Web 应用防火墙

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2023-12-29 10:58:03

什么是 Web 应用防火墙

腾讯云 Web 应用防火墙（Web Application Firewall，WAF）是一款基于 AI 的一站式 Web 业务运营风险防护方案。通过 AI+规则双引擎识别恶意流量，保护网站安全，提高 Web 站点的安全性和可靠性。通过 BOT 行为分析，防御恶意访问行为，保护网站核心业务安全和数据安全。

腾讯云 WAF 提供两种类型的云上 WAF，SaaS 型 WAF 和负载均衡型 WAF，两种 WAF 提供的安全防护能力基本相同，接入方式不同。

SaaS 型 WAF 通过 DNS 解析，将域名解析到 WAF 集群提供的 CNAME 地址上，通过 WAF 配置源站服务器 IP，实现域名恶意流量清洗和过滤，将正常流量回源到源站，保护网站安全。

负载均衡型 WAF 通过和腾讯云负载均衡集群进行联动，将负载均衡的 HTTP/HTTPS 流量镜像到 WAF 集群，WAF 进行旁路威胁检测和清洗，将用户请求的可信状态同步到负载均衡集群进行威胁拦截或放行，实现网站安全防护。

腾讯云 WAF 可以有效防御 SQL 注入、XSS 跨站脚本、木马上传、非授权访问等 OWASP 攻击。此外还可以有效过滤 CC 攻击、提供 0day 漏洞补丁、防止网页篡改等，通过多种手段全方位保护网站的系统以及业务安全。

主要功能

功能	简介
AI + Web 应用防火墙	基于 AI + 规则的 Web 攻击识别，防绕过、低漏报、低误报、精准有效防御常见 Web 攻击，如 SQL 注入、非授权访问、XSS 跨站脚本、CSRF 跨站请求伪造，Webshell 木马上传等 OWASP 定义的十大 Web 安全威胁攻击
0day 漏洞虚拟补丁	腾讯安全团队 7 * 24 小时监测，主动发现并响应，24 小时内下发高危 Web 漏洞，0day 漏洞防护虚拟补丁，受护用户无需任何操作即可获取紧急漏洞、0day 漏洞攻击防护能力，极大缩短漏洞响应周期
网页防篡改	用户可设置将核心网页内容缓存云端，并对外发布缓存中的网页内容，实现网页替身效果，防止网页篡改给组织带来负面影响
数据防泄漏	通过事前服务器应用隐藏，事中入侵防护及事后敏感数据替换隐藏策略，防止后台数据库被黑客窃取
CC 攻击防护	智能 CC 防护，综合源站异常响应情况（超时、响应延迟）和网站行为大数据分析，智能决策生成防御策略。多维度自定义精准访问控制、配合人机识别和频率控制等对抗手段，

	高效过滤垃圾访问及缓解 CC 攻击问题
爬虫 BOT 流量管理	基于 AI + 规则库的网页爬虫及 BOT 机器人管理，协助企业规避恶意 BOT 行为带来的站点用户数据泄露、内容侵权、竞争比价、库存查取、黑产 SEO、商业策略外泄等业务风险问题
30线 BGP IP 接入防护	WAF 支持防护节点 30 线独享 BGP IP 链路接入，节点智能调度，有效解决访问延迟问题，保障 1 ~ 18 线城市用户的站点访问速度，实现网站访问速度影响无感知的云 WAF 安全防护部署

为何需要 Web 应用防火墙

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。羊毛客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。

大流量 DDoS 造成业务中断

为了使得竞争对手业务中断，或者造成关键门户网站不能访问，DDoS 攻击已经成为成本和门槛较低的攻击手段，对业务的连续性和品牌的影响极大，而且往往运营者在被攻击时很被动。

产品分类

最近更新时间：2023-12-29 10:58:57

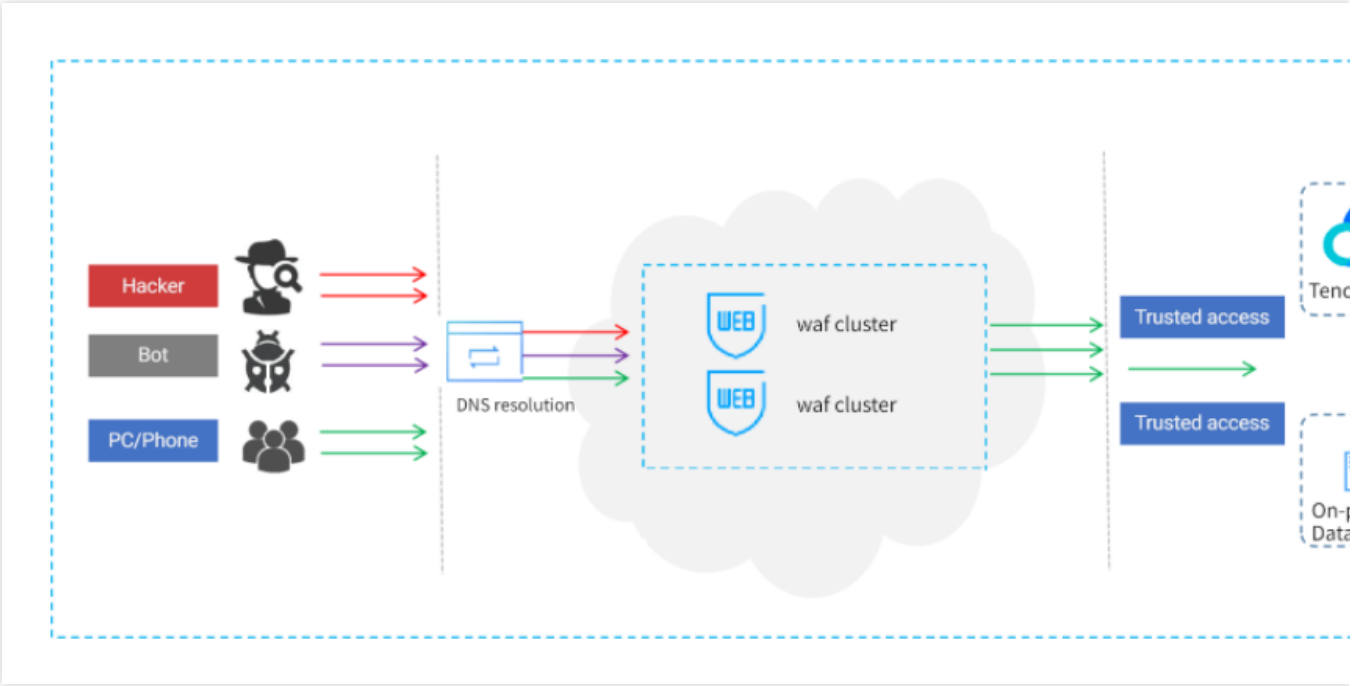
类型概述

腾讯云提供两种类型的云上 WAF，SaaS 型 WAF 和负载均衡型 WAF。两种 WAF 的安全防护能力基本相同，但接入方式不同，适用场景不同，您可以根据实际部署需求选择不同类型的 WAF。

类别	SAAS 型	负载均衡型
适用场景	适合所有用户（腾讯云上用户或本地 IDC 用户），通过 DNS 解析调度实现域名接入。	腾讯云上已使用或计划使用七层负载均衡的用户。
核心优势	适用范围广阔，广泛覆盖腾讯云上用户和非腾讯云上用户。	无感知接入，毫秒级延迟，WAF 接入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。 支持多地域接入。
如何选择	若用户在腾讯云上和本地均有网站需要防护需求，或腾讯云上未使用七层负载均衡，推荐使用 SAAS 型 WAF。	腾讯云上已使用或计划使用七层负载均衡的用户，且有 Web 安全防护、BOT 流量管理、等保合规保护、网站安全运营需求，推荐使用负载均衡型 WAF。
选择区域	SAAS 型 WAF 在购买时需要选择所属区域	负载均衡型 WAF购买时不需要选择区域，购买后在控制台配置时再关联 CLB 的支持区域。

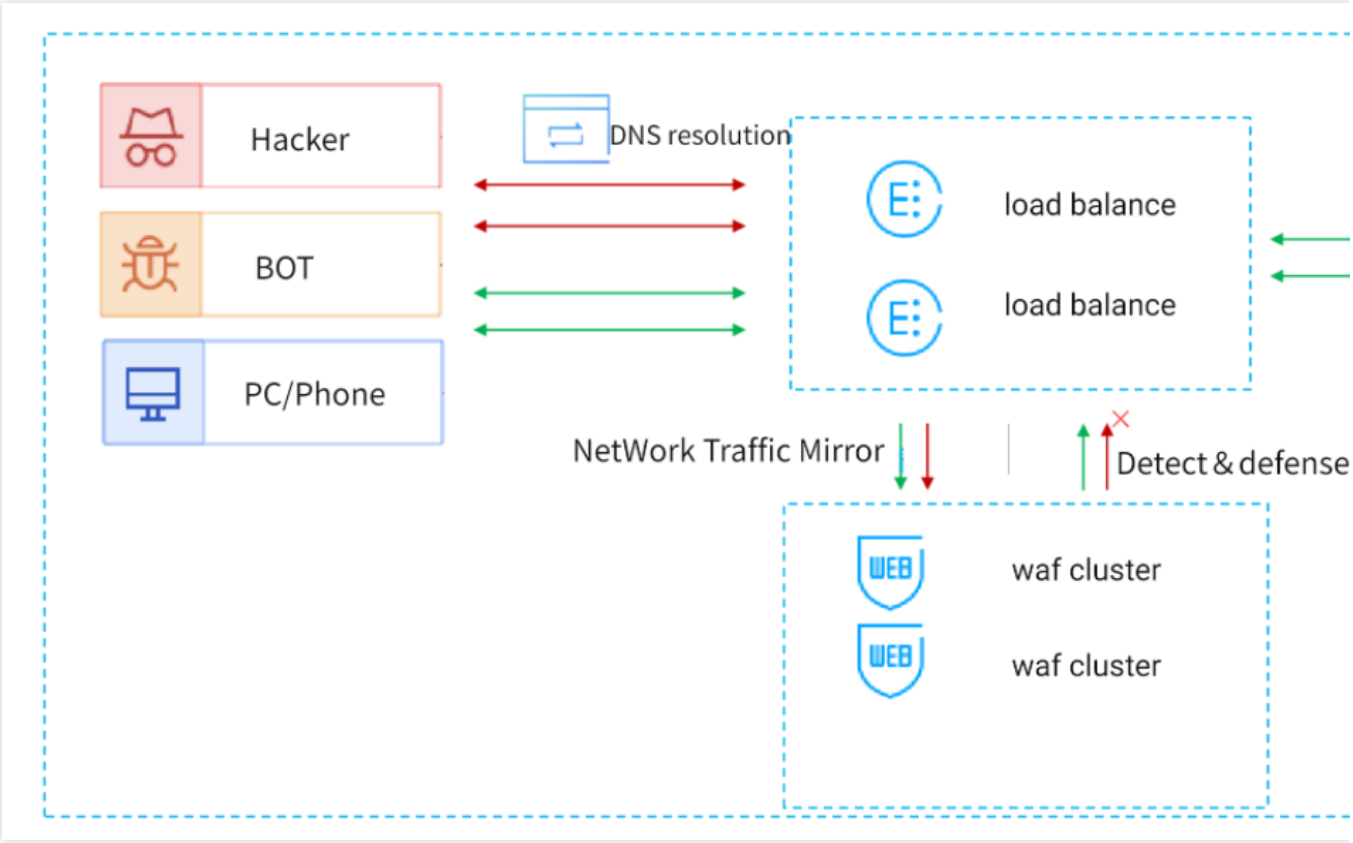
SaaS 型 WAF

用户在 WAF 上添加防护域名并设置回源信息后，WAF 将为防护域名分配唯一的 CNAME 地址。用户可以通过修改 DNS 解析，将原来的 A 记录修改为 CNAME 记录，并将防护域名流量调度到 WAF 集群。WAF 集群对防护域名进行恶意流量检测和防护后，将正常流量回源到源站，保护网站安全。



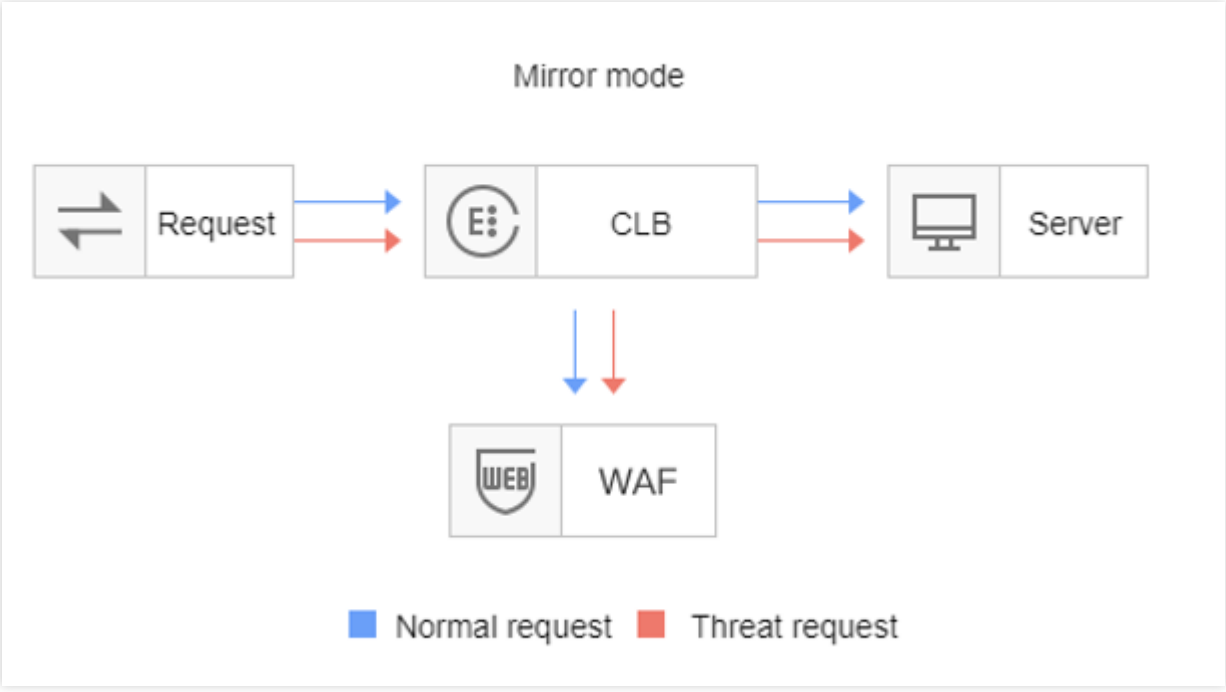
负载均衡型 WAF

WAF 通过配置域名和腾讯云七层负载均衡（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。

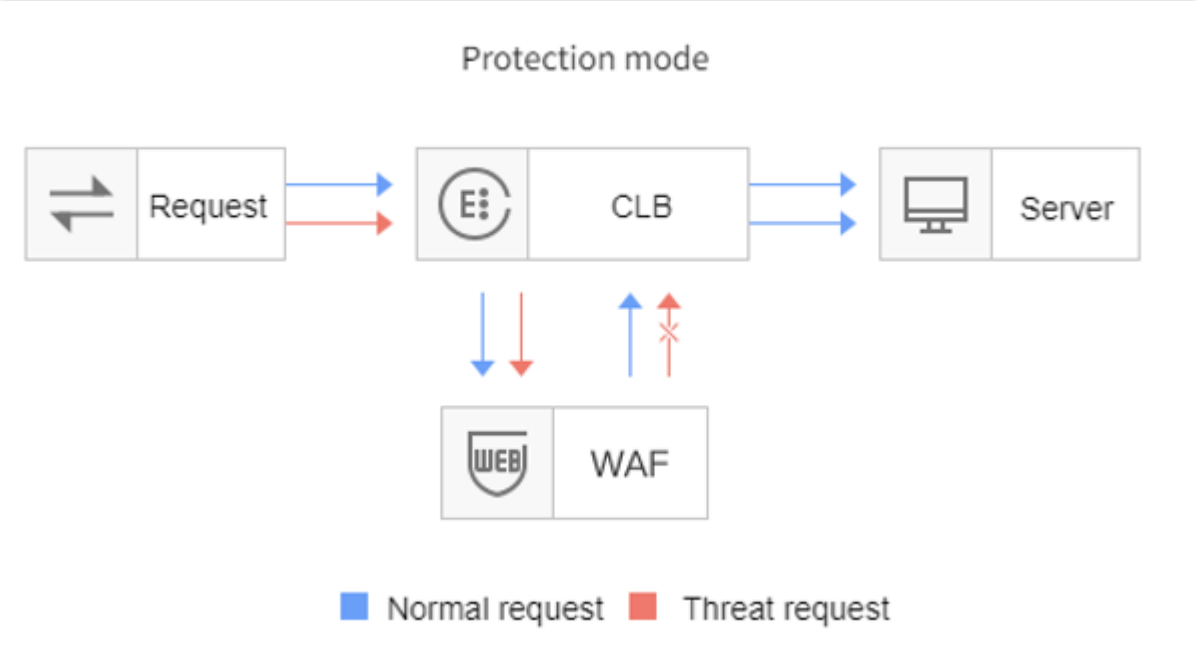


负载均衡型 WAF 提供两种流量处理模式：

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。


Protection mode
Request
CLB
Server
WAF
Normal request
Threat request

产品优势

最近更新时间：2023-12-29 11:01:08

多种接入防护方式

开通 WAF 后，无需进行业务变更即可完成防护接入，一键绑定腾讯云负载均衡实现网站旁路检测和威胁清洗，同时提供 一键 Bypass 功能，实现业务转发和安全防护分离，稳定可靠。
通过 CNAME 接入 WAF，隐藏用户真实源站，将可信流量回源，覆盖腾讯云和非腾讯云上用户。
防护集群资源多地部署、动态扩展，按需使用，避免冗余及单点故障。

AI+规则双引擎防护

在安全规则引擎进行 OWASP Top10 防御（如 SQL 注入、非授权访问、XSS 跨站脚本、CSRF 跨站请求伪造、命令行注入等）的基础上，引入 AI 防御能力，通过交叉验证持续学习，精准有效捕捉各类常规 Web 攻击、0day 攻击及其它新型未知攻击。
通过不断学习海量业务数据特征，生成基于业务的个性化防护策略，避免误报，用户可基于 AI 引擎实现自助误报和漏报处理，提升运营效率。
共享腾讯安全联合实验室为腾讯云安全持续输送安全防护能力，Web 应用防火墙由专业攻防团队7x24小时持续迭代防护系统，保障您的网站防御系统处于行业前沿。

BOT 行为管理

基于 AI 的行为分析引擎，实现实时会话追溯，通过流量画像匹配行为模型及行为标签，进行识别高效率检测恶意 BOT 行为。
提供超过1000种公开 BOT 类型，可快速设定防护策略。
提供爬虫和 IP 情报特征，快速识别 BOT 行为。
提供协议特征和50+会话特征，针对多种业务场景定义防护策略。
提供已知、未知和自定义类型 BOT 详细报表和统计，快速定位和防御恶意 BOT，保护网站业务安全。

智能 CC 防护

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，智能决策生成防御策略，实时拦截高频访问请求，封禁攻击源。
可自定义 session，通过 session 维度进行 CC 防护，更加精确防护 CC 攻击，减少误报。

可实时查看 CC 封堵状态 IP，根据需要快速调整防护策略。

一键无缝接入百 G 抗 DDoS 攻击能力，轻松应对敏感大流量 DDoS 攻击问题，无惧突发风险。

应用场景

最近更新时间：2023-12-29 11:01:27

政务网站防护

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

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，可智能过滤恶意攻击及垃圾访问，保障正常访问业务流畅。

金融网站防护

一键接入防护，可跟大流量 DDoS 防御有机结合，同时具备 Web 安全防护。
可有效检测撞库等异常访问，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

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），通过在四层和七层阻断海量的恶意请求，保障网站可用性。

套餐与版本说明

最近更新时间：2023-12-29 11:01:45

中国大陆版本

SaaS 型 WAF

分类	类别	高级版	企业版	旗舰版	独享版
套餐基础信息	适用场景	适用于中小非业务网站的标准防护	适用于中小型普通业务站点及中大型官网站点定制化防护服务	适用于大型及超大型业务网站及复杂业务站点的定制化防护服务	适用于大型及超大客户 Web 和 AP 务安全防护，资源享，有特殊定制化护需求
	业务 QPS 峰值	2500QPS	5000QPS	10000QPS	50000QPS
	带宽规格（腾讯云内/腾讯云外）	50Mbps/15Mbps	100Mbps/30Mbps	200Mbps/50Mbps	1000Mbps/250M
	独享 IP	-	支持	支持	支持
	支持主域名个数	2	3	4	1000（可自定义
	支持总域名个数（包括防护主域名和其下的子域名）	20	30	40	20000（可自定义
	泛域名防护	-	支持	支持	支持
	IPv6 防护	-	支持	支持	支持
	证书定制	-	-	-	支持
	HTTP2/WebSocket	支持	支持	支持	支持
基础安全防护	规则防护引擎	支持	支持	支持	支持（可自定义）
	0Day 漏洞虚拟补丁	支持	支持	支持	支持
	IP 黑白名单	1000条/域名	5000条/域名	20000条/域名	20000条/域名（可定义）
	地域封禁	支持	支持	支持	支持

	访问控制（自定义策略）	10条/域名	20条/域名	50条/域名	200条/域名
	紧急模式 CC 防护	支持	支持	支持	支持
	基于 IP/Session 自定义 CC 防护	5条/域名	20条/域名	50条/域名	50条/域名
	数据防泄漏	5条/域名	10条/域名	20条/域名	50条/域名
	网页防篡改	10条/域名	20条/域名	50条/域名	50条/域名
	AI 引擎	-	-	支持	支持
	漏洞高级防护功能（AI 引擎）	-	-	支持	支持
日志处理	攻击日志查询和下载	支持	支持	支持	支持
	访问日志查询和下载（需购买日志包）	支持	支持	支持	支持
专业服务	非标准端口支持	-	支持	支持（可自定义）	支持（可自定义）
	一对一售前支持服务	-	支持	支持	支持
	7*24小时远程+微信群支持	-	支持	支持	支持
	远程专家服务	-	-	支持	支持
	1对1专家现场支持	-	-	-	5次
	工单售前售后支持	支持	支持	支持	支持

负载均衡型 WAF

分类	类别	高级版	企业版	旗舰版	独享版
套餐	适用场景	适用于中小非业务	适用于中小普通业务站点及中大	适用于大型及超大型业务网站及	适用于大型及超大型客户 Web 和 API 服务安全防

基础信息		网站的标准防护	型官网站点定制化防护服务	复杂业务站点的定制化防护服务	护，资源独享，有特殊定制化防护需求
	QPS 峰值	2500QPS	5000QPS	10000QPS	50000QPS
	带宽规格	100Mbps	200Mbps	400Mbps	400Mbps
	多地域联动支持	-	-	支持10个地域	支持
	绑定负载均衡监听器个数	200	300	500	1000（可自定义）
	支持主域名个数	2	3	4	1000（可自定义）
	支持总域名个数（包括防护主域名和其下的子域名）	20	30	40	20000（可自定义）
	泛域名支持	-	支持	支持	支持
	IPv6 防护	支持	支持	支持	支持
基础安全防护	规则防护引擎	支持	支持	支持	支持（可自定义）
	0Day 漏洞虚拟补丁	支持	支持	支持	支持
	IP 黑白名单	1000条/域名	5000条/域名	20000条/域名	20000条/域名（可自定义）
	地域封禁	支持	支持	支持	支持
	访问控制（自定义策略）	10条/域名	20条/域名	50条/域名	200条/域名
	基于 IP/Session 自定义 CC 防护	5条/域名	20条/域名	50条/域名	50条/域名
	AI 引擎	-	-	支持	支持
	漏洞高级防护功能（AI 引擎）	-	-	支持	支持

日志处理	攻击日志查询和下载	支持	支持	支持	支持
	访问日志查询和下载（需购买日志包）	支持	支持	支持	支持
专业服务	证书双向认证	支持	支持	支持	支持
	一对一售前支持服务	-	支持	支持	支持
	7*24小时远程+微信群支持	-	支持	支持	支持
	远程专家服务	-	-	支持	支持
	1对1专家现场支持	-	-	-	5次
	工单售前售后支持	支持	支持	支持	支持

非中国大陆版本

说明

资源正在升级中，如需购买请 提交工单 申请。

SaaS 型 WAF

分类	类别	高级版	企业版	旗舰版	独享版
套餐基础信息	适用场景	适用于中小非业务网站的标准防护	适用于中小型普通业务站点及中大型官网站点定制化防护服务	适用于大型及超大型业务网站及复杂业务站点的定制化防护服务	适用于大型及超大客户 Web 和 API 务安全防护，资源享，有特殊定制化护需求
	业务 QPS 峰值	2500QPS	5000QPS	10000QPS	50000QPS
	带宽规格（腾讯云内/腾讯云外）	50Mbps/15Mbps	80Mbps/30Mbps	100Mbps/50Mbps	1000Mbps/250Mb

	独享 IP	-	支持	支持	支持
	支持主域名个数	2	3	4	1000（可自定义）
	支持总域名个数（包括防护主域名和其下的子域名）	20	30	40	20000（可自定义）
	泛域名防护	-	支持	支持	支持
	证书定制	-	-	-	支持
	HTTP2/WebSocket	支持	支持	支持	支持
基础安全防护	规则防护引擎	支持	支持	支持	支持（可自定义）
	0Day 漏洞虚拟补丁	支持	支持	支持	支持
	IP 黑白名单	1000条/域名	5000条/域名	20000条/域名	20000条/域名（可定义）
	地域封禁	支持	支持	支持	支持
	访问控制（自定义策略）	10条/域名	20条/域名	50条/域名	200条/域名
	紧急模式 CC 防护	支持	支持	支持	支持
	基于 IP/Session 自定义 CC 防护	5条/域名	20条/域名	50条/域名	50条/域名
	数据防泄漏	5条/域名	10条/域名	20条/域名	50条/域名
	网页防篡改	10条/域名	20条/域名	50条/域名	50条/域名
	AI 引擎	-	-	支持	支持
日志处理	攻击日志查询和下载	支持	支持	支持	支持
	访问日志查询和下载（需购买日志包）	支持	支持	支持	支持
专业服务	非标准端口支持	-	支持	支持（可自定义）	支持（可自定义）
	一对一售前支持服务	-	支持	支持	支持

	7*24小时远程+微信群支持	-	支持	支持	支持
	远程专家服务	-	-	支持	支持
	1对1专家现场支持	-	-	-	5次
	工单售前售后支持	支持	支持	支持	支持

负载均衡型 WAF

分类	类别	高级版	企业版	旗舰版	独享版
套餐基础信息	适用场景	适用于中小非业务网站的标准防护	适用于中小普通业务站点及中大型官网站点定制化防护服务	适用于大型及超大型业务网站及复杂业务站点的定制化防护服务	适用于大型及超大型客户 Web 和 API 服务安全防护，资源独享，有特殊定制化防护需求
	QPS 峰值	2500QPS	5000QPS	10000QPS	50000QPS
	带宽规格	100Mbps	200Mbps	400Mbps	400Mbps
	多地域联动支持	-	-	支持10个地域	支持
	绑定负载均衡监听器个数	200	300	500	1000（可自定义）
	支持主域名个数	2	3	4	1000（可自定义）
	支持总域名个数（包括防护主域名和其下的子域名）	20	30	40	20000（可自定义）
	泛域名支持	-	支持	支持	支持
基础安全防护	规则防护引擎	支持	支持	支持	支持（可自定义）
	0Day 漏洞虚拟补丁	支持	支持	支持	支持
	IP 黑白名单	1000条/	5000条/域名	20000条/域名	20000条/域名（可自定义）

		域名			
	地域封禁	支持	支持	支持	支持
	访问控制（自定义策略）	10条/域名	20条/域名	50条/域名	200条/域名
	基于 IP/Session 自定义 CC 防护	5条/域名	20条/域名	50条/域名	50条/域名
	AI 引擎	-	-	支持	支持
日志处理	攻击日志查询和下载	支持	支持	支持	支持
	访问日志查询和下载（需购买日志包）	支持	支持	支持	支持
专业服务	证书双向认证	支持	支持	支持	支持
	一对一售前支持服务	-	支持	支持	支持
	7*24小时远程+微信群支持	-	支持	支持	支持
	远程专家服务	-	-	支持	支持
	1对1专家现场支持	-	-	-	5次
	工单售前售后支持	支持	支持	支持	支持

支持地域

最近更新时间：2023-12-29 11:08:04

您可以根据您的业务部署方式和部署位置选择不同的 WAF 类型和 WAF 所在地区，当前 WAF 支持的地域如下：

产品类型	支持地区	详情
SaaS 型 WAF	中国大陆地区	华南地区：广州
		华东地区：上海
		华北地区：北京
		西南地区：成都
	非中国大陆地区	港澳台地区：中国香港
		亚太东南：新加坡、曼谷、雅加达
		亚太东北：首尔、东京
		亚太南部：孟买
		美国西部：硅谷
		北美地区：多伦多
		欧洲地区：莫斯科,法兰克福
		美国东部：弗吉尼亚
		南美地区：圣保罗
负载均衡型 WAF	中国大陆地区	华南地区：广州、深圳金融
		华东地区：上海、南京、上海金融
		华北地区：北京、北京金融
		西南地区：成都、重庆
	非中国大陆地区	港澳台地区：中国香港
		亚太东南：新加坡、曼谷、雅加达
		亚太南部：孟买
		亚太东北：首尔、东京

		美国西部：硅谷
		美国东部：弗吉尼亚
		北美地区：多伦多
		欧洲地区：莫斯科、法兰克福

说明：

SAAS 型 WAF 的实例地域和 Web 源站服务器的地域建议保持一致，可以有效的减少业务时延。

负载均衡型 WAF 通过绑定 IPv6 负载均衡实现对 IPv6 网站防护，如果您需要使用 IPv6 网站防护，请提前确认您所在选择地区是否支持创建 IPv6 负载均衡实例，并且已经完成 IPv6 网站部署。

当前 IPv6 负载均衡实例主要地域均已支持，实际以 负载均衡购买页 显示的地域为准，更多负载均衡 IPv6 支持信息，请参见 IPv6 负载均衡快速入门。

WAF 在没有添加防御域名的情况下，可 联系我们 进行地域更换，已经添加的防护域名的情况下，不支持更换地域。

基本概念

最近更新时间：2022-06-17 15:08:15

SSL 证书

SSL 证书（Secure Sockets Layer）指一种安全协议，目的是为互联网通信提供安全及数据完整性保障。SSL 证书遵循 SSL 协议，可安装在服务器上，实现数据传输加密。

域名解析

域名解析（Domain Name Resolution）指互联网上的机器相互间通过 IP 地址来建立通信，但是人们大多数习惯记忆域名，将 IP 地址与域名之间建立一对多的关系，而它们之间转换工作的过程称为域名解析。
常用域名解析类型：
A 记录解析：用来指定域名的 IPv4 地址。
记录类型选择 “A”。
记录值填写腾讯云提供的主机 IP 地址。
MX 优先级不需要设置。
TTL 设置默认600。
CNAME 记录解析：将域名指向另一个域名，再由另一个域名来提供 IP 地址。
记录类型选择 “CNAME”。
记录值填写 Web 应用防火墙添加防护域名后的 CNAME 值。
MX 优先级不需要设置。
TTL 设置默认600。

安全组

安全组（Security Group）是一种有状态的包过滤虚拟防火墙，它用于设置单台或多台云服务器的网络访问控制，可以将同一地域内，具有相同网络安全隔离需求的云服务器实例，加到同一个安全组内，通过安全组的网络策略，对云服务器的出入流量进行安全过滤。

每秒查询率

每秒查询率（Query Per Second QPS） 是对一个特定的查询服务器，在规定时间内所处理流量多少的衡量标准，在因特网上，作为域名系统服务器的机器性能经常用每秒查询率来衡量，对应 fetches/sec（每秒响应请求数，即是最

大吞吐能力）。

回源 IP 地址

回源 IP 地址（Return Source IP Address）指客户添加域名成功后，Web 应用防火墙根据客户添加的域名，自动分配多个回源 IP 地址，回源 IP 地址作为 Web 应用防火墙的出口 IP，把经过过滤的正常访问流量，导向客户源站。

CC 攻击防护

CC 攻击防护（Challenge Collapsar Protection）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。

防篡改

防篡改（Tamper Proofing）指客户把核心网页内容缓存到云端，并对外发布缓存中的网页内容，实现网页替身效果，当核心页面收到请求时，返回缓存在云端的内容。

防泄露

防泄露（Anti Leakage）指通过检测响应页面中是否带有身份证号、手机号等敏感信息，发现敏感信息后，根据所设置的匹配动作对敏感信息进行观察或替换操作。其中，敏感信息过滤动作以 * 替换敏感信息部分，以达到防止用户敏感信息泄露的目的。

地域封禁

地域封禁（Territorial Prohibition）指判断攻击 IP 所属地域，封禁攻击 IP 所属地域的其它 IP 的访问，以达到快速封禁来自地域的其它 IP 攻击请求的目的。

一键 Bypass

一键 Bypass 功能指的是一键切换为纯转发功能，在 域名管理页面，选择所需域名，单击 WAF 开关处的

，开启该功能后，可快速放行所有被拦截的流量，保障业务快速恢复。