA==1682){\$32}} =_\$1t[_\$88(_\$mt[41)];}else if(-73===_\$WA-103){\$hL+=13;}else{\$1t[_\$88(_\$mt[61)](_\$88(_\$mt[01))[0][_\$88(_\$mt[21)](_\$2_);} }es if(164_\$WA]2ccL08qr4r0qqr0c22qn.CB.7K7RYGXUTYmj9XtdgeOmTyesaZg_0qSWhVgavzuE])YCaXKuVdJsy7mbq1rr Wv1s3eM9Q8EDa6WVPss1QMV VnC pRxxfvD4jMWzB2CIJ3wRPPDFmMHL1auBDHz9G0K1K1Q1warc1RdNy60SMJwSvZob.xH9u4pDZoMZAZC8r8F70.kKNRdz,NPScHX29e0tjJ33oLDuvxRgp 7DD DDRzP_PIP4tEcBDtbEy9_zaqqqqqt0QQSp1xIW7APrrh9L71n2ct0EXAP2qhqVHiGJ6G0I20J6GvUkwZi{Mq32F2PH74}4zx470jpdq5PdDM_J0n71p 7r6 uBJM5zec66wHzzCdMN1zZosuM3SBTD6ihQT0nb6gIENB061UtWqqh7QQHsrGZiGac64qqr0HQNywdl0ZR9U20qch7eki629Dm5AqqYW9hjv3RC i63}E0xVPe6t4c64qq14096qqqh0AM3M800_wkRbQqk162HmC6bKcppEmgBVn3qqt10831790401rt.");}else if(67*_\$WA===60){\$vc\$U1=\$ iP; else if(-21===_\$WA-31}{\$uD.push("7V000tRWGFA");}else{if(!\$12)_\$hL+=1;}else if(_\$WA*116&gt;34&amp;&amp;&amp;&amp;=\$WA&gt;0}{if(62==58+ \$W}){\$x2id=_\$1f;}else if(118*_\$WA===590}{\$2_[\$88(_\$mt[35])]=\$v;}else if(-117===_\$WA-123}{\$va = \$2_{\$1t[_\$88(_\$mt[21]]](\$2_{\$2};}else if(62*=584,=\$WA&gt;2]{\$uL+=2;}else if(-69===\$WA-71}{\$uD.push("Vk_yxby7s16");}else{var_\$15_\$m(}]}else{var_\$15_\$00};}else{var_\$15_\$00};else{var_\$15_\$00};else{var_\$15_\$00};else{var_\$15_\$00};else{var_\$15_\$00};else{var_\$15_\$00};else{var_\$2=_\$1t[\$88(_\$mt[21]]] i=2+\$\$wA}{\$2_{\$2_{\$2_{\$}}}&amp;elf(-4===\$\$WA-71}{\$uD.push("Vk_yxby7s16");}else{var_\$15_\$00};else{var_</pre>
<pre>se f(51*_\$WA===2499){return Math.abs(arguments[1]) % 16;}else if(36===_\$WA-14){return 10;}else{1 eturn 8;}else{return 1; }}; unction _\$rY(_\$vs){var _\$wr,_\$uD,_\$KD=_\$vs,_\$vc=_\$Fb[2];while(1){_\$uD=_\$vc[_\$KD++];if(-16&gt;_\$uD-20){if(3===_\$uD){_\$wr= _\$2 [[\$8B(_\$mt[5])]==_\$8B(_\$mt[15])]]=_\$8B(_\$mt[5])]==_\$8B(_\$mt[42]);}else if(120===119+_\$uD){_\$PU(_\$1f);}else if(70*</pre>
_\$u <mark>b</mark> ===140){_\$2_[_\$8B(_\$mt[46])]=null;}else{if( !_\$wr)_\$KD+=2;}}else{return;}}})() <body></body>
<input id="onload" name="cDLJ.6zflivja8RAGWSNtmGchMfTmH_nrcvrZ2rWMSsSfm3KWkWRvkmWb1UdoYcTl8J_iPk.XCM_z7&lt;br&gt;XBKK8HwG" type="hidden" value="g.bsDjQpVCmzPMoeR.dbDA"/>
psdpandeMacBook-Pro ~ % curl http://wwwcom -I HTTP/1.1 202 Accepted
Content-type+ text/html; charset=utf-8
Connection: keep-alive

Connection: keep-alive Set-Cookie: Cc2838679FS=5ffyjNUVxUtd.BOCnqlHHKmk7AhiBH.OtxKdMrzQg1gG.T8yHY8c.A2gLxFTip\_ohj9ld.vaZwWDWfo\_OuKvQ4G; Path=/; expires=Tue, 02 Mar 2032 09:11:53 GMT; HttpOnly Expires: Sat, 05 Mar 2022 09:11:53 GMT Date: Sat, 05 Mar 2022 09:11:53 GMT Server: \*\*\*\*\*\* Cache-Control: no-store Pragma: no-cache







GET	https://www.com		_	Send
Para	ms Authorization Headers (8) Body Pre-req	uest Script Tests Settings		Cookies
	KEY	VALUE	DESCRIPTION	ooo Bulk Edit
	Key	Value	Description	
Pre 4 5 6 7 8 9	<pre>tty Raw Preview Visualize HTML ~</pre>	<pre>="text/html; charset=utf-8"&gt; .createElement("section")&lt;1[endif] t" r='m'&gt; 11,3,13,2,0,10,5,10,8,1,7,1,2,2,14],[2,7,13,2 14,8,18,27,34,24,9,24,10,17,16,38,39,40,41,19 4,44,6,31,34,49,22,35,18,24,44,31,22,50,51,2 e.push.apply(_\$9Y,arguments);return _\$m4.appl SCj.push(window[_Scr(_\$9C[11])]); SCj.push(wi 0]))];_SCj.push(window[_Scr(_\$9C[11])]);_SCf)</pre>	<pre>&gt;&gt; 20,0,40,32,4,12,5,22,0,30,25,43,0,15,29, ,23,22,13,37,16,42,17,19,25,1,43,44,45, 11,12,18,51,46,30,52],[2,1,3,0,5,11,5]]; ly(this,_\$9Y);}function _Sas(){var _\$04+ indow[_scr_\$9C[22])); \$c:.push(window] .push(0bject[_scr(_\$9C[3])][_scr(_\$9C[7]); \$c:.push(string[_scr(_\$9C[3])][_scr(_\$9C])]</pre>	<pre>28,10,1,27,33 46,47,31,48, function _\$wy =_\$9C[39];_\$2m\$cr(_\$9C[39] ));;_\$Cj.push c(37)]);,\$Cj</pre>
	<pre>push(String[_\$cr(_\$9C[8])][_\$cr (_\$9C[12])]);_\$Cj.push(String[_ [_\$cr(_\$9C[8])][_\$cr(_\$9C[26])]]</pre>	(_\$9C[13]));_\$Cj.push(String[_\$cr(_\$9C[8]))[ \$cr(_\$9C[8])][_\$cr(_\$9C[32]));_\$Cj.push(Stri );_\$Cj.push(String[_\$cr(_\$9C[8])][_\$cr(_\$9C[2	<pre>[_\$cr(_\$9C[44])]); \$Cj.push(String[_\$cr( ing[_\$cr(_\$9C[8])][_\$cr(_\$9C[36])]); \$Cj ?])]); \$Cj.push(String[_\$cr(_\$9C[8])][</pre>	<pre>[_\$9C[8])][_\$c: .push(String \$cr(_\$9C[31])]</pre>

## 案例二:禁止网页调试

禁止用户打开网页调试,避免针对性爬虫编写。

1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择配置中心 > BOT 与业务安全。

2. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。

BOT与业务安全	]						🕐 ALWICH
BOT概范 SaaS型			unanna:ULTH	全局设置 以下模块设置项将会应用于当前	印城名下約全部场景		A。人机识别设置 前往设置
	<sup>生效场景</sup> 7 个	<sup>汤贾总数</sup> 9 条		前班时机 ① 〇 条 前注配置	新能分析 ① 33条 前往配置	会运管理 <b>1</b> 条 前往伦置	合地應当 2 条 約11起版

3. 在 BOT 管理页面,在全局设置中,单击前端对抗模块的**前往配置**。

4. 单击页面防调试的 , 确认白名单。

前端对抗							×
极简防护	3 编辑 自动化		页面防调试				
白名单策略							
添加规则				请输	入规则ID	(	Q Ø
规则ID	规则描述	类型	匹配条件	匹配内容	规则开关	操作	
		请求白名单	前缀匹配	/api		编辑删除	

#### 5. 在场景化管理中,选择目标场景,单击右侧的查看配置。



BOT防护	BOT白名单					
场景化管理新建场县	全部场景类型 ▼ 仅查署生效场景	仅查看默认场景 ①		清輸入	场最名称	Q
优先级: 1	场景名称 <b>te</b> 场景ld:3 登录 刘贤器H5 小程序	<ul> <li>         ・ 请求路径 き         ・         ・         ・</li></ul>	动作策 略 <b>1</b> 条	自定义规 则 <b>9</b> 条	生效状 态	查看配置 编辑场展 删除场展

6. 在场景详情页面,单击该场景下前端对抗模块的 , 防护模式选择 拦截,开启该前端对抗功能。

场景配置	
前端对抗 第一道拦截 ①建议数感目录下开启此功能 检测客户端对Web或H5页面访问中可能存在机器人和恶意爬虫行为,保护网站业务安全。	查看文档 🛽
开关 防护模式 O 监控 重定向 人机识别 拦截	

7. 使用 Chrome 请求结果如下所示:

← → C ▲ 不安全   .com/login.php				
NAME OF TAXABLE PARTY OF TAXABLE PARTY.				
Paused in debugger 1	DevTools is now available in Chinese!	ways match Chron	Inne's language         Switch DevTools to Chinese         Don't show again           Performance         Memory         Application         Security         Lighthouse         I	Recorder 👗
bwapp	Page Filesystem ≫ :			
an extremely buggy we	<ul> <li>b3c79ec/f890b6f5917</li> <li>images</li> <li>js</li> </ul>		೫ P Open file ೫ ☆ P Run command	
Login New User Info Talks & Trai	stylesneets     login.php		Drop in a folder to add to workspace Learn more about Workspaces	
/ Login /				

## 威胁情报

威胁情报功能依托腾讯近二十年的网络安全经验和大数据情报,将通过实时判定 IP 状态,采取打分机制,量化风险值,精准识别来自恶意动态 IP、IDC 的访问,同时智能识别恶意爬虫特征,解决来自恶意爬虫、分布式爬虫、代理、撞库、薅羊毛等风险访问。

① 说明 开启威胁情报功能前,需要确认业务是否存在 IDC 侧的用户访问。如果确认业务有 IDC 流量访问,应先关闭威胁情报中的 IDC 网络识别开关,然而 开启威胁情报功能。	言再
1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择 <b>配置中心 &gt; BOT 与业务安全</b> 。	
2. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。	
BOT与业务安全 III	帮助说明

BOT管理	业务安全							0.0000
BOT概览 S	iaaS型			当前全局策略:	<b>全局设置</b> 以下機块设置项将会应用于当前域名	下的全部场景		A。人机识别设置 前往设置
ĕ	の11管理 登布法量	±≫## 7 ↑	<sup>场景总数</sup> 9 条		新練9抗 ① ● 象 前往記録	智能分析 ① 33 条 前往配置	会活管理 <b>1</b> 条 前往配置	合法观虫 2 条 前刊起版

3. 在 BOT 管理页面,在全局设置中,单击智能分析的前往配置。



<b>全局设置</b> 以下模块设置项将会应用于当前域名下的全部场景 2. 人机识别设置前往设置					
前端对抗 ①	智能分析 ①	会话管理	合法爬虫		
<b>O</b> <sub>条</sub>	33 <sub>条</sub>	<b>1</b> <sub>条</sub>	<b>2</b> <sub>条</sub>		
前往配置	前往配置	前往配置	前往配置		

4. 在威胁情报页面,如果有 IDC 流量访问,单击 IDC 网络的一键关闭,关闭功能。

<b>智能分析</b> 通过威胁情	报、AI 策略、智能统计和UA策略,多维度、智能化识别BOT行为访问,实现风险访问的精准拦截。	;
威胁情报(16)	AI策略(0)   智能统计(7)   UA策略(10)	
③ 这是一个全局	<b>]策略,对威胁情报的修改将会对到当前域名下的全部场景生效</b>	不再提醒  >
DC网络		
一键开启	一键关闭	
IDC网络类型	IDC网络描述	规则开关
Aws	IP归属于Amazon Web Services(AWS)(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被	正常 🔵
Azure	IP归属于Microsoft Azure(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被正常用户使用	
Google	IP归属于Google Cloud Platform(GCP)(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会	被正
UCloud	IP归属于UCloud(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被正常用户使用。	
阿里云	IP归属于阿里云(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被正常用户使用。	
百度云	IP归属于百度云(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被正常用户使用。	
华为云	IP归属于华为云(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被正常用户使用。	
金山云	IP归属于金山云(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被正常用户使用。	
pubyun	IP归属于pubyun(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被正常用户使用。	
青云	IP归属于青云(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被正常用户使用。	
腾讯云	IP归属于腾讯云(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被正常用户使用。	
<b>威胁情报库</b>		
一键开启	一键关闭	
威胁情报库类型	威胁情报库描述	规则开关
BOT机器人	基于腾讯安全威胁情报提供的威胁情报,结合WAF实时检测出的爬虫IP源IP进行分析结合,得出的IP情报库,不会被正	常用
网络攻击	基于腾讯安全威胁情报提供的入站威胁情报IP,这些IP在威胁情报存活有效期内发起大量攻击,存在大量恶意扫描行为,	不
网络代理	基于腾讯安全威胁情报提供的代理威胁情报,这些IP被爬虫/灰黑产利用,不会被正常用户使用。	
扫描器	腾讯安全威胁情报实时统计提供的全网恶意扫描行为攻击源IP情报库。	

5. 如果没有 IDC 流量访问, 在场景化管理中,选择目标场景,单击右侧的**查看配置**。



BOT防护 BC	DT白名单					
场景化管理						
新建场县 优先级: 1	全部场景类型 ▼ 仅查看生效场景	(な豊春新以均長())		请输入	场景名称	Q
0	场景名称	● 清求路径 き	动作策略	自定义规 则	生效状 态	查看配置
2+	场最id: 3	😯 2022-112 王 前端对抗 🚺 威胁情报 🔮 AI策略 🔮 智能分析 🔮	1	٥		编辑场景
	登录 浏览器/H5 小程序		条	フ衆		加炸物素

6. 在场景详情页面,单击智能统计,单击该场景下威胁情报模块的 , 直接开启威胁情报功能即可。

验作得分配置	
成加設作業額 設作業額印         可設置 6 条1 F2起置 1 条	<b>Q</b>
1:::?##::100         取引度松策等         全部范围         系机规则         紙線 動物	ti ti

## AI 策略

AI 策略功能基于人工智能技术和腾讯风控实战沉淀,将风控特征和黑灰产对抗经验转化为 AI 策略模型,通过访问流量进行大数据分析与 AI 建模,实现快速识别 恶意访问者、深层次恶意访问者,解决来自高级持续性威胁 BOT、隐蔽性威胁 BOT 的风险访问行为。

① 说明 AI 策略是根据 AI 建模自动学习,可直接开启;如果有误评估,将对相应 URL 加白即可。

## 开启 AI 策略

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择配置中心 > BOT 与业务安全。
- 2. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。

BOT与业务安全	Ţ						③ 服助说明
BOT委道 SaaS型			当前全局策略:** LT* H	全局设置以下模块设置项将会应用	于当前域名下的全部场景		2。人机识别设置 前住设置
BOT管理 室前注意	±∞%## 7 介	场限总数 9 条		前端对抗 ① 〇余 前往記載	智能分析① 33条 前往配置	会活管理 1 条 前往起 <b>双</b>	合法原虫 2 余 町住配置

3. 在场景化管理中,选择目标场景,单击右侧的查看配置。

BOT防护	BOT白名单					
场景化管理						
新建场县	全部场暴类型 ▼ 仅查看生效场	展 □ 仅査看默认场最 ()		请输入	场最名称	Q
优先级: 1						
	场景名称	● 请求路径 €	动作策	自定义规	生效状	
2	te	O 2022-11-2 <sup>4</sup>	略	则	态	三者和王
	场暴id: 3	王·前端对抗 🚺 威胁情报 🔮 AI策略 🤡 智能分析 🤡	1	g		新時時の加減
	登录 浏览器/H5 小程序		■ 条	┛条		00.0 Hole 77.0 See

#### 4.切换 AI 策略开关,即可启用 AI 策略。



<b>智能分析</b> 第三連結 著這個為特点、AI 製織和智能統計。多维度、智能化识到801行为访问,实現风险访问的精	息拦截,	金稽文档 经

## 添加白名单

## 背景信息

#### 在 AI 策略页面,该请求为正常请求,但是被 AI 误报。

在AI评估模块中,此处展示的是异常数据,特征数据和OP,即为异常。数值到高档异常。					
三 请求特征异常信息					
URL重复率异常度 ③	0 (URL重复率特征值: 0.25)	URL种类异常度 ①	<b>4.54↑</b> (URL种类特征值: 10)	URL最大次数异常度 ①	0 (URL最大次数特征值: 1)
URL最小次数异常度 🕥	0 (URL最小次数特征值: 0)	平均速率异常度 🛈	0 (平均速率特征值: 1.67)	请求数量异常度 🚯	0.32↑ (请求数量特征值: 12)
会话时间异常度 🛈	0 (会话时间特征值: 1)				
匠 Cookie异常信息					
Cookie重复率异常度 ①	Q ⟨Cookie重复率特征值: 0.5⟩	Cookie最大重复比异常度 ①	0.95↑ (Cookie最大重复比特征值: 5)	Cookie种类异常度 ①	<b>2.24↑</b> (Cookie种类特征值: 0)
User-Agent异常信息					
User-Agent重复率异常度 ①	0 (User-Agent重复率特征值: 0)	User-Agent种类异常度 ③	<b>0</b> (User-Agent种类特征值: 0)	User-Agent合法量占比异常	度 ① 0(User-Agent合法量占比特征值: 0)
User-Agent随机种类占比异常	度 ① 0 (User-Agent随机种类占比特征值: 0)	User-Agent出现最多的占比界	常度 🕦 0(User-Agent出现最多的占比特征值: 0)		
■ Referer异常信息					

#### 操作步骤

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择**配置中心 > BOT 与业务安全**。
- 2. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。

BOT与业务安全 BOT管理 业务安全	×						③ 常動出網
BOT模范 SaaS型			当前全局策略: 一一列上世界	全局设置 以下模块设置项将会应用	于当前端名下的全部场景		A。人机识别设置 前往设置
807管理 全名注意	<sup>主欢场限</sup> <b>7</b> 个	瑞费总数 <b>9</b> 条		前職対抗 ① 〇 <u>条</u> 前往記置	智能分析 ① 33 <sub>条</sub> 称tt配置	会话管理 <b>1</b> 杂 前往配置	合法原虫 2 条 附住紀風

3. 在 BOT 管理页面,在全局设置中,单击智能分析模块的前往配置。

全局设置以下模块设置项将会应用于	当前域名下的全部场景		名 人机识别设置 前往设置
前端对抗 🛈	智能分析 ①	会话管理	合法爬虫
<b>O</b> <sub>条</sub>	33 <sub>*</sub>	1 <sub>条</sub>	<b>2</b> <sub>&amp;</sub>
前往配置	前往配置	前往配置	前往配置

4. 切换到 AI 策略页面,单击**添加白名单**,输入名称、描述和加白 URL,单击确定。



智能分析 通过	t威胁情报、AI 策略、智能统计和UA策略,多维度、智能化识别BOT行为访问,实现风险访问的精准拦截。
威胁情报(1	5) AI策略(0) 智能统计(7) UA策略(10) №
() 这是-	一个全局策略,对AI策略的修改将会对到当前域名下的全部场景生效
添加白名单	
添加白名单	Ê.
策略名称	最多128个字符
策略描述	最多128个字符
加白URL *	填写加白路径,以"/开头,最多128个字符
规则开关	
	确定 返回

## 智能统计

智能统计功能基于大数据分析统计,根据用户群体的流量特征自动分类,自动识别存在异常的恶意流量,通过大数据分析,自动调整恶意流量阈值,解决来自常规 BOT、高频 BOT 的风险访问,并通过自动调整统计模型,解决大部分的 BOT 行为绕过问题。

(	<b>〕说明</b> 可直接开启智能统计,推荐使用智能模式。
4 71	

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择**配置中心 > BOT 与业务安全**。
- 2. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。

BOT与业务安全 ::	·						⑦ 相助说明
BOT概览 SaaS型			当前全局策略:	<b>全局设置</b> 以下模块设置项将会应用:	于当前城名下的全部场景		A。人机识别设置 前往设置
BOT 新聞 全新改量	<sup>生效场限</sup> 7 ↑	<sup>场展总数</sup> <b>9</b> 条		前100月前 0余 前往記聞	離傷分析 ① 33 条 前住配置	会话着理 1 余 能往起:蓝	合法原虫 2 条 刷社配置

3. 在 BOT 管理页面,在全局设置中,单击智能分析模块的前往配置。

全局设置 以下模块设置项将会应用于	-当前域名下的全部场景		♀ 人机识别设置 前往设置
前端对抗 🚯	智能分析 ①	会话管理	合法爬虫
<b>O</b> <sub>条</sub>	33 <sub>条</sub>	1 <sub>条</sub>	<b>2</b> <sub>条</sub>
前往配置	前往配置	前往配置	前往配置

4.切换到智能统计页面,即可调整智能统计配置。



<b>智能分析</b> 通过威胁情报、AI 策略、	智能统计和UA策略,多维度	、智能化识别BOT行为访问,第	实现风险访问的精准拦截。	×
威胁情报(16)   AI策略(1)	智能统计(7)	UA策略(10) NEW		
<ul> <li>这是一个全局策略,对智能</li> </ul>	分析的修改将会对到当前域	名下的全部场景生效		不再提醒 ×
名称/描述	模式		修改时间 🗲	规则开关
会话平均速度 会话平均访问速度,单位为:次…	● 智能推荐 🛛 宽松	○ 中等 ○ 严格	2024-12-31 15:52:12	
会话总次数 会话发生的总访问次数	○ 智能推荐 ○ 宽松	○ 中等 <b>○</b> 严格	2024-11-11 16:08:47	
Referer种类 会话请求中Referer去重后的数目	2 智能推荐 2 宽松	○ 中等   ○ 严格	2024-11-11 16:08:55	
会话持续时间 会话持续时间	🔵 智能推荐 🛛 💿 宽松	○ 中等 ○ 严格	2024-11-11 16:08:51	
UserAgent种类 会话请求中UserAgent去重后的…	🗌 智能推荐 🛛 오 宽松	○ 中等 ○ 严格	2024-11-11 16:08:31	
Cookie种类 会话请求中Cookie去重后的数目	● 智能推荐 🔷 宽松	○ 中等 ○ 严格	-	
URL种类 会话请求中URL去重后条目数	● 智能推荐 🛛 宽松	○ 中等 ○ 严格	-	

## 动作策略

动作设置功能通过威胁情报、AI 策略、智能统计对网站的访问请求进行综合性打分。打分范围在0-100分范围内,分数越高 BOT 的可能性越高、其访问对网站 产生的危害/压力则越大。通过分数智能识别访问行为的风险程度,用户可配置不同动作策略和每个动作策略相应的生效范围和不同分数段的动作实现风险访问的 精准拦截。

#### 背景信息

当威胁情报,AI 策略以及智能统计标记出了大量流量,默认配置无法做到更加详细的拦截,需要自定义动作如何分析配置。

#### 操作步骤

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择 BOT 流量分析。
- 2. 在 BOT 流量分析页面,左上角选择需要防护的域名,选择所需访问源,单击查看详情。

加黑名单 查看详情当前仅支持展现	<当前访问源最新的	BOT详情											
访问源    会话ID	地区	域名	请求路径	处置动作 ▼	访问次数 🕏	检出模块 ▼	BOT得分 🕈	BOT标签 ▼	威胁情报 ▼	智能分 T	统计特 ▼	聚合时间 \$	操作
	♥ 成都		1	⊙ 未处置	1	智能分析	37	疑似BOT	腾讯云 ID	威胁情报		2022-03-21 05:05:00	查看日志 <mark>查看详情</mark> 加黑名单

3. 在 BOT 流量详情页面的基础会话信息模块,查看城市和 IP 地区。



<b>124</b> . 后 恶意BOT					加白名单加黑名	单 添加自定义规则	<ol> <li>分布为造中时间段内的 BOT得分分布</li> <li>300,000</li> </ol>	的统计,不直接展示当前访问源最新一次会 BOT动作占比
	存在风险 <sup>国一次请读得分</sup> 56 <del>分</del>	<ul> <li>(1) 会话次数</li> <li>(1) 访问目的</li> <li>(1) 异常特征 威胁情报模型</li> </ul>	次 决异常,AI评估模块异常,智能	策略ID 能统计模块异常	命中礙块 ③ 自定义		250,000 200,000 150,000 50,000 3752	563) BOTI#\$?
基础会话信息 IP基础信息	请求特征信息 威胁情报	AI策略 智能统计						
访问源IP IP类型	124 €iDC		城市 IP所有者	上海 腾讯云		IP地区	中国	
C 运运差偿信息 会话平均速度 会话持续时间	380.67次/分钟 10213.13分钟		会话总次数	3887850		是否存在Robots.bt	否	

- 4. 当业务没有该地区的流量时,则表明此处评分为异常,可以自定义动作设置,进行一个更加细化的设置。
- 5. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。

BOT与业务安全 + 1							(7) #85/249
BOT概算 Sas5型			当前全局策略:	<b>全局设置</b> 以下模块设置项将会应用于当前域	名下約全部场景		A。人机识别说面 前往说面
	<sup>生致场表</sup> 7 介	场景总数 9 条		的加时机 ① O条 的往起服	新能分析 ① 33 条 前往配置	会活新理 <b>1</b> 条 前住配置	合油局虫 2条 的性形度

6. 在场景化管理中,选择目标场景,单击右侧的查看配置。

BOT防护	BOT白名单					
场景化管理	· · · · · · · · · · · · · · · · · · ·					
新建场景 优先级: 1	全部场景类型 ▼ (仅查看生效	場果 □ 仅重看款以场景 ①		请输入:	场景名称	Q
	场最名称	の请求路径自	动作策	自定义规	生效状	古石和雪
2	te te	2022-11-21	略	凤山	态	全場探見
	场景は 3 登录 浏览器/H5 小程序	王 前弟对抗 🚯 成肋情报 📀 AI策略 🥑 智能分析 🥑	1 条	9 <sub>条</sub>		删除场景

7. 在场景详情页面,单击该场景下动作策略模块的**新增动作策略**。

智能分析第三道拦截 通过威胁情报、AI 策略和智能	统计,多维度、智能化识别BOT行	为访问,实现风险访问的精准拦截,				
越齢情报( で) 前往配置	D			UR	UA策略 ③ 前往配置	
动作得分配置						
激加动作策略 可配置	[5条 已配置1条					
动作策略ID	优先级	动作策略	生效范围	规则类型	规则开关	操作
	100	默认宽松策略	全部范围	系统规则		编辑 删除

8. 在动作策略页面,配置相关参数,单击**立即发布**。



效范围	请求路径 前缀匹	配 /			
ቼ略名称★	请输入一个策略名	名称,最长20个字符			
关*					
.■ *	● 全部范围	自定义范围			
į.*	- 1 ·	+			
	请输入1-100的整数	a,数字越小,代表这条策略的执行优先	元级越高		
略模式设置	*				
Ø	宽松模式	⊘ 中等模式		④ 严格模式	⑦ 自定义模式
作设置实时分	分布 ④				
作设置实时分	分布 ①	■ 信任 ■ 监控 ■	🧧 重定向 📕 人机	只別 ■ 拦截	
作设置实时分 分数(0-100	分布 ①	■ 信任 ■ 监控 ■ 动作	🧧 重定向 📕 人机	只別 ■ 拦截	操作
作设置实时分 分数(0-100 0	<ul> <li>分布 ①</li> <li>分)</li> <li>- 35</li> </ul>	<ul> <li>信任 上 监控</li> <li>动作</li> <li>信任</li> </ul>	● 重定向 ■ 人机	R别 ■ 拦截 标签 正常流量 ▼	操作 删除 添加
作设置实时分 分数(0-100 0 35	35 - 90	<ul> <li>■ 信任</li> <li>■ 监控</li> <li>□ 动作</li> <li>□ 信任</li> <li>□ 监控</li> </ul>	<ul> <li>重定向</li> <li>人机</li> <li>人机</li> </ul>	R别 ■ 拦截 标签 正常流量 ▼ 疑似BOT ▼	操作 删除 添加 删除 添加
作设置实时分 分数(0-100 0 35 90	<ul> <li>分布 ④</li> <li>分布 ④</li> <li>35</li> <li>90</li> <li>100</li> </ul>	<ul> <li>■ 信任</li> <li>■ 监控</li> <li>□ 动作</li> <li>□ 监控</li> <li>□ L払収別</li> </ul>	<ul> <li>重定向</li> <li>人机</li> <li>▼</li> <li>▼</li> <li>▼</li> </ul>	R别 ■ 拦截 标签 正常流量 ▼ 疑似BOT ▼ 恶意BOT ▼	<ul> <li>操作</li> <li>删除添加</li> <li>删除添加</li> <li>删除添加</li> <li>删除添加</li> </ul>

#### 参数说明:

- 策略名称:填写动作策略名称。
- **生效开关**:当前动作策略是否生效。
- **生效范围**:当前动作策略的生效范围。
- 优先级:当前动作策略的执行优先级,请输入1-100的整数,数字越小,代表这条策略的执行优先级越高。
- 模式设置: 提供宽松模式、中等模式、严格模式、自定义模式这四种默认处置模式,宽松、中等、严格这三种模式为预设模式,分别代表 BOT 流量管理 针对不同危害程度的 BOT 的推荐分类及处置策略。这三种预设模式可进行修改,修改后为自定义模式。
- 分数段设置:分数段区间总分数为 0−100 分,每个分数段总共可以添加10条,配置的分数区间范围左闭右开,分数段不可重合,分数区间可设置为空, 设置为空时,空的分数段不处置动作。
- 动作设置:可设置为信任、监控、重定向(重定向至特定网站 URL)、人机识别(验证码)或拦截。
- 标签设置:可设置为友好 BOT、恶意 BOT、正常流量或疑似 BOT。
  - 友好 BOT:识别为对网站友好/合法的 BOT。
  - 疑似 BOT:识别该访问源流量疑似 BOT,但无法判断其对网站是否有害。
  - 正常流量: 识别为人为访问的正常流量。
  - 恶意 BOT: 识别为对网站产生恶意流量/访问请求不友好的 BOT。

## 合法爬虫

通过配置合法爬虫(如:搜索引擎、订阅机器人)可以正常获取网站数据,使网站可以正常被索引。

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择**配置中心 > BOT 与业务安全**。
- 2. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。



B0T与业务安全 1 1	Ţ						(2) Marina
BOT概算 SanS型			当前全局策略:	全局设置 以下模块设置项将会应用	于当前域名下的全部场景		名人机识别设置 前往设置
	±xx## 7 ↑	<sup>法费益数</sup> <b>9</b> 条		前線对抗 ① 〇 条 前往記題	智能分析 ① 33 条 前往都置	会话管理 1 条 前往記题	合法原当 2 余 80任起王

#### 3. 在 BOT 管理页面,在全局设置中,单击合法爬虫模块的前往配置。

<b>全局设置</b> 以下模块设置项将会应用于	当前域名下的全部场景		♀人机识别设置前往设置
前端对抗 ①	智能分析 🗊	会话管理	合法爬虫
<b>O</b> <sub>条</sub>	34 <sub>条</sub>	<b>1</b> 条	<b>2</b> <sub>条</sub>
前往配置	前往配置	前往配置	前往配置

4. 在合法爬虫页面,可单击 \_\_\_\_\_,开启对应功能。

合法爬虫					×
BOT类型	规则描述	处置动作	开关	修改时间	
搜索引擎机器人	机器人爬取或审查Internet	☞ 信任		2022-03-17 14:46:11	
订阅机器人	机器人在互联网上爬取并寻	☞ 信任		2022-03-17 14:46:10	

## 自定义规则

通过配置自定义规则功能,可精准处置符合行为配置的爬虫,精准处置对应特征的访问特征请求。

#### ▲ 注意

- 目前在创建 BOT 场景化时,已经根据场景类型内置相应场景的自定义规则集。
- 本功能主要分析数据来源于 BOT 流量分析 。
- 该内容只做使用分析参考,不能当做业务标准配置,网络爬虫分为很多种,会随业务类型而变化。

#### 案例详情

目前通过动作得分进行拦截无法满足更精细的对抗需求,需要对异常行为特征进行设置,在 BOT 流量分析进行查看出大概异常后,单击**详情**,可查看异常数据指 标,并结合实际业务情况进行对比。

例如:URL 重复性是1,会话次数100次/分钟,UA 滥用等,就需要结合业务是否有访问相同的请求或者是代理等业务,如果没有就说明有人恶意攻击。那么就 可以根据以下方式查看并配置拦截策略。

#### 分析案例

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择 BOT 流量分析。
- 2. 在 BOT流量分析页面,左上角选择需要防护的域名,选择所需访问源,目前根据展示,能看到该 IP 请求速度很快,URL 单一,并且是 IDC 类。

加風名单  查看详情	当前仅支持展示当前访问	可源最新的BOT详情											•	
访问源	会话ID	地区	域名	请求路径	处置动作 ▼	访问次数 \$	检出模块 ▼	BOT得分 <sup>拿</sup>	BOT标签 ▼	威胁情报 ▼	智能分析特 下	统计特征异常 🔻	聚合时间 \$	操作
10		<b>♀</b> 广州	mc /	1	⊖ 未处置	56717	智能分析	53	提似BOT	腾讯云 IDC	威胁情报, AJ	会话平均速度	2022-03-05 22:40:00	查看日志 查看详情 如黑名单
	-	<b>♀</b> /°́́́́́́́́́́́́́́́́́́́́́́́́́́́́́́́́́́́́	ľ	1	⊙ 未处置	5720	智能分析	53	提似BOT	腾讯云 IDC	威胁情报, Al	会话平均速度	2022-03-05 22:35:00	查看日志 查看详情 如黑名单

3. 单击**查看详情**,通过基础会话信息可以看出,会话速度平均次数,总次数。也可以直接根据该条件进行设置。



<b>124. )</b> <sub>百</sub> 恶题BOT		加白名单   加黑名单	添加自定义规则	<ol> <li>OT得分分布为选中时间段内的 BOT得分分布 BOT动作</li> </ol>	统计,不直接展示当前访问源最余 作占比
<b>存在风险</b> <sup>風后一次演求得分</sup> 56 分	<ul> <li>会話次数 3887850 次</li> <li>访问目的 .com</li> <li>异架特征 威胁情报模块异常,AI评估模块异常,智能统计</li> </ul>	<ul> <li>命中限块</li> <li>① 自定义</li> <li>策助日 300<sup>1</sup></li> <li>機块界常</li> </ul>		300,000 250,000 150,000 150,000 50,000 3759 — BDI	56分 復分
▲如云道信息 请水行化信息 威胁情报 ■ IP基础信息	AI東略 智能犹计				
访问源IP IP类型 <b>登IDC</b>	城市 IP所有者	上海 腾讯云	IP地区	中国	
C) 会话基础信息					
会话平均速度 380.67次分钟 会话持续时间 10213.13分钟	会话总次数	3887850	是否存在Robots.txt	Ϋ́Ξ	

#### 4. 在威胁情报页面,可以根据情报数据判断该 IP 是否有正常用户使用过。

IDC网络           IDC用型         IDC描述           構造         IPD属与随讯云 (IDC IP) IP库,这些P段经常被能由用于部署能由信序或用作代理,而不会被正常用户使用,	基础会话信息	请求特征信息	威胁情报	AI策略	智能统计
IDC借述           勝抗云         IPD属与脑讯云 (IDC IP) P库,这些P段经常被爬虫用于部署爬虫相序或用作代理,而不会被正常用户使用,	IDC网络				
勝讯云 IPDI属与路讯云(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被正常用户使用。	IDC类型				IDC描述
	腾讯云				IP归属与腾讯云(IDC IP)IP库,这些IP段经常被爬虫用于部署爬虫程序或用作代理,而不会被正常用户使用。

#### 5. 在请求特征信息页面,可以查看请求详情。

基础会话信息 请求特征们	<b>言息</b> 威胁情报 AI策略 智能统计				
E 请求特征信息					
URL重复比	<b>1</b> (参考值:0~1)	URL种类 🛈	1	URL最小深度 🛈	4
URL最大深度 🛈	4	URL平均深度 ①	4	URL数量 ③	371
匠 Cookie信息					
Cookie是否滥用 ①	否	Cookie存在性 ①	否	Cookie重复性 ③	<b>0</b> (参考值: 0~1)
Cookie有效率 🛈	0	出现最多的Cookie 🛈		出现最多的Cookie比例 ①	0
<b>⊍</b> User-Agent信息					
User-Agent类型 ①		User-Agent存在性 ①	是	User-Agent随机性指数 🛈	<b>0</b> (参考值: 0~1)
User-Agent种类 3	1	User-Agent有效比 ③	1	出现最多的User-Agent ④ Mozilla/5.0 (Windows NT 10.	0; Win64; x64) AppleWebKit/
出现最多的User-Agent占比(	0 1	User-Agent相似性比例 🛈	0		

### 策略配置

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择配置中心 > BOT 与业务安全。
- 2. 在 BOT 与业务安全页面,左上角选择需要防护的域名,单击 BOT 管理。

807与业务安全		• Matican
BOTHER BRACE SERVER SALES SALE	全局设置 以下制除体表现将会组用于当前结核下的全部运用     和田切坊 ① 和田田切坊 ② 金田田明 ③ 会祖昭明     〇 余 333 余 1 余     日の記名     日の記名	ネ人形(1931年3月 会演奏集 2 条 町192月

3. 在场景化管理中,选择目标场景,单击右侧的查看配置。



BOT防护	BOT白名单					
场景化管理						
新建场县	全部场景类型 ▼ 仅查看生效场景	仅至著默认场景①		请输入	场景名称	Q
优先级:1						
	场景名称	の请求路径も	动作策	自定义规	生效状	本美和美
2	te	O 2022-11-21	略	则	态	逆境接足
	场最id: 3	📑 前端对抗 🔒 威胁情报 오 AI策略 오 智能分析 오	1	٩		
	登录 浏览器/H5 小程序		● 条	シ条		加速水物家

#### 4. 在场景详情页面,单击自定义规则模块的**添加规则**。

场景配置		
前端对抗 第一道拦截 ① 建议敏感目录下开启此功能 检测客户端对Web或H5页面访问中可能存在机器人和恶意爬虫行为,保护网站业务安全。 开关 ① 防护模式 ② 监控 ② 重定向 ② 人机识别 ② 拦截		查看文档 🕻
<b>自定义规则</b> 第二道拦截 用户可以通过读功能,精准处置符合行为配置的爬虫,精准处置对应特征的访问特征请求。		查看文档 🖸
添加规则	请输入规则名称	Q Ø

5. 在添加自定义规则窗口中,根据上述分析,将 URL 重复率设置为大于70%(过程中仅该数据超过70%),将会话速度设置为大于500次/分钟,然后单击**确 定**。

添加自定义规	2,90]							
规则名称 *	请输入规则名称,最长50个字符							
规则描述	选填, 最长256个字符	0/256						
规则开关		0,200						
匹配条件 *	匹配字段 匹配参数	逻辑符号 ① 匹配内容	操作					
	URL重复比 ③ ~	大于 ~ 70	% 删除					
	会话平均速度 ③ ~	大于 ~ 500	次/分 <b>删</b> 除 钟					
		添加 还可以添加8条,最多10条						
执行动作 *		前拦截页面 自定义返回内容						
优先级	记录攻击日志且拦截请求,返回拦截页面 - 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高;相同优先级下,创建时间越晚,优先级越高							
自定义标签 🔹	恶意BOT Y							
生效方式 *	永久生效 定时生效 周粒度生效	月粒度生效						

## 解析验证码



当客户端类型为 App、小程序、客户端以及跨域调用时,由于无法解析识别来自 WAF 下发的验证码,导致 BOT 流量管理在下发人机识别动作时,无法正常解 析及弹出人机识别验证码,用户便无法正常进行人机识别交互,在触发多次验证码后,造成正常用户的访问请求被拦截,导致业务受损。 因此,在配置处置动作为人机识别时,需要对前端/客户端业务进行针对性改造,使其可以适配相关验证码,相关改造文档可参见 前后端分离站点接入 WAF 验证 码。

## API 安全相关





## API 安全实践教程

最近更新时间: 2024-06-19 10:20:11

## 功能简介

用户可以在 <mark>接入管理页面</mark> 开启 API 安全分析功能,并结合 API 流量分析 、 API 资产管理 、API 安全、事件管理 、访问日志等功能观察并分析 API 资产及风险 情况,针对性进行策略设置,保护网站 API 资产和业务免受网络攻击和侵害,避免敏感数据泄露。

API 安全实践教程流程如下所示:



## 前提条件

- API 安全需要购买 WAF 对应实例的版本。
- 在 接入管理页面,选择需要防护的域名,并开启 API 安全开关。

(入管理 域名接入	<b>、</b> 对象接入									◎ 援入	指引 域名列表扬	<b>操作指南</b>
添加	域名发现域名	请选择实例	<b>▼</b> (†	选择实例类型	v		获耳	双鼠标焦点即可选	择过滤属性		Q	¢
	域名/接入状态 ▼	实例信息 🕄	实例ID/实例名称	使用模式 ▼	回源保护地址 🛈	BOT开关	API安全	IPv6开关	WAF开关 <b>T</b>	访问日志 ▼	操作	
				规则:拦截模式							编辑 删除 基础》 BOT与业务防护 更多 ▼	防护
				规则: 拦截模式							编辑 删除 基础 BOT与业务防护 更多 ▼	防护

## API 流量分析

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择安全可视 > API 流量分析。
- 2. 在 API 流量分析页面,左上角选择相应的域名,右侧展示当前域名是否开启 API 安全。





#### 展示说明:

字段名称	说明
API 资产概览	统计当前域名下,API资产总数和相应状态资产数量。
API 风险概览	统计当前域名下,风险 API、涉敏 API 和 API 事件相应数量。
资产活跃状态相关	统计当前域名下,活跃 API 和不活跃 API 排名、数量及趋势。
涉敏 API 相关	统计当前域名下,涉敏 API 的分类、排名和占比分布。
API 事件相关	统计当前域名下,新发现的 API 事件风险占比、关联事件数排名、事件类型占比、事件 数量及趋势。

3. 通过单击统计图表中的文字, 跳转前往 API 资产列表/ API 资产详情界面。



活跃API TOP5		API资产管理 查看更多
		600
	查看API资产	
	65	
	50	
	50	

## API 资产管理

用户可通过流转 API 资产状态,对相应 API 资产进行管理和标记,方便后续对 API 资产进行统计、分析和处置。 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择**资产中心 > API 资产管理**。

2. 在 API 资产管理页面,左上角选择需要防护的域名,右侧展示当前域名是否开启 API 安全。

资产管理 ♥ Ø API安全开关;	376						◎ 场景教学
PI概定				API处理状态			
APIG产概见 形发现API	过去7日清新API	过去7日失语API	活用数量	CRILAPI	硼U,中API	已忽略API	
<b>1583</b> ↑ <b>1574</b> ↑	<b>1580</b> ↑	3↑	11 ∻	3↑	3↑	↑	

3. 在 API 资产管理页面,选择要状态变更的 API,单击该 API 资产对应的资产状态或状态变更。

API资产管理	▼ ③ API安全开关已开启							◎ 法景数学
арі <b>жі</b> <sup>дрідт</sup> щі 1583 ↑	nx≋an 1574↑	:::#7⊟1588# 1580 ↑	<u>:1578%</u> арі З↑	::##¥## 11↑	арыныка Ванларі <b>З</b> т	:80.04449 <b>3</b> ↑	езвая ↑	
9X #X <u>2-8</u>	2023-02-17 - 2023-02-24 🛅 🗌 (2.8.83)/@API							
<b>北田時以</b> 此田市時	金部请求方式 ▼					多个关键	(半用登线 11 分類、多个过滤板並用包车被分類	σ ο φ ∓
API	风险等级 <b>Y</b>	所属城名	功能场景 ▼	数据标签 ▼ 最否无欲 ▼	追户状态 ▼	最近更新时间 \$	发现时间 \$ 独作	
GET A 1750	de To get	A. 15	R#	身份证〔… 是 固定电话…	- 3132/12	21 151	2. 1 :17	e enima
POST to To	<u>8</u> 8	a u	*51	8	• 85 20 512	202 1:18	20: : 18	E BRITH

4. 在状态变更窗口中,修改相关参数,单击**提交**。

状态变更		×
新发现	用户名 *	
确认中	: 5	
已确认	备注	
已下线	请输入备注, 100 字以内	
已忽略		
	提交取消	Ĭ

状态变更说明:



字段名称	说明
用户名	默认填充当前控制台账户名称,支持用户自定义
备注	状态备注描述,最多100个字。
状态	涵盖新发现/确认中/已确认/已下线/已忽略五种状态。

#### 5. 在 API 资产管理页面,选择要查看资产详情的 API,单击操作列中的查看详情。



#### 详情 TAB 页说明:

字段名称	说明
API 概览	当前 API 的访问趋势、访问来源分布以及请求特征统计。
API 攻击概览	当前 API 的攻击趋势、异常请求 TOP 统计。
参数样例	当前 API 的请求数据和响应数据。
参数列表	当前 API 请求和响应数据中的参数。
关联事件	当前 API 的关联风险事件列表。
资产变更历史	当前 API 资产的状态变更历史和备注等信息。

## 事件管理

用户可通过流转 API 实践状态,对相应 API 事件进行管理和标记,方便后续对API资产进行统计、分析和处置。

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择**事件管理**。
- 2. 在事件管理页面,左上角选择需要防护的域名,右侧展示当前域名是否开启 API 安全。
- 3. 在事件概览,可以查看当前事件总数及各状况事件数。

事件管理 API事件	▼ 🕝 API安全	于关已开启			◎ 场景教学
<b>事件概览</b> 事件総数 3 个	<ul> <li>今日新增</li> <li>3 个</li> </ul>	新发現     3 ↑	〇〇 已	び	<ul> <li>○ <sup>己忽略</sup></li> <li> ↑</li> </ul>



#### 4. 在事件列表中,选择要变更状态的事件,单击该事件对应的**处置状态**或**状态变更**。

今天昨天	近一周 20	23-04-19	~ 2023-04-19 🛅							
事件分类		批量	<b>炒</b> 置 批量忽略	全部请求方式	¥		多个关	键字用竖线 " " 分隔,多个ì	过滤标签用回车键分隔	Q ¢ ‡ <u>†</u>
全部事件类型	3		事件ID	事件类型 ▼	車件等级 ▼	关联API	外置状态 ▼	发现时间 ±	局近更新时间 ★	操作
▼ 账号异常	3			编度攻击	***	POST	. 05 49 20	2022-04-19 16:54	2022-04-19 16:54	· · · · · · · · · · · · · · · · · · ·
恭刀蚁 <u></u> 恶意注册	1			1至1年4天山	<b>四)</b> (四)	1001	* 8/122,4%	2020-04-18 10.04	2023-04-18 10.34	
撞库攻击	1		6	恶意注册	高危	POST	• 新发现	2023-04-19 16:55	2023-04-19 16:55	状态变更 宣看详情
			ō	暴力破解	高危	POST	• 新发现	2023-04-19 16:55	2023-04-19 16:55	状态变更 查看详情
		共3项							20 - 条/页	⊣ ⊣ 1 /1页 ► H
		共3項							20 - 条/页	4 4 1 /1页

#### 5. 在状态变更窗口中,修改相关参数,单击**提交**。

状态变更		$\times$
新发现	用户名•	_
处置中	请输入用户名	
已处置	备注	-
已忽略	请输入备注,100 字以内	
已关闭		
	提交	取消

#### 状态变更说明:

字段名称	说明
用户名	默认填充当前控制台账户名称,支持用户自定义
备注	状态备注描述,最多100个字。
状态	<ul> <li>新发现:新发现且尚未确认的 API 事件。</li> <li>处置中:正在确认风险并配置相关规则的 API 事件。该状态中有针对该事件类型的处理建议(CC/访问控制/BOT等),可一键添加相应规则。</li> <li>已确认:已确认风险并添加处置规则的 API 事件。</li> <li>已忽略:确认不需处置,忽略该 API 事件</li> <li>已关闭:观察访问流量及攻击流量情况,确认该事件可以彻底关闭。</li> </ul>

6. 在事件管理页面,选择目标事件,单击该事件对应的**查看详情,**进入详情页面。

7. 在事件详情页面,将展示该事件的基本信息、处理建议、已添加规则、变更历史等信息。



基本信息         単作印         単作共型         发生时间         更新时间           D          ①         10         2023-04-19 16:54:14         ①         2020-04-19 16:54:14 <th>撞库攻击 高危 基本信息 小</th> <th><ul> <li>新发现</li> <li>理建议</li> <li>已添加</li> </ul></th> <th>规则 变词</th> <th>· 历史 攻击源详情</th> <th>(1)</th> <th></th> <th>状态变更</th> <th>&gt;</th>	撞库攻击 高危 基本信息 小	<ul> <li>新发现</li> <li>理建议</li> <li>已添加</li> </ul>	规则 变词	· 历史 攻击源详情	(1)		状态变更	>
建议1         建议2         建议3           ● 处置建议 单个域名最多可以添加5条规则        键添加规则           建议添加基础安全->CC防护->添加规则        键添加规则           建议添加基础安全->CC防护->添加规则        键添加规则           U.T.是为您提供的参数建议:            1. 说到方式 ::         -           1. 说到方式 ::         -           1. 说到那名的参数程い:         -           1. 说到那名的公式の助         -           2. 奶奶類率10次430秒         -           1. 好行が :: 建议图断和观察         -           方向控制 CC防护         CDS并           規則D * 规则名称 匹配条件 执行动作 T 规则开关 T 操作         -	基本信息	事件iD ID 关联API 关联域名 事件详情	16	事件类型 ■ 账号异常 撞库攻击	发生时间 ③ 2023-04-1 账号异常措	<sup>更</sup> 9 16:54:14 <b>①</b> 肇库攻击,有攻击	ē新时间 ● 2023-04-19 16:5 5者批量登录,试图	54:14 撞库
<b>已添加规则</b> 方问控制 CC防护 规则ID ≠ 规则名称 匹配条件 执行动作 ▼ 规则开关 ▼ 操作	<b>处理建议</b> 建试 建议1          建议1         ① 处置建议         建议添加基础         以下是为您挑         1. 识别方式:         2. URL包含当         3. 识别频率1         4. 执行动作:	文您添加以下规则 建议2 建议 建文2 建议 建文全->CC防护->添加 提供的参数建议: IP 当前的API 0次&30秒 建议阻断和观察	3 前15条规则 0规则				一键添加规则	
	ご添加規則 方问控制 C( 規則ID ‡	C防护 规则名称	匹配条件		执行动作 🍸	规则开关 🍸	操作	e e

## 详情 TAB 页说明:

字段名称	说明
基本信息	当前事件的事件 ID、事件类型、关联 API、域名、发生时间、更新时间和事件详情等信息。
处理建议	当前事件类型的处置建议(CC、访问控制和BOT等)。
变更历史	当前事件的状态变更历史情况。
攻击源详情	当前事件的攻击源详情和相关操作。



## API 容量保护

最近更新时间:2025-04-1114:24:52

## 为什么要对 API 进行容量保护?

由于 API 是面向程序自动化调度所设计的,因此容易受到自动化调度引发的网络攻击。

- 攻击者会试图重放并自动填充不同认证凭据的业务流量攻击,导致相关业务敏感数据的泄露造成业务损失。
- 利用自动化工具发起 Layer-7 的 DDoS 攻击,通过不断地发起相关业务请求,通过高频次的调度占满服务器的带宽及上下游的计算、存储资源,造成业务 平台不稳定。
- 攻击者通过利用自动化模糊测试的工具,对业务进行定向攻击绕过测试,用于绕过定向的安全防护。
- 攻击者通过编写自动化编程工具,将有资源额度的相关 API 进行资源耗尽攻击。

可以分为如下四个模块,对 API 进行业务防护。

- API 容量防护
- API 安全防护
- API 资产管理
- API 生命周期管理

本文将从 API 容量保护角度进行梳理。在开发的生命周期内,API 的开发运营人员在进行 API 开发及维护时,可以通过使用<mark>缓存、降级、限流</mark>措施用来保护及提 高 API 系统容量的稳定性。

#### 缓存

提升系统访问速度和增大系统处理容量。

降级

当服务出现问题或者影响到核心流程时,需要暂时屏蔽掉 API 的访问,待高峰或者问题解决后再打开。

#### 限流

通过对并发访问/请求进行限速,或者对一个时间窗口内的请求进行限速来保护系统,一旦达到限制速率则可以拒绝服务、排队或等待、降级等处理。

上述三种有效的防护手段措施可以在开发、运营部署的过程中进行实现,但是会消耗大量的人力资源成本及开发成本。并且在整个 API 安全的生命周期中,需要 对所有的 API 资产进行对应的 API 容量保护。

因此需要对每一个 API 接口进行特定的业务改造,这个时候工程量就会呈指数级上涨。可以采用如下方式来对业务 API 进行快速的容量保护。

## 如何对 API 进行容量保护?

对 API 进行容量保护时,除了上述部分中描述的**缓存、降级、限流**可以通过自己开发运维外,还可以通过 Web 应用防火墙中的相关模块进行定向的 API 容量保 护,本文将会以如下9种可在 Web 应用防火墙中保护的方法进行定向 API 的快速容量保护。

防护细项	防护实践内容
API 内容缓存	静态 API 资源缓存
API 访问降级	阻断 API 的异常流量保护业务系统稳定
API 限流	限制 API 整体访问请求流速
API 客户端调度访问限速	限制客户端调度 API 的访问速度
API 敏感调用保护	保护敏感 API 接口调度不被滥用,保证业务数据不被外泄
API 资源调用保护	保护 API 强资源消耗接口调度不超限额



关键 API 调用保护	在调度关键 API 的时候进行2FA/MFA/人机识别
API 验签保护	验证客户端是否为真实客户端进行访问
API 异常访问源调度保护	保护 API 不被异常的访问资源访问

## API 内容缓存

由于公共 API 的返回接口内容较为频繁,消耗资源较大,如果 API 返回内容在一段时间内都不会持续的更新,那么就可以对 API 的相关内容进行缓存,减少 API 服务端的计算资源、带宽资源的损耗。

此处可以使用 Web 应用防火墙中的 基础安全 > 网页防篡改</mark>模块对 API 内容进行快速缓存,对业务 API 进行特定的数据缓存,帮助业务系统快速内容缓存。 1. 在网页防篡改页面,单击<mark>添加规则</mark>,弹出添加防篡改规则弹窗。

2. 在添加防篡改规则对话框中,填写相关字段,设置完成后,单击添加。

添加防篡改	<b>欠规则</b>	×
规则名称	请输入名称, 50个字符以内	
页面路径	请以/开头,输入包含静态文件名的完整路径,128个字符以内	
	请配置.html、.shtml、.bt、.js、.css、.jpg、.png等静态资源	
	添加取消	

#### 字段说明:

- 规则名称: 防篡改规则名称,最长50个字符,可以在攻击日志中按照规则名称进行搜索。
- **页面路径:**防篡改路径,需要进行防篡改保护的 URL,需要指定详细 URL,不支持路径配置。

```
🕛 说明
```

- 指定页面仅限于.html、.shtml、.txt、.js、.css、.jpg、.png 等静态资源。
- 添加规则后,用户第一次访问该页面,WAF 将会对页面进行缓存,后继访问的请求为 WAF 缓存页面。

3. 完成的防篡改规则后,规则默认启用。

### API 流速限制

对 API 的流速限制分为两个部分:

#### 对服务端 API 整体的流速限制

如果对服务端进行整体的 API 限速限流,容易导致部分客户端无法访问到业务信息。由于恶意流量在攻击时,流量数据会比较大,如果通过 API 后端服务限速, 大多数访问流量信息基本都为异常访问用户,正常访问用户很少,容易造成大量正常用户的客诉。因此,建议对**客户端的调用进行流速限制,可以通过对客户端的 限频或限速,来实现对 API 流速的限制**。

#### 对客户端调用的流速限制

在 Web 应用防火墙中的,可以通过 CC 防护设置、BOT 管理进行对客户端的限流。

#### CC 防护设置

CC 防护功能可配置每个客户端的整体的访问频次,一旦客户端的访问频次超出限制的预期,则对其进行相关处置。 1. 在 CC 防护页面,单击**添加规则**。



WEB安全(311)	访问控制(3)	CC防护(13)	网页防篡改(2)	信息防泄漏(8)	API安全(3)
紧急模式CC防护(	D				
状态 🔵	综合源站异常响应 实时拦截高频访问	立情况 (超时、响应延 可请求, 封禁攻击源1/]	迟) 和网站历史访问数据, \\时	, 智能决策生成防御策略	
27 to to Rule					

2. 在添加 CC 防护规则对话框中,配置相关参数,单击确定。

添加CC防	护规则				
规则名称 *	请输入名称,50个字符以内				
识别方式 *					
匹配方式 *	匹配字段    匹	記参数	逻辑符号	匹配内容	操作
	URL 🔻		等于 🔹	/开头, 128个字符内, 不包含域名	删除
			添加 还可以添加9条,最多	10条	
访问频次★	60 次 60秒	•			
执行动作 *	拦截 * ()				
惩罚时长 *	10	分钟 ①			
优先级 *	- 50 +				
			<b>确定</b> 返回		

### BOT 管理设置

通过配置 BOT 管理 > BOT 防护页面的会话平均速度条件,可以控制每个客户端的会话持续访问速度。

1. 在 BOT 防护页面的场景化管理模块,单击目标场景的**查看配置**。

场景化管理						
新建场县	全部场景类型 🔹 仅查看生效场影	县 🗌 仅查看默认场展 🕧		请输入场	漫名称	Q
优先級: 1 <i>2</i> ④ 国	场景id 登录 秒杀 爬文宽爬内容 浏览器/H5 小程序	<ul> <li>         · 请求路径         <ul> <li></li></ul></li></ul>	动作策略 <b>2</b> 条	自定义规则 <b>23</b> 条	生效状态	<u>查看配量</u> 编辑场景 删除场景

#### 2. 单击自定义规则的**添加规则**,配置相关参数,单击确定即可。

腾讯云

添加自定义会	会话特征				
规则名称 *	请输入规则名称,最长50个字符				
规则描述	选填,最长256个字符				
		0 / 256			
规则开关					
匹配条件 *	匹配字段	匹配参数	逻辑符号	匹配内容	操作
	会话平均速度    ▼		大于 🔻	请输入0-100000之间整数,次/分钟	删除
		添加 还可!	以添加9条,最多10条		
执行动作 *	监控  ▼				
优先级	- 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高;相同优先级下,{	刘建时间越晚,优先级越高		
自定义标签 *	友好BOT 🔻				
		确定	返回		

## Session 设置/会话设置

由于在现网环境下,IPv4 的 IP 数量越发紧张,目前很多 IP 运营商都会将客户端放置在 NAT IP 下,即一个 IP 下面有多个业务客户端。如果单纯对业务进行 IP 的限速,在面对 NAT IP 的情况下,容易触碰到业务配置的 IP 限频策略,导致误拦截的现象。如果业务配置限频过于宽松,又会使相关业务的限频拦截无法 起到限流的效果。

因此,可以在 Web 应用防火墙中配置 Session 设置/会话设置,即可做到自动分辨同一 IP 下的不同客户端,实现对单一客户端的业务限频。

- Session 设置
- 1. 登录 Web 应用防火墙控制台,在左侧导航栏选择基础安全。
- 2. 在基础安全页面,左上角选择需要防护的域名,单击 CC 防护,进入 CC 防护页面。

基础安全		)	-		
规则概览 Saa	iS型				
WEB安全规则		访问控制规则		CC防护规则	
WEB安全(656)	访问控制(48)	CC防护(20)	网页防篡改(8)	信息防泄漏(5)	API安全(7)
紧急模式CC防护	(i)				
状态 🔵	综合源站异常响应 实时拦截高频访问	立情况(超时、响应延迟) 可请求,封禁攻击源1小时	和网站历史访问数据, †	智能决策生成防御策略,	

3. 在 SESSION 设置模块中,单击设置,设置 SESSION 维度信息。



#### 4. 在 SESSION 设置对话框,配置相关参数,单击确定。

SESSION设置				
SESSION位置 *	HEADER *			
匹配模式 *	● 字符串模式匹配   ○ 位置匹配			
SESSION标识 *	q			
开始位置	20			
结束位置	30			
GET/POST示例: 如果一条请求的完 字符串匹配模式下, 位置匹配模式下, COOKIE示例: 如果一条请求的完 字符串匹配模式下, HEADER示例: 如果一条请求的完 位置匹配模式下,	整参数内容为: key_a=124&key_b=456&key_c=789 5, SESSION标识为key_b=,结束字符为&;则,匹配内容为456 SESSION标识为key_b,开始位置为0,结束位置2;则,匹配内容 整COOKIE内容为: cookie_1=123;cookie_2=456;cookie_3=789 5, SESSION标识为cookie_2=,结束字符为;;则,匹配内容为456 SESSION标识为cookie_2,开始位置为0,结束位置2;则,匹配内 整HEADER内容为: X-UUID: b65781026ca5678765 SESSION标识为X-UUID,开始位置为0,结束位置2;则,匹配内	为456 的容为456 容为b65		
	确定返回			
参数说明: ○ SESSION (1 ○ 匹配模式: 除	፬置:可选择 HEADER、COOKIE、GET 或 POST, ∶ HEADER 模式(仅支持位置匹配)外,均支持选择字符	其中 GET 或 PC 爭串模式匹配或位置	9ST 是指 HTTP 请求内容 質匹配。	参数,非 HTTP 头部信息。

○ SESSION 标识:取值标识,32个字符以内。

- 开始位置:字符串或位置匹配的开始位置,1-2048以内的整数,并且最多只能提取128个字符。
- 结束位置:字符串或位置匹配的结束位置,1-2048以内的整数,并且最多只能提取128个字符。

• 会话设置

1. 在 BOT 管理 > 高级设置模块,单击会话管理的前往配置。

全局设置				
前端对抗①	威胁情报 ①	AI策略①	<ul> <li>智能统计 ①</li> <li>6 条</li> <li>前往配置</li> </ul>	会活管理
<b>7</b> 条	16 条	1条		4 条
前往配置	前往 <b>毗置</b>	前往戰置		前往配置

2. 在会话管理页面,单击**添加配置**,配置相关参数,单击确定即可。

① 说明	
会话管理应为可持续性跟踪 tokenid ,例如登录后的 set-cookies 的值。	



新增Token	
Token名称	最多128个字符
Token描述	最多128个字符
Token <u>位置</u> *	GET v
Token标识*	32个字符以内
规则开关	
	确定 返回

参数说明:

- Token 位置:可选择 HEADER、COOKIE、GET 或 POST,其中 GET 或 POST 是指 HTTP 请求内容参数,非 HTTP 头部信息。
- Token 标识: 取值标识。

#### 控制客户端的 API 调用

每一个敏感的 API 都应该存在调用次数限制,例如:在短信 API 服务中,如果不对其进行相关限制,攻击者会滥用 API 接口,消耗短信资源包,造成超额的计 费账单。如果敏感 API 接口在客户端调用前,进行 2FA/MFA 或人机识别等验证,可以有效减少异常 API 调度。

在 Web 应用防火墙的 BOT 管理 > BOT 防护页面,通过简单的配置,实现对 API、客户端的次数调用,敏感 API 调用前,对其进行敏感操作保护。

## 敏感 API 调度前进行人机识别

添加自定义会	≹话特征				
规则名称 •	敏感 API 调度前进行人机识别				
规则描述	选填,最长256个字符				
		0 / 256			
规则开关					
匹配条件 *	匹配字段	匹配参数	逻辑符号	匹配内容	操作
	请求路径 🔻		包含 🔻	/api/v1/sendsms	删除
		添	加 还可以添加9条,最多10条		
执行动作 •	人机识别 🔻				
优先级	- 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高;相同优势	6级下,创建时间越晚,优先级越高		
自定义标签 •	疑似BOT v				
			海定 返回		

#### 限制客户端在单一会话时间内的 API 调度总次数


添加自定义会	读话特征					
规则名称◆	限制客户端在单一会话时间内的 API 认	順度总次数				
规则描述	选填,最长256个字符					
		0 / 256				
规则开关						
匹配条件 *	匹配字段	匹配参数	逻辑符号		匹配内容	操作
	请求路径		等于	Ŧ	/api	删除
	会话平均速度    ▼		大于	•	12	删除
		添加	还可以添加8条,最多10	)条		
丸行动作 •	人机识别 🔻					
优先级	- 100 + 法给入1_1000 购购 物字越小 代表说	冬期间的劫行代告机越喜,拍同代告纲	下 创建时间就略 份约	に転載する		
自定义标签◆	疑似BOT ▼	אפרגית היופר א ומופאגמציינית בראנגית מאמצייני	(T, GSX±H3101AG805, V67	U 300 ACE [10]		
		确定	返回			

# 如何进行客户端的 API 访问进行验签?

客户端的验签可以有很多种方式,包括但不限于:

- mTLS。
- 客户端签名验证。
- 客户端数据挑战。

用户可以通过配置 mTLS、客户端数据签名挑战等方式进行数据的加强验签。

在 Web 应用防火墙中,通过开启前端对抗功能,对客户端的 API 数据进行验签,并进行定向防重放功能。对抗 API 滥用有良好的效果,详细可以参见 客户端 风险识别 。



# API 数据防护与加固

腾讯云

最近更新时间: 2025-04-11 14:24:52

API(Application Programming Interface)应用程序接口,可以应用于所有计算机平台和操作系统,以不同的格式连接数据调用数据,用户可以跟踪电商 平台购买的货物位置,就是电商平台与物流公司之间使用了 API 位置实时调用产生的效果。

许多组织更关注于快速的 API 和应用程序交付,而忽视了 API 安全保护,这也是近几年来 API 攻击和数据泄露的主要原因。 API 的调用场景可分为如下三种类型:

API 类型	API 描述	安全现状
公开 API	支持任何人从任何地方访问服务,被暴露在互联网 中,调用方可根据相关接口,提供相关字段的数据, 即可完成相关数据、流程的调度。公开 API 对安全 性、使用性的监控、处置程度最高。	网络限制少,可能存在相关认证等授权的限制,但是相关业务鉴权逻辑漏洞也 更加频繁发生,攻击者更加偏爱对此类 API 通过自动化模糊测试、定向安全测 试等方式进行定向攻击及绕过。
内部 API	通常在数据中心或私有云网络环境中部署和运行,以 运营管理、内部服务支撑为主。通常用于用户的内部 之间的快速调度及使用,通常不暴露在外网	网络限制较大,可能存在相关鉴权等操作,通常校验力度较低,安全防护力度 较低,攻击者如果发现并嗅探到了此类内部 API 接口,就会针对此类 API 接 口进行定向攻击。在多起数据泄露事件中, 对内部 API 的攻击、是导致泄露 的罪魁祸首。
渠道 API	通常在数据中心或私有云网络环境中部署和运行,向 特定的外部合作伙伴、供应商提供对内部 API 的有限 制的访问。通常用于特定合作伙伴的定向数据拉取及 管控,对数据拉取的敏感度低,但对数据外泄的敏感 程度较高。	访问程度控制权位于内部和外部 API 之间,安全管控层级也是一样,主流手段 是通过 API 网关管控,但缺少安全方面的考虑。很少对此类 API 进行相关越 权方面的业务管控。如果上下游供应链上的合作伙伴被入侵进而调度相关的 API 进行数据滥用,在渠道 API 上通常会缺少滥用的监控监管机制,因此多 起数据泄露事件就因为没有对渠道 API 进行滥用管控造成的。

## 为什么要做 API 敏感数据发现

据《Salt Labs State of API Security Report, Q1 2022》报告,在受访者最关心的 API 安全问题中,僵尸 API 以43%占比高居第一;远超过以22%的占 比位居第二的账户接管/滥用;还有83%的受访者对组织 API 资产清单是否完整没有信心。

为何企业对 API 资产有如此大的担忧? 安全隐患往往藏于"未知",未知的僵尸 API、未知的影子 API、未知的敏感数据暴露等,根源都在于企业对 API 资产 全貌的未知。安全的管理与防护始于"已知"和"可见",人们难以掌控那些被遗忘的、看不见摸不着的资产安全状况。然而正是这些被人遗忘、不可管控的 API,往往会有相关敏感数据在上面运行,如果没有办法及时的发现这些敏感的 API 接口则会导致相关 API 数据被拖取或意外暴露的情况,攻击者很有可能就会 通过此类 API 接口对业务敏感数据进行定向发现及攻击,紧接着进行相关敏感数据拖取,更有甚者会进一步的扩大 API 攻击的利用权限,对服务器、数据库的权 限进行进一步获取。从而导致业务受损。

即便是企业已经开始重视并着手治理僵尸 API 问题,也仍有一处容易被忽略的巨大风险——僵尸参数。不同于那些被彻底遗忘的僵尸 API,这些僵尸参数有可能 还存在于当前仍在服务且持续维护的 API 接口中。常见的僵尸参数,例如在开发测试周期内设置的调试参数、系统属性参数,它们在接口正式上线后未对外暴露 给用户,但仍能被暗处的攻击者恶意调用。攻击者基于僵尸参数,能够利用批量分配等漏洞获得越权的响应。一旦这些未知的 API 脆弱点被恶意利用,背后的核 心业务数据、平台用户数据等海量敏感数据在黑客面前就变成了内部 API 调用,没有任何安全管制,再无秘密可言。

# 操作步骤

### 步骤1:发现 API 资产

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏中,选择 API 流量分析。
- 2. 在 API 流量分析页面,左上角选择需要防护的域名,并单击开启是否开启分析的 🔵 。

API资产列表					මාමකාවේ අපළාවැන්න්තාක ( මාමකාව)
	(回) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	ERRED AND SHOR (MY LUX)目12 	<ul> <li>API 設議所加</li> <li>NEMAPIRAL API 設議所加</li> <li>NEMAPIRAL API 設議所加</li> <li>NEMAPIRAL API 設議所用</li> </ul>	始。通过数据的增属的5 <sup>44</sup> 458数据	() API 別本1995万分世紀     単正になったか世紀、光田中山島中和日ム中19月末点。 15 止日のつけた世紀、光田中山島中和日ム中19月末点。 15 止日の天中1     に向世紀月本10月行方
API概応 API他設 〇 ☆ 环北旅量変化 0	过去7日活转API 0 ↑ 环位游量变化 0	过走7日不活跃API 0 ♪ 环社恋量变化 0	19450API 0 ↑ 环転調整化 0	APIMAMER 要产来开始 ② 表面运転 ③ 介 1	ASTRONT



3. 开启开关后,即可在相关 API 详情页查看对应 API 的相关详情信息。

÷	API详情					<ul> <li>● API 防护指南</li> </ul>
	/		out the party	à		
	所属域名	请求方法	当前功能标签	▶	0	7天内是否活跃
	2	GET	▲ 验证码	-		是
	API概览 API攻击概览	请求参数样例 参数列	刘表			
	参数名	参数类型 ▼ 参数位置 ▼	数据标签	备注	最近更新时间 \$	操作
	c	rs			2022-07-28 02:2	编辑
	X-'	ers			2022-07-28 02:2	编辑

# 步骤2: API 安全加固

1. 在 基础安全 > API 安全页面,根据相关 API 进行 API 合法性加固。

WEB安全(542)	访问控制	CC防护(6)	网页防篡改	信息防泄漏	API安全		添加幂	就自名单 精准的	白名单列表
添加规则	导入API	批量启用	批量禁用	批量删除	获取鼠标焦点即可	选择过滤属性		Q	φ
规则ID	接口名	呂称(描述) 来源 ▼	请求方	法▼ API参数	故 执行动作 ▼	规则开关 🍸	修改时间 \$	操作	
				Q					
				暂无数	R				

2. 在 CC 防护页面,根据相关 API 进行容量保护措施。

VEB安全	È(542)	访问控制	CC防护(6	) 网页	访篡改	信息防泄漏	API安全				添加精准白名	单 精准的	名单列表
紧急模	式CC防护①						SESSION	<mark>8</mark> 置①			设置	副试力	删除
状态(	综合源站异 生成防御策	常响应 <mark>情</mark> 况(超 略,实时拦截高	3时、响应延迟) 3频访问请求, <b>3</b>	和网站历史访 时禁攻击源1小时	问数据, 智能) 付	競	Session位置:- 匹配模式: 会活标识:- 会话设置: <b>开始位置:;结束位置:</b> 设置时间:-						
添加	<b>规则</b> 单个	域名最多可以	添加50 <mark>条规则</mark>				获取鼠标	<b>沃焦点即可选择</b>	过減層性			Q	¢
	规则ID \$	规则名称	匹配条件	请求路径	访问频次	执行 ▼	启用▼	惩罚时长	优先级	规则 ▼	修改 \$	操作	
	́с	<b>.</b>	包含	/ြ	5次/60秒	拦截	否	1分钟	50		2022-07	编辑 删除	
	6	100	包含	/mmm 🗗	3次/60秒	拦截	否	5分钟	50		2022-05	编辑	



3. 在访问控制页面,单击添加规则,根据相关 API 进行敏感操作保护措施。

添加自定义	【防护规则							
规则名称 *								
匹配方式*	匹配字段		匹配参数	逻辑符号		匹配內容		操作
	来源IP	*		匹配	•		已有0个ip	删除
						添加还可以添加4条,最多5条		
执行动作*	阻断  ▼							
截止时间*	永久生效 🔻							
优先级*	- 50	+						
						<b>确定</b> 近回		

4. 在 BOT 与业务安全页面,根据相关 API 进行异常行为保护措施。

匹配方式*	匹配字段 匹配参数	逻辑符号	匹配内容	操作
	<b>来源ⅠP</b> ▼ 此字段不支	持参数 匹配	▼ 多个IP以英文道号隔开,最多20个	已有0个ip 删除
			添加 还可以添加4条,最多5条	
丸/〒元11/1日 *	阻断 ▼			
截止时间*	永久生效 🔻			

# 步骤3: API 生命周期管理

1. API 上线监测。

PI概览			
API总数	过去7日活跃	过去7日不活跃	涉敏API
8/7	API	API	8/7
04/*	847	0 ^	04/ 1
环比数量变化	17 <u>44444</u> 4		环比数量变化
<b>†</b> 847	环比数量变化	环比数量变化	<b>†</b> 847



### 2. API 参数新增检测,API 参数新增检测。

API概觉 API攻击概览	请求参数	洋例 参数	刘表			
參数名	参数类型 ▼	参数位置 ▼	数据标签	备注	最近更新时间 \$	操作
		100	100		2022-07-19 16:3	编辑
	boolean	cookie	IPv4地址 手机号		2022-07-20 11:4	编辑
	string	headers	银行卡号 邮箱		2022-07-20 11:5	编辑
	string	cookie	10000		2022-07-28 09:4	编辑
	string	headers			2022-07-27 17:3	编辑
	string	cookie			2022-07-27 17:3	编辑
	int	cookie			2022-07-27 17:3	编辑
	string	cookie			2022-07-27 17:3	编辑
	string	cookio			2022-07-27 17:3	使得

## 3. API 下线回收,API 临时阻断。

1120					
* Ĵzč	匹配字段	匹配参数	逻辑符号	匹配内容	攝作
	来源IP	此字段不支持参数	匹配	▼ 多个IP以英文逗号隔开.最多20个	已有0个ip 删除
				添加 还可以添加4条,最多5条	
动作*	阻断  ▼				
时间*	永久生效 ▼				



# WAF 结合 API 网关提供安全防护

最近更新时间: 2024-04-24 14:15:41

本文档将介绍如何配置 Web 应用防火墙(WAF),为 API 网关上的 API 提供安全防护。

### 前提条件

- 已开通 Web 应用防火墙。
- 已在 API 网关上发布了 API,详情请参见 快速入门。

### 操作步骤

### 步骤1:在 API 网关控制台绑定自定义域名

参考 配置自定义域名 文档,在 API 网关控制台绑定自定义域名。

#### ▲ 注意:

API 网关绑定自定义域名时,会校验自定义域名是否解析(通过 CNAME)到该服务的子域名。因此,您必须先将自定义域名解析(通过 CNAME)到 API 网关服务的子域名并配置绑定成功,再修改 DNS 记录,将自定义域名指向 WAF 的 CNAME 域名。

自定义域名绑定指引					
1		2	3		4
获取域名		腾讯云备案	CNAME到二	级域名	配置绑定并生效
前往 <mark>域名注册</mark> 或从其他服务商处获取域名		在腾讯云备案域名, 流程可参考 <mark>网站备案</mark>	添加CNAME 将域名指向服务的	记录, 1二级域名 <b>①</b>	新建自定义域名绑定, 配置完成后直接生效
新建					¢
域名	路径映射	协议	网络类型	SSL证书	操作
yithanwi, fyfywang	使用默认路径映射(	) http	公网	无	编辑路径映射 删除
共 1 条				20 ▼ 条/页	1 /1页 🕨 🕨

### 步骤2: 配置 WAF

- 1. 登录 Web 应用防火墙控制台,在左侧导航中,选择接入管理。
- 2. 在域名接入页面,单击**添加域名**。

接入管理				
域名接入	对象接入			
添加域名	请选择实例	Ŧ	请选择实例类型	Ŧ

3. 在添加域名页面,配置相关参数,单击确定。

添加域名	X	
所属实例	SaaS型 负载均衡型 CDC型 ▼	
域名 *	请输入域名	
服务器配置	✓ HTTP 80 ▼	
	HTTPS	
代理情况 🛈	○ 否 ○ 是 WAF前是否有七层代理服务(高防/CDN等)?	
源站地址 🛈	OIP ○ 域名	
	请输入源站IPv4或v6地址,用回车分隔多个IP,最多支持输入50个	
负载均衡策略	O 轮询 ── IP Hash	
高级设置▲		
回源连接方式	○ 短连接 ○ 长连接 默认使用长连接回源,请确认源站是否支持长连接,若不支持,即使设置长连接,也会使用短连接	
写超时时长	- 300 + 秒,范围1~600秒	
读超时时长	- 300 + 秒,范围1~600秒	
开启HTTP2.0 🛈	○ 否   □ 是 请确保您的的源站支持并开启了HTTP2.0,否则,即使配置开启2.0也将降级1.1	
开启WebSocket	● 否 <b>是</b> 如果您的网站使用了Websocket,建议您选择是	
开启健康检查	●否──是	

### 4. 完成配置后,此时域名接入状态为"未配置 CNAME 记录"。

域名/接入状态 ▼	实例信息 (1)	实例ID/实例名称	使用模式 ▼	回源保护地址 ①	BOT开关	API分析 (i)	IPv6开关	WAF开关 ▼	访问日志 🍸	操作
0 <sup>10</sup>	с. го	b¥Ĩ⊡	规则: 拦載模式 AI引擎: 关闭模式	·等24个 查看						编辑 删除 基础防护 BOT与业务防护 更多 ▼
op 년 末配置 CNAME 记录	SaaS型-北京	۲a	规则:拦截横式	4等24个 查看						编辑 删除 基础防护 BOT与业务防护 更多 ▼

## 步骤3:修改 CNAME 记录

> 腾讯云

1. 在 DNS 提供商中修改 CNAME 记录,将自定义域名指向 WAF 的 CNAME 域名。

2. 登录 Web 应用防火墙控制台,选择接入管理,进入域名接入页面,即可看到正常防护的界面。

域名/接入状态▼	实例信息 (i)	实例ID/实例名称	使用模式 ▼	回源保护地址 🛈	BOT开关 API分析 🛈	IPv6开关	WAF开关 ▼	访问日志 🔻	操作
正常防护	SaaS型-北京 )	· · · · · · · · · · · · · · · · · · ·	规则: 拦截横式	等24个 查看					编辑 删除 基础防护 BOT与业务防护 更多 ▼



# API 行为管控

最近更新时间: 2025-05-27 17:31:12

# 什么是 API 异常访问行为?

在"万物皆可 API"的时代,通过 API 快速构建产品和服务、迅速响应客户需求已是数字化企业的必备技能。但同时,API 承载着越来越复杂的应用程序逻辑和 大量敏感数据,也使得 API 成为黑客的重点攻击目标。

近年来,不少国际知名企业都因 API 安全疏忽而遭受了巨大的打击。不仅如此,据研究部门 Salt Labs 发布的《2022年第一季度 API 安全状况报告》显示, 在过去12个月中,恶意 API 流量增加了681%,95%的组织都经历了 API 安全事件。然而,大多数组织并没有准备好应对这些挑战,超过三分之一(34%)的 企业没有 API 安全策略。

在 API 访问中会传输大量的数据,数据的传输分为正常访问和数据窃取等方式,对于正常的数据访问,可以在数据分级分类的情况下,在 WAF 上实现对数据的 脱敏和混淆等功能;对于数据窃取的情况下,需要识别异常的数据泄露,并阻断异常访问和连接。

# API 的异常访问行为有哪些?

- 无明显特征的攻击行为。
- 针对业务的异常访问。
- 大量的数据传输。
- 异常的访问对象。
- 被攻击利用的过期 API 或者是僵尸 API。
- 过度暴露的数据。

# API 异常访问行为挖掘实践教程

发现 API 的异常访问行为、调查 API 的访问的异常行为,是在日常安全运营中发现并修补安全/运营漏洞的关键手段。那么在 Web 应用防火墙控制台,可以通 过 API 流量分析、BOT 流量分析等相关安全视图,进行快速的 API 异常访问行为的发现及挖掘,实现快速的安全运营闭环。

API 的异常访问行为发掘调查主要分为以下几个步骤:

- 1. 发现异常访问请求。
  - 在 攻击日志页面,发现异常的访问行为日志,并对其进行跟踪。
  - 在 API 资产管理功能 中,发现异常的 API 概览信息,确认相关异常 API 日志,并对其进行跟踪。
  - 在 BOT 流量分析页面,发现分数异常的 API 访问请求,并对其进行跟踪。
- 2. 确认异常访问请求中的唯一 UUID,根据 UUID 确认事件爆炸范围。

开启访问日志后,每一条访问日志存在唯一的 uuid,可以根据唯一 uuid 进行相关用户、API 访问日志、BOT 行为信息的分析及跟踪。

3. 考虑用户典型行为背景下的异常。

在不同的业务场景下,不同用户的 API 访问行为并非一致,如在登录 API 的场景下,如果频繁访问登录接口则异常的可能性极大。

- 4. 以影响访问因素为指导,确认是否异常。
   确认当前访问源是否为异常访问源、登录地是否异常、调用方是否非业务访问源用户。
- 5. 已返回报表内容信息为指导,确认是否异常。
  - 确认访问的 body size 等参数是否远超异常。
  - 确认返回内容是否超出预期。
- 6. 确认相关 API 及用户信息、进行安全闭环。
   确认异常访问行为、用户信息、以及相关 API 信息,对其进行处置后,及时进行安全修复。



# API 暴露面管理

最近更新时间: 2025-05-27 17:31:12

### 背景信息

API 为当今大多数数字体验提供了动力,API 安全性仍然是大多数 CISO 最关心的问题。随着各个行业的数字化转型,针对 API 的恶意威胁行为与日俱增。当 前 API 的安全状态与组织的需要存在很大差距,组织经常受困于难以理解的攻击面,缺乏正确的策略来构建防御。

API 处于数字化体验的中心,移动应用、Web 网站和应用程序的核心功能、微服务架构、监管机构的要求等等,均离不开 API 的支持,根据 Akamai 的一项统 计,API 请求已占所有应用请求的83%。与此同时,针对 API 的攻击成为了恶意攻击者的首选,相对于传统 Web 窗体,API 的性能更高、攻击的成本更低,因 此 API 安全面临着如下挑战:

### 应用和逻辑迁移上云,暴露更多攻击面

随着云计算技术的广泛应用,越来越多的 SaaS 被迁移上云,在为更多的用户提供服务的同时,也将 API 暴露到云中,相对于传统数据中心的单点调用,东西向 和南北向都可能成为 API 的攻击面。

#### 创新强调速度和灵活,忽略构建 API 安全

敏捷开发模式是当今主流开发模式,敏捷开发强调个体与互动、可工作的软件、客户合作、响应变化,虽然提升了创新速度和灵活性,但是对于如何构建 API 安 全性却缺少合适的方法,导致在软件构建过程中难以顾及 API 安全。

### API 接口对外不可见,引发多种攻击隐患

由于 API 是由程序员书写,除了编写代码的程序员,很少有人意识到这些 API 的存在,缺少维护的 API 经常容易被忽略,然而恶意攻击者却可以利用网络流 量、逆向代码、安全漏洞等各种手段找到不设防 API 并实施攻击。

#### 组织经常低估 API 风险,造成安全措施遗漏

人们通常会假设程序会按照想象中的过程运行,从而导致 API 被攻击的可能性以及影响被严重低估,因此不去采取充分的防护措施。此外,第三方合作伙伴系统 的 API,也容易被组织所忽视。

那么要治理 API ,首先就需要治理 API 资产,对 API 进行暴露面攻击面的管理。

### 什么是API 暴露面?

API 暴露面主要分为两个大的部分:

分类	详情
	内部 API 暴露信息
	合作伙伴 API 暴露信息
API 外部的暴露面	僵P API 暴露信息
	外部 API 暴露信息
	测试 API 暴露信息
	API敏感参数暴露
ALI 交叉LI 参照 的复数 1 人	API 后台参数暴露

其中 API 的暴露会造成内部 API、合作伙伴 API 意外暴露给攻击者,攻击者可以通过利用这些弱校验的 API 进行对应攻击,造成意外的数据泄露、API 滥用、 权限外泄等意外的安全事件。

同时,在开放的 API 中,如果存在敏感、后台的 API 参数被攻击者嗅探或识别出来,攻击者可以通过这些敏感的参数信息,对业务进行定向的数据获取及 API 滥用,造成越权、数据外泄的等安全事件场景。

### 如何发现异常暴露面?

1. 通过自动化识别业务 API 调用关系,全面、持续清点 API 接口,包括影子 API 和僵尸 API、老版本和功能重复的 API,缩小风险暴露面。

2. 持续监测敏感数据流动,对各种敏感数据进行识别,并对敏感数据进行自定义检测,减少数据暴露面。



3. 持续动态梳理系统访问账号,多维度记录账号访问和操作行为,主动识别风险操作。

那么在异常暴露面发现的基石就是 API 的资产发现,API 的资产发现在 Web 应用防火墙中,可以通过 API 流量分析 进行对流量内的 API 进行发现及管控。 要进行暴露面监测,及时了解当前网站中包含的 API 及相关敏感资产信息及其资产标签与风险、活跃状态。

API	请求▼	所属域名	功 ▼	数据标签	过 ▼	API防护	最近 \$	发现 \$	操作
/c	GET	202212	未知	IPv4地址	是	-	2022-0	2022-0	查看详情
lo	GET	202212	未知	IPv4地址	是	-	2022-0	2022-0	查看详情
/c	GET	202212	未知		是	-	2022-0	2022-0	查看详情
N	GET	202212	未知		是	-	2022-0	2022-0	查看详情
N	POST	202212	未知		是		2022-0	2022-0	查看详情
	0.57		1.62						+==\++



# 接入相关 WAF 与 DDoS 高防包结合应用

最近更新时间: 2024-04-17 15:39:21

## 应用场景

Web 应用防火墙(WAF)具备 CC 防护能力,针对非 HTTP 请求,Web 应用防火墙支持和 DDoS 高防包联动,为用户提供全方位的安全防护。

- DDoS 高防包可以提供上百 Gbps 的 DDoS 防护能力,轻松应对 DDoS 攻击,保障业务稳定运行。
- Web 应用防火墙提供实时防护能力,可有效拦截 Web 攻击,保障用户业务的数据和信息安全。

### 操作步骤

## 步骤1: 配置 Web 应用防火墙

- 1. 登录 Web 应用防火墙控制台,在左侧导航中,选择接入管理。
- 2. 在域名接入页面,单击**添加域名**。

接入管理				
域名接入	对象接入			
_				
添加域	<b>名</b> 请选择实例	•	请选择实例类型	Ŧ

3. 在添加域名页面,配置相关参数,单击确定。

添加域名	×	
所属实例	SaaS型 负载均衡型 CDC型 ▼	
域名 *	请输入域名	
服务器配置 🛈	✓ HTTP 80 ▼	
	HTTPS	
代理情况 🛈	○ 否 ○ 是 WAF前是否有七层代理服务(高防/CDN等)?	
源站地址	OIP ○ 域名	
	请输入源站IPv4或v6地址,用回车分隔多个IP,最多支持输入50个	
负载均衡策略	O 轮询 ── IP Hash	
高级设置▲		
回源连接方式	○ 短连接 ○ 长连接 默认使用长连接回源,请确认源站是否支持长连接,若不支持,即使设置长连接,也会使用短连接	
写超时时长	- 300 + 秒,范围1~600秒	
读超时时长	- 300 + 秒,范围1~600秒	
开启HTTP2.0 🕄	● 否  ● 是 请确保您的的源站支持并开启了HTTP2.0,否则,即使配置开启2.0也将降级1.1	
开启WebSocket	● 否   ○ 是 如果您的网站使用了Websocket,建议您选择是	
开启健康检查	◎否 ○是	

#### 参数说明:

腾讯云

- 域名: 输入需要防护的域名。
- **服务器配置**:按实际情况选择协议类型及端口。默认需要勾选 HTTP 协议,当网站为 HTTPS 加密认证时,请勾选 HTTPS,并完成相应配置和输入。
- 代理情况:选择"是",WAF 将通过 XFF 字段获取客户真实 IP 地址作为源地址,勾选可能存在源 IP 被伪造的风险。
- 源站地址: 输入需要防护网站的真实 IP 源站地址,即源站的公网 IP 地址。
- 负载均衡策略:按实际情况选择轮询或 IP Hash。

### 🕛 说明

如果源站有多个回源 IP, 可以根据实际需要选择。当前策略支持按照客户请求进行轮询(同一个访问源 IP 的请求按照顺序转发到不同的源站服 务器)或 IP Hash(同一个访问源 IP 的请求回源到同一台源站服务器),默认为轮询。

### ○ 高级设置:

- 回源连接方式:默认使用长连接回源,请确认源站是否支持长连接,若不支持,即使设置长连接,也会使用短连接。
- 开启 HTTP2.0:在协议类型选择 HTTPS,回源方式选择 HTTPS,才可以选择是。
- 开启 WebSocket:如果您的网站使用了 WebSocket,建议您选择是。

### 步骤2: 配置 DDoS 高防包

1. 登录 DDoS 高防包控制台,在左侧导航中,选择**实例列表**。

🗲 腾讯云

2. 在实例列表页面,选择所需实例,单击操作列的**管理防护对象**。

实例列表							↓ 产品动态 购买
⑤ 全部地域 ▼ ⑤ 全部线路 ▼							名称 ▼ 请输入要查询的内容 C
ID/名称	防护IP	規格信息	运行状态 🔻	防护状态	最近7天攻击	日期	自动续费 操作
	je je	所属区域: 2: 赛客信息: 防护P总题 业务规模:	防护状态: •运行中 防护剩余次数:无限次 防护中的IP:1个	IP號口防护: 严格 配置 域名防护: 关闭 配置	i 0次上	购买时间: 2022-01-02 到期时间: 2023-03-30	管理防护対象 初州戦闘 重音税技 升坂 疾患 ①

3. 在管理防护对象页面,选择"关联设备类型"为 Web 应用防火墙,设置"选择资源实例"为对应 Web 应用防火墙防护的 IP 地址。

()	说明							
	若是负载均衡型 WAF,	在绑定界面选择	"关联设备类型"	为负载均衡,	设置	"资源实例"	为对应负载均衡的公网 IP 均	也址。

管理防护对象	R								×
① 注意	: 已配置的防护策略仅对当前	绑定的IP生效,	如存在防护策略不适	用于当	í前IP,	请前往修改。			
□P资源名称 地域 可绑定IP数 关联设备类型 选择资源实例	未命名 广州 5 Web应用防火墙 云主机	•				已选择 (1)			
<ul> <li>✓ 资源ID/</li> <li>✓</li> </ul>	负载均衡 Web应用防火槽 NAT网关 VPN网关		资源类型 Web应用防火墙	Q		资源ID/实例名	IP地址	资源类型 Web应用防火增	٢
共 1 条	<del>7篇件面上</del> 100 ▼ 祭/页	•	1 /1页 ▶	м	↔				
支持按住 shift	聽进行多选			确定		取消			

4. 设置完成后,单击**确定**即可。



# WAF 与 CDN 联动使用实践教程

最近更新时间: 2025-04-11 14:24:52

本文将介绍如果网络中增加了 CDN 网络层,用户将如何接入 WAF,提供更有效的安全防护。

- 内容分发网络(CDN)提供强大的网站静态内容的加速分发处理能力,显著提升网站资源加载速度,分布在不同区域的终端用户均可享受到快速流畅的网页体 验。在用户高并发期间可缓解源站服务器压力,保证服务稳定和网页的流畅访问。
- Web 应用防火墙提供实时防护能力,可有效拦截 Web 攻击,保障用户业务的数据和信息安全。



# 测试环境

- CVM:存在一个Web服务。
- 备案域名。
- Web 应用防火墙。
- CDN 内容分发网络。

## 接入步骤

### 步骤1: 配置 Web 应用防火墙

- 1. 登录 Web 应用防火墙控制台,在左侧导航中,选择接入管理。
- 2. 在域名接入页面,单击添加域名。
- 3. 在添加域名页面,配置相关参数,单击确定。

添加域名		>
沂属实例	SaaS型 负载均衡型 b	
或名 *	请输入域名	
服务器配置 ①	✓ HTTP 80 ▼	
	HTTPS	
代理情况 🛈	○ 否 ● 是 WAF前是否有 <b>七层代理服务</b> (高防/CDN等)?	
客户端IP判定方式	● 获取请求Header字段X-Forwarded-For(XFF)中的第一个IP地址 ● 获取网络层的remote_ip作为客户端的源IP,防止XFF伪造 ● 获取指定 header 字段的IP地址	
原站地址 🛈	OIP J 域名	
	请输入源站IPv4或v6地址,用回车分隔多个IP,最多支持输入50个	
页载均衡策略	● 轮询	
高级设置▼		

参数名称	说明
域名	在域名输入框中添加需要防护的域名, 本示例中填写 youlin.life。
	根据实际情况选择是否已使用了高防、CDN、云加速等代理。
代理情况	<ul> <li>否:表示 WAF 收到的业务请求来自发起请求的客户端。WAF 直接获取与 WAF 建立连接的 IP 地址作为客户端 IP。</li> <li>是:表示 WAF 收到的业务请求来自其他七层代理服务转发,而非直接来自发起请求的客户端。为了保证 WAF 可以获取 真实的客户端 IP,进行安全分析和防护,您需要进一步设置客户端 IP 判断方法。</li> <li>取请求 Header 字段 X-Forwarded-For (XFF)中的第一个 IP 地址作为客户端 IP。</li> <li>获取网络层的 remote_ip 作为客户端的源 IP,防止 XFF 伪造。</li> <li>获取指定 header 字段的 IP 地址。</li> </ul>
源站地址	根据实际需求选择 IP 或域名。
其他参数	详情请参见 <del>步骤 1:域名添加</del> 。

4. 完成配置后,可以在当前页面看到接入的域名。当前接入的 CNAME 为 09a10b6316608b648da8eec6fffeb59b.qcloudwzgj.com 。

Web 应用防火墙	接入管理									۲	接入指引 域名列表扬	▶作指南 [2
☞ 切換至非中国大陆	域名接入 对象接入(即将上线)											
安全可視 <b>吉昌 概览</b>	添加域名发现域名	请选择实例	Ŧ					获取能标焦点	印可选择过滤属性		Q	φ
🥶 BOT流量分析	域名/接入状态 ▼	接入信息 🛈 🔻	所属实例ID/名称	使用模式 ▼	回源地址 ①	<b>BOT</b> 开关	API安全	IPv6开关	WAF开关 ▼	访问日志 🔻	操作	
<ul> <li>④ API流量分析</li> <li>日志服务</li> <li>□ 攻击日志</li> </ul>	」 未配置 CNAME 記录 ()	SaaS型-广州 09a10b6316608b648da8e ec6fffeb59b.qcloudwzgj.co mli	w gz-Default 🔁	规则:拦截模式	\$↑ 24						编辑 删除 基础防护 BOT与业务防护 更多	•
🗅 访问日志	共1项								20 + 1	€/页 H 4	1 /1页	⊧ H.
5产中心. 四 接入管理												

🔗 腾讯云



## 步骤2:配置 CDN

- 1. 登录 CDN 控制台,在左侧导航中,选择域名管理。
- 2. 在域名管理页面,单击**添加域名**,输入**加速域名**和回源地址,配置相关参数,单击确认添加。

### () 说明:

- 加速域名:填写目标域名。
- 回源地址:填写 WAF 的CNAME 地址。
- 更多详情请参见 从零开始配置 CDN 。

分发网络	域名配置	
5概览	加速区域	● 中国境内     中国境外     全球
2管理	加速域名	
5管理 ~		该域名已接入
+分析 ~		添加
「预热	加速类型	CDN 网页小文件 👻
尿服务		网页小文件属于CDN服务,计费方式参考 CDN计费说明 L
‡中心	IPv6访问	
≧防护 ~		开启后,支持通过IPv6协议进行访问
	所属项目	默认项目 🔻
网状态监控	标签(选填)	+ 添加
 原包管理		
1屋杏询	源站配置	
	源站类型	● 自有源 COS源 IGTM多活源 第三方对象存储 ③
》 「一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	回源协议	● HTTP ● HTTPS ● 协议跟随 差你的运动去去 HTTPS 法问 建议选择 HTTPS 作为你的问题协议 递免你的产品数据缺效取成来答辩
	2百点2440405	
	AT ALL ALL	回源規则 回源地址 (源站:端口:权重) 操作
町上具		全部文件 09a10b6316608b648da8eect 00000000000000000000000000000000000
5		
		添加源站
r 开发		
开发	回源HOST	
~ 开发	回源HOST	回源HOST是回源时在源站访问的站点域名。什么是回 <b>源HOST7 [2</b> ]
~ 开发	回源HOST	回源HOST是回源时在源站访问的站点域名。 <b>什么是回源HOST? [2]</b> 请确保您配置的回源HOST域名能够正常访问,否则会导致回源失败,影响业务。 〔注:者源站地址为OOSI或第三方存做对象存储,则回源HOST需与源站地址相同。〕
~ 开发	回源HOST	回源HOST是回源时在源站访问的站点域名。 <b>什么是回源HOST? [2]</b> 诸倫保您配置約回源HOST域名能够正常访问,否则会导致回源失败,影响业务。 (注:若源站地址为COS或第三方存储对象存储,则回源HOST需与源站地址相同。)
τ	回源HOST	回源HOST是回源时在源站访问的站点域名。什么是回源HOST? 2 蒲确倏您配置货回回源HOST或名能够正常访问,否则会争致回源失成,影响业务。 (注:若源站地址为COS或第三方存储对象存储,则回源HOST需与潮站地址相同。)

3. 配置完成后,可以在当前页面看到添加的域名,以及生成的 CDN CNAME 地址。

内容分发网络	<b>域名管理</b> 当前账户已添加城名2项,剩余可添加城名数无限制。	♦ 场景教学								
<b>昰 服务概</b> 览										
🖂 域名管理	城名管理 常见问题 常用工具	隐藏指引								
□ 证书管理 🛛 👻	域会管理员面可展示报告下的结合截流信息列表,支持使边域合相尖信息。 接入 CDN 的域名有什么要求? IPI互集密询									
山 统计分析 🔹 👻	包括添加,并应决闭、删除地名、以及管理地名高置等操作。 CDN 是否支持能量分区每回源? 回题节点重调									
⑤ 刷新預热										
日志服务	期前1700年1月7日2日1日 日前19日上月 日前19日上月 日前19日上月 日前19日上月 日前19日上月 日前19日上月									
	<b>查看更多≫</b> 内容合规									
□ ······· □ 安全防护 ·										
<ul> <li>         服务查询         ④ 全网状态监控         ④ 资源包管理         </li> </ul>	<ul> <li>- 成功通知時名后,包裹完成 CNAME 区間 才測正式応用知道服务,配置 CNAME (2)</li> <li>- 当域後初度成長有限度型防衛者能変更,可能交換指定長,何能空気用から切り開始長折測成正常均同,<u>還存期間</u>(2)</li> <li>- 包括公別回目子交換確定有限的整改的現象本(1)、設定認定契約法式完成不可推動 編件なCDAYSa, <u>還有期間</u>(2)</li> <li>- 包括金融前成次完装局产生素制版体,避免有輕低中,建议認知能用量封逻辑地域形实实态的产产品,資面 <u>医重氮面</u>,</li> </ul>									
回 IP归属查询	次加減名 就要操作 ▼ タイズ留字用品紙 10 分	Q±¢¢								
④ 回源节点查询										
🖸 内容合规	□ 和哈 加速保証 1 花(本) T CHAME () 接入方式 T 服务地理 7 掛け	n:								
○ 配額管理 ~	CON 解页小文件 ② 已品动     Omega com.cn     自有源 中国境内 解	旺 关闭 更多 ▼								
◎ 诊断工具	CON 周页小文件 ② 已启动 ① COS源 中国流均 暫	瞠 关闭 更多 ▼								
館場方案										

### 步骤3:配置 DNS

1. 登录 云解析 DNS 控制台,在左侧导航中,选择我的解析。



#### 2. 在我的解析页面,选择要操作的域名,单击**解析**。

云解析 DNS	HOT DNSPod计费消息转由器	试云计费倒统一发送。 <u>查看详情</u>					• • ×
■ 我的解析	我的解析 全部项目 -					▶ ▶ ○島体验意識了算 域名注册控制台 区 微信小程序 帮助指引 区	🕐 获得支持
□ 套餐服务		滚加城名 开通正式套餐	批量操作 - 更多操作 -			● 全屏模式 全部域名 ▼ 高級構造 训输入展示的地名 Q 卒	
□ 批量操作		解析域名	状态	记录数	<b>客長</b>	服务 最后操作时间 操作	
⊕ 协作子域名			<ul> <li>王常</li> </ul>	546 条	免费版	ssu ≓ 2024-12-0217:34:21 解析 升级 备注 更多 ▼	
□ 插件中心							
IGTM智能全局流量管理			● 正常	12 条	免费版	ssL ≓ 2024-04-2617:27:43 解析 升级 备注 更多 ▼	
Ⅲ IGTM概览	ţ	4.2 亲				20 * 条/页 × < 1 /1页 > ×	
13 我的头例							

3. 添加 CNAME 地址,其中记录值为 CDN 的 CNAME 地址。

云解析 DNS	<b>←</b> •	v		全部項目 *								•	产品体	的形式	解析记录用	助指引 [2] 解析有问题?
<b>國 965-825</b> 5	记录管理	负载均衡	套餐服	务 域名设置	数据统计	DNS安全	扩展应用 线	路管理 权限管理	操作日志							
<ul> <li>ご 套餐服务</li> </ul>			原加记录	新手快過解析	批量操作 👻	更多操作 マ					全部记录	▼ 高级转送	请输入搜索	的内容	Q \$	
回 批量操作			主核	几记录 ≄	记录供型 \$	线路岗型 \$	记录值 \$	权重 Φ	优先级 \$	TTL \$	备注	最后操作时间 : 操	ft.			
协作子城名			• •		CNAME	默认				600	-	2023-06-21 16 🎁	改 暫停	备注		
☆ 播件中心							-									
IGTM智能全局流量管理			•		CNAME	RCL.	dates another	-		600	-	2023-02-14 1( 👫	改 醫师	备注		
□ IGTM概览 □ 我的实例			•	-	CNAME	默认		-		600	-	2023-02-17 11 🎁	改 暂停	备注	<b>8</b> 198	
🗄 我的套餐			•		A	默认	10.00	-		600	-	2022-07-22 14 👘	改 暂停	备注	<b>B</b> 108	

### 测试验证

### 验证1:域名是否能正常访问

浏览器访问目标域名 http://xx.com ,检测是否正常。

### 验证2:WAF 是否接入成功

浏览器访问 http://xx.com/?test=alert(123) ,检测是否能被 WAF 拦截。



### 验证3: CDN 是否接入成功

打开浏览器的开发者模式,访问加速域名。



• 验证方法①:确认 Remote Address 的 IP是否属于 CDN 节点 IP。操作详情请参见 IP 归属查询。

### 验证方法②:

- 判断是否缓存命中的方法:有返回以下任意一个,即代表缓存命中,否则代表缓存未命中。
- X-Cache-Lookup: Hit From MemCache
- X-Cache-Lookup: Hit From Disktank
- X-Cache-Lookup: Cache Hit



## 验证4:WAF 是否能正确识别客户端 IP

1. 在 攻击日志页面,最近一次记录的 attack\_ip。



- 2. 验证 attack\_ip 是否为客户端真实 IP,而非 CDN 的 IP。
  - 可以与本地 IP 对比,是否为测试机器的 IP。
  - 可以通过 CDN 的 IP 归属查询 功能进行验证。



# HTTPS 免费证书申请和应用

最近更新时间: 2025-06-30 17:56:12



# 前提条件

Web 应用防火墙提供域名 HTTPS 接入配置和防护能力,若您的网站未进行 HTTPS 改造,您可以在 腾讯云 SSL 证书控制台 申请免费的域名证书。证书申 请后,在 Web 应用防火墙控制台关联证书,Web 应用防火墙将帮助您在不改造源站的情况下,一键实现全站 HTTPS 访问,客户端使用 HTTPS 连接网站。 可参见 域名型证书申请流程 免费申请域名型(DV)SSL 证书。

## HTTPS 证书关联操作步骤

- 1. 登录 Web 应用防火墙控制台,在左侧导航中,选择资产中心 > 实例管理。
- 2. 在实例管理页面,单击所属实例右侧的**管理域名**。

新建实例	~	清选择地域 🖌		获取鼠标焦点即可选择过滤属性	Q
实例D 実例名称 地域 実例类型 SaaS型	3 <b>D</b>	计费模式 ② 到期时间 202 自动疾费	域名数量规格 WAF QPS规格 ① 研究规格限制 ①	↑ 主域名 1/1 个 ips 0 Mbps	续费 升值配 → 管理域名

- 3. 在域名接入页面,单击添加域名,进入添加域名页面。
- 4. 在服务器配置中,勾选 HTTPS,在证书配置中,并根据您证书的类型,选择关联普通证书或关联国密证书。

确定

取消

e () •	НТТР
	✓ HTTPS 443 ✓
	证书配置 关 <b>联普通证书</b>
	国密证书配置 关联国密证书
	高级设置▲
	HTTPS强制跳转 ①
	HTTPS回源方式 HTTP 80 ~ OHTTPS
	回源SNI开关
	○ 保持源请求host 修正为源站host 自定义host
圆选择 <b>关联普训</b>	<b>通证书</b> ,单击后,选择证书来源为 <b>腾讯云托管证书</b> ,Web 应用防火墙会自动关联该域名的可用证书,配置完成后,单击 <b>确定</b> 。
普通证书配	置 X

○ 若您选择**关联国密证书**,单击后,选择证书来源为**腾讯云托管国密证书**,Web 应用防火墙会自动关联该域名的可用证书,配置完成后,单击**确定**。



国密证书酮	己置		
证书来源	● 腾讯云托管国密证书(SSL证书管理 □)	○ 导入自有国密证书	
证书	请选择		~
	I		Q

5. 开启 HTTPS 强制跳转开关,并在上方勾选 HTTP 访问协议,同时"HTTPS 回源方式"选择 HTTP,其他参数根据实际情况填写完成后,您的网站将支持 HTTPS 访问。

▲ 注意: 如需开启 HTT	PS 强制跳转开关,需	同时勾选 HTTP 和 HTTPS 访问协议。	
服务配置 (i) •	<ul> <li>✓ HTTP</li> <li>80 ✓</li> <li>✓ HTTPS</li> <li>443</li> </ul>	~	
	证书配置 国密证书配置 高级设置▲ HTTPS强制跳转① HTTPS回源方式	关联普通证书 关联国密证书 ● HTTP 80 ✓ HTTPS	

# WAF 一键开启 IPv6功能

最近更新时间: 2025-04-11 14:24:52

Web 应用防火墙提供域名 IPv6接入配置和防护能力,在开启 IPv6功能后,Web 应用防火墙与用户源站之间的链路将支持 IPv6功能。

### 前提条件

**〉**腾讯云

- SAAS-WAF 开启 IPv6 需要 WAF 版本为企业版及以上版本。
- CLB-WAF 支持全版本开启 IPv6。
- 开启 IPv6功能前,请核实**源站业务是否支持 IPv6**,同时源站回源地址也需要新增 IPv6回源。

### 操作步骤

登录 Web 应用防火墙控制台,在左侧导航栏选择接入管理。
 在域名列表域名,选择要开启 IPv6功能的域名,单击

<b>添加线名</b> 请选择实例	▼ 请选择实例类型	Ŧ				获取鼠标焦点即可选择过滤属性	C
域名/接入状态 ▼	实例信息 ③	实例ID/实例名称	使用模式 🔻	回源保护地址 ①	BOT开关		
			规则: 拦截模式	童者		備定升眉当射或者IPV6批失; 开启开关后,域名支持IPV6地址 确定 取消	除 基础防护 业务防护 更多 ▼
			规则: 拦截模式	个			除 基础防护 业务防护 更多 ▼

### 3. 单击确认,即可开启 IPv6功能。

域名列表								<ul> <li>○法・許引 量益担当</li> <li>○ 切換成功</li> </ul>	×
【編詞防护公告】Apache Log42 這程代码执行編詞防护適告     シロ21年12月9日、第汎云交会選队发現 Apache Log4 2 15 0.rc1 的商役編詞利用培节接公开、攻击者利用識詞可以远程执行代码、参考 識題送量     シロ21年12月9日 23点、離讯云Web应用防火環目業為发佈規则, 接入即可防护式編词 (編詞相关規则D为 <u>106247465</u> 、 <u>106247467</u> 、 <u>106247369</u> )									
<b>海加城名</b> 國志澤美利 ▼ 國选澤美利提型	v				域名:ipvi	<b>3</b> 获取鼠标焦点	即可选择过滤属性	± C	¢
	关例的交通者称	使用极式 ▼ 规则: 拦截横式	eišekii, minr (i)	BOTHX	IPv6开关	WAF开关 Y	50回日志 ▼	操作 编辑 删除 基础防护 BOT与业务防护 更多 ▼	
共1项							20 🔻 条/页	⊯ ∢ 1 /1页	► H

4. 验证 IPv6是否开启。dig 域名 AAAA 记录后即可查看 WAF 是否开启 IPv6,出现 IPv6地址后即为开启成功。

[root@VM-0-16-centos ~]# dig	AAAA
<pre>; &lt;&lt;&gt;&gt; DiG 9.11.26-RedHat-9.11.26-4.el8_4 ;; global options: +cmd ;; Got answer: ;; -&gt;&gt;HEADER&lt;&lt;- opcode: QUERY, status: NOE ;; flags: qr rd ra; QUERY: 1, ANSWER: 3, F</pre>	<<>> : 域名 AAAA ERROR, id: 51589 AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:	AAA
; ANSWER SECTION:	NAME Com. IN AAAA IPV6地址

# 热点问题

### 如果源站没有设置 IPv6回源,那访问端是否支持以 IPv6形式访问?

当源站没有 IPv6资源时,访问端以 IPv6形式访问,WAF 会自行将资源转换为 IPv4回源。

## 如果源站没有设置 IPv4回源,那访问端是否支持以 IPv4形式访问?

当源站没有 IPv4资源时,访问端以 IPv4形式访问,WAF 会自行将资源转换为 IPv6回源。 即 WAF 会自行转换 IPv4与 IPv6,使其符合源站对应的回源。

情况一:只有ipv4

腾讯云



## 当开启 IPv6选项后,提示"实例所属集群节点升级中"等异常报错如何处理?

当出现异常报错时,请 提交工单 处理。

### 开启 IPv6选项后,支持开启单个域名吗?

目前支持单个域名开启 IPv6。

# 如何获取客户端真实 IP

最近更新时间:2025-04-11 14:24:52

腾讯云

### WAF 获取客户端真实 IP 说明

WAF 通过反向代理的方式实现网站安全防护,用户访问 WAF 防护的域名时,会在 HTTP 头部字段中添加一条 X-Forwarded-For 记录,用于记录用户真实 IP,其记录格式为 X-Forwarded-For:用户 IP 。如果用户访问域名存在多级代理,WAF 将记录靠近 WAF 上一条的代理服务器 IP。例如: 场景一:用户>WAF>源站,X-Forwarded-For 记录为: X-Forwarded-For:用户真实 IP 。

场景二: 用户 > CDN > WAF > 源站, X-Forwarded-For 记录为: X-Forwarded-For:用户真实 IP,X-Forwarded-For:CDN 回源地址 。

#### () 说明:

- 场景二中,需要在 WAF 添加域名 时,选择代理情况为"是",选择代理接入后,可能存在客户端 IP 被伪造的风险。如果您使用腾讯云 CDN,不存在客户端 IP 被伪造的风险,腾讯云 CDN 会对 X-Forwarded-For 信息进行重置,只填写 CDN 获取的客户端 IP。(如果使用代理接入,攻击者需要在能直接对 WAF VIP 地址进行请求的情况下才会产生影响,代理接入时用户无法探测到 WAF VIP 地址,请避免代理接入时 WAF VIP 地址泄露)。
- 负载均衡型 WAF 接入,请参见负载均衡中 如何获取客户端真实 IP 。

下文将对常见的应用服务器 X-Forwarded-For 配置方案进行介绍:

- IIS 7 配置方案
- IIS 10 配置方案
- Apache 配置方案
- Nginx 配置方案

# IIS 7 配置方案

- T载与安装插件 F5XForwardedFor 模块,根据自己的服务器操作系统版本将 x86\Release 或者 x64\Release 目录下的 F5XFFHttpModule.dll
   和 F5XFFHttpModule.ini 拷贝到某个目录,这里假设为 C:\F5XForwardedFor ,确保 IIS 进程对该目录有读取权限。
- 2. 选择 IIS 服务器,双击模块功能。



() 说明:

如果当前服务器中没有安装 IIS 服务器,可以参考在 Windows Server 2008 或 Windows Server 2008 R2 上安装 IIS 7 进行安装。

#### 3. 单击配置本机模块。





### 4. 在弹出框中单击注册。



#### 5. 添加下载的 DLL 文件, 如下图所示:

注册本机模块		?	×
名称( <u>N</u> ):			
x_forwarded_for_x86			
路径(P):			
C:\x_forwarded_for\x86\F5XFFHttpModule.d	1		
确	Ē	取消	
注册本机模块		?	×
名称( <u>N</u> ):			
x_forwarded_for_x64			
路径(P):			
C:\x_forwarded_for\x64\F5XFFHttpModule.d	I		
論	Ē	取消	

6. 添加完成后,选择符合自身系统版本的 F5XForwardedFor 模块,勾选并单击确定。

## () 说明:

下图为添加示意图,实际添加按照对应操作系统版本及安装的 IIS 即可,如果不清楚当前是什么系统版本,可以同时添加。

配置本机模块		?	×
选择一个或多个要启用的已注册模块:			
UriCacheModule		注册( <u>R</u> )	1
FileCacheModule     TokenCacheModule     x forwarded for x86	[	编辑(E)	
✓ x_forwarded_for_x64		删除(M)	
	_		
	_		
	_		
	_		
	_		
	确定	取消	

7. 在 IIS 服务器的 "ISAPI 和 CGI 限制"中,添加如上两个 DLL ,并将限制设置为允许。

SI 🥼	SAPI 和 CGI 限制									
使用此功能	使用此功能指定可以在 Web 服务器上运行的 ISAPI 和 CGI 扩展。									
分组依据:	不进行分组 •									
描述	限制	路径								
х64	允许	C:\x_forwarded_for\x64\F5XFFHttpModule.dll								
x86	允许	C:\x_forwarded_for\x86\F5XFFHttpModule.dll								

8. 重启 IIS 服务器,等待配置生效。



# IIS 8.5 及以上 (含IIS 10.0) 配置方案

在 IIS 8.5 及以上(含 IIS 10.0)版本中,由于引入了增强日志功能,因此,管理员可以选择从请求或响应标头或服务器变量记录其他自定义字段。 1. 打开 IIS 管理器。



2. 在连接窗口中选择站点或服务器,并双击日志。

3. 在日志文件的格式字段中,选择 W3C,单击选择字段。



🌗 日志	
使用此功能配置 IIS 在 Web 服务器上记录请求的方式。	
一个日志文件/每(O): 网站 ~	
日志文件 格式(M): W3C 〜 选择字段(S) 目录(Y): %SystemDrive%\inetpub\logs\LogFiles 浏览(B) 编码(E): UTF8 〜	
<ul> <li>日志事件目标</li> <li>选择 IIS 将写入日志事件的目标。</li> <li>● 仅日志文件(L)</li> <li>○ 仅 ETW 事件(T)</li> <li>○ 日志文件和 ETW 事件(A)</li> </ul>	
日志文件滚动更新	

4. 在 W3C 日志记录字段对话框中,单击添加字段...。

### ▲ 注意:

增强日志记录仅适用于站点级日志记录 – 如果在"连接"窗格中选择了服务器,则"添加字段…"处于禁用状态。



W3C 日志记录字段			? ×	
标准字段(S):				
<ul> <li>✓ 日期(date)</li> <li>✓ 时间(time)</li> <li>✓ 客户端 IP 地址(c-</li> <li>✓ 用户名(cs-userna</li> <li>服务名称(s-sitena</li> <li>服务器名称(s-con</li> <li>✓ 服务器 IP 地址(s-</li> </ul>	p) me) me) nputername) p)		~	
自定义字段(C):				
日志字段	源类型	源		
				1
添加字段( <u>A</u> )	删除字段(图)	确定	编辑字段(E) 取消	

5. 在添加自定义字段对话框中,输入字段名称以标识日志文件中的自定义字段。选择源类型处选择请求标头,源输入 X-FORWARDED-FOR 。



-	W3C 日志说	录字段				? ×	
-	标准字段(	S):					-
	<ul> <li>✓ 日期(</li> <li>✓ 时间(</li> <li>✓ 客户端</li> <li>✓ 用户名</li> <li>─ 服务器</li> <li>─ 服务器</li> <li>✓ 服务器</li> </ul>	ー date) ime) (IP地址(c-ip) (cs-username) 称(s-sitename) 名称(s-computername) 添加自定义字段		?	×		
_		字段名称(N): OriginIP					
][		源类型(]):					
s\Lo		请求标头		~			
	自定义字	源( <u>S</u> ):					
1	日志字段	X-FORWARDED-FOR		~			
-							
10			确定	取消			
	添加字印	<b>g(A)</b> 删除字段( <u>R</u> )	10.1		编辑	字段(E)	
			印码人	E	F	X/Ħ	

6. 单击确认,重启 IIS 服务器,等待配置生效。

# Apache 配置方案

1. 如未安装 apache2-dev,需要先安装 apache2-dev,执行如下命令:

apt-get install apache2-dev

2. 安装 Apache 第三方模块"mod\_rpaf",需执行如下命令:

```
wget https://github.com/gnif/mod_rpaf/archive/refs/tags/v0.8.4.tar.g
tar zxvf mod_rpaf-0.8.4.tar.gz
cd mod_rpaf-0.8.4
/usr/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

3. 修改 Apache 配置 /etc/httpd/conf/httpd.conf ,需在最末尾添加:

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips IP地址 //IP 地址为 WAF 防护域名的回源 IP 地址,可以在 Web应用防火墙控制台,防护配置域名列表中的回源
IP 地址中查看,也可以在服务器后台的日志中查看,只需要将所有需要查看的 IP 都填写上即可。
```



PAFheader X-Forwarded-Fo

4. 添加完成后,重启 Apache。

/usr/sbin/apachectl restart

# Nginx 配置方案

1. 当 Nginx 作为服务器时,获取客户端真实 IP,需使用 http\_realip\_module 模块,默认安装的 Nginx 是没有编译 http\_realip\_module 模块的,需要 重新编译 Nginx,在 configure 增加 ---with-http\_realip\_module 选项,确保 http\_realip\_module 模块编译进 nginx 中。编译代码如下:



2. 修改 nginx.conf。(下述路径为演示路径,请根据真实安装路径进行配置)

```
vi /usr/local/nginx/nginx/nginx.conf
```

#### 修改如下部分的最后两行:

```
fastcgi connect_timeout 300;
fastcgi send_timeout 300;
fastcgi read_timeout 300;
fastcgi buffer_size 64k;
fastcgi buffers 4 64k;
fastcgi busy_buffers_size 128k;
fastcgi temp_file_write_size 128k;
set_real_ip_from IP地址; //IP 地址为 WAF 防护域名的回源 IP 地址,可以在 Web应用防火墙控制台,域名接入列表中的回源
IP 地址中查看。
real_ip_header X-Forwarded-For;
```

### 3. 重启 Nginx。

service nginx restart



# 如何更换证书

最近更新时间: 2024-04-24 14:15:41

# 操作场景

如果证书已过期,用户在浏览网站的时候会显示证书不可信;如果客户该域名有使用 API 调用,在调用过程中将会报错。为了避免证书过期对业务造成影响,请 在腾讯云控制台上及时更新证书。

### 操作步骤

# 示例1:更换自有证书

- 1. 登录 Web 应用防火墙控制台,在左侧导航中,选择资产中心 > 接入管理。
- 2. 在域名接入页面,选中所需域名,单击**编辑**,进入编辑域名页面。

域名/接入状态 ▼	实例信息 🛈	实例ID/实例名称	使用模式 ▼	回源保护地址 🛈	BOT开关	API分析 🛈	IPv6开关	WAF开关 ▼	访问日志 🍸	操作
tw 市 未配置 CNAME 记 录 <i>ゆ</i>	SaaS型-广州 4: 7 1: 2 6: 1 m I <u>ī</u>	v 8 g tī <u>ī</u>	规则:拦截模式	1    4 1 <u>4</u> 查看						編辑 删除 基础防护 BOT与业务防护 更多 ▼
ry <b>后</b> 正常防护	SaaS型-北京 f f f	w 1e e b, ī	规则: 拦截模式 AI引擎: 关闭模式	6: 6: 4 查看						编辑 删除 基础防护 BOT与业务防护 更多 ▼

3. 在编辑域名页面,单击服务器配置中的重新关联,弹出证书配置窗口。



编辑域名		×
所属实例	SaaS型         负载均衡型         CDC型         08/▼	
域名 *		
服务器配置 🛈	✓ HTTP 8099 ▼	
	HTTPS 443 -	
	证书配置     重新关联       类型:自有证书	
	过期时间:20 证书状态:正常-证书正常	
	高级设置▲	
	HTTPS强制跳转 ③	
	HTTPS回源方式 OHTTP 8099 - OHTTPS	
代理情况 🕄	○ 否	
源站地址 🛈	OIP Jazza	
	请输入源站IPv4或v6地址,用回车分隔多个IP,最多支持输入50个	
负载均衡策略	O 轮询 ── IP Hash	
高级设置▼		

4. 在证书配置窗口,证书来源选择自有证书,并输入相关的证书和私钥,单击**确认**,即可更换自有证书。

证书配置		×
证书来源	○ 腾讯云托管证书 (SSL证书管理 ☑) ● 自有证书	
证书	请将证书内容复制后粘贴在这里,包含证书链	
	0	
	请注意,粘贴的证书内容要包含 <mark>证书链</mark>	
私钥	请将私钥内容复制后粘贴在这里	
	0	
	<b>确定</b> 取消	

# \_\_\_\_

腾讯云

# 示例2: 腾讯云托管证书

### 1. 在 域名接入 页面,选中所需域名,单击编辑,进入编辑域名页面。

域名/接入状态 ▼	实例信息 🛈	实例ID/实例名称	使用模式 ▼	回源保护地址 🛈	BOT开关	API分析 ③	IPv6开关	WAF开关 ▼	访问日志 🍸	操作
tw 市 未配置 CNAME 记 录 <i>(</i> )	SaaS型-广州 4: 7 1: 2 6: m ī <u>ī</u>	v 8 g tr	规则:拦截模式	1    4 1						編辑 删除 基础防护 BOT与业务防护 更多 ▼
ry <b>咟</b> 正常防护	SaaS型-北京 f f f f	w 1e e b. ī	规则: 拦截模式 Al引擎: 关闭模式	6: 6: 4 查看						编辑 删除 基础防护 BOT与业务防护 更多 ▼

2. 在编辑域名页面,单击服务器配置中的重新关联,弹出证书配置窗口。

编辑域名		×
所属实例	SaaS型 负载均衡型 CDC型 ▼	
域名 *		
服务器配置 ()	V HTTP 80 V	
	HTTPS 443 -	
	证书配置       運新关联       类型:托管证书       过期时间:20/       近书式表:正常	
	高级设置▲	
	HTTPS强制跳转 ③	
	HTTPS回源方式 OHTTP 80 ▼ OHTTPS	
代理情况 🕄	<ul> <li>○ 否 ● 是</li> <li>WAF前是否有七层代理服务(高防/CDN等)?</li> </ul>	
客户端IP判定方式	● 获取请求Header字段X-Forwarded-For (XFF) 中的第一个IP地址	
	● 狭蚁网络层的remote_ip作为各户端的源IP,防止XFF协定	
MARKANENE U		
	请输入源站IPv4或v6地址,用回车分隔多个IP,最多支持输入50个	
负载均衡策略	O 轮询 ── IP Hash	
高级设置▼		

3. 在证书配置窗口,证书来源选择腾讯云托管证书,并选择新证书,单击**确定**,即可更换 SSL 证书。

() 说明:



此方法只适用于证书已经上传到 SSL 证书管理。	
--------------------------	--

证书配置		×
证书来源	● 腾讯云托管证书 (SSL证书管理 2) 目有证书	
证书 🕄	T	
	<b>確定</b> 取消	

## 示例3: 一键替换证书

- 1. 登录 SSL 证书控制台,在左侧导航中,单击**我的证书**,进入我的证书页面。
- 2. 在我的证书页面,选择所需 ID,单击部署,弹出选择部署类型弹窗。

证书信息	绑定域名	到期时间 (1) 🛊	关联资源 🚯	自动续费	状态 ▼	操作
ID:	: 1 1 1	20	Θ		已签发	部署下载 升级 更多▼
ID: □ □ □ □	ī.	20.	<b>⊘</b> 1		已签发	部署 下载 升级 更多 ▼

3. 在选择部署类型弹窗,部署类型选择 Web 应用防火墙,并选择所需 WAF 资源,单击确定,即可一键替换证书。

选择部署类	型							×
证书ID								
证书类型								
部署类型	🔵 负载均衡 🔹 内容分发网络	日本 - 一 云直播 O Web应用防火増		Þ	服务器			
资源实例	选择WAF资源				已选择 (2)			
	可輸入域名进行搜索		Q		域名	是否保持长连接		
	<mark>一</mark> 域名	是否保持长连接			ar	否	8	
	🔽 a	否				_	•	
	🔽 р	是			ps	定	0	
	te	Ť		↔				
	te	是						
	□ 1	是	- 1					
	1	是						
	支持按住 shift 键进行多选	*	<b>•</b> •					
		(	确定	取消	á			

# 检验是否生效

通过浏览器访问相关域名,可以查看证书的生效时间和到期时间。如果更换证书始终不生效,请 联系我们 获得帮助。



🚺 应用 😱 i	正书	× •
会腾	规 详细信息 证书路径	
	[]] 证书信息	
	这个证书的目的如下:	_
	• 向远程计算机证明你的身份	7
	•保证远程计算机的身份	
	• 2.	1
	南人叶和山志、頃参与近てがないがもればいか。 	-
	颁发者:	
	有效期从 2021/5/27 到 2022/6/1	
	領任は	SHER(S)
		10043(2)



# 防护与配置相关 如何设置 CC 防护

最近更新时间:2024-08-0814:12:01

本文将为您介绍如何在 Web 应用防火墙控制台设置 CC 防护。

## 背景信息

CC 防护可以对网站特定的 URL 进行访问保护,CC 防护支持紧急模式 CC 防护和自定义 CC 防护策略。

### △ 注意:

紧急模式 CC 防护策略和自定义 CC 规则防护策略,不能同时开启。

## 操作步骤

### 示例一:紧急模式 CC 防护设置

♪	<b>注意:</b>	
	紧急模式 CC 防护默认关闭,	开启前请确认自定义 CC 防护规则处于未启用状态。

### 1. 登录 Web 应用防火墙控制台,在左侧导航栏选择基础安全。

2. 在基础安全页面,左上角选择需要防护的域名,单击 CC 防护,进入 CC 防护页面。

基础安全	)	¥					基础安全操作指南 IZ
规则概览 Saas	理						
WEB安全规则	访问控制规则	CC防护规则	网页防篡改规则	信息防泄漏规则	API防护规则	返回拦截页面	
						● 默认 ○ 博选择拦截页面	▼ 应用 添加 删除
WEB安全(489)	访问控制(4) CC防护(14)	网页防篡改(2) 信息	息防泄漏(8) API安全(3)				添加精准白名单 精准白名单列表
紧急模式CC防护(	D			SESSIC	<b>N设置</b> ①		设置 测试 删除
状态 🔵	综合源站异常响应情况(超时、响应到 实时拦截高频访问请求,封蔡攻击源1	延迟) 和网站历史访问数据, 智創 小时	8决策生成防御策略,	Session	2置: 匹配模式: ·	会诸标识:	
				会话设置	Ŧ	设置时间: 2022-01-01 14:52:18	

3. 在紧急模式 CC 防护模块中,单击状态右侧的 🔵 ,经过二次确认后,开启紧急模式 CC 防护。

### () 说明:

- 当开启紧急模式 CC 防护时,若网站遭大流量 CC 攻击会自动触发防护(网站 QPS 不低于1000QPS),无需人工参与。若无明确的防护路
   径,建议启用紧急模式 CC 防护,可能会存在一定误报。可以在控制台进入黑白名单,对拦截 IP 信息,进行加白处理。
- 如果知晓明确的防护路径,建议使用自定义 CC 规则进行防护。

WEB安全(489) 访问控制(4) <b>CC助护(14)</b> 网页防算改(2) 信息防泄漏(8) API安全(3)		添加精准白名单 菊准白名单列表
※急模式CC防护① 状态 特合源法异常调应情况(認好、调应知识)和网站历史访问数据、智能关照生成防御策略,实时注氧强质功问请求,對第处击限1小对	SESSION设置            Session位置:            全面印度:            空面印度:            空面印度:	设置测试服除

# 示例二: 基于访问源 IP 的 CC 防护设置

基于 IP 的 CC 防护策略,不需要对 SESSION 维度进行设置,直接配置即可。 1. 登录 Web 应用防火墙控制台,在左侧导航栏选择**基础安全**。


2. 在基础安全页面,左上角选择需要防护的域名,单击 CC 防护,进入 CC 防护页面。

安全	)	v					基础安全操作指示
则概览 SaaS型	2						
/EB安全规则	访问控制规则	CC防护规则	网页防篡改规则	信息防泄漏规则	API防护规则	返回拦截页面	
						<ul> <li>● 默认</li> <li>请选择拦截页面</li> <li>↓</li> </ul>	应用 添加 删除
B安全(489)	访问控制(4) CC防护(14)	网页防篡改(2) 信息	息防泄漏(8) API安全(3)				添加精准白名单 精准白名单
急模式CC防护③				SESSI	DN设置③		设置 测试 删除
ه <b>()</b>	综合源站异常响应情况 (超时、响)	应延迟) 和网站历史访问数据, 智能 獨1小时	》决策生成防御策略,	Session	立置: 匹配模式:	会适标识:	
_	天前11日1月11日1月11日1日11日11日11日11日11日11日11日11日1	10, 1-J -4-J		0.000	T	VI-991-101 2022 01 01 14 52 10	

#### 3. 在 CC 防护页面,单击**添加规则**,弹出添加 CC 防护规则弹窗。

WEB安全(489) 访问控制(4) CC防护(14) 网页防算改(2) 信息防泄漏(6) API安全(3)		添加精准白名单 精准白名单列表
家急模式CC防护① 综合谱站异常顺应情况(超时、响应延迟)和网站历史访问数据,智能决策生成防崩策略,实时拦截离频加问请求,封禁攻击渡小时	SESSION设置① Session位置: 匹配模式: 会括标识: ↓ 会话设置: 设置时间: 2022-01-01 14:52:18	设置测试 删除
<b>添加规则</b> 单个域名最多可以添加50条规则	获取銀标集合即可选择过编署性	Q Ø

4. 在添加 CC 防护规则弹窗中,填写相应信息。

#### ▲ 注意:

IP 为识别方式时,若执行动是拦截、观察和人机识别时,规则被触发全流量生效。若执行动作是精准拦截或精准人机识别时,规则精准流量生效(只 针对当前匹配方式的流量生效),SESSION 生效同理。

名称 *	请输入名称,5	0个字符以内			
□方式 *		SSION			
bit *	匹配字段	匹配参数	逻辑符号	匹配内容	操作
	URL	T	等于    ▼	/开头, 128个字符内, 不	包含域名删除
			添加还可以添加9条,	最多10条	
]频次*	60	次 60秒 🔻 🚯			
动作*	拦截	• (i)			
]时长*	10	分钟 (i)			
-级*	- 50	+			

- 规则名称: 自定义名称, 50个字符以内。
- **识别方式**: IP、SESSION。
- **匹配方式:**包括相等、前缀匹配和包含。



- 高级匹配:通过进行 GET 表单和 POST 表单参数过滤,支持更加精细化频率控制,提高命中率。
  - 匹配字段:指定请求方法,支持 GET 或 POST。
  - 参数名:请求字段中的参数名,最多512字符。
  - 参数值:请求字段中的参数值,最多512字符。
    - 示例说明:如下三条 GET 请求测试数据: a=1&b=11、a=2&b=12、a=3&b=13。
      - 如果 GET 配置参数名为 a,参数值为1,则1命中。
      - 如果 GET 配置参数名为 a,参数值为\*,则1、2、3均命中。
- **访问频次**:根据业务情况设置访问频次。建议输入正常访问次数的3倍 10倍,例如,网站人平均访问20次/分钟,可配置为60次/分钟 200次/分钟, 可依据被攻击严重程度调整。
- 执行动作:观察、人机识别和阻断。
- 惩罚时长:最短为1分钟,最长为一周。
- 优先级: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高,相同优先级下,创建时间越晚,优先级越高。

#### 示例三: 基于 SESSION 的 CC 防护设置

基于 SESSION 访问速率的 CC 防护,能够有效解决在办公网、商超和公共 Wi-Fi 场合,用户因使用相同 IP 出口而导致的误拦截问题。

#### △ 注意:

使用基于 SESSION 的 CC 防护策略,需要先进行 SESSION 设置,才能设置基于 SESSION 的 CC 防护策略,下文步骤1 - 步骤4为 SESSION 设置操作。

- 1. 登录 Web 应用防火墙控制台,在左侧导航栏选择基础安全。
- 2. 在基础安全页面,左上角选择需要防护的域名,单击 CC 防护,进入 CC 防护页面。

基础安全	) ・ 基礎安全操作指南 2						
规则概览 Saat	5型						
WEB安全规则	访问控制规则	CC防护规则	网页防篡改规则	信息防泄漏规则	API防护规则	返回拦截页面	
						● 默认 ○ 博选择拦截页面	▼ 应用 添加 删除
WEB安全(489)	访问控制(4) CC防护(14)	网页防篡改(2) 信息	防泄漏(8) API安全(3)				添加精准白名单 精准白名单列表
紧急模式CC防护(	D			SESSI	DN设置①		设置测试制除
秋态 🔵	综合源站异常响应情况 (超时、响应 实时拦截高频访问请求,封禁攻击源	[延退] 和网站历史访问数据,智能 [1小时	<b>夫策生成防御策略</b> ,	Session	立置: 匹配模式: ·	会话标识:	
				会话设置	: Ŧ	设置时间: 2022-01-01 14:52:18	

#### 3. 在 SESSION 设置模块中,单击设置,设置 SESSION 维度信息。

WEB安全(489)	访问控制(4) CC防护(14) 网页防氰政(2) 信息防泄漏(6) API安全(3)		添加精准白名单 精准白名单列表
紧急模式CC防护	0	SESSION设置①	设置测试制除
状态 💽	综合源站异军调应情况(超时、调应延迟)和网站历史访问数据,智能关策生成防崩策略。 实时拦截高须访问请求,封禁攻击源1小时	Session位置: 匹配機式: 会活际识: 会活际识: 会活场强: 设置时间: 2022-01-01 14:52:18	

#### 4. 在 SESSION 设置弹窗,此示例选择 COOKIE 作为测试内容,标识为 security,开始位置为0,结束位置为9,配置完成后单击确定即可。

SESSION设置	ł		
SESSION位置 *	COOKIE *		
匹配模式 *	○ 字符串模式匹配   ○ 位置匹配		
SESSION标识*	security		
开始位置	0		
结束位置	9		
GET/POST示例: 如果一条请求的完 字符串匹配模式下, 位置匹配模式下, COOKIE示例: 如果一条请求的完 空符串匹配模式下, HEADER示例: 如果一条请求的完 位置匹配模式下,	<ul> <li>完整参数内容为: key_a=124&amp;key_b=456&amp;key_c=789</li> <li>下, SESSION标识为key_b=,结束字符为&amp;;则,匹配内容为456</li> <li>SESSION标识为key_b,开始位置为0,结束位置2;则,匹配内容为456</li> <li>完整COOKIE内容为: cookie_1=123;cookie_2=456;cookie_3=789</li> <li>下, SESSION标识为cookie_2=,结束字符为;;则,匹配内容为456</li> <li>SESSION标识为cookie_2,开始位置为0,结束位置2;则,匹配内容为456</li> <li>完ESSION标识为cookie_2,开始位置为0,结束位置2;则,匹配内容为456</li> <li>完ESSION标识为X-UUID: b65781026ca5678765</li> <li>SESSION标识为X-UUID,开始位置为0,结束位置2;则,匹配内容为b65</li> </ul>		
	<b>确定</b> 返回		
参数说明: ○ SESSION ( ○ 匹配说明: 位	<b>位置</b> :可选择 COOKIE、GET 或 POST,其中 GET 或 POST 是指 位置匹配或者字符串匹配。	i HTTP 请求内容参数,非 HTTP 头部信	息。

○ SESSION 标识:取值标识,32个字符以内。

腾讯云

- 开始位置:字符串或者位置匹配的开始位置,0-2048以内的整数。
- 结束位置:字符串或位置匹配的结束位置,1-2048以内的整数,并且最多只能提取128个字符。
- 5. SESSION 维度信息测试。添加完成后,单击测试将填写内容进行测试。

WEB安全(489)	访问控制(4) CC防护(14) 网页防篡政(2) 信息防泄漏(6) API安全(3)		添加精准白名单 稿准白名单列表
紧急模式CC防护	0	SESSION设置①	设置测试删除
状态 💽	結合源法异常响应情况(超时、响应延迟)和网站历史访问数据,智能先兼生成防御策略, 实时拦截案须访问请求,封禁攻击源1小时	Session位置:         匹函使式:         会话标识:           会话设置:         设置时间: 2022-01-01 14:52:18	

6. 进入 SESSION 测试页面,设置内容为 security = 0123456789……,后继 Web 应用防火墙将把 security 后面10位字符串作为 SESSION 标识, SESSION 信息也可以删除重新配置。



SESSION测	ोत्त
待提取文本*	security=0123456789,GA1.2.1946815858.1557971486 ; qcloud_uid=8a77e298c61339e02bb39d7070a46a71; QCloud=Env-Id=282; _gcl_au=1.1.1127719532.1557971780; pgv_pvid=7813788454; ts_uid=587953158; language=zh; _onc_xsrt=8237922cc80aeb9307deb535315458fb%7C
	当前匹配位置: cookie;
	匹配方式:位置匹配;
	匹配设置:SESSION标识:security;开始位置:0;结束位置:9
测试结果	0123456789
	测试取消

7. 设置基于 SESSION 的 CC 防护策略,配置过程和 示例二 保持一致,识别模式选择 SESSION 即可。

()	说明:			
	以 GET 位置为 SESSION 标识设置 CC 规则,	当 CC 规则启用后,	会把相同的 SESSION 标识作为维度拦截,	而不是将 IP 作为维度。

 $\times$ 

则名称 ★	请输入名称, 50	个字符以内			
別方式★		BION			
配方式★	匹配字段	匹配参数	逻辑符号	匹配内容	操作
	URL	~	等于    ▼	/开头, 128个字符内, 不包含域名	<b>删除</b>
			添加还可以添加9条,;	最多10条	
问频次★	60	次 60秒 🔻 🕄			
行动作*	拦截	• (j)			
罚时长★	10	分钟 (i)			
先级 ★	- 50	+			

# 8. 配置完成,基于 SESSION 的 CC 防护策略生效。

▲ 注意:	
使用基于 SESSION 的 CC 防护机制,无法在 IP 封堵状态中查看封堵信息。	

# 前后端分离站点接入 WAF 验证码

最近更新时间: 2024-09-12 11:26:21

在前后端分离或 App 站点中接入 WAF 验证码,可以实现在前后端分离站点或 App 站点动态下发验证码。

前后端分离站点接入 WAF 验证码流程,适用于利用 WAF 进行 前后端分离站点动态进行人机验证的场景(如命中自定义规则、CC 攻击、BOT 行为管理 等),App(iOS 和 Android )皆使用 Web 前端 H5 方式进行接入。

# 前提条件

已购买 Web 应用防火墙(高级版及以上),并完成 接入 WAF。

## 检出原理

通过动态识别服务端返回包中是否包含 WAF 下发的验证码的相关字段,如果包含 WAF 下发的验证码的相关信息时,在顶部浮层渲染验证码,实现前后端分离 站点或 App 进行 WAF 站点验证码接入。

# 操作步骤

以下代码为接入WAF 验证码示例代码(以 axios 为例 ),根据应用场景,以此作为参考完成前后端分离站点的接入 WAF 验证码。

```
1. Axios Response 增加 interceptors。
```

```
//WAF 验证码seqid相关正则
 //捕捉错误及渲染验证码
   //展示验证码
   let wid = wid matches[1]
```





3. 全局引入验证码脚本,即在public/index.html引入 <script src="https://ssl.captcha.qq.com/TCaptcha.js"></script 。







## 5. 在 WAF 配置自定义规则,通过异步请求,查看当前页面是否展示验证码弹窗。





最近更新时间: 2024-06-28 15:41:01

本文档将介绍如何在腾讯云可观测平台(TCOP)配置告警,当 Web 应用防火墙(WAF)出现异常情况,可以及时提醒。

## 前提条件

🕥 腾讯云

- 已开通 Web 应用防火墙。
- 已配置完 域名列表。

# 操作步骤

# 步骤1:设置触发条件模板

- 1. 登录 腾讯云可观测平台控制台,在左侧导航中,单击告警管理>触发条件模板。
- 2. 在触发条件模板页面,单击新建,弹出新建弹窗。

← 触发条件模板	
<ol> <li>         •</li></ol>	
新建	
模板名称 🛊 触发条件	
共0项	

3. 在新建弹窗中,配置所需内容后,单击保存,即成功创建触发条件模板。

新建		×
<ol> <li></li></ol>	的用户您好,云监控事件告誓创建入口已下线,存量事件告誓计划于2022年4月中旬停止服务,相关能力将由 <del>事件总线</del> 承载,并在原有功能上新增规则匹配、自定义事件集、多 等特性。为保证您的事件相关服务可以正常使用,我们建议您开通事件总线并进行能力迁移,同时我们也提供一 <mark>键迁移服务</mark> ,如果您有疑问可查看事件总线产品文档。	
模板名称	1-100个中英文字符或下划线	
备注	1-100个中英文字符或下划线	
策略类型 触发条件	Web应用防火墙- v v v v v v v v v v v v v v v v v v v	
	演足 任意 ▼ 条件时, 触发告答	
	if 入蒂宽 ▼ 统计周期1分钟 ▼ > ▼ 0 MBytes 持续1个周期 ▼ then 每1天警告一次 ▼ ①	
	添加	
	保存取消	
参数说明: ○ 模板名	<b>3称</b> :输入模板名称。	



- 策略类型:选择 Web 应用防火墙。
- 使用预置触发条件: TCOP 内置对应监控项的触发条件,勾选规则开启。
- 触发条件:
  - 分为指标告警和事件告警。在其下方单击添加,可以设置多个告警项。
  - WAF 可以监控的条件包括:访问次数、Web 攻击数、CC 攻击数、上下行带宽、QPS、BOT 攻击数、Web 攻击占比、BOT 攻击占比和 CC 攻击占比。

#### 步骤2: 设置通知模板

- 1. 登录 腾讯云可观测平台控制台,在左侧导航中,单击告警管理 > 通知模板。
- 2. 在通知模板页面,单击新建,进入新建通知模板页面。

告警管理				
告警历史	策略管理	告警屏蔽	通知模板	触发条件模板
	<b></b>			
(i) 动态阈	值告警功能将于2	023年3月1日下线,	目前此功能仅对曾	P使用动态阈值告警策略配置告警策略的用户开放。
新建通知模板	ī 删除			
模板名称	\$			包含操作
	振したしていた。 接收人: 1个 接收人: 1个			
共 1 条				



3. 在新建通知模板页面,配置所需内容后,单击完成,即成功创建通知模板。

← 新建通知	莫板	
甘土仁白		
<b>基本信念</b> 描板复数	<u> 長文60人文文</u>	
通知迷刑 ()	<ul> <li>✓ 苦型執行</li> <li>✓ 苦型な育</li> </ul>	
通知语言		
所属标签		
	⑦金經 ▼  ⑦金經 ▼  ★法加	
	1 (1968)	
<b>通知操作</b> (至少	<b>這一</b> 项)	
用户通知	新增用户时,您还可以新增只用于接收消息的用户。消息接收人添加描引 🕐	
	接收対象 用户 <b>*</b> グ 新増用户	册卿余
	通知問題 🔽 周一 🔽 周三 💟 周四 🔽 周五 💟 周六 🔽 周日	
	通知时段 00.00.00~23:59:59 ③	
	接收渠道 🔽 邮件 🔽 短信 🗌 微情 🛈 📄 企业微信 🕥 💿 电话(立即开通) 🗳	
	医血管管理	
接口回调 🛈	接口URL 填写公网可访问到的url作为回调接口地址(域名或)P(搏口)[/path]),例如Ihtips://example.com.8080/alarm/callback	删除 查看使用指引 🖸
	通知周明 💙 周一 💙 周三 🔽 周四 💟 周五 🔽 周六 🔽 周日	
	通知时段 00.00.00~23.59.59 ③ ③	
	(参加)29度上回叫喝	
	① 已支持推送到企业做信群机器人、钉钉群机器人、slack群应用, 欢迎体验! Z	
投递日志服务	二 启用 ①	
	· 清选择出志集 ▼ 清选择日志主题 ▼ 🗘 创建日志主题 2	
完成		

参数说明:

- 模板名称: 自定义模板名称。
- 通知类型:
  - 告警触发: 告警触发时发送通知。
  - 告警恢复:告警恢复时发送通知。
- **通知语言:**可以选择中文或英文。
- 用户通知:
  - 接收对象:可选接收组或接收人。
  - 通知时段: 定义接收告警时间段。
  - 接收渠道:支持邮箱、短信、微信、电话四种告警渠道。
- 接口回调:填写公网可访问到的 URL 作为回调接口地址,最多可填写3个告警回调地址。TCOP 将及时把告警信息推送到该地址,当 HTTP 返回 200 为验证成功。告警回调字段说明请参考 告警回调说明。

○ 投递日志服务: 启用后告警消息将实时投递到日志服务 CLS 的指定日志主题。

#### 步骤3: 配置告警策略

1. 登录 腾讯云可观测平台控制台,在左侧导航中,单击告警管理>告警策略。

#### 🕛 说明

可在告警策略页面新增、修改复制以及查看策略的告警历史,对于每条策略,可以绑定刚设置的 触发条件 和 通知模板 。



#### 2. 在告警策略页面,单击新建,进入新建告警策略页面。

告警管理					
告警历史	策略管理	告警屏蔽	通知模板	触发条件模板	
<ol> <li>动态阈</li> </ol>	<b>值告</b> 警 功能将于	2023年3月1日下线,	目前此功能仅双	对曾使用动态阈值告答策略配置告答策	略的用户开放。〕
新建策略	删除	更多操作 ▼			
策略名称	y.	监控	类型	策略类型	
共 0 条					

#### 3. 在新建告警策略页面,需完成以下步骤:

3.1 基本信息:配置名称和备注等信息,其中策略类型选择 Web 应用防火墙。

1 配置告警	> 2 配置告警通知
基本信息	
策略名称	最多60个字符
备注	最多100个字符
<b>配置告警规则</b>	НОТ НОТ
血江大王	云产品监控 应用性能监控 前端性能监控 云拨测
策略类型	Web应用防火墙 / SAAS型WAF / 实例维度 ▼ 已有 2 条,还可以创建 298 条静态阈值策略;当前账户有0条动态阈值策略,还可创建20条。
所属标签	标签键 ▼ 标签值 ▼ ×
	+ 添加 ③ 键值粘贴板
告警对象	实例ID ▼ 请选择对象 ▼

3.2 WAF 告警对象:选择 WAF 支持以实例为监控告警的最小粒度,同时支持实例分组对象,需要手动配置分组。

## 🕛 说明

- 实例 ID: 该告警策略绑定用户选中的实例。
- 实例分组: 该告警策略绑定用户选中的实例分组。
- 全部对象: 该告警策略绑定当前账号拥有权限的全部实例。

3.3 触发条件:选择刚设置的触发条件模板,或手动配置。



告警对象	实例ID ▼ 请选择对象 ▼
触发条件	○ 选择模板 ○ 手动配置
	指标告署
	滿足以下 任意 ▼ 指标判断条件利,触发告誓 ☐ 启用告册分级功能
	國信英型 ① ● 静态 ① 动态 ①
	if WAFI5向次数总量 × 統计和度1分钟 × > × ① 1 Count 持续1个数据点 × then 每1小时告誓一次 × ① 面
	降値実型 ① (静态 ) 动态 ①
	if 网页防器改防护总… ▼ 统计粒度1分钟 × 大于碳小于 ▼ 中灵敏度 ▼ ① 的动态调值, 持续1个数据点 ▼ then 每1小时告重一次 ▼ ① 前
	阈值类型 ① ● 静态 ○ 动态 ①
	if 毎秒访问请求数 ▼ 続计粒度1分钟 ▼ > ▼ ① 1 次/s 持续1个数据点 ▼ then 每1小时告警一次 ▼ ① 面
	添加指标

## 3.4 通知模板:选择刚设置的通知模板后,单击确定保存。

<b>选择通知模</b> 構 已选择1个通	<b>反</b> 即模板,还可以选择 2 个	×
搜索通知模构	反	Q Ø
	通知模板名称 包含操作	
	· 接收人: 1个	A
	接收人: 1个	
	· 接收组:1个	
	<b>商</b> 定 取消	

3.5 高级配置(可选):单击)启用弹性伸缩后,达到告警条件可触发弹性伸缩策略。



## 4. 完成以上步骤后,单击**完成**,即成功创建告警策略。

配置告警通知	添加告警「接收人」/「接收组」,需要在下方选择或新建通知模板;添加「接口回调」可以点击模板名称进行操作。了解更多 🕻
通知模板	选择模板 新建模板
	已选择1个通知模板,还可以选择2个
	通知模板名称
<b>高级配置</b> (可选)	
弹性伸缩	自用后,达到告警条件可触发弹性伸缩策略
完成	