DDoS 防护

产品简介

腾讯云

文档目录

产品简介
- 产品概述
- 产品优势
- 应用场景
- DDoS 防护容量说明
- 封堵策略

产品简介
产品概述

最近更新时间：2026-09-11 14:24:31

> **说明：**
> 2026年09月10日之后接入的客户适用于以下说明。若您为存量高防包或高防 IP 客户，请参考 历史相关文档 。

什么是 DDoS 高防服务

DDoS 高防服务旨在保护您的业务以应对各类 DDoS 攻击，有效提升业务的连续性和稳定性，适用于游戏、互联网、电商、视频、金融、政务等对业务连续性要求较高的行业。
DDoS 高防服务的核心能力包括：

核心能力	说明
多层 DDoS 防护	提供 L3/4/7 DDoS 防护能力；支持与边缘安全加速平台 EO 联动进行 L7 防护策略配置，以防护 HTTP DDoS 攻击
丰富清洗资源	提供清洗集群防护能力，境外区域提供基于 Anycast 架构的高弹性防护，境内区域可通过扩展包扩展至 Tbps 级
灵活的套餐与扩展包	提供实用版、尊享版两档基础套餐，并可按业务需要加购防护能力扩展包
安全运营与可观测	提供攻击分析、解封中心等运营能力，帮助您实时掌握攻击与防护情况

产品原理

DDoS 高防服务通过腾讯云清洗集群实现攻击流量的检测与清洗：

1. 攻击流量到达防护资源前，先被牵引至腾讯云 DDoS 清洗集群。
2. 清洗集群通过一系列检测和识别算法，将恶意的攻击流量从正常业务流量中分离并丢弃。
3. 清洗后的正常业务流量回注至防护资源，不影响正常访问。

DDoS 高防服务支持为云上资源（CVM、CLB、EIP、WAF、LH）与 EO 资源（站点域名、四层代理实例、代播网段）建立防护链路，具体防护资源类型请参见 DDoS 防护容量说明 。

产品功能

多层 DDoS 防护

L3/4 DDoS 防护

针对网络层与传输层攻击（如 UDP Flood、SYN Flood、TCP Flood、ICMP Flood、ACK Flood、FIN Flood、RST Flood、DNS/NTP/SSDP 反射攻击、空连接、Frag Flood、Smurf、Stream Flood、Land Flood、IP 畸形包、TCP 畸形包、UDP 畸形包等）提供自动检测与清洗。

L7 DDoS（CC）防护

DDoS 高防服务为 L7 DDoS（CC）攻击提供防护容量支撑；具体防护策略配置（如自适应频控、智能客户端过滤、慢速攻击防护、速率限制等）由 EdgeOne（EO）提供。

灵活的套餐与防护容量

弹性套餐与扩展包

提供实用版、尊享版两档基础套餐，并支持按业务需要加购防护能力扩展包，扩展防护容量或覆盖更多地域，详情请参见 计费概述 。

分级防护容量

根据绑定套餐的不同，提供标准防护、增强防护、卓越防护三档防护容量，覆盖不同规模的防护需求，详情请参见 DDoS 防护容量说明 。

便捷的资源绑定

一键关联防护资源

支持将防护资源快速关联至防护实例，以获得针对具体资源的 DDoS 防护能力。

安全运营与可观测

攻击与业务分析

提供多维度统计报表，清晰展示攻击流量、防护效果及业务流量趋势，帮助您及时掌握攻击实况。

解封中心

遭受攻击导致业务被封堵时，可通过解封中心自助解除封堵。

为什么选择 DDoS 高防服务

1. **攻击规模持续增长，传统防护带宽难以应对**：DDoS 攻击流量已从早期的数十 Gbps 发展至 Tbps 级别。DDoS 高防服务提供大流量攻击防护能力，境外区域提供基于 Anycast 架构的高弹性防护，境内区域可通过扩展包弹性扩展至 Tbps 级，从容应对大流量攻击。
2. **攻击手法多样，网络层与应用层均需具备防护能力**：除了传统的流量型攻击，针对应用层的 CC 攻击也日益频繁。DDoS 高防服务提供 L3/4 网络层防护的完整能力（容量+策略配置），并为 L7 DDoS（CC）应用层攻击提供防护容量支撑，结合 EdgeOne（EO）的策略配置能力，共同构成完整的多层防护体系。

3. **安全事件响应滞后，缺乏实时可观测能力**：DDoS 高防服务提供攻击分析、告警通知、解封中心等安全运营能力，帮助您在攻击发生时及时获知、快速响应，避免因信息滞后扩大业务影响。
4. **采购与接入流程复杂，运维成本高**：DDoS 高防服务采用套餐制计费，购买后绑定需要防护的资源即可使用；后续可按需加购防护能力扩展包，无需重新采购或迁移。

了解更多产品优势，请参见 产品优势 。

产品优势

最近更新时间：2026-09-11 14:24:31

> **说明：**
> 2026年09月10日之后接入的客户适用于以下说明。若您为存量高防包或高防 IP 客户，请参考 历史相关文档 。

DDoS 高防服务为您的业务提供 DDoS 攻击自动缓释防护能力，具有以下优势：

丰富清洗资源，从容应对大流量攻击

提供 DDoS 清洗防护能力，境外区域提供基于 Anycast 架构的高弹性防护（当前防护能力可达 10 Tbps 以上），境内区域可通过防护能力扩展包扩展至 Tbps 级防护能力，从容应对大流量 DDoS 攻击。

网络层与应用层协同防护，统一接入体验

多数方案需要分别购买、独立部署网络层与应用层防护产品，接入与运维成本较高。DDoS 高防服务提供 L3/4 网络层防护的完整能力（防护容量+策略配置）；针对域名业务所面临的 L7 DDoS（CC）应用层攻击，DDoS 高防服务提供防护容量支撑，结合 EdgeOne（EO）的策略配置能力，共同构成完整的多层防护体系。

多维检测技术，精准识别各类攻击

依托腾讯自研防护集群，采用阈值检测、流量模型特征识别等多维算法，并通过 AI 智能引擎持续更新防护算法，持续提升攻击检测的准确率，灵活应对各类攻击行为。

套餐制弹性计费，按需加购不浪费

传统安全产品往往需要预先按最大攻击规模购买保底防护带宽，无论是否遭受攻击都需支付相应费用，资源利用率较低。DDoS 高防服务采用套餐制计费，您可根据防护需求灵活选择实用版或尊享版套餐，并按需加购防护能力扩展包，降低日常安全支出。

丰富的攻击报表，实时掌握防护详情

提供多维度统计报表，清晰呈现攻击防护流量及攻击详情信息，使您及时了解攻击实况。

专业的服务经验，深厚的重保运维积累

DDoS 团队有着丰富的重保和日常运维经验，具备海量业务割接、重大项目保障等优势服务资源，具备 7 × 24 小时监测经验，主动发现并响应，有效缩短响应周期。

应用场景

最近更新时间：2026-09-11 14:24:31

> **说明：**
> 2026年09月10日之后接入的客户适用于以下说明。若您为存量高防包或高防 IP 客户，请参考 历史相关文档 。

DDoS 高防服务适用于以下典型业务场景：

业务痛点	常见场景	适用行业	DDoS 高防服务解决方案
业务因大流量攻击导致带宽或连接资源耗尽，造成服务中断	游戏对战服务器、政企官网等直接暴露公网 IP 或域名的业务	游戏、政府、金融、互联网	为云上资源（CVM、CLB、EIP、WAF、LH）与 EO 资源（站点域名、四层代理实例、代播网段）提供 L3/4 DDoS 防护，自动检测并清洗 UDP Flood、SYN Flood 等网络层攻击流量。
登录、交易、查询等接口被大量伪造请求刷爆，导致处理性能耗尽	电商大促、金融交易、社交平台的登录注册与查询接口等	电商、金融、社交娱乐	针对 L7 DDoS（CC）攻击，DDoS 高防服务提供防护容量支撑，结合 EdgeOne（EO）的策略配置能力，共同构成完整防护。
重大活动或业务上线期间攻击风险显著上升，需要临时提升防护能力	大促预热、版本发布、重大赛事直播等短期高风险窗口期	电商、游戏、视频	支持按需升配套餐版本或加购防护能力扩展包，活动结束后可视需要降配，详情请参见 购买指引 、升降配说明 。
业务分布在中国大陆及海外多地域，需要统一管理的防护能力	出海业务、全球化游戏或社交应用等在中国大陆和全球（不含中国大陆）均有部署	游戏、社交娱乐、跨境电商	结合中国大陆防护能力扩展包、全球（除中国大陆外）防护能力扩展包、跨地域防护能力扩展包，覆盖不同地域的防护需求，详情请参见 计费概述 。

DDoS 防护容量说明

最近更新时间：2026-09-11 14:24:31

> **说明：**
> 2026年09月10日之后接入的客户适用于以下说明。若您为存量高防包或高防 IP 客户，请参考 历史相关文档。

DDoS 防护是腾讯云为各类云上资源提供的 DDoS 攻击自动缓解服务。接入腾讯云后，部分产品将默认提供标准防护（免费基础防护），可帮助业务抵御日常规模较小的流量型攻击，无需额外配置即可生效。当业务面临更高强度的攻击风险，或需要在基础防护之上进行更细粒度的流量管控（如黑白名单、限速策略等）时，可选购 DDoS 高防服务套餐，以获取更大的防护容量和自定义防护策略能力。

防护资源类型与防护级别

支持的防护资源类型

DDoS 防护支持以下防护资源类型。根据不同防护资源类型的网络部署架构特性，DDoS 防护的范围有所不同。其中，云上资源（CVM、CLB、EIP、WAF、LH）仅支持 L3/4 DDoS 防护；EdgeOne 资源中，域名支持 L3/4 与 L7 DDoS（CC）防护，四层代理实例与代播网段仅支持 L3/4 DDoS 防护。

防护资源类型	子资源类型	L3/4 DDoS 防护	L7 DDoS 防护（CC 防护）
云服务器（CVM）	已分配 普通公网 IP 的 CVM	支持	不支持
负载均衡（CLB）	公网负载均衡实例	支持	不支持
弹性公网 IP（EIP）	常规 BGP IP、静态单线 IP、高防 EIP	支持	不支持
Web 应用防火墙（WAF）	-	支持	不支持
轻量应用服务器（LH）	-	支持	不支持
EdgeOne（EO）	域名	支持	支持
EdgeOne（EO）	四层代理实例	支持	不支持
EdgeOne（EO）	代播网段	支持	不支持

防护级别

针对单个防护资源而言，支持在标准防护、增强防护、卓越防护三者中择其一配置防护级别。DDoS 防护对于不同防护级别的防护资源提供不同的防护容量，具体见下方各防护资源类型的说明。

防护级别	开通条件	适用防护资源类型
标准防护	默认免费提供，无开通条件	CVM、CLB、EIP、WAF、LH、EO 等腾讯云上具备公网访问能力的资源
增强防护	绑定任意 DDoS 高防套餐	CVM、CLB、EIP（常规 BGP IP、静态单线 IP）、WAF、LH、EO（域名、四层代理实例）
卓越防护	绑定任意 DDoS 高防套餐 + 任意防护能力扩展包	• **EO 域名、四层代理实例：**可绑定中国大陆防护能力扩展包、跨地域防护能力扩展包 • **EO 代播网段：**可绑定全球（除中国大陆外）防护能力扩展包 • **高防 EIP：**可绑定中国大陆防护能力扩展包、全球（除中国大陆外）防护能力扩展包

基础设施层 DDoS 防护（标准防护级别）

基础设施层 DDoS 防护对应标准防护级别，是腾讯云为具备公网访问能力的云上资源默认提供的免费基础防护。该防护始终开启、自动运行，无需购买与配置，资源接入腾讯云后即生效，可自动缓解 UDP Flood、SYN Flood 等常见的基础设施层（L3/4）DDoS 攻击。

防护资源类型	标准防护能力
CVM、CLB、EIP、WAF、LH 等具备公网访问能力的腾讯云资源	最高不超过 2 Gbps 的 L3/4 DDoS 防护能力[1]
EO 资源（域名、四层代理实例）	EO 平台默认防护，不承诺用于 DDoS 防护的资源容量[2]

说明：

注1：通常情况下，DDoS 防护仅对具备攻击特征的流量进行清洗，不会影响正常业务流量。特殊情况下（如公网入向流量异常突增且可能影响平台稳定时），即使流量无明确攻击特征，平台也可能采取临时处置措施（如限速或封禁）。处置前将通过消息中心（站内信、邮件、短信等渠道）通知；如您认为属于正常业务流量，可通过解封中心自助解封，或 联系我们 申请提前解封。

注2：“不承诺用于 DDoS 防护的资源容量”指的是 EO 将在保障基础设施稳定的前提下使用有限资源为您的业务提供防护，不承诺最小防护带宽与防护效果。

针对具体资源的 DDoS 防护（增强防护、卓越防护级别）

云上普通资源（CVM、CLB、EIP-常规 BGP IP、EIP-静态单线 IP、WAF、LH）

当您订阅 DDoS 高防套餐后，可将云上普通资源（CVM、CLB、EIP-常规 BGP IP、EIP-静态单线 IP、WAF、LH）关联至**增强防护**级别的防护实例上，防护能力按资源所在地域提供，具体参考下表：

地域		防护能力
中国大陆境内	华东地区（上海、上海金融、南京）	最大 30 Gbps - 600 Gbps
	华北地区（北京、北京金融）	最大 120 Gbps - 480 Gbps
	华南地区（广州）	最大 300 Gbps - 500 Gbps
	西南地区（重庆、成都）	最大 15 Gbps - 350 Gbps
	西北地区（西安）	最大 120 Gbps
全球（不含中国大陆）	-	防护能力有限（可能不达 10 Gbps）

说明：

- DDoS 防护为增强防护级别的云上普通资源（CVM、CLB、EIP-常规 BGP IP、EIP-静态单线 IP、WAF、LH）提供**全力防护**能力。全力防护指以成功防护每一次 DDoS 攻击为目标，整合当前本地清洗中心能力，全力对攻击进行抵御，同时随着腾讯云网络能力的不断提升，全力防护也会随之提升，无需您付出额外的升级成本。
- 如果您的业务遭受的 DDoS 攻击影响到腾讯云高防清洗中心的基础设施，则腾讯云保留压制流量的权利。流量压制可能对您的业务造成一定影响，例如业务访问流量可能会被限速，甚至被封堵。

高防 EIP

当您订阅 DDoS 高防套餐以及中国大陆防护能力扩展包或全球（除中国大陆外）防护能力扩展包后，可将高防 EIP 关联至**卓越防护**级别的防护实例上，以获得相应 DDoS 防护能力。

地域		防护能力
中国大陆境内	北京、广州、上海	最大 600 Gbps - 1 Tbps
全球（不含中国大陆）	中国香港、新加坡、硅谷、法兰克福、东京、弗吉尼亚、圣保罗、雅加达、首尔、利雅得	最大 Tbps 级别（全力防护）

EO 域名、四层代理实例

当您订阅 DDoS 高防套餐后，可将 EO 域名或四层代理实例关联至**增强防护**级别的防护实例上；若您额外订阅了中国大陆防护能力扩展包，则可将 EO 域名或四层代理实例关联至**卓越防护**级别的防护实例上，以获得更高 DDoS 防护能力。

防护区域[3]		绑定实用版/尊享版套餐时（防护级别=增强防护）	绑定实用版/尊享版套餐+中国大陆防护能力扩展包时（防护级别=卓越防护）
L3/4 DDoS 防护容量	中国大陆境内	可承诺防护 200 Gbps 以内 DDoS 攻击	扩展至可承诺防护 1 Tbps 以内 DDoS 攻击
	全球（不含中国大陆）	基于 Anycast 架构的高弹性防护[4]	
L7 DDoS 防护容量	中国大陆境内	可承诺防护 30万 QPS 以内 DDoS 攻击	扩展至可承诺防护 60万 QPS 以内 DDoS 攻击
	全球（不含中国大陆）	基于 Anycast 架构的高弹性防护	

说明：

注1：默认仅对超过 100Mbps 的攻击流量进行自动化清洗防护（攻击流量基于单一地区的流量统计，阈值仅供参考，请以实际防护为准）。

注2：DDoS 防护功能的实际防护容量根据基础设施的实际容量和资源分配情况动态调整。当 DDoS 攻击规模超过 EdgeOne 基础设施防护容量时，EdgeOne 将进行包括（不限于）流量调度、流量限速、封禁访问等缓解措施，以保障基础设施稳定。

注3：DDoS 高防的防护区域与 EO 站点或四层代理实例的加速区域保持一致。

注4：“基于 Anycast 架构的高弹性防护”指的是 EO 将在全球（不含中国大陆）区域利用 DDoS 流量清洗中心提供基于 Anycast 架构的防护能力，最高防护能力可达 10Tbps 以上，最新防护带宽容量详情，请参见 产品介绍页 。

EO 代播网段

当您订阅 DDoS 高防套餐以及全球（除中国大陆外）防护能力扩展包后，可将 EO 代播网段关联至**卓越防护**级别的防护实例上，以获得相应 DDoS 防护能力。

地域	防护能力

中国大陆境内	不适用
全球（不含中国大陆）	最大 Tbps 级别

封堵策略

最近更新时间：2026-09-11 14:24:31

> **说明：**
> 2026年09月10日之后接入的客户适用于以下说明。若您为存量高防包或高防 IP 客户，请参考 历史相关文档 。

什么是封堵

腾讯云通过共享基础设施的方式降低用云成本，所有用户共享腾讯云的外网出口。当某个防护对象遭受的攻击流量超过其防护容量时，为避免该攻击影响到云平台内其他未被攻击的用户、保障整个云平台网络的稳定，腾讯云将通过运营商的服务屏蔽该防护对象的所有外网访问，即触发封堵。

> **说明：**
> 封堵是腾讯云向运营商购买的服务，解除封堵的次数、频率均受运营商侧规则限制，因此无法频繁手动解除。

触发封堵的条件

封堵阈值等于该防护对象当前生效的防护容量上限。不同防护对象类型、不同防护级别对应的防护容量不同，具体数值请参见 DDoS 防护容量说明 。
当攻击流量超过该防护容量时，即触发封堵。

封堵时长

封堵时长默认为 2 小时，实际封堵时长与封堵触发次数和攻击峰值相关，最长可达 24 小时。封堵时长耗尽后，系统将自动解封云资源。
封堵时长主要受以下因素影响：

- 攻击是否持续：若攻击一直持续，封堵时间会延长，封堵时间从延长时刻开始重新计算。
- 攻击是否频繁：被频繁攻击的资源遭遇持续攻击的概率较大，封堵时间会自动延长。
- 攻击流量大小：被超大型流量攻击的资源，封堵时间会自动延长。

> **说明：**
> 针对个别封堵过于频繁的用户，腾讯云保留延长封堵时长和降低封堵阈值的权利。

封堵期间的影响

- 防护对象在封堵期间无法接受任何外网访问，包括正常业务流量。

如何预防封堵

- **提升防护容量**：订阅 DDoS 高防套餐，将具备公网访问能力的云资源绑定至增强防护或卓越防护级别的防护实例，提升云资源的防护容量上限，降低触发封堵的概率，详情请参见 购买指引 。
- **监控攻击态势**：通过攻击分析持续关注云资源的攻击趋势，及时评估是否需要提升防护级别。

如何解除封堵

订阅 DDoS 高防套餐后，单个腾讯云主账号每天拥有 3 次自助解封机会，超过后需等待系统自动解封或等待次日零点重置。