DDoS 高防 IP

DDoS 高防 IP（旧版）

产品文档

腾讯云

文档目录

DDoS 高防 IP（旧版）
产品简介
产品概述

最近更新时间：2020-03-23 16:00:04

简介

DDoS 高防 IP 是针对游戏、互联网及金融等业务遭受大流量 DDoS 攻击导致用户服务不可用的情况而推出的付费防护服务。用户通过配置高防 IP，将攻击流量引流到高防 IP 进行清洗，确保源站业务的稳定可用。
DDoS 高防 IP 使用公网代理的接入方式，支持 TCP，UDP，HTTP，HTTPS 和 HTTP2 等协议，覆盖金融、电商、游戏等各类业务。

主要功能

多类型防护

防护分类	描述
畸形报文过滤	过滤 frag flood，smurf，stream flood，land flood 攻击，过滤 IP 畸形包、TCP 畸形包、UDP 畸形包
网络层 DDoS 攻击防护	过滤 UDP Flood、SYN Flood、TCP Flood、ICMP Flood、ACK Flood、FIN Flood、RST Flood、DNS/NTP/SSDP 等反射攻击、空连接
应用层 DDoS 攻击防护	过滤 CC 攻击和 HTTP 慢速攻击，支持 HTTP 自定义特征过滤如 host 过滤、user-agent 过滤、referer 过滤

高级防护策略灵活

DDoS 高防 IP 默认提供基础安全策略，策略基于 IP 画像、行为模式分析、AI 智能识别等防护算法，有效应对常见 DDoS 攻击行为。同时提供 DDoS 高级防护策略，用户可针对自身业务需求配置，通过 IP 黑白名单、禁用协议/端口、报文特征过滤策略、空连接防护等操作，提供针对性防护。

清洗模式自定义

开放多套防护等级，提供自定义清洗阈值，用户可根据攻击情况灵活调整，对不同类型的 DDoS 攻击快速响应，充分匹配不同用户不同业务类型。

防护统计及分析

提供 DDoS 攻击、CC 攻击、转发流量等多维度数据的统计与展示，帮助用户实时掌握业务和攻击情况。同时支持对攻击自动抓包，方便用户快速定位异常问题。

支持的地域

DDoS 高防 IP 可防护任何公网服务器，包括但不限于IDC 机房、腾讯云、其他的云。目前已开放 DDoS 高防 IP 的地域包括：

- 中国内地（大陆）区域：华南地区（广州）、华东地区（上海）和华北地区（北京）。
- 境外区域：中国港澳台地区（香港、台湾）、亚太地区（新加坡、首尔、曼谷、印度、日本）、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（法兰克福）和欧洲地区（莫斯科）。

DDoS 高防 IP 在不同地域提供的高防能力请参考如下表格：

地区	保底防护	弹性防护	最大防护能力
广州	20Gbps - 50Gbps	30Gbps - 100Gbps	100Gbps
北京	20Gbps - 50Gbps	30Gbps - 100Gbps	100Gbps
上海	20Gbps - 100Gbps	30Gbps - 300Gbps	300Gbps
境外区域	10Gbps - 100Gbps	30Gbps - 400Gbps	400Gbps

建议选择最靠近业务源站的地域，可降低访问时延、提高访问速度。

产品优势

最近更新时间：2020-05-09 18:03:48

DDoS 高防 IP 是腾讯云针对云外用户业务在遭受大流量 DDoS 攻击后导致服务不可用时推出的付费产品，其产品优势如下：

超大防护资源

腾讯云 BGP 链路对接全国各地30家运营商，单客户单点可提供高达900Gbps的防护能力。境外数十个防护节点，高达400Gbps防护能力，轻松应对各类 DDoS 攻击。

领先的清洗能力

依托腾讯自研防护集群，采用 IP 画像、行为分析、Cookie 挑战等多维算法，并通过 AI 智能引擎持续更新防护算法，精准快速检测业务流量，灵活应对各类攻击行为。

极速访问体验

腾讯云 BGP 链路对接全国各地30家运营商，覆盖面广，能有效解决访问时延问题，保障各类用户群的访问速度，带来极速访问体验。

隐藏用户源站

DDoS 高防 IP 服务可对用户源站进行替换并隐藏。使用高防 IP 作为源站的对外服务地址，所有业务访问流量都经过高防 IP，将正常访问流量转发到源站，攻击流量在高防 IP 上被清洗后将干净流量返回给源站，增加源站安全性。

全业务支持

DDoS 高防 IP 服务支持网站和非网站业务，覆盖金融、电商、游戏、政府等各类业务，充分满足用户不同业务的安全防护需求。

定价灵活，优化成本

提供“保底防护+弹性防护”相结合计费方式，为用户降低日常安全费用，在需要时按需调整弹性防护，无需新增任何设备，无需调整配置。当攻击流量超过保底防护峰值时，腾讯云仍为用户继续防护，保障业务不中断，按当天实际攻击量付费。

丰富的攻击防护报表

提供精准的防护流量报表及攻击详情信息，使用户及时了解攻击实况。支持对攻击自动抓包，方便事后进行分析以及溯源。

应用场景

最近更新时间：2020-04-03 14:35:44

游戏

游戏行业是 DDoS 攻击的重灾区，DDoS 高防 IP 能有效保证游戏的可用性和持续性，保障游戏玩家流畅体验。同时为活动、新游戏发布或节假日游戏收入旺季时段保驾护航，确保游戏业务正常。

互联网

保证互联网网页的流畅访问，业务正常不中断。对电商大促等重大活动时段，提供安全护航。

金融

满足金融行业的合规性要求，保证线上交易的实时性、安全稳定性。

政府

满足国家政务云建设标准的安全需求，为重大会议、活动，敏感时期提供安全保障。保障民生服务正常可用，维护政府公信力。

企业

保证企业站点服务持续可用，避免 DDoS 攻击带来的经济及企业品牌形象损失问题。零硬件零维护，节省安全成本。

相关概念

最近更新时间：2020-04-21 17:38:09

DDoS 攻击

Distributed Denial of Service（DDoS），即分布式拒绝服务攻击，是指攻击者通过网络远程控制大量僵尸主机向一个或多个目标发送大量攻击请求，堵塞目标服务器的网络带宽或耗尽目标服务器的系统资源，导致其无法响应正常的服务请求。

网络层 DDoS 攻击

网络层 DDoS 攻击主要是指攻击者利用大流量攻击拥塞目标服务器的网络带宽，消耗服务器系统层资源，导致目标服务器无法正常响应客户访问的攻击方式。
常见攻击类型包括 SYN Flood、ACK Flood、UDP Flood、ICMP Flood 以及 DNS/NTP/SSDP/memcached 反射型攻击。

CC 攻击

CC 攻击主要是指通过恶意占用目标服务器应用层资源，消耗处理性能，导致其无法正常提供服务的攻击方式。
常见的攻击类型包括基于 HTTP/HTTPS 的 GET/POST Flood、四层 CC 以及 Connection Flood 等攻击方式。

防护峰值

防护峰值分为保底防护峰值和弹性防护峰值。

- 保底防护峰值：指高防服务实例的保底防护带宽能力。
- 弹性防护峰值：指高防服务实例的最大弹性防护带宽能力，弹性部分为按天后付费。

若未开启弹性防护，则保底防护峰值为高防服务实例的最高防护峰值。 若已开启弹性防护，则弹性防护峰值作为高防服务实例的最高防护峰值。当攻击流量超过高防服务实例的最高防护峰值后触发封堵。

> 弹性防护默认关闭。如需开启弹性防护，请在知悉弹性相关收费后自助开启。用户可以根据自身业务需求，随时调整弹性防护峰值。

弹性防护峰值的作用

开启弹性防护后，当攻击流量峰值超过购买的保底防护峰值且在弹性防护峰值范围内时，腾讯云 DDoS 高防 IP 可继续为用户提供防护，保障业务访问持续性。

弹性防护如何收费

开启弹性防护后，当攻击流量超过保底防护峰值时，会触发弹性防护并收取费用，取当天实际产生的最高攻击峰值所对应区间进行计费，账单次日生成。
例如，您购买的保底防护为20Gbps，且设置的弹性防护为50Gbps。若当天的实际攻击峰值为35Gbps，则需要支付30Gbps - 40Gbps区间的弹性防护费用。
详细费用请参见 计费概述 。

清洗

当目标 IP 的公网网络流量超过设定的防护阈值时，腾讯云大禹系统将自动对该 IP 的公网入向流量进行清洗。通过 BGP 路由协议将流量从原始网络路径中重定向到大禹系统的 DDoS 清洗设备上，通过清洗设备对该 IP 的流量进行识别，丢弃攻击流量，将正常流量转发至目标 IP。
通常情况下，清洗不会影响正常访问，仅在特殊场景或清洗策略配置有误时，可能会对正常访问造成影响。

封堵

当目标 IP 受到的攻击流量超过其封堵阈值时，腾讯云将通过运营商的服务屏蔽该 IP 的所有外网访问，保护云平台其他用户免受影响。简而言之，当您的某个 IP 受到的攻击流量超过您所购买的高防套餐最大 防护峰值 时，腾讯云将屏蔽该 IP 的所有外网访问。当您的防护 IP 被封堵时，您可以登录管理控制台 自助解封。
封堵

封堵阈值

DDoS 高防 IP 实例的防护 IP 的封堵阈值等于实际购买的最大 防护峰值。DDoS 高防 IP 有多种不同规格，详情请参考 计费概述。

封堵时长

封堵时长默认为2小时，实际封堵时长与当日封堵触发次数和攻击峰值相关，最长可达24小时。
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。被频繁攻击的用户被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用户，封堵时间会自动延长。

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。

为什么进行封堵

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。当发生大流量攻击时，除了会影响被攻击对象，整个腾讯云的网络都可能会受到影响。为了避免攻击影响到其他未被攻击的用户，保障整个云平台网络的稳定，需要进行封堵。

为什么不提供免费无限抗攻击

DDoS 攻击不仅影响受害者，也会对整个云网络造成严重影响，影响云内其它未被攻击的用户。DDoS 防御的成本非常高，一是带宽成本，二是清洗成本。其中最大的成本就是带宽费用，带宽费用以总流量计算，不会考虑是正常流量或是攻击流量而区别收费。
因此，腾讯云在成本可承受的范围内为云服务用户提供免费的 DDoS 基础防护服务，当攻击流量超出免费防护阈值时，腾讯云会屏蔽被攻击 IP 的外网流量。
有关封堵的更多信息，请参见 封堵相关问题。

购买指南
计费概述

最近更新时间：2021-03-18 10:46:46

计费方式

BGP 高防 IP 的计费方式为“保底防护峰值（冻结付费）+ 弹性防护峰值（后付费）+ 业务带宽（冻结付费）”。

计费项	计费模式	付费方式	付费说明
保底防护峰值	包年包月	冻结付费	提供基础防护带宽，冻结付费价格由保底防护峰值和购买时长确定。购买成功后先冻结费用，次月1号再结算上月费用，以此类推。
弹性防护峰值	按天按量计费	后付费	触发弹性防护后，按当天最高攻击峰值所对应的弹性防护峰值区间计费，账单次日生成。若未触发弹性防护，则不收取任何费用。支持升级、降级配置。
转发规则数	包年包月按个数计费	后付费	默认免费为每个高防 IP 提供60个转发规则数。当配置的规则数大于免费额度时，每增加10个按增加65美元/月计算。单个 DDoS 高防 IP 实例最高可支持300个转发规则数。
业务带宽	包年包月按带宽计费	冻结付费	业务带宽限制是针对业务 IN 方向（高防回源流量）和业务 OUT 方向（高防出流量），业务带宽规格需要大于业务 IN 和业务 OUT 中最大流量值。如果实际业务带宽持续超过购买 DDoS 高防 IP 时所设置的业务带宽，可能会出现丢包现象，影响业务，建议及时调整业务带宽。

保底防护

保底防护按月冻结付费，具体价格请参考如下表格：

DDoS 防护	CC 防护	大陆 BGP（美元/月）	境外 BGP（美元/月）
10Gbps	20,000QPS	-	2,500
20Gbps	40,000QPS	2,400	4,800
30Gbps	70,000QPS	3,500	7,000
40Gbps	100,000QPS	-	8,200

50Gbps	150,000QPS	9,500	10,500
60Gbps	200,000QPS	-	12,000
80Gbps	250,000QPS	-	15,000
100Gbps	300,000QPS	28,000	16,500

说明：

- Query Per Second（QPS），此处用于衡量 BGP 防护 IP 实例每秒可防护的 CC 攻击请求数。
- 可提供 T 级防护能力，如有需要，请联系您的商务经理进行定制。

弹性防护

用户可根据实际业务防护需求自助开启弹性防护。

- 未开启弹性防护时，最高防护峰值为保底防护峰值且不会产生后付费。
- 开启弹性防护时，弹性防护峰值为实例的最高防护峰值。
  - 未触发弹性防护时，不产生费用。
  - 当触发弹性防护（攻击峰值超过保底防护峰值且在弹性防护范围内）时，取当天实际发生的最高攻击峰值所对应计费区间进行计费，账单次日生成。

弹性防护具体价格请参考如下表格：

DDoS 防护峰值	大陆 BGP（美元/天）	境外 BGP（美元/天）
10Gbps ≤ 攻击峰值 < 20Gbps	-	320
20Gbps ≤ 攻击峰值 < 30Gbps	260	400
30Gbps ≤ 攻击峰值 < 40Gbps	450	700
40Gbps ≤ 攻击峰值 < 50Gbps	600	800
50Gbps ≤ 攻击峰值 < 60Gbps	800	1,200
60Gbps ≤ 攻击峰值 < 70Gbps	1,200	1,800

70Gbps ≤ 攻击峰值 < 80Gbps	1,500	2,200
80Gbps ≤ 攻击峰值 < 90Gbps	1,700	2,500
90Gbps ≤ 攻击峰值 < 100Gbps	1,900	2,700
100Gbps ≤ 攻击峰值 < 120Gbps	2,100	2,900
120Gbps ≤ 攻击峰值 < 150Gbps	2,300	3,200
150Gbps ≤ 攻击峰值 < 200Gbps	2,700	4,000
200Gbps ≤ 攻击峰值 < 250Gbps	4,800	4,800
250Gbps ≤ 攻击峰值 < 300Gbps	5,600	5,600
300Gbps ≤ 攻击峰值 < 400Gbps	-	6,600

转发规则数

规则数	价格（美元/月/10个）
端口数（或防护域名数）≤ 60	免费
端口数（或防护域名数） > 60	65

说明：

转发规则数指，单个高防 IP 实例，在非网站接入配置时支持添加的 TCP/UDP 端口数量，或网站接入配置时支持添加的 HTTP/HTTPS 域名数量。单个高防 IP 实例的转发规则数等于上述两种接入方式的转发规则数量之和。

业务带宽

业务带宽是指经过腾讯云高防机房完成清洗后转发回源站机房的正常业务流量所消耗的带宽。
目前支持的收费模式为包年包月冻结付费，**对于大陆地区的非腾讯云上用户，购买保底套餐后默认赠送100Mbps转发带宽**。具体价格请参考如下表格：

带宽	价格（美元/月）
50Mbps	750
100Mbps	1,500
150Mbps	2,250
200Mbps	3,000
500Mbps	7,500
1Gbps	15,000
2Gbps	30,000

带宽与七层请求数对应关系请参考如下表格：

业务带宽	HTTP/HTTPS
50Mbps	5,000QPS
100Mbps	10,000QPS
150Mbps	15,000QPS
200Mbps	20,000QPS
500Mbps	50,000QPS
1Gbps	100,000QPS
2Gbps	200,000QPS

⚠ 注意：

- 业务带宽限制是针对业务 IN 方向（高防回源流量）和业务 OUT 方向（高防出流量），业务带宽规格需要大于业务 IN 和业务 OUT 中最大流量值。如果实际业务带宽持续超过 购买 DDoS 高防 IP 时所设置的【转发业务带宽】，可能会出现丢包现象，影响业务，建议及时升级业务带宽。
- 此处 QPS 用于衡量非攻击状态下每秒的正常业务请求量。如果您的正常业务请求消耗过大超出所购买的规格，请及时 调整 DDoS 高防 IP 实例规格 以免因丢包造成业务影响。您可以参考上表中的带宽与七层请求

数对应关系合理增加 DDoS 高防 IP 实例的业务带宽，提高 HTTP/HTTPS 的正常 QPS 规格。

其他规格

其他规格说明请参考如下表格：

规格名称	规格参数	说明
转发端口数	60个 - 300个/单个防护 IP	TCP/UDP 协议+ HTTP/HTTPS 协议转发规格条目总数，对于 TCP、UDP 协议，若使用相同的转发端口值，则需要配置两条。
支持域名数		
源站 IP 数	20个/单个实例	4层与7层源站服务器 IP 地址总数
每秒新建连接数	50000个/单个防护 IP	单个防护 IP 的每秒新建连接数
并发连接数	200000个/单个防护 IP	单个防护 IP 的并发连接数

说明：

以上规格仅针对线上售卖，如果此配置不足以满足您的业务需求，请联系 腾讯云技术支持 定制更大的规格。

计费示例

DDoS 高防 IP 使用组合计费方式，计费示例说明如下：
例如，用户在上海区域购买了一个 DDoS 高防 IP，规格是“20Gbps 保底防护峰值+50Gbps 弹性防护峰值”。
若当天发生 DDoS 攻击事件且最高攻击流量峰值为45Gbps，则45Gbps超过保底防护峰值范围且使用了弹性防护峰值，落入了 40Gbps＜弹性峰值≤ 50Gbps 计费区间，当天产生弹性费用600美元。
则用户需支付费用合计为3000美元，其中包含当月的保底防护费用2400美元，当天产生的弹性费用600美元。

购买指引

最近更新时间：2022-05-09 16:58:29

前提条件

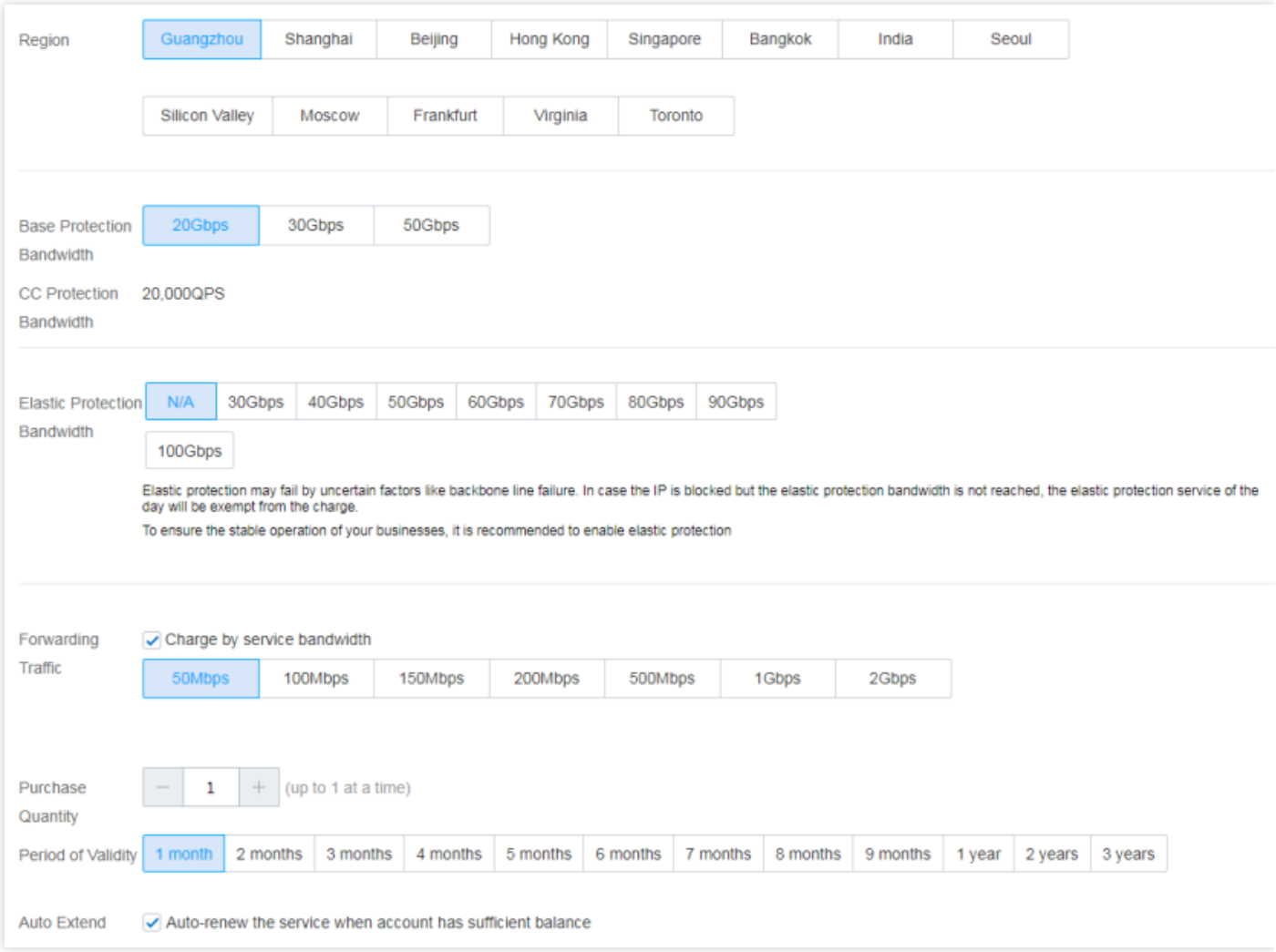
在购买 BGP 高防 IP （中国大陆）实例前，您需要完成注册腾讯云账号。

操作步骤

1.登录到 Anti-DDoS Advanced 控制台，单击 ***Create*** 进行购买。

2.根据实际需求选择防护配置。

- 地域：BGP 高防 IP 提供代理转发方式，请选择靠近源站服务器位置的地域，减少访问时延。
- 保底防护峰值：该实例的基础防护能力。建议以历史攻击流量的平均值为参考，选择的保底防护峰值略高于平均值，以便足够防御大部分攻击行为。
- 弹性防护峰值：该实例的弹性防护能力。建议以历史最高攻击流量为参考，选择的弹性防护峰值略高于历史最高峰值，以便足够防御大流量攻击，避免超过防护峰值而引起的 IP 封堵。弹性防护峰值按实际防护量计费，每日结算。
- 转发业务带宽：非攻击状态下的正常业务流量转发到源站服务器的流量，建议根据正常业务流量特点选择带宽。
- 购买个数：设置需要购买的实例数量。
- 购买时长：设置需要购买的时长，将根据 IP 数量、保底防护峰值以及购买时长计算需要预付的费用。
- 自动续费：用户可自行勾选。开启自动续费后，在腾讯云账号余额充足情况下，服务到期后将按月自动续费，保障业务防护不中断。



3. 单击 **Subscribe now**，完成支付流程。

更多信息

- BGP 高防 IP 详细计费说明
- 计费相关常见问题

欠费说明

最近更新时间：2019-08-08 15:16:02

到期提醒

BGP 高防 IP 服务到期7天前内，系统会向您推送服务即将到期，并提醒您及时续费等相关信息，信息通过站内信、短信及邮件的方式通知到腾讯云账号创建者以及所有协作者。

欠费提醒

BGP 高防 IP 服务在到期当天及以后，系统会通过邮件/短信的方式向腾讯云账号的创建者以及所有协作者推送欠费隔离提醒信息。

续费说明

- BGP 高防 IP 服务在到期前7天内，系统会给腾讯云账号的创建者以及所有协作者发送续费提醒通知。
- 在账户余额充足的情况下，若用户已设置自动续费，系统在到期当日会自动续费，成功续费后冻结费用，下一次月1号再结算上月费用。

快速入门
接入非网站业务

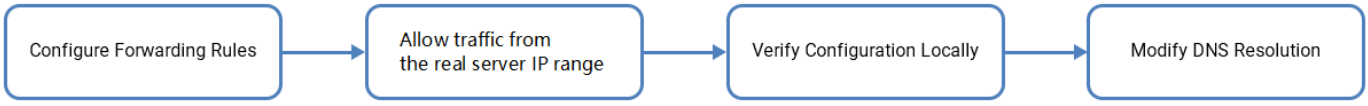
最近更新时间：2021-11-17 10:37:52

本文档介绍了非网站类业务用户如何将业务接入 DDoS 高防 IP 实例并验证转发配置。

前提条件

- 在添加转发规则前，您需要成功 购买 DDoS 高防 IP 实例。
- 在修改业务域名 DNS 信息前，您需要成功购买域名解析产品。

操作流程



操作步骤

配置转发规则

1. 登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【接入配置】。

2. 在【非网站业务】页签，查找并选择目标 DDoS 高防 IP 实例，添加转发规则。

   - 单个添加转发规则：

     a. 单击【新建】。
     b. 在添加转发规则页面中，根据实际需求配置如下参数，单击【确定】。

- 转发协议：目前支持 TCP 和 UDP。

- 转发端口：用于访问的高防 IP 端口，建议选择跟源站相同端口。
- 源站端口：用户业务站点的真实端口。
- 回源方式：支持 IP 回源和域名回源。
- 负载均衡方式：目前仅支持加权轮询。
- 源站IP+权重或源站域名。根据【回源方式】填写源站 IP+权重或源站域名。最多支持20个 IP+权重或域名。
  - 若勾选【IP 回源】，则填写源站服务器的 IP 地址+权重。一个域名对应多个源站 IP+权重时，可全部填入并用回车分隔多个 IP+权重，最多支持20个。如1.1.1.1 50。
  - 若勾选【域名回源】，则填写回源域名。一个域名对应多个源站域名时，可全部填入并用回车分隔多个域名，最多支持20个。
  - 批量添加转发规则：

    a. 选择【批量导入】>【导入转发规则】。
    b. 在批量导入页面的规则输入框中，粘贴需要导入的规则。

注意：

- 粘贴内容从左至右依次是转发协议、转发端口、源站端口、源站 IP、权重（或回源域名），中间由空格分隔。一行只能填写一条转发规则。
- 批量添加的转发规则条目数不允许超过当前配额。在配额限制内，单次最大导入条目为30条。

放行回源 IP 段

为了避免源站拦截 DDoS 高防 IP 的回源 IP 而影响业务，建议在源站的防火墙、Web 应用防火墙、IPS 入侵防护系统、流量管理等硬件设备上设置白名单策略，将源站的主机防火墙和其他任何安全类的软件（如安全狗等）的防护功能关闭或设置白名单策略，确保高防的回源 IP 不受源站安全策略的影响。
用户可以通过登录 DDoS 防护管理控制台，在左侧导航栏选择【DDoS 高防 IP】>【资产列表】，找到目标 DDoS 高防 IP 实例所在行，单击“ID/名称”，在弹出的“基础信息”页面中查看详细的高防 IP 回源地址段。

本地验证配置

转发配置完成后，DDoS 高防 IP 实例的高防 IP 将按照转发规则将相关端口的报文转发到源站的对应端口。
为了最大程度保证业务的稳定，建议在全面切换业务之前先进行本地测试。具体的验证方法如下：

- **使用 IP 访问的业务**

  对于直接通过 IP 进行交互的业务（如游戏业务），可通过 `telnet` 命令访问高防 IP 端口，查看是否能连通。

  若能在本地客户端直接填写服务器 IP，则直接填入高防 IP 进行测试，查看本地客户端是否可以正常连接。

  例如高防 IP 为10.1.1.1，转发端口为1234，源站 IP 为10.2.2.2，源站端口为1234。本地通过 `telnet` 命令访问10.1.1.1:1234，`telnet` 命令能连通则说明转发成功。

- **使用域名访问的业务**

  对于需要通过域名访问的业务，可通过以下的方法来验证配置是否生效：

  i. 修改本地 hosts 文件，使本地对于被防护站点的请求经过高防。

  以Windows操作系统为例：

  a. 打开本地计算机 C:\Windows\System32\drivers\etc 路径下的 hosts 文件，在文末添加如下内容：

  `<高防 IP 地址> <被防护网站的域名>`

  例如高防 IP 为10.1.1.1，域名为 www.qq.com，则添加：

  `10.1.1.1 www.qq.com`

  b. 保存 hosts 文件。

  ii. 在本地计算机对被防护的域名运行 `ping` 命令。

  当解析到的 IP 地址是 hosts 文件中绑定的高防 IP 地址时，说明转发成功。

  > 说明：
  > 若解析到的 IP 地址依然是源站地址，可尝试在 Windows 的命令提示符中运行 `ipconfig/flushdns` 命令刷新本地的 DNS 缓存。

  iii. 确认 hosts 绑定已经生效后，使用域名进行验证。

  若能正常访问则说明配置已经生效。

> 说明：
> 若使用正确的方法仍验证失败，请登录 DDoS 防护管理控制台 检查配置是否正确。排除配置错误和验证方法不正确后，若问题依然存在，请联系 腾讯云技术支持 。

修改业务域名 DNS 解析

使用 DDoS 高防 IP 防护前，需要将业务域名 DNS 的 A 记录更换为高防 IP 地址，使所有用户访问网站的流量都先经过高防 IP 再回到源站（即先将所有流量都牵引到高防 IP 再回到源站）。

说明：
不同域名解析产品的配置原理相同，具体配置步骤可能有细微差别，本文以使用腾讯云域名解析产品为例。

1. 登录 DNS 解析 DNSPod 控制台，在【域名解析列表】中，单击目标域名所在行的【解析】。
2. 在域名记录管理页签，单击【添加记录】，将 A 记录指向的 IP 地址修改为 DDoS 高防 IP，单击【保存】。

接入网站业务

最近更新时间：2021-01-25 12:18:17

本文档介绍了网站类业务用户如何将业务接入 BGP 高防 IP 实例并验证转发配置。

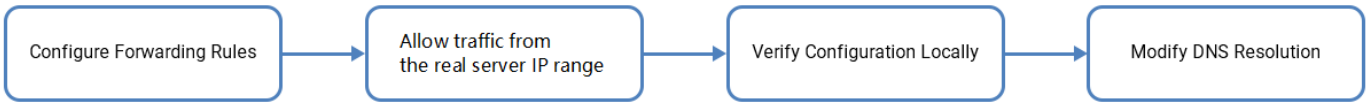
说明：

目前网站业务支持北京、上海、广州地区接入，暂不支持境外区域。

前提条件

- 在添加转发规则前，您需要成功 购买 BGP 高防 IP 实例。
- 在修改业务域名 DNS 信息前，您需要成功购买域名解析产品。

操作流程



操作步骤

配置转发规则">

配置转发规则

1. 登录 BGP 防护管理控制台，在左侧导航栏选择【BGP 高防 IP】>【接入配置】。
2. 在接入配置页面，单击【网站业务】，查找并选择目标 BGP 高防 IP 实例，添加转发规则。
   - 单个添加转发规则：
     a. 单击【新建】。
3. 在添加转发规则页面中，根据实际需求配置如下参数，单击【确定】。

参数说明：

- 域名：填写需要配置防护的网站域名。
- 协议：支持 HTTP 和 HTTPS，请根据实际业务需求勾选：

业务场景	相关操作
只包含 HTTP 协议的网站	勾选【HTTP】。
只包含 HTTPS 协议的网站	▪ 勾选【HTTPS】。 ▪ 证书来源：默认选择腾讯云托管证书。 ▪ 证书：选择对应的 SSL 证书名称。

- 回源方式：支持 IP 回源和域名回源。
- 根据【回源方式】填写源站 IP 或源站域名：

  - 若勾选【IP 回源】，则填写源站服务器的 IP （或 IP + 端口）。一个网站域名对应多个源站 IP （或 IP + 端口）时，可全部填入并用回车分隔多个 IP（或 IP + 端口），最多支持16个 IP（或 IP + 端口）。
  - 若勾选【域名回源】，则填写回源域名（CNAME）或域名（CNAME）+端口。一个网站域名对应多个源站域名（CNAME）或域名（CNAME）+端口时，可全部填入并用回车分隔多个域名（CNAME）或域名（CNAME）+端口，最多支持16个域名（CNAME）或域名（CNAME）+端口。

  ▪ 批量添加转发规则：

  a. 选择【批量导入】>【导入转发规则】。

  b. 在批量导入页面的规则输入框中，粘贴需要导入的规则

> **⚠ 注意：**
>
> ▪ 粘贴内容从左至右依次是域名、协议、源站 IP（暂不支持源站域名）、源站端口。源站 IP 与源站端口之间以英文":"分隔，其它的中间由空格分隔。一行只能填写一条转发规则。
>
> ▪ 批量添加的转发规则条目数不允许超过当前配额。

放行回源-IP-段">

放行回源 IP 段

为了避免源站拦截 BGP 高防 IP 的回源 IP 而影响业务，建议在源站的防火墙、Web 应用防火墙、IPS 入侵防护系统、流量管理等硬件设备上设置白名单策略，将源站的主机防火墙和其他任何安全类的软件（如安全狗等）的防护功能关闭或设置白名单策略，确保高防的回源 IP 不受源站安全策略的影响。

用户可以通过登录 BGP 防护管理控制台，在左侧导航栏选择【BGP 高防 IP】>【资产列表】，找到目标 BGP 高防 IP 实例所在行，单击"ID/名称"，在弹出的"基础信息"页面中查看详细的高防 IP 回源地址段。

本地验证配置">

本地验证配置

转发配置完成后，BGP 高防 IP 实例的高防 IP 将按照转发规则将相关端口的报文转发到源站的对应端口。
为了最大程度保证业务的稳定，建议在全面切换业务之前先进行本地测试。具体的验证方法如下：

1. 修改本地 hosts 文件，使本地对于被防护站点的请求经过高防。
   以Windows操作系统为例：
   i. 打开本地计算机 C:\Windows\System32\drivers\etc 路径下的 hosts 文件，在文末添加如下内容：
   `<高防 IP 地址> <被防护网站的域名>`
   例如高防 IP 为10.1.1.1，域名为 www.qq.com ，则添加：
   `10.1.1.1 www.qq.com`
   ii. 保存 hosts 文件。
2. 在本地计算机对被防护的域名运行 `ping` 命令。
   当解析到的 IP 地址是 hosts 文件中绑定的高防 IP 地址时，说明转发成功。

> **说明：**
> 若解析到的 IP 地址依然是源站地址，可尝试在 Windows 的命令提示符中运行 `ipconfig/flushdns` 命令刷新本地的 DNS 缓存。

3. 确认 hosts 绑定已经生效后，使用域名进行验证。
   若能正常访问则说明配置已经生效。

> **说明：**
> 若使用正确的方法仍验证失败，请登录 BGP 防护管理控制台 检查配置是否正确。排除配置错误和验证方法不正确后，若问题依然存在，请联系 腾讯云技术支持 。

修改业务域名-DNS-解析">

修改业务域名 DNS 解析

使用 BGP 高防 IP 防护前，需要将业务域名 DNS 的 A 记录更换为高防 IP 地址，使所有用户访问网站的流量都先经过高防 IP 再回到源站（即先将所有流量都牵引到高防 IP 再回到源站）。

> **说明：**
> 不同域名解析产品的配置原理相同，具体配置步骤可能有细微差别，本文以使用腾讯云域名解析产品为例。

1. 登录 DNS 解析 DNSPod 控制台，在【域名解析列表】中，单击目标域名所在行的【解析】。
2. 在域名记录管理页签，单击【添加记录】，将 A 记录指向的 IP 地址修改为 BGP 高防 IP，单击【保存】。

操作指南

操作总览

最近更新时间：2020-04-21 17:38:10

您在使用 DDoS 高防 IP 时，可能碰到诸如配置 DDoS 高防 IP 实例、查看统计报表、查看操作日志以及设置安全事件通知等问题。本文将介绍使用 DDoS 高防 IP 的常用操作，供您参考。

实例管理

- 查看实例详情
- 设置资源名称
- 配置弹性防护
- 调整 DDoS 高防 IP 实例规格
- 解封防护 IP

防护配置

- 配置业务场景
- 配置清洗阈值与防护等级
- 管理 DDoS 高级防护策略
- 配置 CC 防护等级
- 管理 CC 防护策略
- 配置健康检查
- 配置会话保持

统计报表

查看统计报表

操作日志

查看操作日志

安全事件通知

设置安全事件通知

使用限制

最近更新时间：2020-03-23 16:00:05

防护对象建议

建议使用 DDoS 高防 IP 为腾讯云内外的业务 IP 或域名提供防护，支持对网站（七层）业务和非网站（四层）业务进行防护。

> 目前网站（七层）业务暂不支持境外区域接入，仅非网站（四层）支持境外区域接入。

转发能力限制

1个 DDoS 高防 IP 实例默认支持60条转发规则，最高可扩展至300条，非网站（四层）协议下每条规则支持20个源站 IP/域名，网站（七层）协议下则支持16个源站 IP/域名。

黑白名单配置限制

- DDoS 黑白 IP 名单之和最多支持添加100个 IP 地址。
- HTTP CC/HTTPS CC 黑白 IP 名单分别最多支持添加50个 IP 地址。
- HTTP CC/HTTPS CC URL 白名单最多支持添加50个 URL。

地域限制

目前已开放 DDoS 高防 IP 的地域包括:

- 中国内地（大陆）区域：华南地区（广州）、华东地区（上海）和华北地区（北京）。
- 境外区域：中国港澳台地区（香港、台湾）、亚太地区（新加坡、首尔、曼谷、印度、日本）、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（法兰克福）和欧洲地区（莫斯科）。

DDoS 高防 IP 在不同地域提供的高防能力请参考如下表格：

地区	保底防护	弹性防护	最大防护能力
广州	20Gbps - 50Gbps	30Gbps - 100Gbps	100Gbps

地区	保底防护	弹性防护	最大防护能力
北京	20Gbps - 50Gbps	30Gbps - 100Gbps	100Gbps
上海	20Gbps - 100Gbps	30Gbps - 300Gbps	300Gbps
境外区域	10Gbps - 100Gbps	30Gbps - 400Gbps	400Gbps

防护配置
配置业务场景

最近更新时间：2020-04-21 17:38:10

应用场景

DDoS 高防 IP 支持自定义 DDoS 高级防护策略，用户可以根据业务特点或攻击行为针对性地设置防护策略。通常每个 DDoS 高防 IP 实例最多绑定一个 DDoS 高级防护策略。当用户的账号下拥有多个高防 IP 实例时，最多拥有5个 DDoS 高级防护策略可供选择。
为满足实际业务需要或应对不断变化的攻击手法，用户可能需要不断优化策略配置。为简化 DDoS 精细化防护管理，DDoS 高防 IP 提供业务场景设置功能，通过创建业务应用场景，后台收集、识别并自动生成高级防护策略，实现灵活的配置或维护策略。

创建业务场景

- **方法一**：
  若用户所购 DDoS 高防 IP 实例未配置业务场景，登录 DDoS 防护管理控制台，在左侧导航中选择【DDoS 高防 IP】>【防护配置】，会弹出如下图所示提示信息，单击【去创建】，进行业务场景创建。

> 最多支持创建5个业务场景。

- **方法二**：

1. 登录 DDoS 防护管理控制台，在左侧导航中选择【DDoS 高防 IP】>【防护配置】，在配置页面中，选择【DDoS 高级防护策略】>【创建业务场景】。

2. 在创建业务场景页面，根据实际业务特点，输入以下参数，单击【确定】，完成1个业务场景的设置。
   - **业务名称：**必填项，输入业务名称，长度为1 - 32个字符，不限制字符类型。
   - **平台开发：**勾选平台开发对应的类型。可供选择的有 PC 客户端、移动端、电视端和主机。
   - **细分品类：**选择业务所属类型。可供选择的有游戏、应用、网站或其他类型。
   - **基础信息：**
     - **是否有海外客户？**
       勾选【是】、【否】或【暂无法确认】。对应生成策略的配置项为关闭或开启【拒绝海外流量】。

- **是否会主动对外发起 TCP 请求？**
  勾选【是】、【否】或【暂无法确认】。选择【是】时，需要填写主动对外发起 TCP 请求的端口。存在多个请求业务端口时，全部填入并用英文“,”分隔。
- **是否会主动向外发起 UDP 业务请求（如 DNS 请求，NTP 请求等）？**
  勾选【是】、【否】或【暂无法确认】。选择【是】时，需要填写主动对外发起 UDP 业务请求的端口。存在多个请求业务端口时，全部填入并用英文“,”分隔。

- **其他信息：**（单击【展开+】即可对参数进行选择）
  - **UDP 载荷是否有固定特征？**
    勾选【是】或【否】。默认【否】，当选择【是】时，需要填写 UDP 载荷特征内容。
  - **TCP 载荷是否存在固定特征？**
    勾选【是】或【否】。默认【否】，当选择【是】时，需要填写 TCP 载荷特征内容。
  - **是否存在 Web API 业务？（使用英文“,”分隔）**
    勾选【是】或【否】。默认【否】，当选择【是】时，需要填写 API 业务 URL。存在多个 API 业务 URL 时，全部填入并用英文“,”分隔。

3. 后台对用户创建的业务场景进行分析后，自动生成1条以“业务场景名称_ policy_序号”（如“test_policy_1”）命名的高级防护策略，用户再根据实际特殊业务防护需求，自主配置或调整该条防护策略。

> - 在用户**只拥有一个 DDoS 高防 IP 实例（资源）**情况下，若**只创建一个业务场景**，则**自动将对应生成的高级防护策略绑定到当前实例（资源）中**。
> - **当对业务场景信息修改后，对应生成的高级防护策略会自动同步相关配置项信息。**若对该条高级防护策略进行调整，则不会同步到对应的业务场景信息。
> - 当以“业务场景名称 _ policy_序号”的高级防护策略绑定了一个或多个实例（资源）时，若对其中一个实例（资源）的转发规则参数（如下列参数）进行修改后，**则对应高级防护策略中对应的配置项信息会自动同步**。
>   - （四层）非网站业务：TCP/UDP 协议，转发端口范围。
>   - （七层）网站业务：HTTP/HTTPS 协议，转发端口默认80/443。

修改和删除业务场景

1. 登录 DDoS 防护管理控制台，在左侧导航中选择【DDoS 高防 IP】>【防护配置】。
2. 单击【DDoS 高级防护策略】，找到目的业务场景，单击【配置】或【删除】，进行修改或者删除。

> 当对目的业务场景进行删除操作，则对应的高级防护策略也将删除。

若想了解更多信息，请参见 管理 DDoS 高级防护策略。

配置清洗阈值与防护等级

最近更新时间：2020-02-14 18:32:58

应用场景

DDoS 高防 IP 服务提供防护策略调整功能，针对 DDoS 攻击提供三种防护等级供您选择，各个防护等级的具体防护操作如下：

> 如果业务需要使用 UDP，建议联系 腾讯云技术支持 进行策略定制，以免严格模式影响业务。

防护等级	防护操作	描述
宽松	• 过滤明确攻击特征的 SYN、ACK 数据包。 • 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 • 过滤具有明确攻击特征的 UDP 数据包。	清洗策略相对宽松，仅对具有明确攻击特征的攻击包进行防护。 建议在怀疑有误杀时启用，遇到复杂攻击时可能会有攻击透传。
正常	• 过滤明确攻击特征的 SYN、ACK 数据包。 • 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 • 过滤具有明确攻击特征的 UDP 数据包。 • 过滤常见基于 UDP 的攻击数据包。 • 对部分访问源 IP 进行主动验证。	清洗策略适配绝大多数业务，可有效防护常见攻击。 默认为正常模式。
严格	• 过滤明确攻击特征的 SYN、ACK 数据包。 • 过滤不符合协议规范的 TCP、UDP、ICMP 数据包。 • 过滤具有明确攻击特征的 UDP 数据包。 • 过滤常见基于 UDP 的攻击数据包。 • 对部分访问源 IP 进行主动验证。	清洗策略相对严格，建议在正常模式出现攻击透传时使用。

	• 过滤 ICMP 攻击包。 • 过滤常见的 UDP 攻击数据包。 • UDP 数据包严格检查。	

默认情况下，您所购买的 DDoS 高防 IP 实例采用正常防护等级，您可以根据实际业务情况自由调整 DDoS 防护等级。同时，您还可以自定义设置清洗阈值，当攻击流量超过设置的阈值时，将启动清洗策略。

配置示例

下面以配置华南地区（广州）的实例“bgpip-000002ai”为例，进行配置说明：

1. 登录 DDoS 防护管理控制台，在左侧导航栏选择【DDoS 高防IP】>【资产列表】，在地区选择框中，单击【华南地区（广州）】。
2. 在下方实例列表中，找到目标高防 IP 实例 ID 为“bgpip-000002ai”的高防 IP 实例，在右侧操作项中，单击【防护配置】，进行配置。
3. 在弹出的 DDoS 防护配置的页面中，开启【防护状态】，进行清洗阈值、防护等级的设置。

> 仅当【防护状态】为  状态时，配置项才可见。若手动将防护状态关闭，则配置项隐藏且配置不生效。重新开启后，配置项可见且保持原有的配置数据。

配置参数说明：

- 防护状态

默认开启，您可根据实际业务需求开启或关闭防护。关闭防护时，可进行关闭时长的设置，目前只能临时关闭防护1 - 6小时，超过所设置的时长或当攻击流量超过100wpps或2Gbps时，DDoS 高防包将自动开启防护。

- 清洗阈值

- 清洗阈值是高防产品启动清洗动作的阈值。当流量小于阈值时，即使检测到攻击也不会进行清洗操作。

- 默认在开启“防护状态”的情况下，业务刚接入的 DDoS 高防IP实例的清洗阈值采用默认值，并随着接入业务流量的变化规律，系统自动学习形成一个基线值。您可以根据实际业务情况自由设置清洗阈值。

> 若明确该清洗阈值，可进行自定义设置。若无法明确该清洗阈值，DDoS 防护系统将根据 AI 算法自动学习并生成一套专属的默认阈值。
>
> **- 防护等级**
>
> 默认在开启“防护状态”的情况下，业务刚接入的 DDoS 高防 IP 实例采用正常防护等级，您可以根据实际业务防护需求自由调整 DDoS 防护等级。
>
> **- 其他配置项**

- **业务场景**

您可以根据实际业务需求，从已创建的业务场景中选择一个匹配的业务场景，且支持修改。当选择某一个业务场景后，对应的“高级策略”会自动匹配该业务场景生成的策略。详情请参见 配置业务场景 ，进行业务场景创建。

- **高级策略**

您可根据业务防护特性，从已创建的高级策略中选择一个匹配的高级策略，且支持修改。详情请参见 管理 DDoS 高级防护策略 ，进行高级防护策略创建。

- **DDoS 攻击告警阈值**

DDoS 攻击告警阈值配置功能。若检测的指标超过您设定的阈值，将触发告警，并向您推送攻击告警信息。详情请参见 配置攻击告警阈值 ，进行告警指标设置。

- **TCP 业务 AI 增强防护**

针对四层 TCP 业务，DDoS 高防 IP 提供 TCP 业务 AI 增强防护功能。功能开启后，通过 AI 模型日常业务特征的自学习，能够自动识别业务流量与攻击流量，有效防护线上的四层 CC 攻击。

目前 TCP 业务 AI 增强防护功能仅对白名单开放。

管理 DDoS 高级防护策略

最近更新时间：2020-04-21 17:38:11

DDoS 高防 IP 提供面向 DDoS 攻击的高级防护策略功能，用户可针对自身业务防护需求对 DDoS 防护策略进行调整和优化。通过黑白名单、禁用协议、端口禁用（丢弃）或放行、报文特征过滤策略、连接耗尽防护、水印防护等功能，为业务提供针对性防护。

配置项简介

配置项	功能简介	生效时间
黑白名单	基于 IP 地址级别的防护。 • 白名单中的 IP，访问时将被直接放行，不经过任何防护策略过滤。 • 黑名单中的 IP，访问时将会被直接阻断。	当被防护的 IP 处于被攻击状态时生效。
禁用协议	可禁用业务不使用的协议。 当检测到攻击行为时，大禹高防集群会清洗掉该协议的流量。	当被防护的 IP 处于被攻击状态时生效。
端口禁用（丢弃）或放行	可禁用或放行来自指定类型端口的流量。	当检测到攻击行为时，大禹高防集群会清洗掉（或放行）该指定端口或指定端口范围的流量。
报文过滤特征	可以针对业务报文特征或攻击报文特征，将协议、端口范围、包长范围、是否检测载荷、偏移量、检查深度、是否包括特征字符串等条件进行组合，设定策略动作。 当检测到报文匹配到策略条件时，可以执行直接转发、丢弃、拉黑源 IP 或断开连接等操作。	当被防护的 IP 处于被攻击状态时生效。
限速	基于目的IP的防护，对访问协议进行限速控制。	当被防护的 IP 处于被攻击状态时生效。
拒绝海外流量	可拒绝来自中国（大陆地区及港澳台）以外的 TCP 流量请求。	当被防护的 IP 处于被攻击状态时生效。
连接耗尽防护	基于 IP 地址的防护，对于接入高防 IP 的非网站业务的 IP 的连接速度、包长度等参数进行限制，实现缓解小流量的连接型攻击的防护功能。	当被防护的 IP 处于被攻击状态时生效。

配置项	功能简介	生效时间
异常连接检测	当一个源 IP 接收到的一个 TCP 连接符合所配置的参数特征时，将判断为异常连接，同时当该源 IP 所接收到的异常连接数超过所设置的最大异常连接数时，会被加入黑名单一定时间，禁止被访问。	当被防护的 IP 处于被攻击状态时生效。
水印防护	支持 UDP 和 TCP 报文，在配置的端口范围内，其载荷进行水印检测和剥离。通过接入水印防护，高效全面防护 4 层 CC 攻击，如模拟业务报文攻击和重放攻击等。 • 业务端和腾讯云大禹安全防护系统端共享水印算法和密钥。 • 客户端每个发出的报文都嵌入了水印特征，而攻击报文却无水印特征。 • 大禹安全防护系统将甄别出攻击报文并将其丢弃。	当被防护的 IP 处于被攻击状态时生效。

添加新策略

> 高级安全防护策略功能具有一定专业性，建议有相关经验的用户在阅读以下操作指南后根据实际情况进行配置。

登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【防护配置】。在【DDoS 高级防护策略】页签，单击【添加新策略】。根据实际业务需求设置以下参数，单击【确定】。

- **策略名称**
  输入策略名称，长度为1 - 32个字符，不限制字符类型。

- **黑白名单**
  - 若需设置黑名单：单击【添加】，选择【黑名单】，填写需要拦截的 IP，存在多个 IP 时可全部填入并用回车分隔多个 IP，单击【确定】。
  - 若需设置白名单：单击【添加】，选择【白名单】，填写需要放行的 IP，存在多个 IP 时可全部填入并用回车分隔多个 IP，单击【确定】。

> 黑白 IP 名单之和最多支持添加100个 IP，批量添加的 IP 数不允许超过当前配额。

- **禁用协议**
  选择需要禁用的协议，支持可选的禁用协议有 ICMP、TCP、UDP 和其他协议，这里的其他协议指除了 ICMP、TCP、UDP 以外的协议。

- **端口号**
  选择协议和端口类型，然后填写对应的端口，根据您的业务选择丢弃或放行动作。若需要对连续的端口范围进行配置，您可以按照"起始端口-结束端口"进行配置。

- **报文过滤特征**
  支持将协议、端口范围、包长范围、是否检测载荷、偏移量、检查深度、是否包括特征字符串等条件进行组合，设定策略动作且即刻生效。

  - 偏移量：表示报文内容中开始匹配的特征的位置。
  - 检查深度：配合偏移量使用，表示从偏移量设定的位置开始向后匹配的报文内容长度。
  - 策略：
    - "丢弃报文"表示丢弃匹配该报文过滤特征的数据包。
    - "丢弃且拉黑源 IP"表示丢弃匹配该报文过滤特征的数据包并将源 IP 临时拉黑一段时间。
    - "丢弃且断开连接"表示丢弃匹配该报文过滤特征的数据包并断开 TCP 连接。
    - "丢弃，断开连接且拉黑源 IP"表示丢弃匹配该报文过滤特征的数据包，同时断开 TCP 连接并将源 IP 临时拉黑一段时间。
    - "直接转发"表示直接转发匹配该报文过滤特征的数据包。

- **限速**
  单击【添加】，选择需要限速的协议，设置限速阈值。支持限速的可选协议有 ICMP、TCP、UDP 和其他协议，这里的其他协议指除了 ICMP、TCP、UDP 以外的协议。

- **拒绝海外流量**
  勾选开启或关闭。DDoS 高防 IP 的防护引擎内置海外 IP 库，开启拒绝海外流量后将基于该 IP 库对来源进行判断并执行阻断。勾选【开启】时，需处于被攻击状态才生效。勾选【关闭】时即刻生效。

- **连接耗尽防护**
  - **空连接防护**：勾选开启或关闭。勾选【开启】时，需处于被攻击状态才生效。由于基于 TCP 代理原理实现，对于业务的首次访问体验可能会有影响。
  - **源新建连接限速**：勾选开启或关闭。勾选【开启】时，设置抑制速率（单位：个/秒），可填范围 0-∞。表示单一源IP每秒新建连接速率，超过限制的新建连接将被丢弃。

- **源并发连接限速**：勾选开启或关闭。勾选【开启】时，设置抑制数（单位：个），可填范围 0-∞。表示单一源IP并发连接数，超过限制的并发连接将被丢弃。
- **目的新建连接限速**：勾选开启或关闭。勾选【开启】时，设置抑制速率（单位：个/秒），可填范围 0-∞。表示目的IP每秒最大新建连接速率，超过限制的新建连接将被丢弃。由于防护设备为集群化部署，新建连接限速存在一定误差。
- **目的并发连接限速**：勾选开启或关闭。勾选【开启】时，设置抑制数（单位：个），可填范围 0-∞。表示目的IP 最大并发连接数，超过限制的并发连接将被丢弃。由于防护设备为集群化部署，并发连接限速存在一定误差。

- **异常连接检测**
  - **源IP最大异常连接数**：单击【开启】，填写源 IP 最大异常连接数量，可填范围 0-∞（单位：个）。表示当一个源 IP 符合异常连接行为识别的连接数，超过所指定阈值时，会被认为是异常攻击源，在一定时间内被限制访问。

    > 只有开启源 IP 最大异常连接数，以下参数才能进行配置。

  - **Syn 报文占比检测**：勾选开启或关闭。勾选【开启】时，设置 Syn 报文占比值，可填范围 0-100。表示当一个 TCP 连接中的 Syn 报文数与 Ack 报文数的比例超过所配置阈值时，会被识别为一个异常连接。
  - **Syn 报文数检测**：勾选开启或关闭。勾选【开启】时，设置最大报文数，可填范围 0-65535。表示当一个 TCP 连接中的 Syn 报文数超过所配置最大报文数时，会被识别为异常连接。
  - **连接超时检测**：勾选开启或关闭。勾选【开启】时，设置检测周期（单位：秒），可填范围 0-65535。表示一个 TCP 连接创建后在所设置的时间内没有任何报文传输则判断为异常连接。
  - **异常空连接检测**：勾选开启或关闭。表示一个 TCP 连接创建后没有任何带有载荷的报文传输则判断为异常连接。

- **水印防护**
  单击【开启】进行水印防护配置。填写指定的 TCP 协议防护端口和 UDP 协议防护端口，单击【确定】水印防护功能即刻开启。添加 DDoS 高级防护策略后，自动产生一条密钥信息，需要完成线下客户端接入水印配置。

- **TCP 协议防护端口、UDP 协议防护端口**
  TCP/UDP 防护端口最多可以配置5个端口段；不同端口段不可以互相重合；起止端口号相同则认为是一个端口；TCP 或 UDP协议端口段中需要至少配置一条。

  > 只有在配置 UDP 协议端口段时，才可进行 UDP 水印剥离，同时可以指定水印标签在 UDP 报文中的偏移量。

- **UDP 水印剥离**
  勾选 【自动剥离 UDP 报文水印】。数据报文经过大禹高防系统后，自动剥离 UDP 报文中的水印，再前传到源站。

  > 若不需要大禹安全防护系统剥离 UDP 协议水印，则客户端仍需要做剥离水印的改造。

- **偏移量**
  指定水印标签在 UDP 报文中的偏移量，默认为0，可填范围 0-99。偏移量只有在 UDP 水印剥离开启后才起作用。

绑定与解绑资源

登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【防护配置】。在【DDoS 高级防护策略】页签，单击目标策略所在行的【绑定资源】。

- 绑定资源：在弹出的【绑定资源】对话框中，根据实际业务需求勾选一个或多个资源，单击【确定】。
- 解绑资源：在弹出的【绑定资源】对话框中，根据实际业务需求单击【已选择】区域中已选资源右侧的，单击【确定】。

客户端接入水印

登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【防护配置】。在【DDoS 高级防护策略】页签，单击目标策略所在行的【水印客户端文件下载】，线下完成客户端的接入。

添加、删除或停用/启用水印密钥

登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【防护配置】。在【DDoS 高级防护策略】页签，单击目标策略所在行的【水印密钥配置】。

- **添加密钥**：在弹出的【密钥信息】对话框中，单击【添加密钥】即刻生成新密钥。
- **停用/启用密钥**：支持对密钥进行停用或启用操作。在弹出的【密钥信息】对话框中，单击目的密钥所在行的【停用】；如需重新开启则单击【启用】即可。
- **删除密钥**：只能对已停用的密钥进行删除。在弹出的【密钥信息】对话框中，单击目的密钥所在行的【删除】即可。

最多可存在2个密钥，如果需要添加新密钥，请先删掉其中一个旧密钥；当仅有一个密钥生效时，不可将其停用或删除。

配置策略

登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【防护配置】。在【DDoS 高级防护策略】页签，单击目标策略所在行的【配置】。根据实际业务需求更新以下参数，单击【确定】保存修改。

当目的策略是以“业务场景名称_policy_序号”形式命名的，则不能对策略名称进行修改。

- 策略名称
- 黑白名单
- 禁用协议
- 端口号
- 报文过滤特征
- 拒绝海外流量
- 连接耗尽防护
- 异常连接检测
- 水印防护

删除策略

- 未绑定资源的策略可直接删除，已绑定资源的策略需要先将所有资源解绑再执行删除操作。
- 若已开启 UDP 水印剥离开关，则删除策略会同步关闭 UDP 水印剥离开关，请确认业务客户端和服务器已完成相应的配置或者变更后，再执行删除操作。
- 策略删除后不可恢复，请谨慎操作。
- **不能对根据用户创建的业务场景自动生成的高级防护策略进行删除操作。**

登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【防护配置】。在【DDoS 高级防护策略】页签，单击目标策略所在行的【删除】。在弹出的对话框中，单击【确定】。

配置 CC 防护等级

最近更新时间：2021-01-27 11:11:23

防护说明

为了提升防护效果，减少防护出现误拦截风险，DDoS 高防 IP 服务针对 CC 攻击设计了3种防护等级供用户选择，默认提供正常等级。

- **宽松等级**：当受防护网站无明显流量异常时，可以采用此等级。同时该等级对受防护网站的所有请求都进行较为宽松的人机识别算法校验，即针对每个访问者进行验证，只有通过认证后访问者才允许访问网站。由于此等级下的 CC 防护策略较为宽松，可能会存在少部分异常请求透传的风险。
- **正常等级**：此等级为默认的 CC 防护等级，当发现受防护网站遭受 CC 攻击时，建议采用此等级。 相对于宽松等级，正常等级的 CC 防护可以覆盖大部分攻击场景，能够防御大部分的 CC 攻击。同时，该等级会对受防护网站的所有请求，都进行人机识别算法校验，即针对每个访问者进行验证，只有通过认证后访问者才允许访问网站。
- **严格等级**：此等级下 CC 攻击防护策略较为严格，能防护更为复杂的 CC 攻击。同时，该等级会对所有访问请求实行严格的人机识别算法验证，即针对每个访问者都将进行验证，只有通过认证后才允许访问网站。由于此模式验证机制较为严格，部分正常请求存在被误拦截的风险。

> ⚠ **注意：**
>
> - 上述三种 CC 防护等级所采用的防护算法只适用于网页或 H5 页面类的站点。
> - 如果被访问网站的业务是 API 或原生 App 应用，由于该类业务一般无法正常响应算法验证，所以会存在很大的误拦截的风险。
> - 如果用户存在 API 业务或原生 App 类业务的 CC 防护需求，请 提交工单 进行防护策略定制。

操作步骤

默认情况下，用户的 DDoS 高防 IP 实例所防护的网站域名采用正常等级的 CC 防护策略，用户可以根据实际情况自由调整防护模式。

1. 登录 DDoS 防护控制台，在左侧导航栏中，选择【DDoS 高防 IP】>【防护配置】，在防护策略页面，单击【CC 防护】。
2. 在 CC 防护页面中，定位到页面下方 HTTP CC 防护和 HTTPS CC 防护区域，选择对应协议下需要开启 CC 防护的域名，设置 CC 防护等级。

> ⚠ **注意：**

- CC 防护等级策略仅对接入配置为网站业务（七层接入）的域名生效。
- 如果用户还未将需要配置的网站域名接入高防 IP 实例，请参考 接入网站业务 将域名添加至已购买的高防 IP 实例。

更多信息请参考 管理 CC 防护策略。

管理 CC 防护策略

最近更新时间：2020-02-14 18:45:40

DDoS 高防 IP 支持 HTTP/HTTPS CC 防护功能。当高防 IP 统计的 HTTP/HTTPS 请求量超过设定的【http/https 请求数阈值】时，将自动触发 HTTP/HTTPS CC 防护。
DDoS 高防 IP 提供设置访问控制策略功能。开启 HTTP/HTTPS CC 防护功能，用户可以使用常见 HTTP/HTTPS 报文的字段（如 host 参数、CGI 参数、Referer 和 User-Agent 等）设置匹配条件，对公网用户的访问请求进行管控，对命中条件的请求执行阻断、人机识别动作。用户也可以设置限速规则，对访问 IP 执行限速处理。
DDoS 高防 IP 还支持 URL 白名单、IP 白名单、IP 黑名单策略配置：

- 白名单中的 URL，其访问请求将无需执行 CC 攻击检测，直接被放行。
- 白名单中 IP，其 HTTP/HTTPS 访问请求将无需执行 CC 攻击检测，直接被放行。
- 黑名单中 IP，其 HTTP/HTTPS 访问请求将直接被拒绝。

开启CC防护

HTTP CC 防护

1. 登录 DDoS 防护管理控制台，在左侧导航中选择【DDoS 高防 IP】>【防护配置】，在防护配置页面下，单击【CC 防护】，选择目标实例。
2. 在【HTTP CC 防护】区域，单击【防护状态】右侧的  开启 HTTP CC 防护，单击【http 请求数阈值】右侧的下拉框选择合适的阈值即可。

> CC 防护状态默认关闭。防护状态开启后，才可设置 HTTP 请求数阈值。

HTTPS CC 防护

1. 登录 DDoS 防护管理控制台，在左侧导航中选择【DDoS 高防 IP】>【防护配置】，在防护配置页面下，单击【CC 防护】，选择目标实例。
2. 在【HTTPS CC】区域，选择防护域名，单击【防护状态】右侧的  开启 HTTPS CC 防护，单击【https 请求数阈值】右侧的下拉框选择合适的阈值。

> CC 防护状态默认关闭。防护状态开启后，才可设置 HTTPS 请求数阈值。

自定义 CC 防护策略

- **需要开启 HTTP/HTTPS CC 防护，才可设置自定义 CC 防护策略，最多可添加5条。**
- **仅在该高防 IP 正在被攻击状态时，自定义策略才会生效。**
- **匹配模式下**，每个自定义策略最多可以设置**4**个策略条件进行特征控制，且多个条件之间是“与”的关系，需要所有条件全部匹配策略才生效。
- **限速模式下**，每个自定义策略只允许设置**1**条策略条件。

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择【DDoS 高防 IP】>【防护配置】，进入防护配置页面，单击【CC 防护】，选择地域和线路，选择目的实例，单击【添加访问控制策略】。
2. 在【添加访问控制策略】弹出框，根据实际业务需求设置以下参数，单击【确定】即可。
   - 策略名称
     输入策略名称，长度为1 - 20字符，不限制字符类型。
   - 协议
     目前支持 HTTP、HTTPS 两种协议。
   - 防护域名
     只有勾选 HTTPS 协议，才需要选择对应的防护域名。可选择的防护域名范围，等于已完成配置的转发规则中，属于 HTTPS 协议的网站域名。
   - 模式
     - 匹配模式：匹配到 HTTP / HTTPS 对应字段头的请求，执行拦截或人机识别操作。
     - 限速模式：对源 IP 访问进行限速处理，**HTTPS 协议不支持选择限速模式**。
   - 策略
     - **当选择【匹配模式】时，协议是 HTTP**，支持从 HTTP 报文的 host 参数、CGI 参数、Referer 和 User-Agent 多个特征进行组合，组合逻辑包括包含、不包含和等于。最多可以设置4个策略条件进行特征控制。若**协议是 HTTPS 时**，支持从 HTTPS 报文的 CGI 参数、Referer 和 User-Agent 多个特征进行组合，组合逻辑包括包含、不包含和等于。最多可以设置3个策略条件进行特征控制，字段描述如下：

匹配字段	字段描述	适用的逻辑符
host	访问请求的域名。	包含、不包含、等于
CGI	访问请求的 URI 地址。	包含、不包含、等于

Referer	访问请求的来源网址，表示该访问请求是从哪个页面跳转产生的。	包含、不包含、等于
User-Agent	发起访问请求的客户端浏览器标识等相关信息。	包含、不包含、等于

- 当选择【限速模式】时，对每个源 IP 访问进行限速处理。只允许设置1个策略条件。

- 执行

  仅当选择【匹配模式】时，需要设置该参数。表示策略匹配后，需执行的处理动作，包括拦截和验证码。

设置黑白名单

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择【DDoS 高防 IP】>【防护配置】，进入防护配置也页面，单击【CC 防护】，选择地域和线路，选择目的实例。
2. 勾选页面右侧【HTTP】或【HTTPS】，选择【URL 白名单】、【IP 白名单】或【IP 黑名单】，进行黑白名单设置，支持添加、修改，也支持批量导入导出。

配置健康检查

最近更新时间：2020-04-21 17:38:11

操作场景

DDoS 高防 IP 通过健康检查帮助用户自动识别后端服务器的运行状况，自动隔离异常的服务器。以此降低了后端服务器异常对整体业务可用性的影响。

- **非网站业务（四层）健康检查**
  DDoS 高防 IP 非网站业务防护的健康检查机制，由高防集群节点向配置中指定的服务器端口发起访问请求，如果端口访问正常则视为后端服务器运行正常，否则视为后端服务器运行异常。
  在 TCP 协议下，探测端口能否连接。在 UDP 协议下，使用 ping 进行可达性检查。
- **网站业务（七层）健康检查**
  DDoS 高防 IP 网站业务防护的健康检查机制，由高防转发集群向后端服务器发送 HTTP 请求的方式来检查后端服务，高防系统根据 HTTP 返回状态码来判断服务是否正常。
  用户可以自定义设置响应代码所代表的状态。假定在某场景下，HTTP 返回值为 http_1xx、http_2xx、http_3xx、http_4xx 和 http_5xx，用户可以根据业务需要勾选 http_1xx 及 http_2xx 为服务正常状态，则返回 http_3xx 至 http_5xx 的值则代表异常状态。

> 配置四层或七层转发规则时，如果单条规则中仅配置1个源站 IP，健康检查功能将不开启，该功能适合多源站 IP 的情况下开启。

操作步骤

非网站业务健康检查配置

下面将为您介绍配置 DDoS 高防 IP 非网站业务防护的健康检查规则的详细步骤。

1. 登录 DDoS 防护控制台，在左侧导航栏中，选择【DDoS 高防 IP】>【接入配置】，进入管理页面。

2. 单击【非网站业务】，选择目的 DDoS 高防 IP 实例和相应规则，单击健康检查列下的【编辑】。

3. 在健康检查编辑页面，单击【显示高级选项】，设置配置项后，单击【确定】即可。

- 默认开启健康检查。
- 在配置健康检查时，建议使用默认值。
- 支持对健康检查配置信息批量导入导出。导入后，系统将根据导入的“转发协议、转发端口”与规则进行一一匹配，其中“转发端口”必须为已配置了规则的转发端口。

网站业务健康检查配置

下面将为您介绍配置 DDoS 高防 IP 网站业务防护的健康检查规则的详细步骤。

1. 登录 DDoS 防护控制台，在左侧导航栏中，选择【DDoS 高防 IP】>【接入配置】，进入管理页面。

2. 单击【网站业务】，选择目的 DDoS 高防 IP 实例和相应规则，单击健康检查列下的【编辑】。

3. 在健康检查编辑页面，单击 按钮开启健康检查功能，同时单击【显示高级选项】，进行配置项设置，确认无误后，单击【确定】即可。

- 默认关闭健康检查。
- 在配置健康检查时，建议使用默认值。
- 支持批量导入导出健康检查配置信息。导入后，系统将根据导入的“转发协议、业务域名”与规则进行一一匹配，其中“业务域名”必须为已配置了规则的业务域名。

配置项说明

四层健康检查

配置项	说明
响应超时	每次健康检查响应的最大超时时间。如果后端服务器在指定的时间内没有正确响应，则判定为健康检查失败。
检测间隔	进行健康检查的时间间隔。

配置项	说明
不健康阈值	在健康检查状态为成功时，连续 n 次（n 为填写的数值）收到健康检查失败状态，则识别为不健康，控制台显示异常。
健康阈值	在健康检查状态为失败时，连续 n 次（n 为填写的数值）收到健康检查成功状态，则识别为健康，控制台无显示。

七层健康检查

配置项	说明
检测间隔	进行健康检查的时间间隔，默认为15秒。
不健康阈值	在健康检查状态为成功时，连续 n 次（n 为填写的数值）收到健康检查失败状态，则识别为不健康，控制台显示异常。
健康阈值	在健康检查状态为失败时，连续 n 次（n 为填写的数值）收到健康检查成功状态，则识别为健康，控制台无显示。
HTTP 请求方式和检查路径 URL	默认使用 HEAD 方法，服务器仅返回响应消息报文头。使用 GET 方法，服务器返回完整的响应消息。对应后端服务器需要支持 HEAD 和 GET。 • 如果用来进行健康检查的页面并不是应用服务器的缺省首页，用户需要指定具体的检查路径。 • 如果对 HTTP HEAD 请求限定了 host 字段的参数，用户需要指定检查路径，即用于健康检查页面文件的 URI。
HTTP 状态码检测	判断健康检查是否正常的 HTTP 状态码。默认情况或不做任何选择时，该值为 http_1xx、http_2xx、http_3xx 和 http_4xx，如果 HTTP 返回状态码非默认状态值，则识别为不健康，支持修改。

配置会话保持

最近更新时间：2020-04-21 17:38:11

操作场景

DDoS 高防 IP 非网站业务防护提供基于 IP 地址的会话保持，支持将来自同一 IP 地址的请求转发到同一台后端服务器处理。
四层转发场景支持简单会话保持能力，会话保持时间可设为30 - 3600秒中的任意整数值。超过该时间阈值，会话中无新的请求则自动断开连接。

操作步骤

下面将为您介绍配置 DDoS 高防 IP 非网站业务防护的健康检查规则的详细步骤。

1. 登录 DDoS 防护控制台，在左侧目录中，单击【DDoS 高防 IP】>【接入配置】，进入管理页面。

2. 在【非网站业务】页签，选择目的 DDoS 高防 IP 实例和相应规则，单击其会话保持查列下的【编辑】。

3. 在【会话保持编辑】页面，单击按钮开启会话保持功能，设置保持时间后，单击【确定】即可。

- 默认关闭会话保持。
- 在设置保持时间时，建议使用默认值。
- 支持对会话保持配置信息批量导入导出。导入后，系统将根据导入的“转发协议、转发端口”与规则进行一一匹配，其中“转发端口”必须为已配置了规则的转发端口。

配置智能调度

最近更新时间：2019-12-05 19:09:20

应用场景

一般每个账号下可能拥有多个高防实例，且每个高防实例至少拥有一条高防线路，因此每个账号下可能会存在多条高防线路。当将业务添加至高防实例进行防护后，表示您已经为该业务配置一条高防线路作为防护线路。若您的业务配置存在多条高防线路作为防护线路，您需要考虑该业务流量的最佳调度方式，即如何将业务流量调度到最优的高防线路进行防护，保证业务访问速度和高可用性。
目前 DDoS 防护（大禹）服务提供优先级方式的 CNAME 智能调度功能，您可以根据实际需要，勾选高防实例并设置高防线路的优先级。

> 支持设置解析的高防实例有 BGP 高防包、BGP 高防 IP，其中 BGP 高防包包括独享包和共享包。

优先级调度方式

指针对所有的 DNS 请求均以优先级最高的高防线路进行响应，即所有访问流量被调度至当前优先级最高的高防线路。您可以编辑高防线路的优先级，默认优先级为100，优先级的值越小，则表示该高防线路优先级越高。具体调度规则如下：

- 如果业务配置的高防实例包含多条不同高防线路，且优先级相同时，则按照 DNS 请求的运营商来源进行响应。当其中某条高防线路遭遇封堵后，将按照 BGP > 电信 > 联通 > 移动 > 境外（包括中国香港、中国台湾）的线路顺序进行调度。
- 如果同一优先级的高防线路均遭遇封堵后，访问流量将自动调度到当前可用的优先级次高的高防线路。

> 若当前无次高优先级的高防线路可用，则无法进行自动调度，业务访问将会中断。

- 如果业务配置的高防实例，包含多条相同高防线路，且优先级相同时，则按负载均衡方式进行调度，将访问流量平均分发至这些相同运营商的高防线路上进行处理。

示例

假设您拥有高防实例：BGP 高防 IP 1.1.1.1和1.1.1.2、电信高防 IP 2.2.2.2、联通高防 IP 3.3.3.3，其中1.1.1.1、2.2.2.2和3.3.3.3的优先级都为1，1.1.1.2的优先级为2。正常情况下，所有流量被调度至当前优先级为1的一组高防线

路进行分发处理，因此来自联通的流量调度到3.3.3.3进行处理，来自电信的流量调度到 2.2.2.2进行处理，来自其他运营商的流量调度到1.1.1.1进行处理。当1.1.1.1进入封堵时，该 IP 下的访问流量将自动调度到2.2.2.2进行处理，当1.1.1.1和3.3.3.3都被封堵时，则原本调度至1.1.1.1和3.3.3.3的访问流量，都将分发至2.2.2.2进行处理，当该组高防线路全部进入封堵时，流量将被调度至1.1.1.2进行处理。

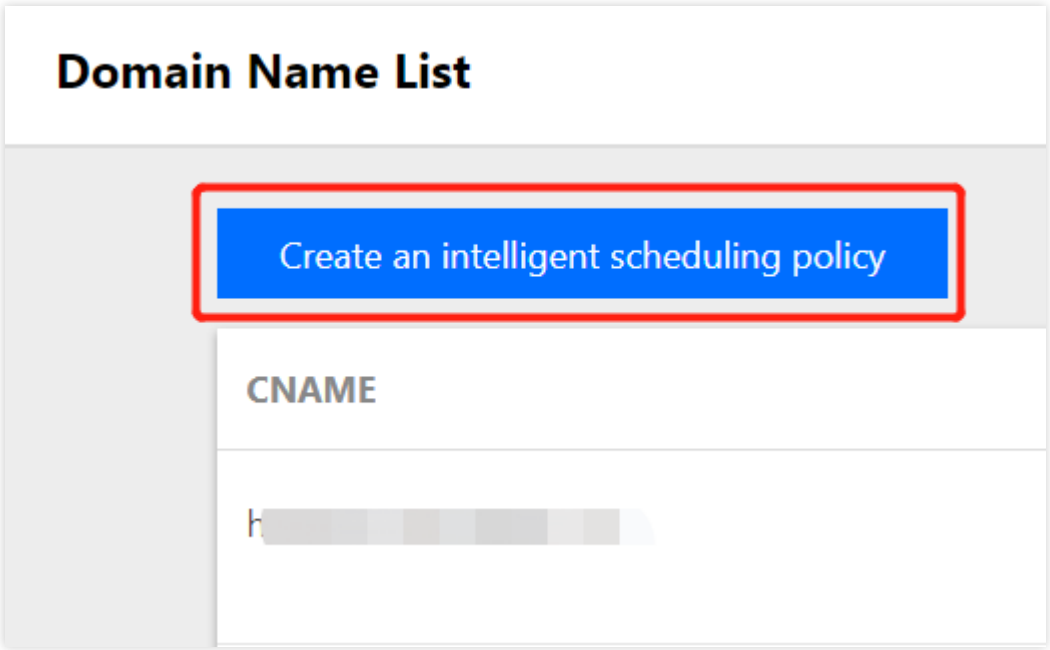
前提条件

- 在开启智能调度前，请将需要防护的业务接入高防实例进行防护。
  - 若您需要将防护的云上产品 IP 添加至已购买的高防包实例，请参见 BGP 高防包 快速入门 。
  - 若您需要将四层或七层业务添加至已购买的 BGP 高防 IP 实例，请参见 BGP 高防 IP 接入非网站业务。
- 在修改 DNS 解析前，您需要成功购买域名解析产品。

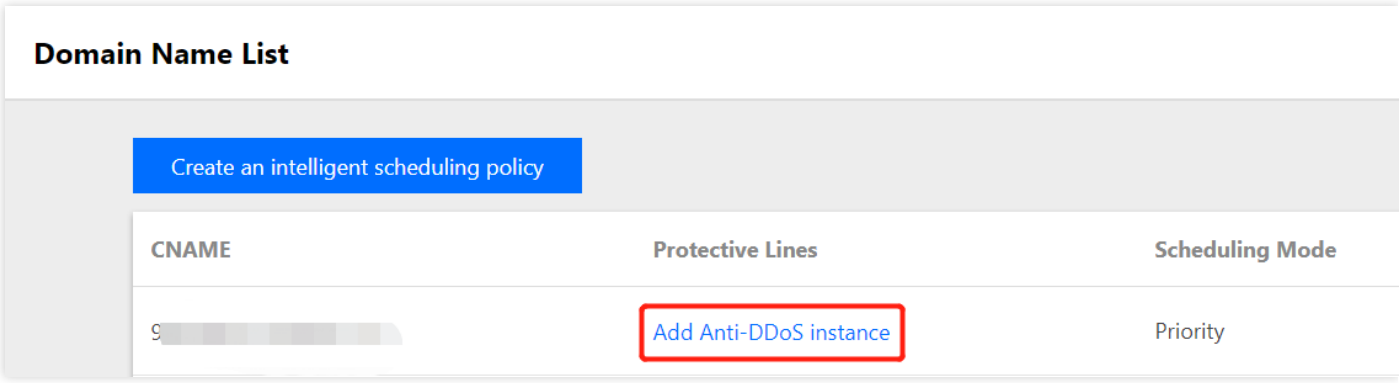
设置线路优先级

请参考以下步骤，按照设想的调度方案为您的高防线路设置优先级：

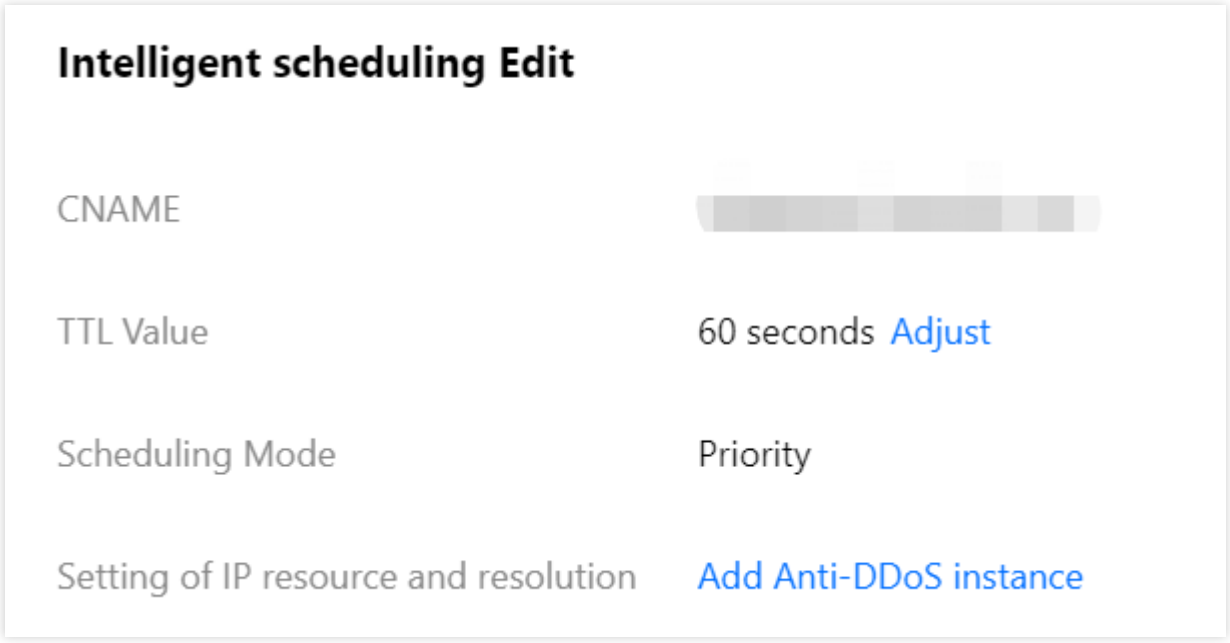
1. 登录Anti-DDoS控制台，在左侧导航栏选择【智能调度】>【域名列表】，进入域名列表页面，单击【创建智能调度】，系统自动生成一个 CNAME 记录。



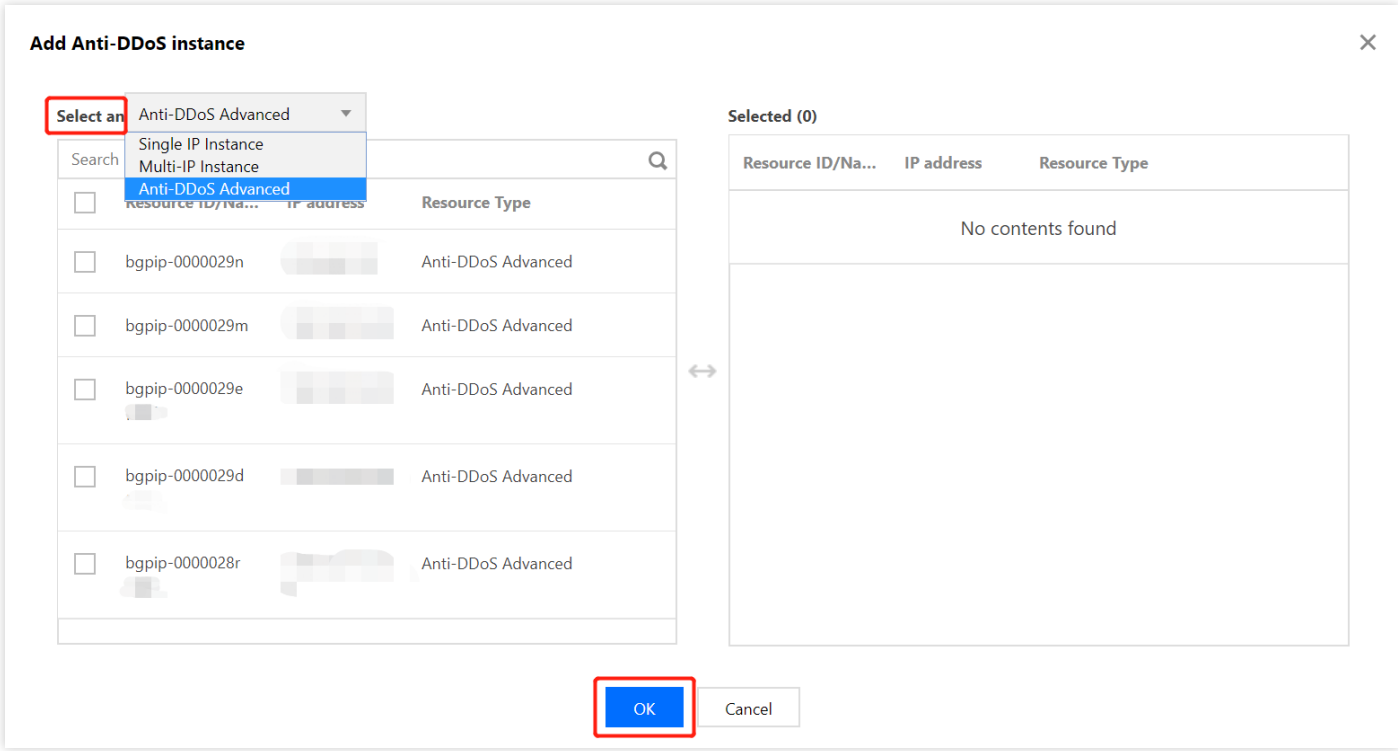
2. 找到该 CNAME 记录所在行，单击【添加高防实例】，进入智能调度编辑页面。



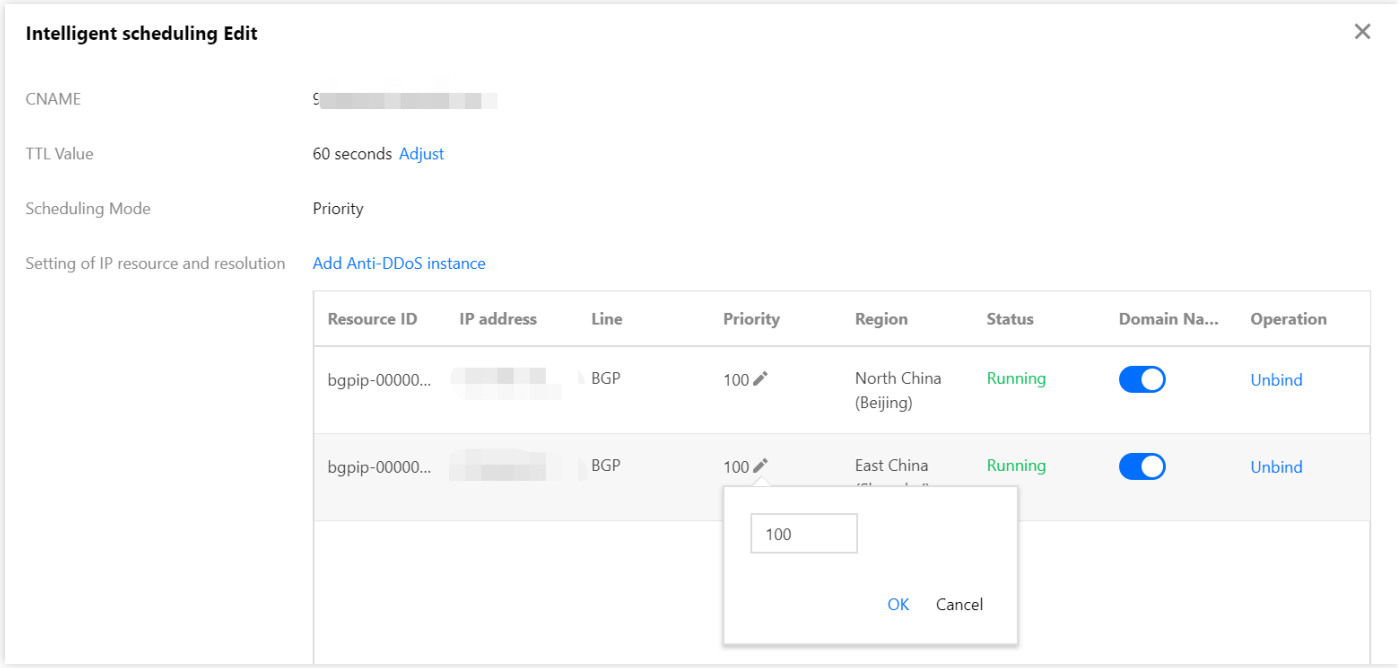
3. 在智能调度编辑页面中，TTL 值默认60秒，取值范围为1 - 3600（秒），调度方式为默认优先级。



4. 进入添加高防实例页面，勾选需要设置高防线路优先级的实例，可选高防实例包括独享包、共享包、BGP 高防 IP，单击【确定】。



5. 选择高防实例后，实例的高防线路默认开启域名解析，再为其设置优先级。



修改 DNS 解析

使用 CNAME 智能调度前，建议您将业务域名 DNS 的 CNAME 记录，修改为 DDoS 防护（大禹）智能调度系统自动生成的 CNAME，使所有用户访问业务网站的流量都牵引至高防系统。

配置攻击告警阈值

最近更新时间：2020-04-21 17:38:11

应用场景

当您所使用的 DDoS 高防 IP 遭受攻击、受攻击结束、被封堵以及解除封堵时，系统将以站内信、短信、邮件的方式向您推送攻击告警信息。为更加合理、准确地推送攻击告警信息，减少困扰，新增攻击告警阈值配置功能。若检测的指标超过您设定的阈值，将触发告警，并向您推送攻击告警信息。若发生正常业务操作（如同步数据等）引起流量突增，但被判定为攻击的情况，该功能可以较好地过滤这类情况，帮助您更加准确、清晰地掌握当前业务遭受的攻击状况。如何接收告警信息，请参见 设置安全事件通知。

配置 DDoS 攻击告警阈值

本配置示例可实现如下功能： DDoS 高防 IP 实例“bgpip-0000021y”遭受的攻击流量超过清洗阈值触发 DDoS 攻击清洗，当累计的清洗流量（值）超过1000Mbps时，将向指定用户群体发送 DDoS 攻击告警信息。

> 需要开启 DDoS 防护状态，才可设置攻击告警阈值。

1. 登录 DDoS 防护控制台，在左侧导航栏中，选择【DDoS 高防 IP】>【资产列表】，进入高防 IP 页面，找到高防 IP 实例“bgpip-0000021y”，单击实例所在行的操作项【防护配置】。
2. 进入 DDoS 防护配置页面，在 DDoS 攻击告警阈值右侧的下拉框，选择告警指标【清洗流量】，并设置阈值为1000Mbps。

> DDoS 攻击告警阈值默认【未设置】，支持可选的告警指标有【入流量带宽】和【清洗流量】。

配置 CC 攻击告警阈值

本配置示例可实现如下功能：DDoS 高防 IP 实例“bgpip-0000021y”触发 CC 防护后，当 HTTP CC 防护峰值超过2000QPS时，将向指定用户群体发送 CC 攻击告警信息。

需要开启 HTTP CC 防护状态，才可设置攻击告警阈值。

1. 登录 DDoS 防护控制台，在左侧导航栏中，选择【DDoS 高防 IP】>【防护配置】，进入防护配置页面，单击【CC 防护】。
2. 在 CC 防护页面中，定位到页面下方的“HTTP CC 防护”区域，在 “HTTP CC 攻击告警阈值”处设置阈值为2000QPS。

实例管理
查看实例详情

最近更新时间：2020-02-14 18:24:18

操作场景

您可以通过 DDoS 防护管理控制台 查看所购买的 DDoS 高防 IP 的基础信息（如实例保底防护峰值、运行状态）及实例的弹性防护配置。

操作步骤

本文将以查看广州地区高防 IP 实例“bgpip-0000020n”的详细信息为例进行详细说明。

1. 登录 DDoS 防护管理控制台，在左侧导航栏选择【DDoS 高防 IP】>【资产列表】，在地区选择框中，单击【华南地区（广州）】，并在下方列表中，找到并单击实例 ID 为“bgpip-0000020n”的高防 IP，查看实例信息。
2. 在弹出的页面查看如下信息：

参数说明：
- **基础信息**：
- **高防 IP 名称**

该 DDoS 高防 IP 实例的名称，用于辨识与管理 DDoS 高防 IP 实例。长度为1 - 20个字符，不限制字符类型。资源名称由用户根据实际业务需求自定义设置，具体操作请参考 设置资源名称。

- **IP**

该 DDoS 高防 IP 实例所提供的高防 IP，作为源站的前置 IP 对外提供服务。

- **所在区域**

购买 DDoS 高防 IP时选择的【地域】。

- **转发目标**

该 DDoS 高防 IP 实例所防护业务源站的位置。

- **DDoS 保底防护峰值**

该 DDoS 高防 IP 实例的保底防护带宽能力，即购买时选择的【保底防护峰值】。若未开启弹性防护，则保底防护峰值为高防服务实例的最高防护峰值。

- **CC 防护峰值**

该 DDoS 高防 IP 实例应对突发 CC 攻击的能力。

- **当前状态**

DDoS 高防 IP 实例当前的使用状态。状态包括运行中，清洗中以及封堵中等。

- **到期时间**

根据购买时选择的【购买时长】以及具体的提支付购买订单的具体时间计算所得，精确到秒级。腾讯云会在此时间前的第7天，通过站内信、短信及邮件的方式向腾讯云账号的创建者以及所有协作者推送服务即将到期并提醒及时续费的信息。

- **回源 IP 段**

根据当前 DDoS 高防 IP 的地域，显示该地域下的 DDoS 高防 IP 回源地址段信息，供用户查看了解。

- **弹性防护信息：**

- **当前状态**

表示弹性防护是否开启。若 购买 DDoS 高防 IP 实例时未开启弹性防护，用户可在使用过程中自助开启，具体操作请参见 配置弹性防护。

- **弹性峰值**

表示当前 DDoS 高防 IP 实例的最大弹性防护带宽能力，用户可以根据自身业务需求，随时 调整弹性防护峰值。

> 仅当开启弹性防护时，弹性峰值参数项才可见。

设置资源名称

最近更新时间：2020-02-14 18:25:48

当使用多个 DDoS 高防 IP 实例时，可通过设置【资源名称】快速辨识与管理实例。

方式一

登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【资产列表】，选择地域和线路，单击目标实例的【ID/名称】列的名称，输入名称即可。

> 名称长度为1 - 20个字符，不限制字符类型。

方式二

1. 登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【资产列表】，在左上角选择地域。
2. 在下方列表中，单击目标实例的“ID/名称”列的实例 ID，在弹出页面的【基础信息】区域，单击【编辑】，输入或修改名称，并单击【确定】即可。

> 名称长度为1 - 20个字符，不限制字符类型。

配置弹性防护

最近更新时间：2020-02-14 18:26:17

DDoS 高防 IP 实例启用弹性防护后，当攻击流量峰值超出保底防护峰值时，DDoS 高防 IP 会根据用户设置的弹性防护峰值继续进行防护。
若购买 DDoS 高防 IP 实例时，未开启弹性防护，用户可在使用过程中自助开启。当天未触发弹性防护，不产生额外费用。在触发弹性防护（攻击峰值超过保底防护峰值）时，取当天实际产生的最高攻击峰值所对应区间进行计费，账单次日生成。用户可根据实际业务情况实时更改 DDoS 高防 IP 实例的弹性防护峰值。

开启弹性防护

> 若购买 DDoS 高防 IP 实例时未开启弹性防护，用户可在使用过程中开启，并以历史最高攻击流量为参考，选择略高于历史最高峰值的弹性防护峰值，以便足够防御大流量攻击，避免超过防护峰值而引起的 IP 封堵。

1. 登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【资产列表】，在目标实例所在行，单击【开启弹性防护】。
2. 在【开启弹性防护】对话框中，选择需要的【弹性防护峰值】。
3. 单击【确定提交】。

更改弹性防护峰值

1. 登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【资产列表】，单击目的实例 ID，进入实例的基础信息界面。
2. 找到“弹性防护”部分，在“弹性峰值”右侧，单击【更改】。
3. 在【更改弹性防护】对话框中，选择合适的【弹性防护峰值】。

> - 弹性防护峰值支持调升调降，不同地域支持的防护能力不同，弹性防护峰值的具体取值范围请参考 产品概述。
> - 弹性防护峰值修改后立即生效。

4. 单击【确定提交】。

关闭弹性防护

关闭弹性防护后，最大防护峰值降为保底防护峰值，请确保是否满足实际需求再执行此操作。

1. 登录 DDoS 防护管理控制台，选择【DDoS 高防 IP】>【资产列表】，在目标实例所在行，单击【关闭弹性防护】。
2. 在【关闭弹性防护】对话框中，单击【确定提交】。

调整 DDoS 高防 IP 实例规格

最近更新时间：2020-04-21 17:38:10

操作场景

如果在使用 DDoS 高防 IP 过程中发现当前规格（如保底防护峰值、转发规则数或业务带宽等）已无法满足实际业务需求，您可以通过升级 DDoS 高防 IP 实例的规格来提升防护能力。
调整 DDoS 高防 IP 实例规格支持调高保底防护峰值，增加转发规则数（防护域名数或端口数）和调高业务带宽。

> 目前暂不支持降低已购买 DDoS 高防 IP 实例的规格。

升级 DDoS 高防 IP 实例规格，需要加收额外的费用。支付完成后，DDoS 高防 IP 实例规格升级即时生效。

操作步骤

1. 登录 DDoS 防护管理控制台。
2. 选择【DDoS 高防 IP】>【资产列表】。
3. 单击目标 DDoS 高防 IP 实例所在行的【升级】。
4. 根据实际需求设置【升级保底防护】、【升级业务带宽】以及【升级转发规则数】。
5. 单击【立即升级】，进入【核对信息】页面。
6. 确认无误后，根据实际情况选择是否使用代金券，单击【确认购买】。
7. 完成支付后，返回 DDoS 高防 IP 资产列表即可查看规格调整已即刻生效。

查看统计报表

最近更新时间：2022-05-09 16:42:05

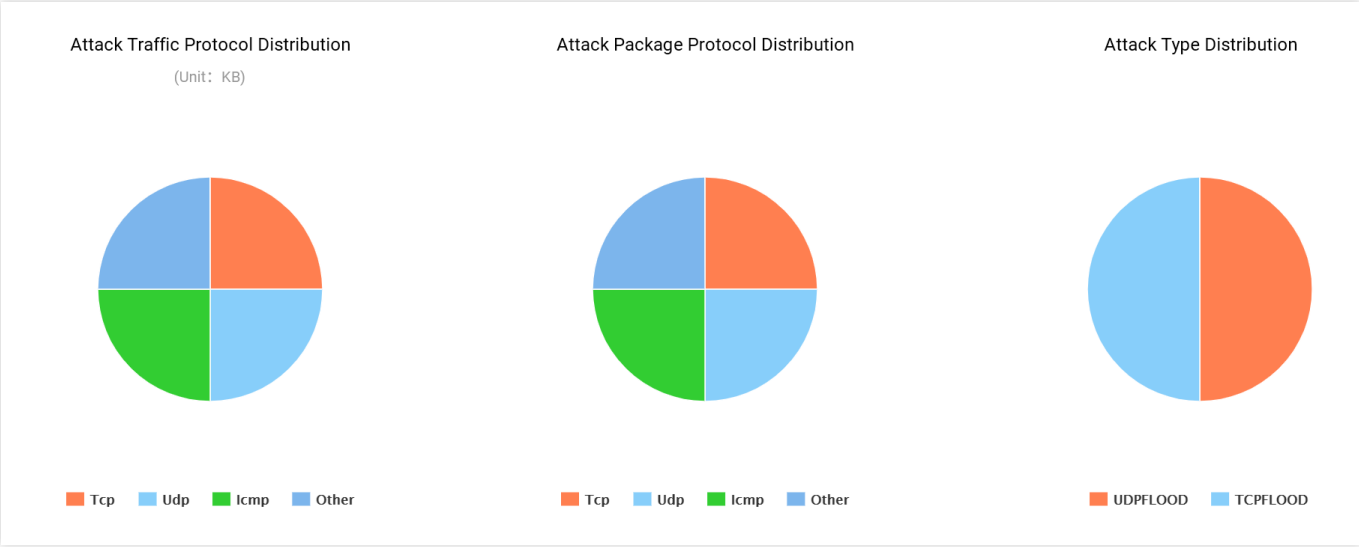
当用户收到 DDoS 攻击提醒信息或发现业务出现异常时，需要快速了解攻击情况，包括流量大小、当前防护效果等，在掌握足够信息后，才可以采取更有效的处理方式，第一时间保障业务正常。
DDoS 高防 IP 管理控制台的统计报表提供丰富的信息，可帮助用户快速了解当前业务或攻击情况。

查看 DDoS 攻击防护情况

1. 登录 DDoS 防护管理控制台。
2. 定位到【DDoS 高防 IP】>【统计报表】。
3. 在【DDoS 攻击防护】页签，设置查询时间范围，选择地域和线路，选择目的实例和高防 IP，查看是否存在攻击。

> 支持查询最多180天以内的攻击流量信息及 DDoS 攻击事件。

- 查看该时间范围内所选择的高防 IP 遭受的攻击情况，包括网络**攻击流量带宽 / 攻击包速率**趋势。当遭受攻击时，在流量趋势图中可以明显看出攻击流量的峰值。
- 通过攻击流量协议分布、攻击包协议分布和攻击类型分布，查看这三个数据维度下的攻击分布情况。
  - **攻击流量协议分布**：查看该时间范围内，所选择的高防 IP 遭受攻击事件中各协议总攻击流量的占比情况。
  - **攻击包协议分布**：查看该时间范围内，所选择的高防 IP 遭受攻击事件中各协议攻击包总数的占比情况。
  - **攻击类型分布**：查看该时间范围内，所选择的高防 IP 遭受的各攻击类型总次数占比情况。



- **攻击来源分布**：在【攻击来源分布】区域查看该时间范围内所遭受的 DDoS 攻击事件的攻击源在中国内地（大陆）、全球的分布情况，便于用户清晰了解攻击来源情况，为进一步防护措施提供基础依据。

- 在【DDoS 攻击记录】区域查看该时间范围内所遭受的 DDoS 攻击事件，了解每一次攻击事件的攻击（开始）时间、持续时间、攻击类型以及攻击状态。
  - 支持攻击包下载，供用户进行 DDoS 攻击分析及溯源支撑。
  - 单击【攻击详情】，了解 DDoS 攻击事件中的最大包速率、最大攻击流量带宽和总的清洗流量情况。
  - 单击【攻击源信息】，查看该时间范围内，所遭受攻击的攻击源 IP 地址、来源地区、产生的攻击流量及攻击包量大小等信息。

> 攻击源信息为抽样数据，即随机抓包统计的数据，在攻击结束后大约2小时才会显示数据。

查看 CC 攻击防护情况

1. 登录 DDoS 防护管理控制台。
2. 选择【DDoS 高防 IP】>【统计报表】。
3. 单击【CC 攻击防护】页签，设置查询时间范围，选择地域和线路，选择目的实例和高防 IP，查看是否存在 CC 攻击。

> 支持查询最多180天以内的攻击请求数信息及 CC 攻击事件。

   - 用户可以选择【今天】查看所选择的高防IP的攻击请求数趋势。通过观察总请求值是否远高于正常情况下的业务访问量（QPS），并查看攻击 QPS 是否有数值且数值超大。
   - 如果存在 CC 攻击，系统会记录下攻击的开始时间、结束时间、被攻击域名、被攻击 url、总请求峰值、攻击请求峰值和攻击源等信息。
     - **总请求峰值**：统计遭受攻击时，高防 IP 接收到的总请求流量峰值。
     - **攻击请求峰值**：统计遭受攻击时， 由高防系统阻断的请求次数峰值。

查看业务流量情况

1. 登录 DDoS 防护管理控制台。
2. 选择【DDoS 高防 IP】>【统计报表】。
3. 单击【业务】页签，设置查询时间范围，选择地域和线路，选择目的实例和高防 IP，查看所选择时间范围内的**入/出业务流量带宽趋势**、**入/出业务包速率的趋势**及**新建连接数或并发连接数的趋势**。同时，还可以查看该时间范围内的入/出方向的业务流量带宽峰值，及入/出方向的业务包速率峰值。

- **并发连接数**：系统在某个时间点存在的已建立的全连接数。
- **新建连接数**：系统在1秒内建立的 TCP 连接数。

> 支持查询最多180天以内的业务信息。

查看操作日志

最近更新时间：2020-04-21 17:38:11

操作场景

DDoS 高防 IP 支持查看近90天内重要操作的日志，如有需要，您可以登录 DDoS 防护管理控制台 查看。可查看的日志包含以下类别：

- 转发规则变更操作日志
- DDoS 高级防护策略变更操作日志
- 清洗阈值调整日志
- 防护等级变更日志
- CC 防护策略变更操作日志
- 弹性防护峰值调整日志
- 资源名称的修改日志

操作步骤

1. 登录 DDoS 防护管理控制台。
2. 选择【操作日志】，进入操作日志查询页面。
3. 设置时间范围，通过【产品类型】筛选【高防 IP】，查看对应的操作记录。

设置安全事件通知

最近更新时间：2020-02-14 09:39:49

操作场景

当您所使用的高防 IP 受到攻击、受攻击结束、IP 被封堵以及解除封堵时，将以站内信、短信或邮件的方式向您推送告警信息：

- 攻击开始时，您将会收到攻击开始提示。
- 攻击结束后15分钟，您将收到攻击结束提示。
- IP 封堵被封堵时，您将收到封堵提示。
- IP 解除封堵时，您将收到解除封堵提示。

您可以根据实际情况修改告警信息的接收人和接收方式。

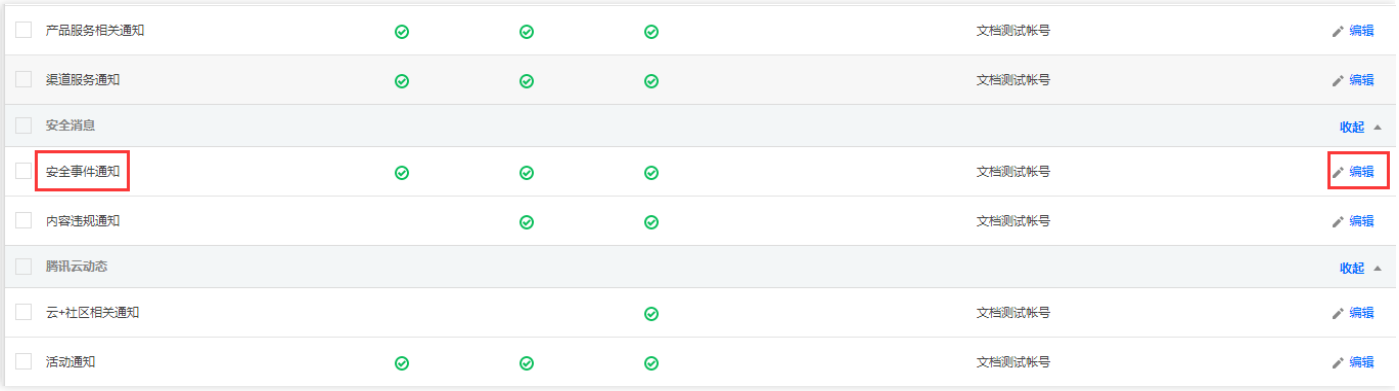
操作步骤

1. 登录您的腾讯云账号，进入 消息中心。

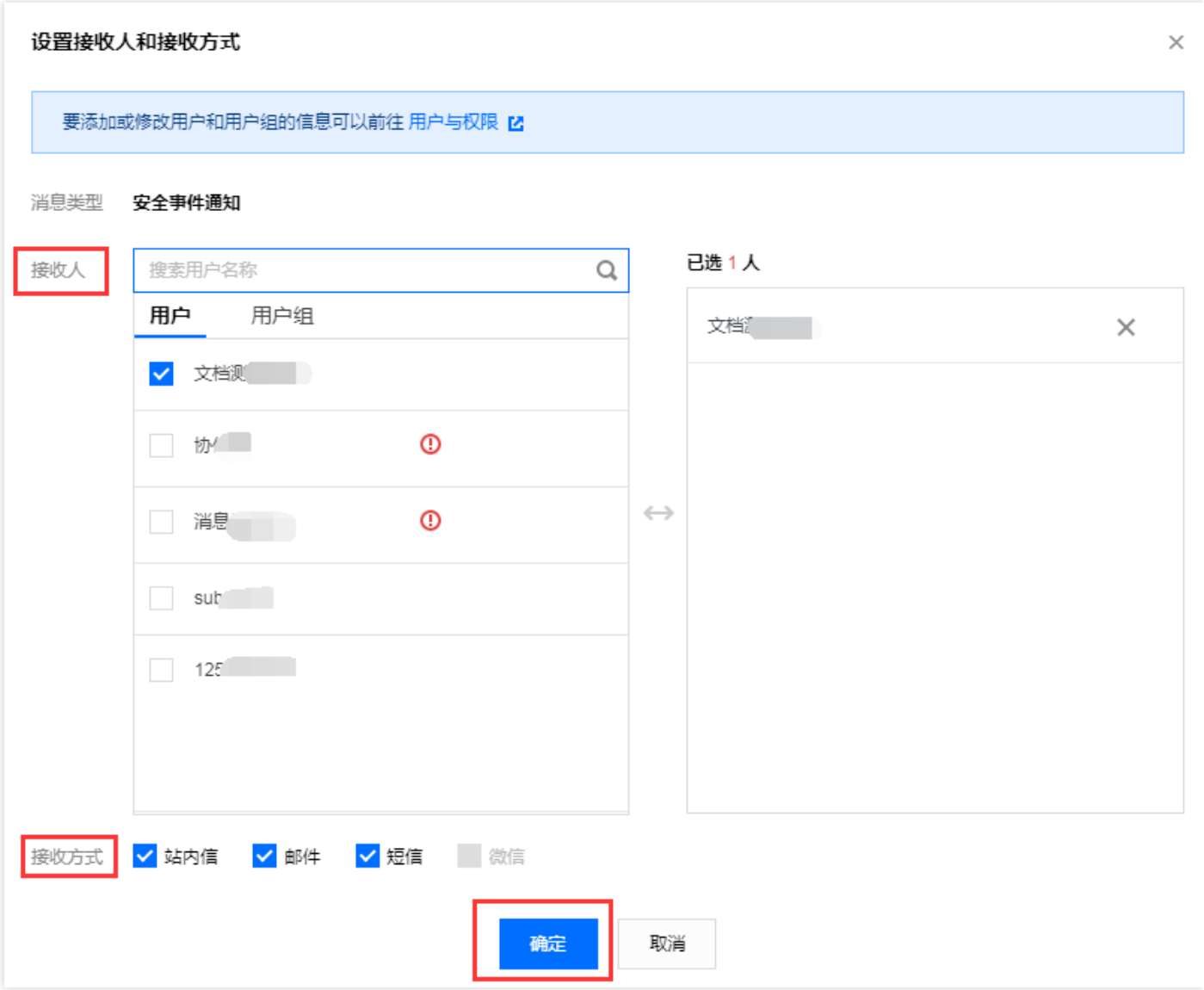
> 您也可以登录 控制台，单击右上角的  ，单击弹出页面底部的【进入消息中心】。

2. 单击左侧目录中的【消息订阅】，进入消息列表。

3. 在消息列表中，单击【安全事件通知】所在列的【编辑】，进入编辑页面。



4. 选择接收人和接收方式，单击【确定】。



最佳实践
平滑切换线上业务至 BGP 高防 IP

最近更新时间：2020-05-09 18:03:49

需求背景

已上线的业务可能存在较多的特定设置和限制条件，且业务中断影响较大。因此建议用户将已上线运行的业务切换到本产品之前，参考本节相关建议，采用合适的切换方式，规避可能存在的风险。

建议

以下建议是基于腾讯云过往线上业务切换而总结的相关经验，用户需结合自身实际业务情况进行完善和补充，确保将切换过程中的风险降至最低。

技术维度

- 通过本地修改 hosts 文件来替代直接修改 DNS A 记录，由测试人员本地进行业务测试，验证可用性，测试延时等相关指标。
- 若已使用智能域名解析产品，可基于部分运营商或部分地域进行 DNS A 记录修改，先小范围将流量牵引到高防 IP 灰度上线再逐步完成全部业务切换。
- 减小 DNS 的 TTL，一旦出现问题可尽快切回。
- 提前准备回退方案，一旦出现问题可根据回退方案有序操作。

业务维度

- 选取备份业务、非重要业务、非关键业务先进行迁移。
- 选择业务较少的时段进行迁移。

源站 IP 暴露的解决方法

最近更新时间：2020-04-03 14:35:45

由于部分攻击者会记录源站使用过的 IP，因此在使用 DDoS 高防 IP 后，如果还存在绕过高防直接攻击源站 IP 的情况，建议更换源站 IP。
如不想更换源站 IP 或已经更换过 IP但仍存在 IP 暴露情况，为防止出现攻击绕过高防直接攻击源站 IP 的情况，强烈参考下面方法以保护源站 IP：

- 不使用与旧源站 IP 相同或相近网段的 IP 作为新的源站 IP，避免攻击者对 C 段或相近网段进行猜测和扫描。
- 提前准备备份链路和备份 IP。
- 设置访问来源范围，避免攻击者的恶意扫描。
- 参考 与源站结合的防护调度方案，结合实际情况进行应用。

> 更换源站 IP 之前，请务必确认已消除所有可能暴露源站 IP 的因素。

在更换源站 IP 前可参考下列检查方法，对暴露源站 IP 的可能因素进行逐一排查，避免新更换的源站 IP 继续暴露。

检查方法

DNS 解析记录检查

检查该遭到攻击的旧源站 IP 上所有 DNS 解析记录，如子域名的解析记录、邮件服务器 MX（Mail Exchanger）记录以及 NS（Name Server）记录等，确保全部配置到高防 IP，避免部分解析记录直接解析成新更换的源站 IP。

信息泄露及命令执行类漏洞检查

- 检查网站或业务系统是否存在信息泄露的漏洞，如 phpinfo() 泄露、GitHub 信息泄露等。
- 检查网站或业务系统是否存在命令执行类漏洞。

木马、后门检查

检查源站服务器是否存在木马、后门等隐患。

获取客户端真实 IP

最近更新时间：2020-03-20 17:06:38

使用非网站业务转发规则

DDoS 高防 IP 使用非网站业务转发规则时，源站需使用 toa 模块获取客户端的真实 IP。
业务请求经过高防 IP 的 4 层转发后，业务服务器端接收到报文后，其看到的源 IP 地址是高防 IP 的出口 IP 地址。为了让服务器端能够获取到用户端实际的 IP 地址，可以使用如下 TOA 的方案。在业务服务的 Linux 服务器上，安装对应的 TOA 内核包，并重启服务器后。业务侧就可以获取到用户端实际的 IP 地址。

TOA 原理

高防转发后，数据包同时会做 SNAT 和 DNAT，数据包的源地址和目标地址均修改。
TCP 协议下，为了将客户端 IP 传给服务器，会将客户端的 IP，port 在转发时放入了自定义的 tcp option 字段。

```
#define TCPOPT_ADDR 200
#define TCPOLEN_ADDR 8 /* |opcode|size|ip+port| = 1 + 1 + 6 */

/*
*insert client ip in tcp option, now only support IPV4,
*must be 4 bytes alignment.
*/
struct ip_vs_tcpo_addr {
__u8 opcode;
__u8 opsize;
__u16 port;
__u32 addr;
};
```

Linux 内核在监听套接字收到三次握手的 ACK 包之后，会从 `SYN_REVC` 状态进入到 `TCP_ESTABLISHED` 状态。这时内核会调用 `tcp_v4_syn_recv_sock` 函数。Hook 函数 `tcp_v4_syn_recv_sock_toa` 首先调用原有的 `tcp_v4_syn_recv_sock` 函数，然后调用 `get_toa_data` 函数从 TCP OPTION 中提取出 TOA OPTION，并存储在 `sk_user_data` 字段中。

然后用 `inet_getname_toa hook inet_getname`，在获取源 IP 地址和端口时，首先调用原来的 `inet_getname`，然后判断 `sk_user_data` 是否为空，如果有数据从其中提取真实的 IP 和 port，替换 `inet_getname` 的返回。

客户端程序在用户态调用 getpeername，返回的 IP 和 port 即为客户端的原始 IP。

内核包安装步骤

Centos 6.x/7.x

1. 下载安装包：
   - Centos 6.x 下载
   - Centos 7.x 下载
2. 安装包文件。

```
rpm -hiv kernel-2.6.32-220.23.1.el6.toa.x86_64.rpm --force
```

3. 安装完成之后重启主机。

```
reboot
```

4. 执行命令检查 toa 模块是否加载成功。

```
lsmod | grep toa
```

5. 没有加载的话手工开启。

```
modprobe toa
```

6. 可用下面的命令开启自动加载 toa 模块。

```
echo "modprobe toa" >> /etc/rc.d/rc.local
```

Ubuntu 16.04

1. 下载安装包：
   - 内核包下载
   - 内核 header 包下载
2. 安装步骤：

```
dpkg -i linux-image-4.4.87.toa_1.0_amd64.deb
```

   Headers 包可不装，如需要做相关开发则安装。
3. 安装完成之后重启主机，然后 `lsmod | grep toa` 检查 toa 模块是否加载 没有加载的话 `modprobe toa` 开启。

   可用下面的命令开启加载 toa 模块：

```
echo "modprobe toa" >> /etc/rc.d/rc.local
```

Debian 8

1. 下载安装包：
   - 内核包下载

- 内核 header 包下载

2. 安装方法与 Ubuntu 相同。
   请根据业务服务器 Linux 操作系统的类型和版本下载对应的内核包，按如下步骤操作。如果没有和用户操作系统一致的内核包，用户还可以参考下文的 **TOA 源代码安装指引**。

TOA 源代码内核安装指引

源码安装

1. 下载打好 toa 补丁 的源码包，单击 toa 补丁即可下载安装包。
2. 解压。
3. 编辑 .config，将 `CONFIG_IPV6=M` 改成 `CONFIG_IPV6=y` 。
4. 如果需要加上一些自定义说明，可以编辑 Makefile。
5. make -jn (n 为线程数)。
6. `make modules_install` 。
7. `make install` 。
8. 修改 /boot/grub/menu.lst 将 default 改为新安装的内核（title 顺序从0开始）。
9. Reboot 重启后即为 toa 内核。
0. `lsmode | grep toa` 检查 toa 模块是否加载 没有加载的话 `modprobe toa` 开启。

内核包制作

您可自己制作 rpm 包，也可由我们提供。

1. 安装 kernel-2.6.32-220.23.1.el6.src.rpm。

```
rpm -hiv kernel-2.6.32-220.23.1.el6.src.rpm
```

2. 生成内核源码目录。

```
rpmbuild -bp ~/rpmbuild/SPECS/kernel.spec
```

3. 复制一份源码目录。

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/ cp -a linux-2.6.32-220.23.1.el
6.x86_64/ linux-2.6.32-220.23.1.el6.x86_64_new
```

4. 在复制出来的源码目录中打 toa 补丁。

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/linux-2.6.32-220.23.1.el6.x86_64
_new/
patch -p1 < /usr/local/src/linux-2.6.32-220.23.1.el6.x86_64.rs/toa-2.6.32-220.2
3.1.el6.patch
```

5. 编辑 .config 并拷贝到 SOURCE 目录。

```
sed -i 's/CONFIG_IPV6=m/CONFIG_IPV6=y/g' .config
echo -e '\n# toa\nCONFIG_TOA=m' >> .config
cp .config ~/rpmbuild/SOURCES/config-x86_64-generic
```

6. 删除原始源码中的 .config。

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/linux-2.6.32-220.23.1.el6.x86_64

rm -rf .config
```

7. 生成最终 patch。

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/
diff -uNr linux-2.6.32-220.23.1.el6.x86_64 linux-2.6.32-220.23.1.el6.x86_64_new/ >
~/rpmbuild/SOURCES/toa.patch
```

8. 编辑 kernel.spec。

```
vim ~/rpmbuild/SPECS/kernel.spec
```

在 ApplyOptionPath 下添加如下两行（还可修改 buildid 等自定义内核包名）：

```
Patch999999: toa.patch
ApplyOptionalPatch toa.patch
```

9. 制作 rpm 包。

```
rpmbuild -bb --with baseonly --without kabichk --with firmware --without debuginfo --target=x86_64 ~/rpmbuild/SPECS/kernel.spec
```

0. 安装内核 rpm 包。

```
rpm -hiv kernel-xxxx.rpm --force
```

1. 重启，加载 toa 模块。

使用网站业务转发规则

DDoS 高防 IP 使用网站业务转发规则时，可利用 HTTP 头部的 X-Forwareded-For 字段获取客户端真实 IP。

X-Forwareded-For：是一个 HTTP 头部扩展字段，目的是使服务器可以识别通过代理等方式链接的客户端真正的 IP。

格式为：

`X-Forwareded-For：Client, proxy1, proxy2, proxy3……`

当高防 IP 将用户的访问请求转到后端服务器时，会把请求用户的真实 IP 记录在 X-Forwareded-For 字段的首位。因此，源站应用只需要获取 HTTP 头部的 X-Forwarded-For 字段的内容即可。
更多详情请参考 七层转发获取来访真实 IP 的方法。

与源站结合的防护调度方案

最近更新时间：2020-05-09 18:03:49

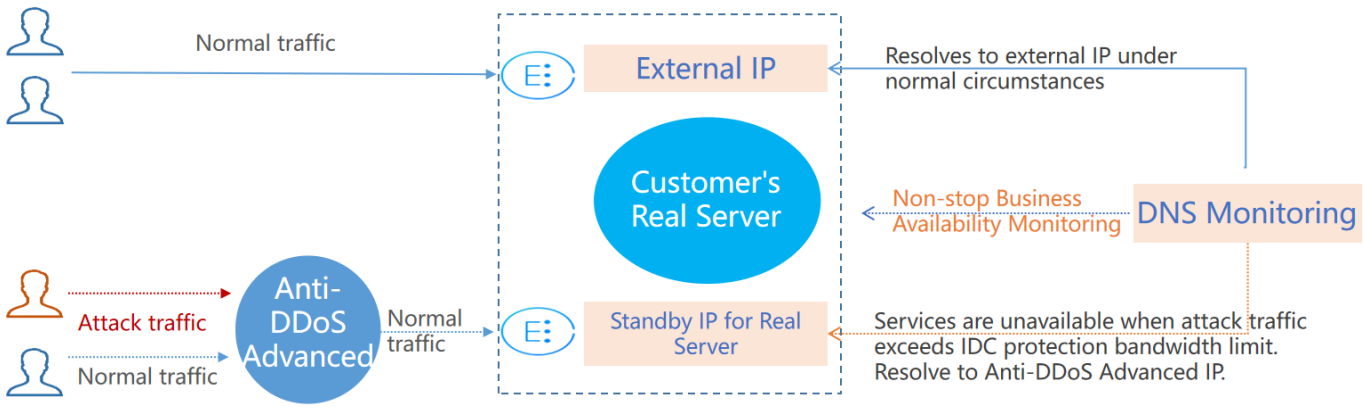
需求背景

部分用户的业务对延时要求严格，或者受限于业务要求常态化情况下必须直接访问源站，此时可考虑结合源站的防护调度方案。
该方案可满足流量常态化情况下直接访问源站，但遭到攻击后可迅速具备防护能力的要求。

防护方案

与源站结合的防护调度方案如下图：

> 本方案依赖于 DNS 服务商，需要具备监控和智能切换功能。



方案说明

本方案主要由高防 IP、DNS 监控、客户源站的对外业务 IP 和源站备用 IP 组成。

- 常态化情况下，业务的域名解析到正常的对外业务 IP，业务流量直接访问源站。DNS 监控实时监控源站业务是否可以正常访问。

- 当 DNS 监控检测到正常的对外业务 IP 无法访问时，依据智能切换的设置规则，迅速将业务域名解析到高防 IP 上。高防 IP 对攻击流量进行清洗，将干净的业务流量转发到源站的备用 IP，从而保障业务可用。

> 为避免由于网络抖动等因素造成的误切换，确保监控效果，建议进行手动切换。

方案效果

- 满足常态化情况下直接访问源站的需求。
- 适用于对延时要求非常严格的业务。
- 遭到攻击超出源站防护能力后，可自动切换到高防 IP 进行防护。

建议与注意事项

- 需提前完成源站备用 IP、高防 IP 转发规则等配置。
- 建议将源站备用 IP 与正常的业务 IP 分布在不同的物理线路，以获得更好的防护效果。
- 建议定期进行验证和演练，熟悉方案细节，解决可能存在的问题。

业务系统压力测试建议

最近更新时间：2020-05-09 18:03:50

压力测试的过程在一定程度上与 DDoS 攻击类似，为确保压力测试取得相应效果，建议用户在进行压力测试前先参考本文档获取适用建议，再拟定合适实施方案。

> 以下建议主要是基于 DDoS 防护对压力测试的影响而提出。其他与压力测试有关的方面，如网络带宽、链路负载或其他基础资源情况等，请用户结合实际情况考虑和补充。

调整防护策略

- 建议关闭 CC 防护策略，如存在某些客观原因不能关闭 CC 防护策略，请将 CC 攻击防护的 HTTP 请求数阈值调整到压测最大值以上。
- 建议关闭 DDoS 防护策略，如存在某些客观原因不能关闭 DDoS 防护策略，请将 DDoS 防护的清洗阈值调整到压测最大值以上。

控制压测流量及请求数

- 建议将压测流量值小于1Gbps，否则将有可能触发攻击防护。
- 建议将压测的 HTTP 请求数限制在20,000QPS以内（即 HTTP 请求数每秒不超过20,000个），否则将有可能触发攻击防护。
- 建议将压测的每秒新建连接数小于50,000个，最大连接数小于2,000,000个，每秒入包量小于200,000个。

> 如压测需要超出以上限制范围，请联系 腾讯云技术支持，售后团队将配合进行压测工作。

提前评估压测可能的影响

建议用户在压测前联系腾讯云架构师或 腾讯云技术支持，全面评估压测可能产生的影响及范围，制定合理的风险规避措施。

常见问题
封堵相关问题

最近更新时间：2020-05-09 18:03:50

为什么进行封堵？

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。当发生大流量攻击时，除了会影响被攻击对象，整个腾讯云的网络都可能会受到影响。为了避免攻击影响到其他未被攻击的用户，保障整个云平台网络的稳定，需要进行封堵。

为什么不提供免费无限抗攻击？

DDoS 攻击不仅影响受害者，也会对整个云网络造成严重影响，影响云内其它未被攻击的用户。DDoS 防御的成本非常高，一是带宽成本，二是清洗成本。其中最大的成本就是带宽费用，带宽费用以总流量计算，不会考虑是正常流量或是攻击流量而区别收费。
因此，腾讯云在成本可承受的范围内为云服务用户提供免费的 DDoS 基础防护服务，当攻击流量超出免费防护阈值时，腾讯云会屏蔽被攻击 IP 的外网流量。

为什么不能立即解除封堵？

通常 DDoS 攻击会持续一段时间，不会在封堵后立即停止，具体持续时间不定，腾讯云安全团队会根据大数据分析的结果，设定默认封堵时长。
由于封堵是在运营商网络部分生效，被攻击外网 IP 进入封堵后，腾讯云无法监控到攻击流量是否停止。如果在攻击未停止的情况下解除封堵，被攻击外网 IP 将再次进入封堵，同时在解除封堵至再次封堵生效的这段时间内，攻击流量将直接进入腾讯云的基础网络，可能会影响到云内其它客户。另外，封堵是腾讯云向运营商购买的服务，解封次数、频率都有限制。

紧急情况下，通过哪些途径可以提前解封？

- 升级保底容量后，可自动提前解封。
- 使用 DDoS 高防 IP 的用户每天将拥有三次自助解封机会，可在紧急情况下，进行 自助解封。

为什么自助解封会有次数限制？有哪些限制？

封堵是腾讯云向运营商购买的服务，而运营商有明确的封堵解除时间和频率限制，所以封堵状态无法频繁手动解除。
使用 DDoS 高防 IP 的用户每天将拥有**三次**自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点时重置自助解封次数，当天未使用的解封次数不会累计到次日。

怎样预防被封堵？

购买 DDoS 高防 IP 时，可根据历史攻击流量数据，选择适当的防护峰值，尽可能地确保最大防护峰值大于攻击峰值。

怎样避免解封后再次被封堵？

建议您升级保底防护峰值或弹性防护峰值，提高防御能力。开启弹性防护可帮您抵御大规模流量攻击，且弹性防护按天按量灵活付费，有效节约您的安全成本。

计费相关问题

最近更新时间：2020-04-30 14:27:48

高防服务的弹性防护计费模式是否一样？如何计算的？

一样，都是按照当日可防护的攻击流量峰值对应弹性防护峰值区间进行计费，计费详情请参考 计费概述。
例如，您购买的 BGP 高防 IP 实例规格是20Gbps保底防护峰值 + 50Gbps弹性防护峰值。如果当天发生 DDoS 攻击事件且最高攻击流量峰值为45Gbps。45Gbps已超过保底防护峰值范围触发弹性防护，且属于40Gbps ＜ 弹性峰值 ≤ 50Gbps计费区间，当天产生弹性费用按照40Gbps ＜ 弹性峰值 ≤ 50Gbps计费区间收取。

如果 BGP 高防 IP 所防护的 IP 因遭受大流量攻击被封堵，该部分攻击流量是否会列入计费？

BGP 高防 IP 服务的弹性防护计费规则是针对超出保底防护峰值且小于等于弹性防护峰值的攻击流量进行计费。被封堵即意味着攻击流量已超过所设置的弹性防护峰值，因此超出弹性防护峰值的部分攻击流量不在计费范围内。

购买弹性防护后，如果一个月都没有遭受攻击，是否需要费用？

这种情况下，不产生弹性防护费用。

若购买了100Gbps的保底防护，是否可以降到50Gbps ？

不可以。保底防护级别仅支持升级，不支持降级。

业务遭受攻击过程中，是否支持升级弹性防护峰值？

支持。BGP 高防 IP 服务基础信息界面支持调整弹性防护峰值，支持调升也支持调降。不同地域支持的防护能力不同，弹性防护峰值的具体取值范围请参考 产品概述。

> 若当日发生的攻击已经产生计费，修改后次日将以最新的弹性防护峰值进行计费。

受防护的 IP 一天之内遭受多次攻击，是否需要收取多次费用呢？

BGP 高防 IP 服务是以当日防护的最高攻击流量峰值来计算，只收取一次费用。

如果购买了两个高防服务套餐，且两个高防服务实例遭受的攻击流量都超过保底防护，如何收取弹性防护费用？

弹性防护费用以产品实例为计算单位，如果两个高防服务实例都超过保底防护，则需要分别收取两个高防实例的弹性防护费用。

功能相关问题

最近更新时间：2020-05-09 18:03:51

DDoS 高防 IP 支持腾讯云外用户接入防护吗？

支持。DDoS 高防 IP 可以防护任何公网服务器，包括但不限于在腾讯云、其他的云、IDC 机房等。

> 在中国大陆地区接入的域名必须按照工信部要求进行 ICP 备案。如果域名未备案，将不能提供 DDoS 高防服务。

DDoS 高防 IP 是否支持泛域名？

DDoS 高防 IP 网站业务转发规则配置中，支持对泛域名进行防护。
泛域名解析是指利用通配符（*）作为次级域名，以实现所有的次级域名均指向同一 IP。例如，支持配置 *.tencent.com。

DDoS 高防 IP 服务是否会自动将回源 IP 地址加入安全组?

不会。用户需手动将回源 IP 段添加至 CVM 安全组中。若用户在源站部署了防火墙或其它主机安全防护软件，也需将回源 IP 段添加至相应的白名单中，防止将高防回源 IP 拦截或限速导致业务流量受损。

DDoS 高防 IP 中的源站 IP 可以填写内网 IP 吗？

DDoS 高防 IP 是通过公网进行回源的，不可以直接填写内网 IP。

修改 DDoS 高防 IP 服务的源站 IP 是否有延迟？

修改高防 IP 服务已防护的源站 IP 可秒级生效。

在 DDoS 高防 IP 服务控制台中，更改配置后大约需要多少时间生效？

DDoS 高防 IP 服务中更改配置是秒级生效的。

DDoS 高防 IP 的 IP 回源支持 IPv6 协议吗？

暂时不支持 IPv6协议。

DDoS 高防 IP 服务是否支持 HTTPS 双向认证？

- 网站接入方式不支持 HTTPS 双向验证。
- 非网站接入且使用 TCP 转发方式时，支持 HTTPS 双向验证。

DDoS 高防 IP 服务是否有抓包文件？

DDoS 高防 IP 服务支持下载抓包文件，具体操作请参考 查看统计报表 。

DDoS 高防 IP 在配置多个源站 IP 时如何负载？

- 网站业务采用源 IP 哈希方式进行负载均衡。
- 非网站业务采用加权轮询方式依次轮流转发。

DDoS 高防 IP 支持转发端口数及支持的域名数分别是多少？

- 转发端口数：TCP/UDP 协议支持转发规则条目总数，默认免费提供60个，支持扩展。
- 支持域名数：HTTP/HTTPS 协议支持转发规则条目总数，默认免费提供60个，支持扩展。

什么是业务带宽，超过之后会有什么影响？

购买的业务带宽是针对整个高防 IP 实例的，指该实例所有正常业务的 IN 或者 OUT 方向的流量。
如果用户的业务流量超过所赠送的规格，将触发流量限速，可能导致随机丢包。若持续出现这种情况，请及时升级更大的业务带宽。

> 购买 DDoS 高防 IP 服务，默认赠送100M转发业务带宽。

DDoS 高防 IP 服务是否支持会话保持？

DDoS 高防 IP 服务支持会话保持，默认不开启。非网站业务可以通过控制台进行配置操作，请参考 配置会话保持。

DDoS 高防 IP 服务是否支持健康检查？

非网站业务默认开启健康检查，建议使用默认值，如需要修改，请参考操作步骤 配置健康检查。

在用户业务绑定 DDoS 高防 IP 后，源站服务器未开启窗口因子 WS 时，访问源站为什么会出现速度慢？

高防服务器默认是开启窗口因子 WS（Window Scaling），若源站服务器未开启，将会导致接收稍大文件数据时，很快把滑动窗口占满出现延迟。建议用户将源站所有服务器开启 WS。