DDoS 高防包

DDoS 高防包（旧）

产品文档

腾讯云

文档目录

DDoS 高防包（旧）
产品简介
产品概述

最近更新时间：2020-04-02 10:00:56

简介

DDoS 高防包是针对业务部署在腾讯云内的用户提升 DDoS 防护能力的付费产品。DDoS 高防包直接对腾讯云上 IP 生效，无需更换 IP，购买后只需绑定需要防护的 IP 即可使用，具备接入便捷、零变更等特点。DDoS 高防包支持为 IPV6 和 IPV4 两种类型的 IP 提供防护，同时支持单 IP 防护，也提供多 IP 共享防护资源功能，满足多个 IP 地址都需要提升防护能力的需求。
腾讯云 DDoS 高防包提供独享包与共享包两种类型的高防包，用户可根据需求自行选择：

- 独享包：提供一个 IP 独享防护能力。
- 共享包：提供多个 IP 共享防护能力。

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

防护对象可切换

DDoS 高防包支持单 IP，也支持多个 IP 共享防护资源，满足各种业务场景。用户可根据业务需要，切换防护对象，支持切换的对象包括 CVM、CLB、WAF、NAT 网关等。

高级安全策略灵活

DDoS 高防包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，用户可根据特殊业务特点灵活设置，应对不断变化的攻击手法。

防护统计及分析

DDoS 高防包提供实时详细的流量报表及攻击防护详细信息，便于用户及时、准确了解 DDoS 高防包的防护效果。同时支持攻击取证，可对攻击情况进行抓包下载，方便快速分析异常问题以及溯源。

产品优势

最近更新时间：2020-04-02 10:00:56

DDoS 高防包是一键为腾讯云内 CVM、CLB、NAT 网关等云产品提升 DDoS 防护能力的付费服务，其产品优势如下：

一键接入，无需任何业务变更

无需进行业务变更，接入配置便捷，购买 DDoS 高防包后，只需绑定需要防护的云产品的 IP 地址即可使用，只需几分钟即可生效。

超大防护资源

采用 DDoS 防护带宽，可为单用户单点提供高达300Gbps的 DDoS 防护能力，轻松抵御 DDoS 攻击，满足活动大促、活动上线等重要业务的安全稳定性保障需求。

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 DDoS 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。

支持双协议防护

DDoS 高防包支持同时为 IPV6 和 IPV4 两种类型的 IP 提供防护，满足客户对 IPV6 类型服务器需要防护的需求，无需额外购买或升级高防包，只需绑定需要防护的云产品的 IP 地址后即可实现 DDoS 防护。

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：2020-04-02 10:00:56

游戏

游戏行业是 DDoS 攻击的重灾区，DDoS 高防包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：2021-01-19 14:43:06

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，保底部分为冻结付费。
- 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。

> **说明：**
>
> 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主开启。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 高防包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 DDoS 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。

封堵阈值

DDoS 高防包实例的防护 IP 的封堵阈值等于实际购买的最大 防护峰值。DDoS 高防包有多种不同规格，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。

⚠ 注意：

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。

相关产品

最近更新时间：2020-04-22 16:51:36

使用 DDoS 高防包可为如下产品提升 DDoS 防护能力：

- 云服务器
- 负载均衡
- Web 应用防火墙
- NAT 网关
- VPN 连接
- 全球应用加速
- 弹性网卡

购买指南
计费概述

最近更新时间：2021-01-19 14:41:29

目前 BGP 高防包支持购买的区域：

- 中国内地（大陆）区域：华北地区（北京）、华东地区（上海）和华南地区（广州）。

计费方式

BGP 高防包服务使用组合计费方式，包括冻结付费和按量计费两种方式。其中，保底防护峰值为冻结付费，弹性防护峰值为按实际用量后付费，按天结算。

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。

产品价格

保底防护

保底防护具体价格请参考如下表格：

类型	保底防护峰值	防护 IP 个数	CC 防护峰值	单价（美元/月）
独享包	5Gbps	1	10,000QPS	77
	20Gbps		40,000QPS	2,558
	30Gbps		70,000QPS	3,946
	50Gbps		150,000QPS	8,723
	100Gbps		300,000QPS	28,790
共享包	20Gbps	5	40,000QPS	3,583

		10		6,808
		20		12,900
		50		25,084
		100		43,000
	50Gbps	5	150,000QPS	12,213
		10		23,204
		20		43,966
		50		85,489
		100		146,553
	100Gbps	5	300,000QPS	34,548
		10		65,642
		20		124,374
		50		241,838
		100		414,580

说明：

- Query Per Second（QPS），此处用于衡量 BGP 高防包实例每秒可防护的 CC 攻击请求数。
- 购买并绑定高防包后，被绑定 IP 仅具有购买的高防包的防护能力，不叠加基础防护。
- 保底防护峰值为20Gbps/30Gbps/50Gbps的独享包，不支持升级为100Gbps及以上的保底防护规格，最大支持升级为50Gbps。

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：

BGP 防护峰值	单价（美元/天）
20Gbps ≤ 攻击峰值 < 30Gbps	260
30Gbps ≤ 攻击峰值 < 40Gbps	450
40Gbps ≤ 攻击峰值 < 50Gbps	600
50Gbps ≤ 攻击峰值 < 60Gbps	800
60Gbps ≤ 攻击峰值 < 70Gbps	1,200
70Gbps ≤ 攻击峰值 < 80Gbps	1,500
80Gbps ≤ 攻击峰值 < 90Gbps	1,700
90Gbps ≤ 攻击峰值 < 100Gbps	1,900
100Gbps ≤ 攻击峰值 < 120Gbps	2,100
120Gbps ≤ 攻击峰值 < 150Gbps	2,300
150Gbps ≤ 攻击峰值 < 200Gbps	2,700
200Gbps ≤ 攻击峰值 < 250Gbps	4,800
250Gbps ≤ 攻击峰值 < 300Gbps	5,600

计费示例

BGP 高防包使用组合计费方式，计费示例说明如下：

- **单 IP 类型费用计算示例**
  例：用户在上海区域购买了一个独享型单 IP 的 BGP 高防包，规格是“20Gbps保底防护峰值 + 50Gbps弹性防护峰值”。
  若当天发生 BGP 攻击事件且最高攻击流量峰值为45Gbps，超过保底防护峰值范围且使用了弹性防护峰值，落入 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3158美元，其中包含当月的保底防护费用2558美元，当天产生的弹性费用600美元。
- **多 IP 类型费用计算示例**
  例：用户在上海区域购买了一个共享型多 IP 的 BGP 高防包，规格是“20Gbps保底防护峰值 + 80Gbps弹性防护峰值，IP 数量5个”。
  若当天发生多个 IP 同时被攻击的事件，有3个 IP 同时受到攻击攻击流量分别为10Gbps、15Gbps和30Gbps。则

同时遭受攻击的叠加峰值为10 + 15 + 30 = 55Gbps，超过了20Gbps的保底防护峰值且使用了弹性防护峰值，落到了50Gbps ＜ 弹性峰值 ≤ 60Gbps计费区间，当天产生弹性费用800美元。

则用户需支付费用合计为4383美元，其中包含当月的保底防护费用3583美元，当天产生的弹性费用800美元。

快速入门

最近更新时间：2020-03-23 16:30:01

DDoS 高防包为腾讯云公网 IP 提供更高的 DDoS 防护能力，可支持防护 CVM、CLB、NAT、WAF 等产品和服务。
DDoS 高防包接入便捷，无需变更业务 IP，可快速完成防护配置。
目前，腾讯云 DDoS 高防包提供独享包与共享包两种类型的高防包。

前提条件

在绑定防护 IP 前，您需要成功购买 DDoS 高防包实例。

操作步骤

1. 登录 DDoS 防护管理控制台，前往【DDoS 高防包】>【资产列表】。
   - 若您的 DDoS 高防包实例是独享包，则选择【独享包】页签。
   - 若您的 DDoS 高防包实例是共享包，则选择【共享包】页签。

2. 选择目的高防包实例所在地域，单击目的高防包实例所在行的操作项【绑定设备】。

3. 在【绑定设备】页面，根据实际防护需求选择【关联设备类型】与【选择关联机器】。

   - 若您的 DDoS 高防包实例是独享包，仅支持绑定一个关联机器。

   - 若您的 DDoS 高防包实例是共享包，【关联设备类型】与【选择关联机器】均允许多选，【选择关联机器】数量不得超过购买 DDoS 高防包实例 时设置的【IP 数量】。

DDoS 高防包支持托管 IP，目前在白名单中。如用户使用腾讯云的托管 IP，需要接入 DDoS 高防包，请致电 95716转1（工作日9:00am - 6:00pm）进行咨询，或 提交工单 申请加入白名单。
4. 单击【确定】。

操作指南

操作总览

最近更新时间：2020-04-22 16:51:37

您在使用 DDoS 高防包时，可能碰到诸如配置 DDoS 高防包实例、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 高防包的常用操作，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
- 更换防护对象 IP
- 解封防护 IP

防护配置

- 配置清洗阈值与防护等级
- 配置业务场景
- 管理 DDoS 高级防护策略
- 管理 CC 防护策略

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：2020-01-02 17:09:52

防护对象限制

BGP 高防包仅适用于腾讯云产品，包含云服务器、负载均衡、黑石物理服务器、NAT 网关等。

接入限制

BGP 高防包仅支持绑定同一地域内的腾讯云公网 IP。

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。
- CC 黑白 IP 名单分别最多支持添加50个 IP 地址。
- CC URL 白名单最多支持添加50个 URL。

地域限制

BGP 高防包只能绑定同一地域内的腾讯云设备，目前开放购买的地域包括：华北（北京）、华东（上海）、华南（广州）。
BGP 高防包在不同地域提供的高防能力请参考如下表格：

类型	地区	保底防护	弹性防护	最大防护能力
独享包	广州	5Gbps - 50Gbps	30Gbps - 100Gbps	100Gbps
	北京	5Gbps - 50Gbps	30Gbps - 100Gbps	100Gbps
	上海	5Gbps - 100Gbps	30Gbps - 300Gbps	300Gbps
共享包	广州	• 20Gbps • 50Gbps • 100Gbps	30Gbps - 100Gbps	100Gbps
	北京		30Gbps - 100Gbps	100Gbps
	上海		30Gbps - 300Gbps	300Gbps

实例管理
查看实例详情

最近更新时间：2020-03-23 16:34:49

操作场景

您可以通过 DDoS 防护管理控制台查看所购买的 DDoS 高防包的基础信息（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

示例：查看广州地区独享包实例“bgp-000006ee”的详细信息。

1. 登录 DDoS 防护管理控制台，在左侧导航栏中，选择【DDoS 高防包】>【资产列表】，单击【独享包】，在地区选择框中，单击【华南地区（广州）】，找到实例 ID 为“bgp-000006ee”的独享包，单击 “ID/独享包名”查看实例信息。

参数说明：

- **基础信息：**
  - **服务包名**
    该 DDoS 高防包实例的名称，用于辨识与管理 DDoS 高防包实例。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。
  - **所在地区**
    购买 DDoS 高防包时选择的【地域】。
  - **绑定 IP**
    该 DDoS 高防包实例所防护业务的实际 IP。
  - **保底防护峰值**
    该 DDoS 高防包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。
  - **当前状态**
    DDoS 高防包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前7天内，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。

- **标签**

  表示该 DDoS 高防包实例所属的标签名称，可以编辑、删除。
- **弹性防护信息：**
- **当前状态**

  表示弹性防护是否开启。若购买 DDoS 高防包实例 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**

  开启弹性防护时，该参数项才可见，表示当前 DDoS 高防包实例的最大弹性防护能力。用户可以根据自身业务需求，随时调整弹性防护峰值，具体操作请参见 配置弹性防护。

设置资源名称

最近更新时间：2020-03-23 16:32:10

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

方式一

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择【DDoS 高防包】>【资产列表】，在资产列表左上方，选择地域。
2. 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，在左侧导航中，选择【DDoS 高防包】>【资产列表】，在资产列表左上方，选择地域。
2. 在下方实例列表中，单击目标实例的“ID/名称”列的实例名称，进入实例的基础信息页面。
3. 在实例的基础信息页面中，单击基础信息右侧的【编辑】，输入或修改名称，并打击【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：2020-03-24 17:27:04

BGP 高防包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，BGP 高防包会根据用户设置的弹性防护峰值继续进行防护。

若 购买 BGP 高防包实例 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 BGP 高防包实例的弹性防护峰值。

开启弹性防护

> 若 购买 BGP 高防包实例 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。

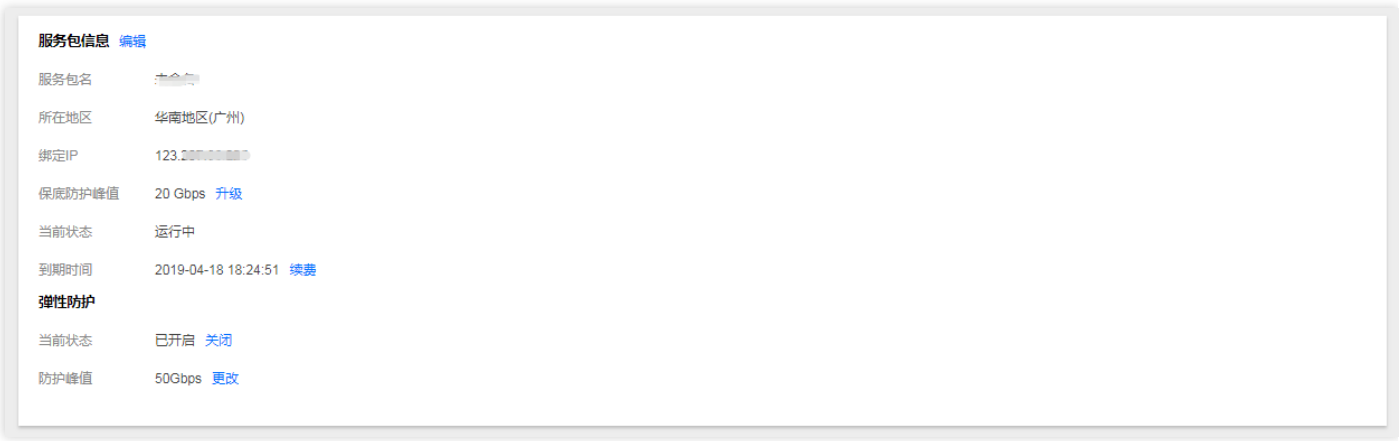
1. 登录 DDoS 防护（大禹）管理控制台，选择【BGP高防包】>【资产列表】，在目标实例所在行，单击【开启弹性防护】。
2. 在【开启弹性防护】对话框中，选择合适的【弹性防护峰值】。

3. 单击【确定提交】。

更改弹性防护峰值

1. 登录 DDoS 防护（大禹）管理控制台，选择【BGP高防包】>【防护配置】。

2. 从实例下拉菜单中选择目标实例，单击【防护峰值】右侧的【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（大禹）管理控制台，选择【BGP高防包】>【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】。

管理防护对象 IP

最近更新时间：2020-03-23 16:30:02

操作场景

DDoS 高防包为腾讯云公网 IP 提供更高的 DDoS 防护能力，可支持防护 CVM、CLB、NAT、WAF 等产品和服务。用户根据实际业务需求，可以更换已绑定到 DDoS 高防包实例的防护对象 IP，也可以一键解绑已绑定到 DDoS 高防包的防护对象 IP。

前提条件

在更换、或解绑防护对象 IP，您需要成功购买 DDoS 高防包实例 并已为其 绑定防护对象 IP。

操作步骤

更换防护对象 IP

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择【DDoS 高防包】>【资产列表】，在页面上方，选择地域。
   - 若您的 DDoS 高防包实例是独享包，则选择【独享包】页签。
   - 若您的 DDoS 高防包实例是共享包，则选择【共享包】页签。
2. 单击目标 DDoS 高防包实例所在行的【更换设备】。
3. 在【绑定设备】页面，根据实际防护需求选择【关联设备类型】与【选择关联机器】。
   - 若您的 DDoS 高防包实例是独享包，仅支持绑定一个关联机器。
   - 若您的 DDoS 高防包实例是共享包，【关联设备类型】与【选择关联机器】均允许多选，【选择关联机器】数量不得超过购买 DDoS 高防包实例 时设置的【IP 数量】。
4. 单击【确定】。

解绑防护对象 IP

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择【DDoS 高防包】>【资产列表】，在页面上方，选择地域。

- 若您的 DDoS 高防包实例是独享包，则选择【独享包】页签。
- 若您的 DDoS 高防包实例是共享包，则选择【共享包】页签。

2. 单击目标 DDoS 高防包实例所在行的【更多】>【解绑】，在弹出的会话框中，单击【确定】即可。

解封防护 IP

最近更新时间：2020-03-06 16:56:53

BGP 高防包对进入封堵状态的防护 IP 提供解封的功能，您可以登录 DDoS 防护（大禹）管理控制台 进行自助解封操作。

自助解封次数

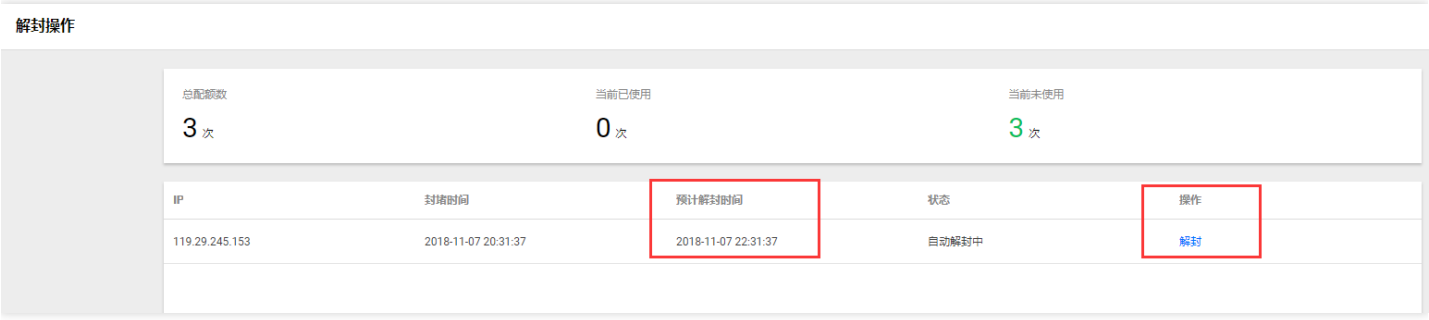
使用 BGP 高防包的用户每天将拥有**三次**自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点时重置自助解封次数，当天未使用的解封次数不会累计到次日。

- 由于解封涉及腾讯云大禹后台系统的风控管理策略，解封可能失败（解封失败不会扣减您的剩余解封次数），请您耐心等待一段时间后再次尝试。
- 在执行解封操作前，建议您先查看预计解封时间，预计解封时间受到部分因素影响，可能会推后。如果您可以接受预计时间，则无需手动操作。
- 当天自助解封配额为0时，建议提升保底防护能力或弹性防护能力，以便足够防御大流量攻击，避免被持续封堵。

自助解封操作

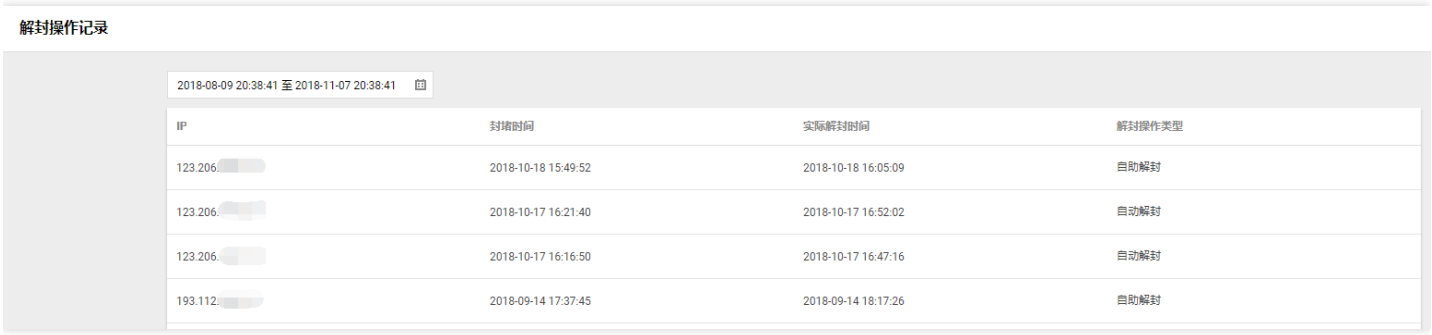
登录 DDoS 防护（大禹）管理控制台，选择【自助解封】>【解封操作】，找到状态为自动解封中的防护 IP，单击【操作】列中的【解封】。在【解除封堵】对话框中，单击【确定】。

- 如果解封失败，您会收到解封失败提示信息，请您耐心等待一段时间后再尝试。
- 如果收到解封成功提示信息，则表示封堵状态已成功解除，您可以刷新页面确认该防护 IP 是否已恢复运行中状态。



解封操作记录

登录 DDoS 防护（大禹）管理控制台，选择【自助解封】>【解封操作记录】，根据时间范围筛选，可查看所有解封操作记录，包括自动解封、手工自助解封等操作记录。



防护配置
配置清洗阈值与防护等级

最近更新时间：2020-03-23 16:30:02

应用场景

DDoS 高防包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：

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。 • 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。	清洗策略相对严格，建议在正常模式出现攻击透传时使用。

如果您的业务需要使用 UDP，建议您联系 腾讯云技术支持 进行策略定制，以免严格模式影响业务流程。

默认情况下，您所购买的 DDoS 高防包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。

配置示例

下面以配置华南地区（广州）的实例“bgp-000006ee”为例，进行配置说明：

1. 登录 DDoS 防护管理控制台，在左侧导航栏中，选择【DDoS 高防包】>【资产列表】，单击【独享包】，在地区选择框中，单击【华南地区（广州）】，找到实例 ID 为“bgp-000006ee”的独享包，在右侧操作项中，单击【防护配置】进行配置。
2. 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，下面配置项才可见。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 高防包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 高防包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，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。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，支持修改。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**
  新增 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。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 高防包提供 TCP 业务 AI 增强防护功能，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。

配置业务场景

最近更新时间：2020-03-23 16:30:03

应用场景

DDoS 高防包支持自定义 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。通常每个高防包实例最多绑定一个 DDoS 高级防护策略。当用户的账号下拥有多个高防包实例时，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 高防包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 高防包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 高防包】>【防护配置】，会弹出如下图所示的提示信息，单击【去创建】，进行业务场景的创建。

> 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【BGP 高防包】>【防护配置】，在防护配置页面中，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：**
     - **当前正在使用的协议：**勾选正在使用的协议，支持可选的协议有 ICMP、TCP、UDP 和其他协议（指除了 ICMP、TCP、UDP 以外的协议）。

> 当勾选 TCP、UDP协议时，则需要输入 TCP/ UDP 业务端口范围，可填范围为1 - 65535，同时其他信息区域会弹出 TCP/ UDP 业务报文包长范围配置，该配置为选填项，可填的报文包长范围为0 - 1500。

- **是否有海外客户**？
  勾选【是】或【否】，对应生成策略的配置项为关闭 / 开启【拒绝海外流量】。
- **是否会主动对外发起 TCP 请求**？
  勾选【是】或【否】。选择【是】，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（DNS 请求，NTP 请求等）**？
  勾选【是】或【否】。选择【是】，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+】即可选择对应参数）
  - **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**？
    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。
  - **是否存在 VPN 业务**？
    勾选【是】或【否】。默认【否】，若选择【是】时，则不会禁用“其他协议”。

> 在“当前正在使用的协议”、“是否存在 VPN 业务”两项参数中，只要存在条件之一即勾选“其他协议”或选择“【是】存在 VPN 业务”，则不会禁用“其他协议”。

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 高防包实例的情况下，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。

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 高防包】>【防护配置】。
2. 在【DDoS 高级防护策略】页面，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。

若需要了解更多信息，请参见 管理 DDoS 高级防护策略。

管理 DDoS 高级防护策略

最近更新时间：2019-11-13 16:34:53

BGP 高防包提供面向 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、禁用端口、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

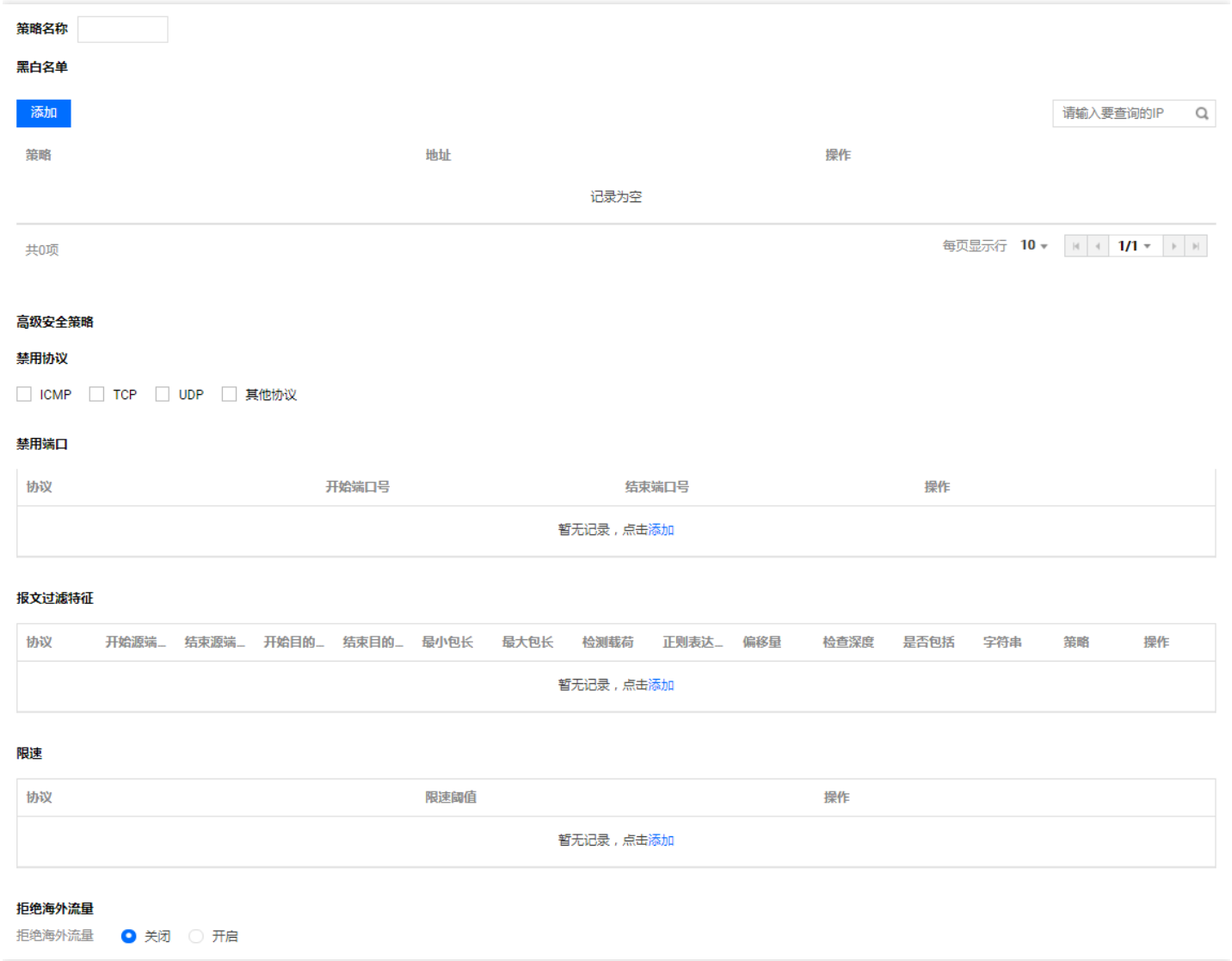
配置项	功能简介	生效时间
黑白名单	基于 IP 地址级别的防护。 • 白名单中的 IP，访问时将被直接放行，不经过任何防护策略过滤。 • 黑名单中的 IP，访问时将会被直接阻断。	保存配置后即刻生效。
禁用协议	可禁用业务不使用的协议。 当检测到攻击行为时，大禹高防集群会清洗掉该协议的流量。	保存配置后即刻生效。
禁用端口	可禁用业务不使用的端口。 当检测到攻击行为时，大禹高防集群会清洗掉该端口的流量。	保存配置后即刻生效。
报文过滤特征	可以针对业务报文特征或攻击报文特征，将协议、端口范围、包长范围、是否检测载荷、偏移量、检查深度、是否包括特征字符串等条件进行组合，设定策略动作。 当检测到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。	保存配置后即刻生效。
限速	基于目的IP的防护，对访问协议进行限速控制。	保存配置后即刻生效。
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。	被防护的 IP 处于被攻击状态时生效。
空连接防护	应对空连接攻击。	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，对于接入高防包的防护 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。	保存配置后即刻生效。

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。	保存配置后即刻生效。
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。	保存配置后即刻生效。

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（大禹）管理控制台，选择【BGP 高防包】>【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。

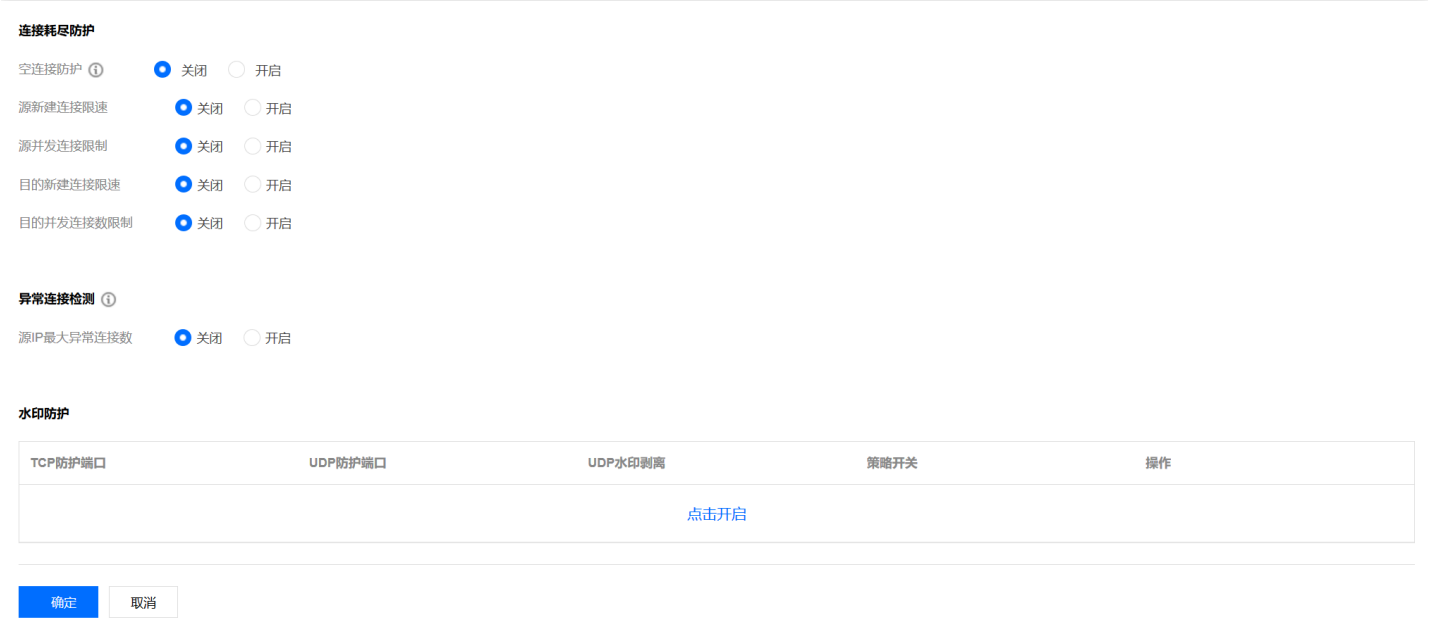
- **禁用端口**
  选择协议，然后填写对应需要禁用的端口。若某条记录中仅需禁用一个端口，则开始端口号和结束端口号填写相同值即可。单击列表下方的【增加】可新增多条记录。

- **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。BGP 高防包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。

绑定与解绑资源

登录 DDoS 防护（大禹）管理控制台，选择【BGP 高防包】>【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 **X**，单击【确定】。

客户端接入水印

登录 DDoS 防护（大禹）管理控制台，选择【BGP 高防包】>【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（大禹）管理控制台，选择【BGP 高防包】>【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（大禹）管理控制台，选择【BGP 高防包】>【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
- 禁用端口
- 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；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（大禹）管理控制台，选择【BGP 高防包】>【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 防护策略

最近更新时间：2020-04-02 10:00:57

操作场景

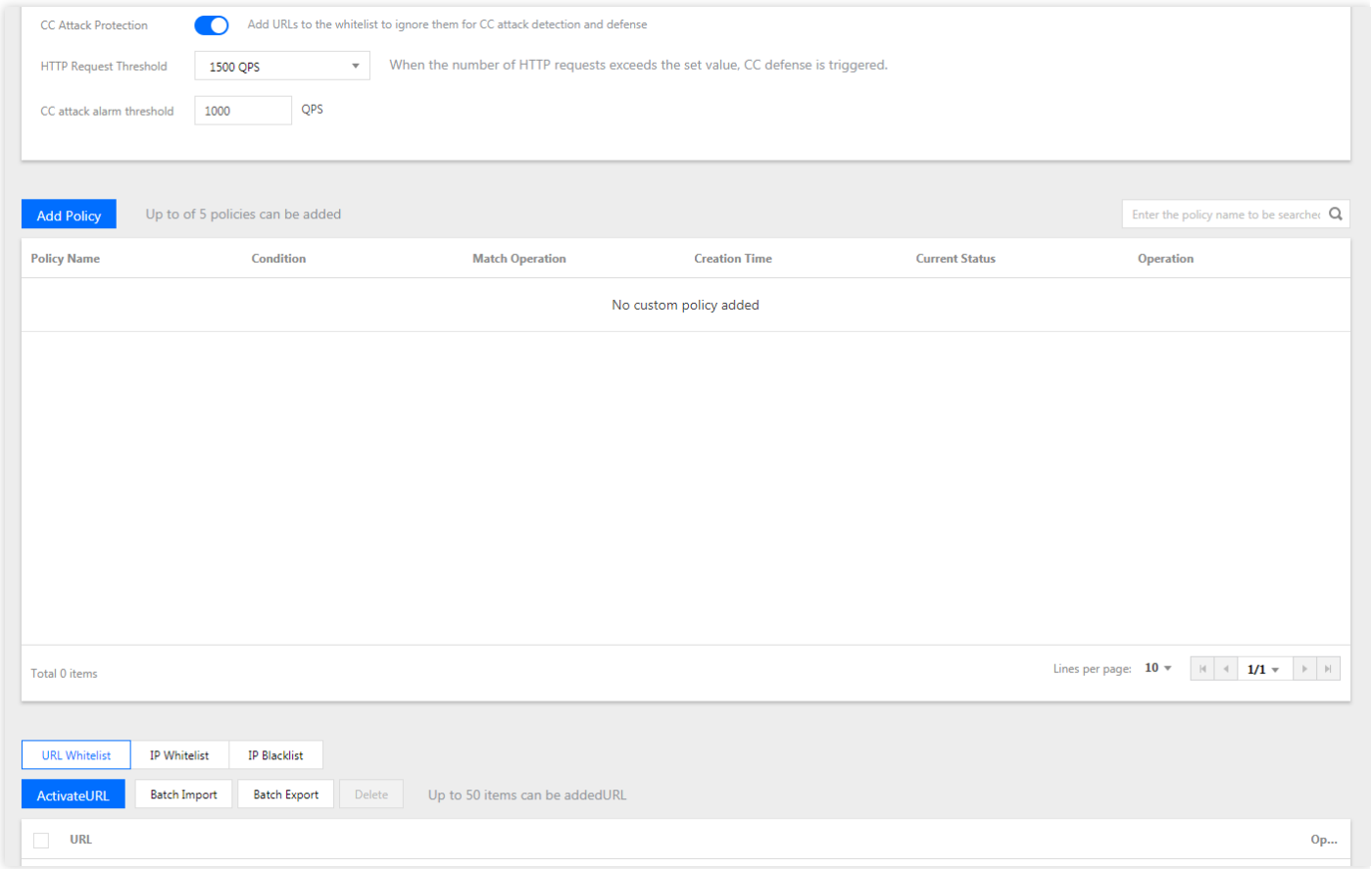
DDoS 高防包支持 CC 防护功能，当高防包统计的 HTTP 请求量超过设定的【http 请求数阈值】时，自动触发 CC 防护。同时，DDoS 高防包还支持 URL 白名单、IP 白名单和 IP 黑名单策略：

- 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 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 访问请求将直接被拒绝。

用户可根据业务特点和防护需求，自定义防护策略实现更精准的 CC 攻击拦截。

操作步骤

1. 登录 DDoS 防护管理控制台，选择【DDoS 高防包】>【防护配置】，在【CC 防护】页签，选择目标地域和高防包实例，进行 CC 防护配置。

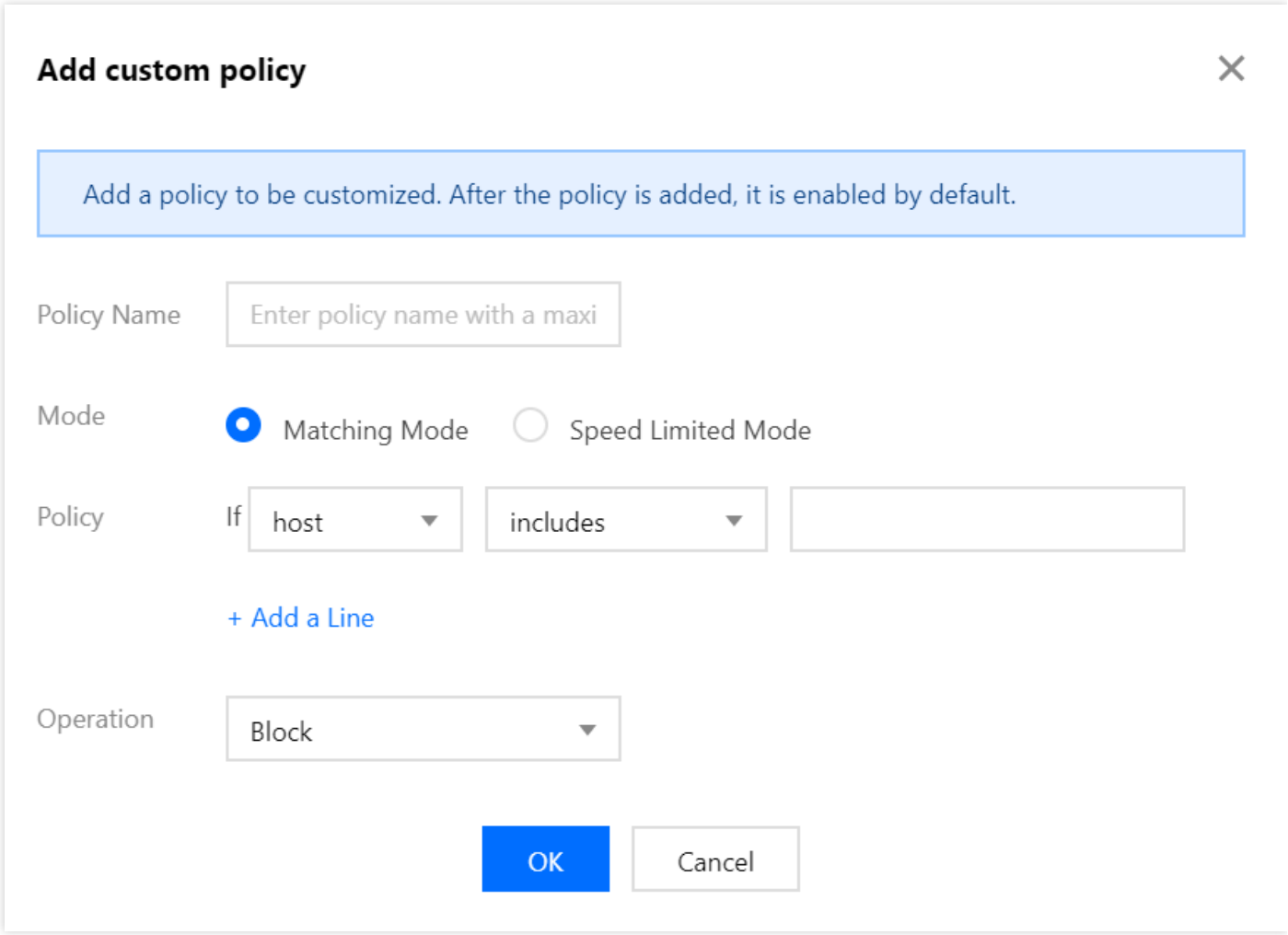


2. 单击【CC 防护】右侧的开启 CC 防护。

- CC 防护默认关闭。
- 开启 CC 防护后，才可设置 HTTP 请求数阈值、自定义 CC 防护策略以及黑白名单。

3. 单击【http 请求数阈值】右侧的下拉框选择合适的阈值。

4. 单击【添加访问控制策略】，在【添加访问控制策略】弹出框中，根据实际业务需求设置以下参数，单击【确定】完成配置。



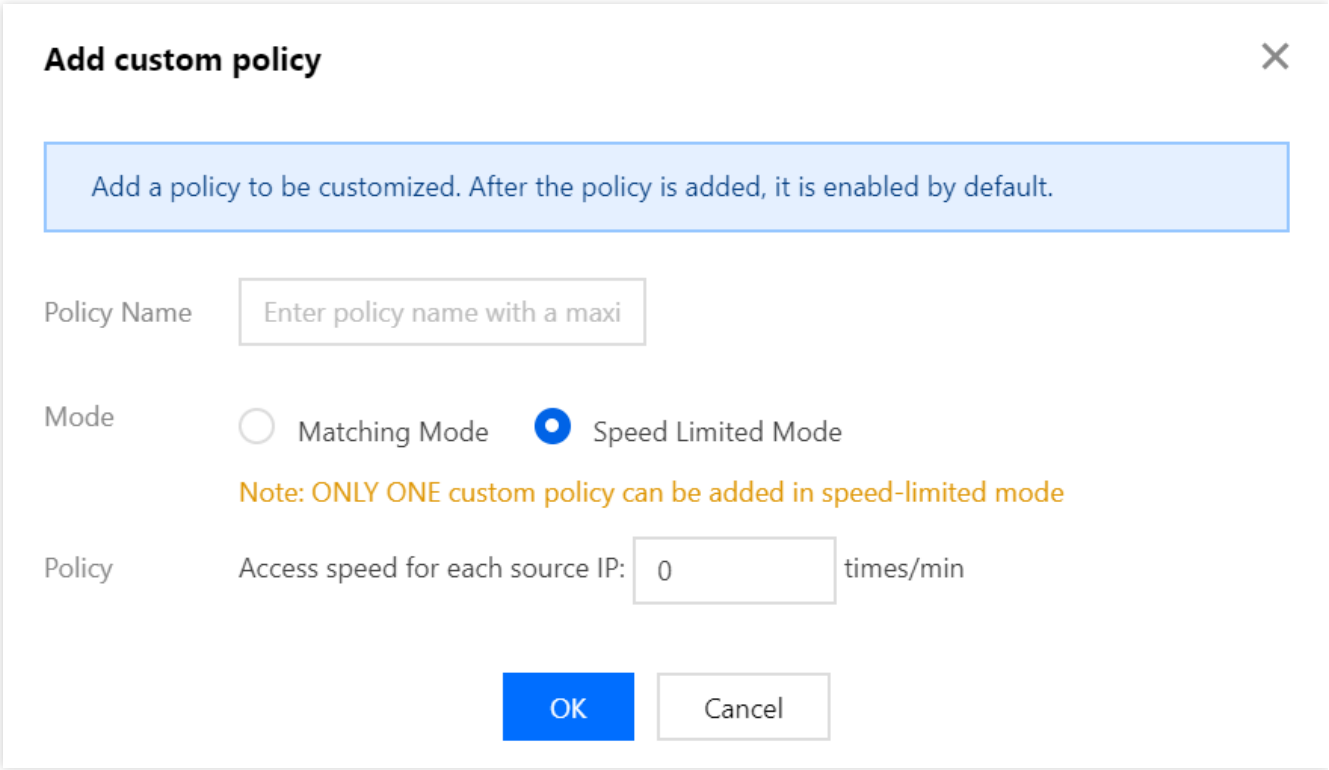
- **仅在该高防包正在被攻击状态时，自定义策略才会生效。**
- **匹配模式下**，每个自定义策略最多可以设置**4**个策略条件进行特征控制，且多个条件之间是“与”的关系，需要所有条件全部匹配策略才生效。
- **限速模式下**，每个自定义策略只允许设置**1**条策略条件。
- **策略名称**
  输入策略名称，长度为1 - 20字符，不限制字符类型。
- **模式**
  - 匹配模式：匹配到 HTTP 对应字段头的请求，执行拦截或人机识别操作。

- 限速模式：对源 IP 访问进行限速处理。

- **策略**
  - 当选择【匹配模式】时，支持从 HTTP 报文的 host 参数、CGI 参数、Referer 和 User-Agent 等多个特征进行组合，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，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 URL 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。



5. 单击【URL 白名单】、【IP 白名单】或【IP 黑名单】页签，进行黑白名单配置，支持添加、删除。

DDoS 高防包添加 URL 白名单时，可以带 HTTP 协议头信息，也可以不带 HTTP 协议头信息，但 DDoS 高防包仅支持 HTTP 协议。例如可以填写 `http://test.com/index.php` 或 `www.test.com/index.php` 。

配置攻击告警阈值

最近更新时间：2020-04-02 10:00:57

应用场景

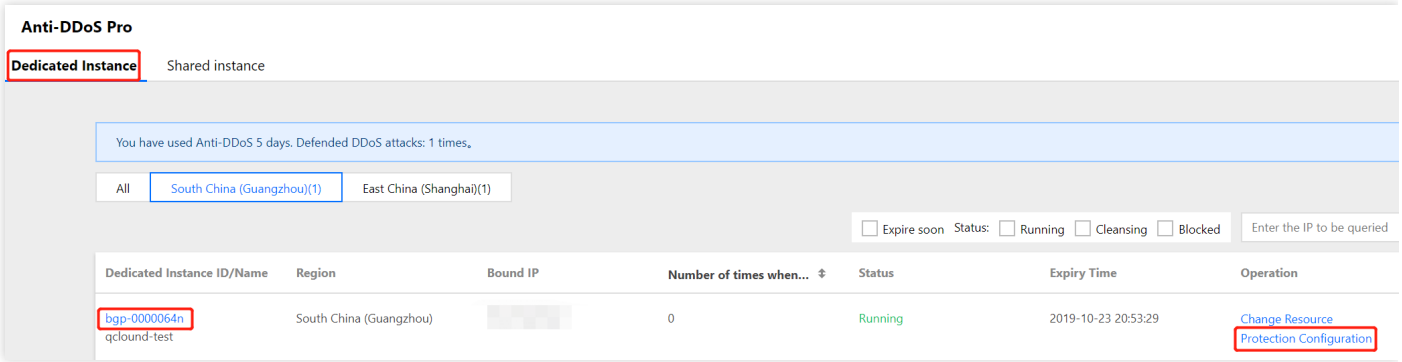
当您所使用的 DDoS 高防包遭受攻击、受攻击结束、被封堵以及解除封堵时，系统将以站内信、短信、邮件的方式向您推送攻击告警信息。为更加合理、准确地推送攻击告警信息，减少困扰，新增攻击告警阈值配置功能。若检测的指标超过您设定的阈值，将触发告警，并向您推送攻击告警信息。若发生正常业务操作（如同步数据等）引起流量突增，但被判定为攻击的现象，该功能可以较好地过滤这类情况，帮助您更加准确、清晰地掌握当前业务遭受的攻击状况。如何接收告警信息，请参见 设置安全事件通知。

配置 DDoS 攻击告警阈值

本配置示例可实现如下功能：当高防系统检测到独享型高防包实例“bgp-000005w1”的入流量带宽超过1000Mbps时，将向指定用户群体发送 DDoS 攻击告警信息。

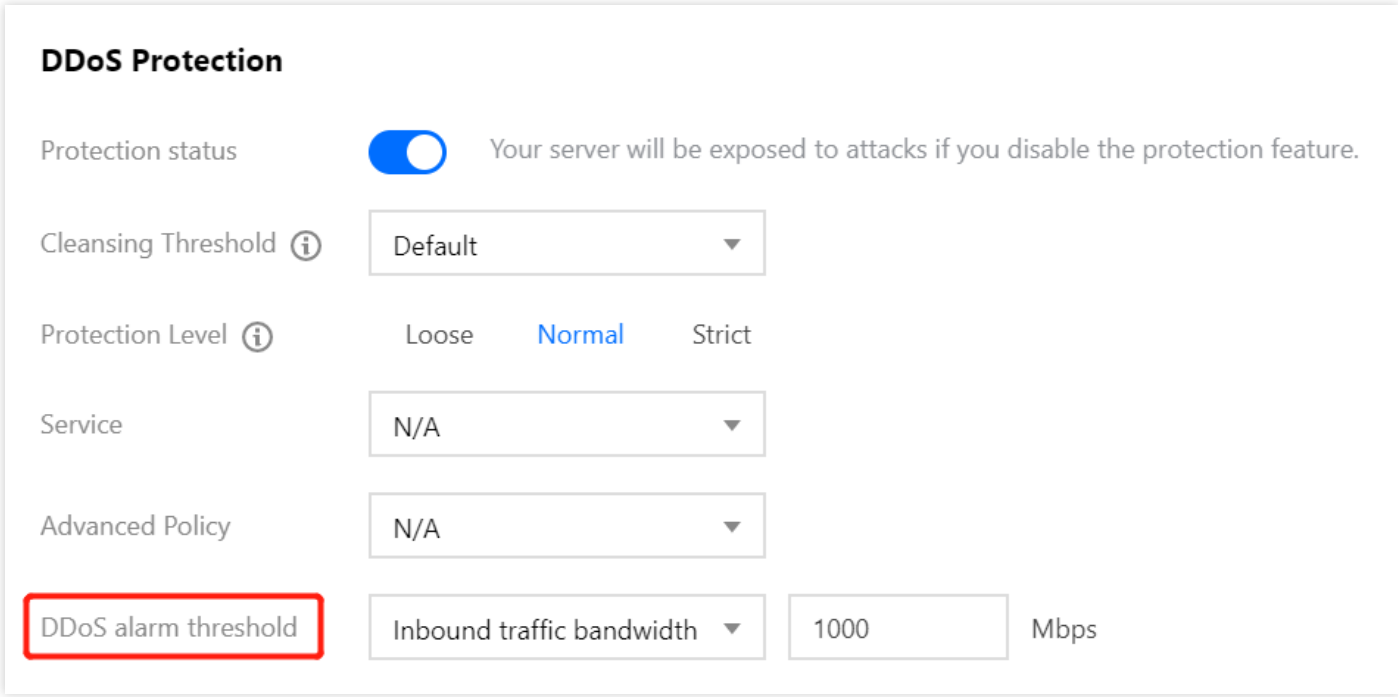
> 需要开启 DDoS 防护状态，才可设置攻击告警阈值。

1. 登录 DDoS 防护控制台，在左侧导航栏中，选择【DDoS 高防包】>【资产列表】，进入 BGP 高防包页面，单击【独享包】，找到高防包实例“bgp-000005w1”，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【入流量带宽】，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】。



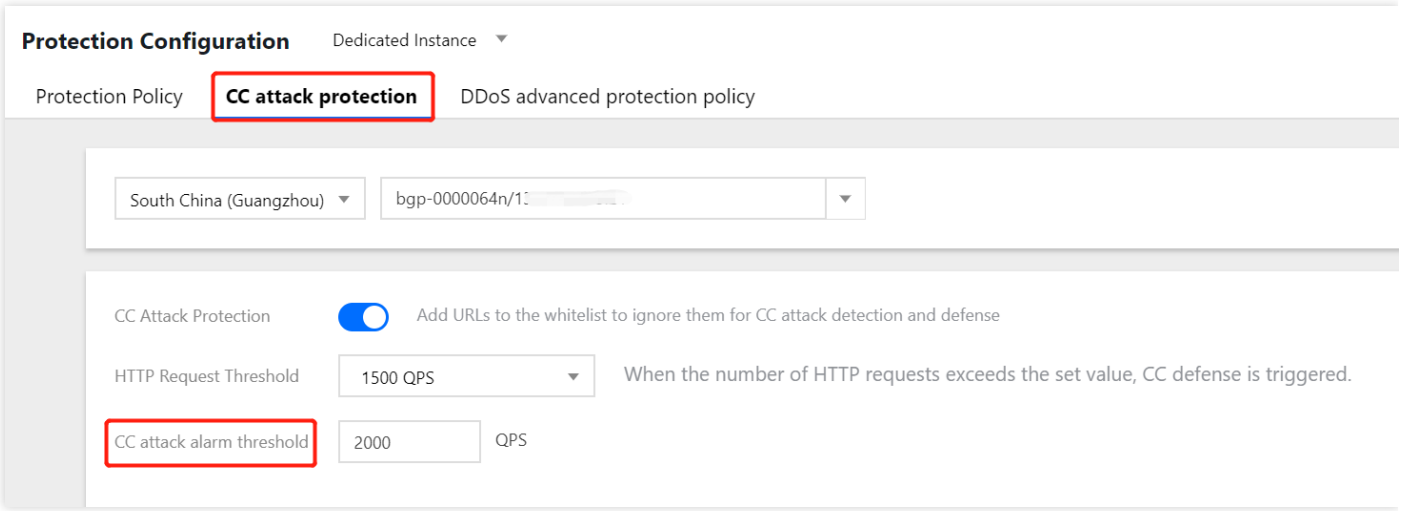
配置 CC 攻击告警阈值

本配置示例可实现如下功能：独享型高防包实例“bgp-000006i9”触发 CC 防护后，当 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 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 高防包】>【防护配置】，进入防护配置页面，选择【独享包】>【CC 防护】。

2. 开启【CC 防护】，在 CC 攻击告警阈值处，设置阈值为2000QPS。



配置智能调度

最近更新时间：2020-04-02 10:00:58

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 DDoS 高防包、DDoS 高防 IP 和 DDoS 高防 IP 专业版，其中 DDoS 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。

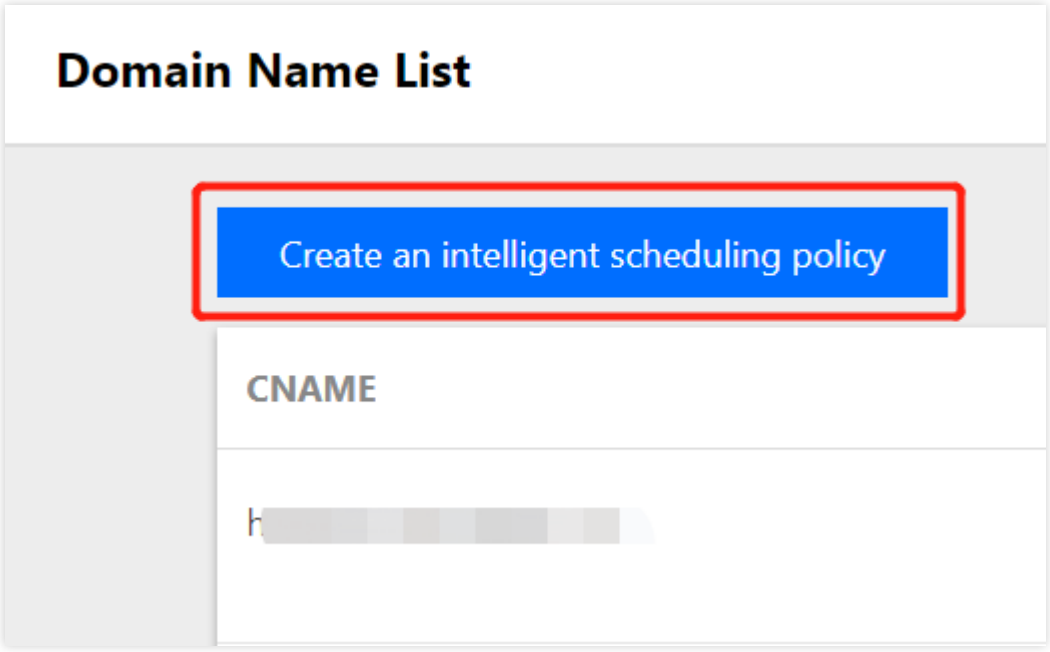
  - 若您需要将防护的云上产品 IP 添加至已购买的高防包实例，请参见 DDoS 高防包 快速入门 。
  - 若您需要将四层或七层业务添加至已购买的 DDoS 高防 IP 实例，请参见 DDoS 高防 IP 接入非网站业务 或 接入网站业务 。

- 在修改 DNS 解析前，您需要成功购买域名解析产品。

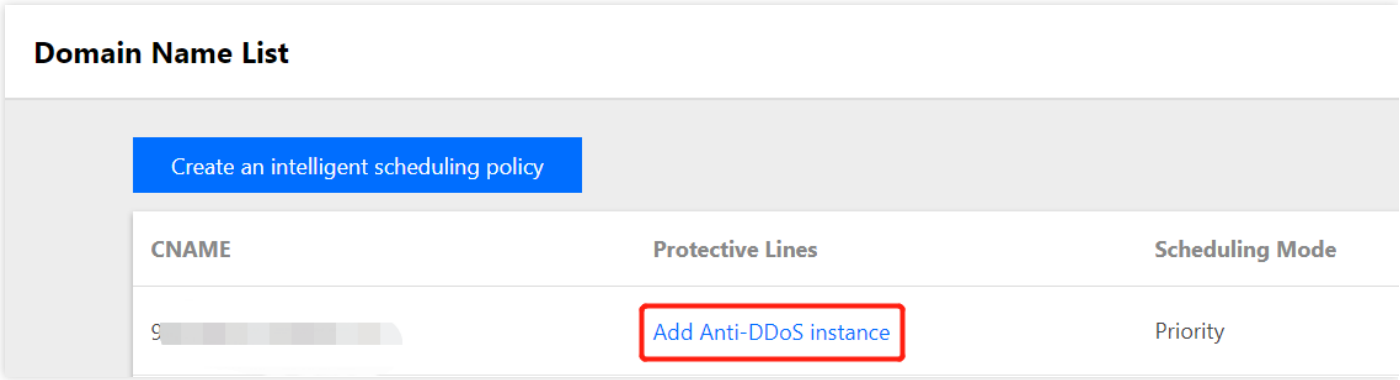
设置线路优先级

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：

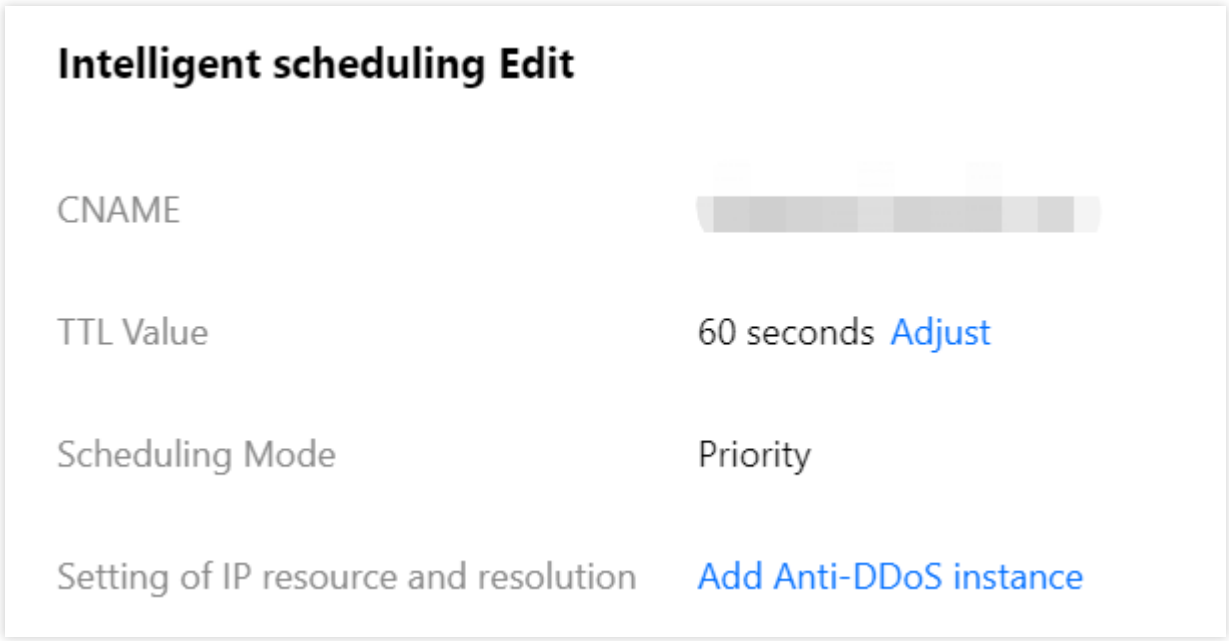
1. 登录 DDoS 防护管理控制台，在左侧导航栏选择【智能调度】>【域名列表】，进入域名列表页面，单击【创建智能调度】，系统自动生成一个 CNAME 记录。



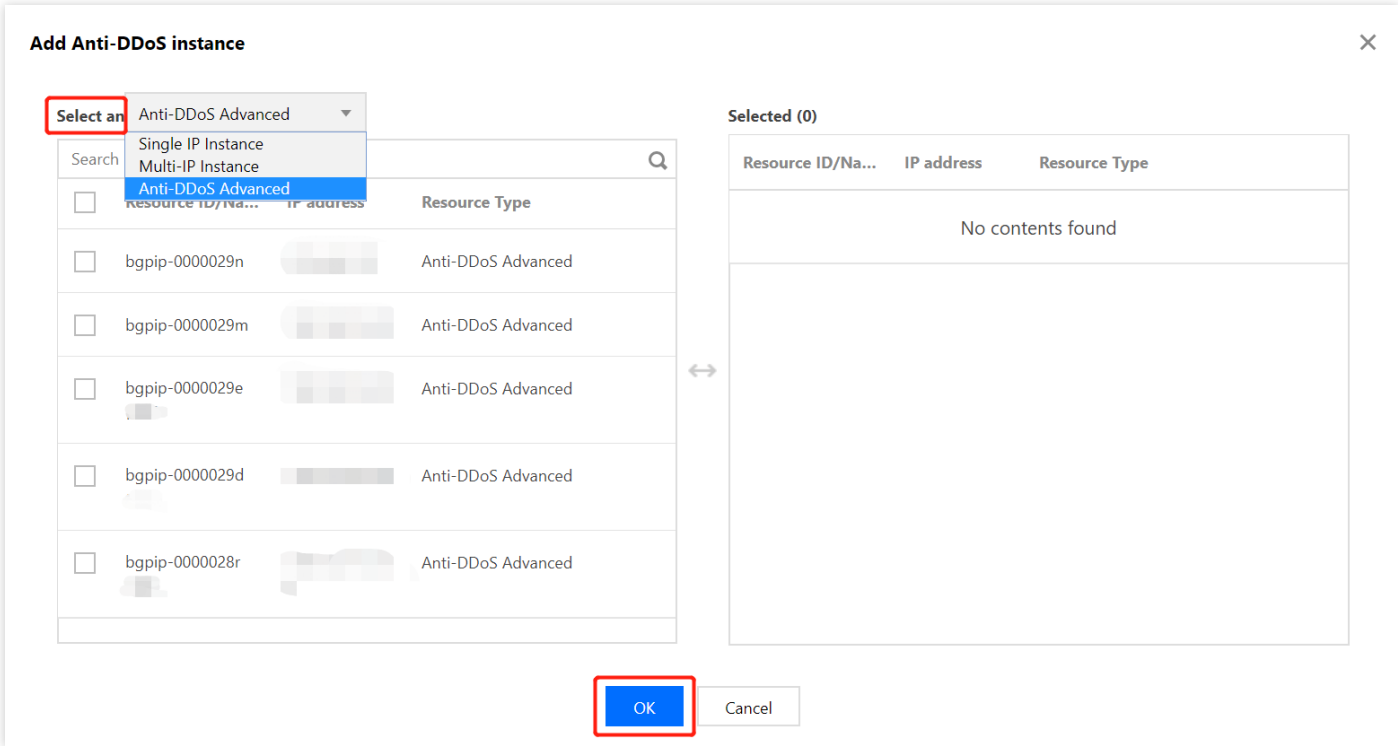
2. 找到该 CNAME 记录所在行，单击【添加高防实例】，进入智能调度编辑页面。



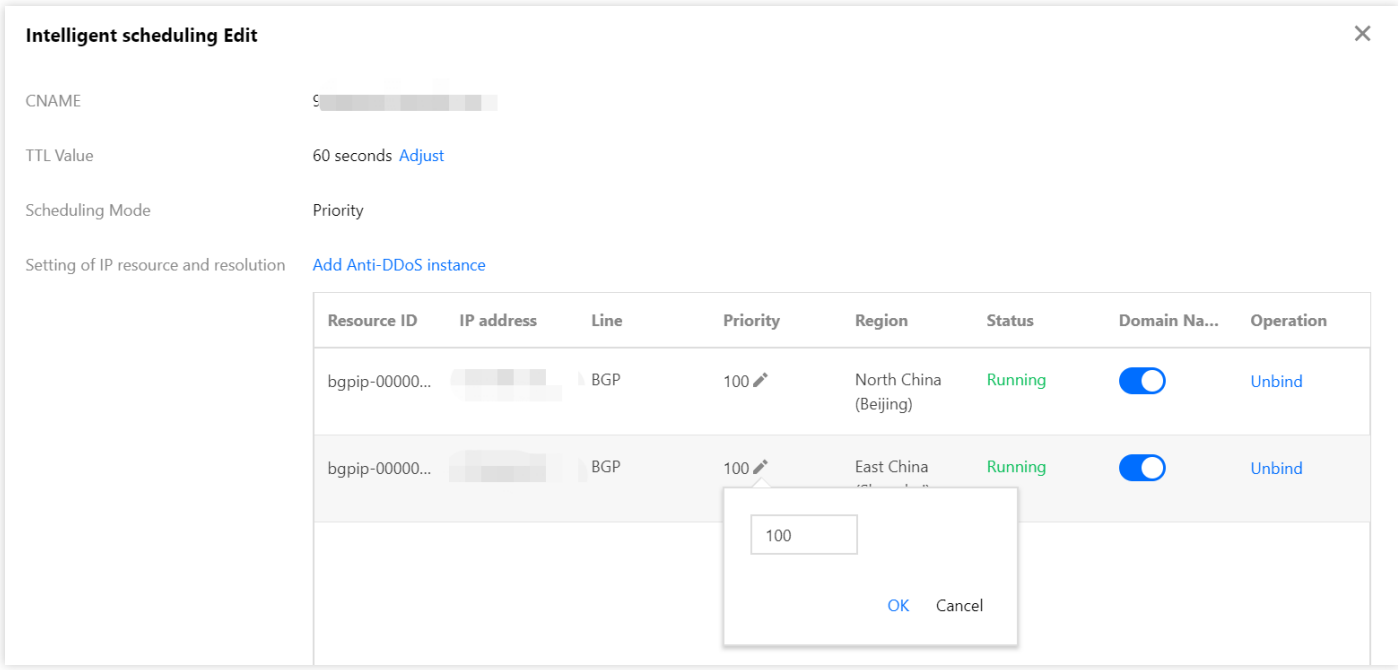
3. 在智能调度编辑页面中，TTL 值默认60秒，取值范围为1 - 3600（秒），调度方式为默认优先级。



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、DDoS 高防 IP 和 DDoS 高防 IP 专业版，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。



示例

例如，您想要将业务流量先调度到 BGP 高防线路，当 BGP 高防线路被攻击遭到封堵后，将流量自动调度到电信高防线路。如果电信高防线路也被封堵，则将流量调度到联通高防线路。当 BGP 高防线路的封堵解除后，流量将自动恢复调度至 BGP 高防线路。

优先级设置方式：您可以将防护业务的高防实例中属于 BGP 高防线路的优先级设置成1、电信高防线路的优先级设置成2、联通高防 IP 线路的优先级不变，即可满足上述调度方案。

如果您暂时不希望联通高防 IP 线路加入流量调度机制，单击  关闭域名解析即可，后面再根据需要重新开启域名解析并设置优先级。若想从当前调度机制中剔除该线路，可直接找到该线路对应实例所在行，单击【解除绑定】即可。

查看统计报表

最近更新时间：2022-05-09 17:00:19

将防护 IP 接入到 DDoS 高防包服务后，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，包括攻击流量大小、防护效果等，可在控制台进行查看。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。

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 高防包】>【统计报表】。选择【独享包】。
   说明：当选择【共享包】，可查看该类型高防包中每个防护 IP 的 DDoS 攻击防护情况。

3. 在【DDoS 攻击防护】页签，设置查询时间范围，选择目的地域和高防包实例，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包防护遭受的攻击情况，包括网络**攻击流量带宽 / 攻击包速率**趋势。
   - 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，所选择的高防包实例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，所选择的高防包实例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，所选择的高防包实例遭受的各攻击类型总次数占比情况。
   - 在“攻击来源分布”区域查看该时间范围内，所遭受 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

4. 登录 DDoS 防护管理控制台。

5. 定位到【DDoS 高防包】>【统计报表】，选择【独享包】。
   说明：当选择【共享包】，可查看该类型高防包中每个防护 IP 的 CC 攻击防护情况。

6. 单击【CC 攻击防护】页签，设置查询时间范围，选择目的地域和高防包实例，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】查看所选择的高防包的攻击请求数趋势。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，高防包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。

查看操作日志

最近更新时间：2020-04-02 10:00:58

操作场景

DDoS 高防包支持查看近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：

- 防护对象 IP 更换日志
- 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【独享包】或【共享包】，查看对应的操作记录。

> - 独享包：指提供单个 IP 独享 DDoS 防护能力的 DDoS 高防包。
> - 共享包：指提供多个 IP 共享 DDoS 防护能力的 DDoS 高防包。

设置安全事件通知

最近更新时间：2020-03-23 16:30:03

操作场景

当您所使用的高防包防护 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、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【设置】，进入设置页面。

4. 选择接收人和接收方式，单击【确定】。

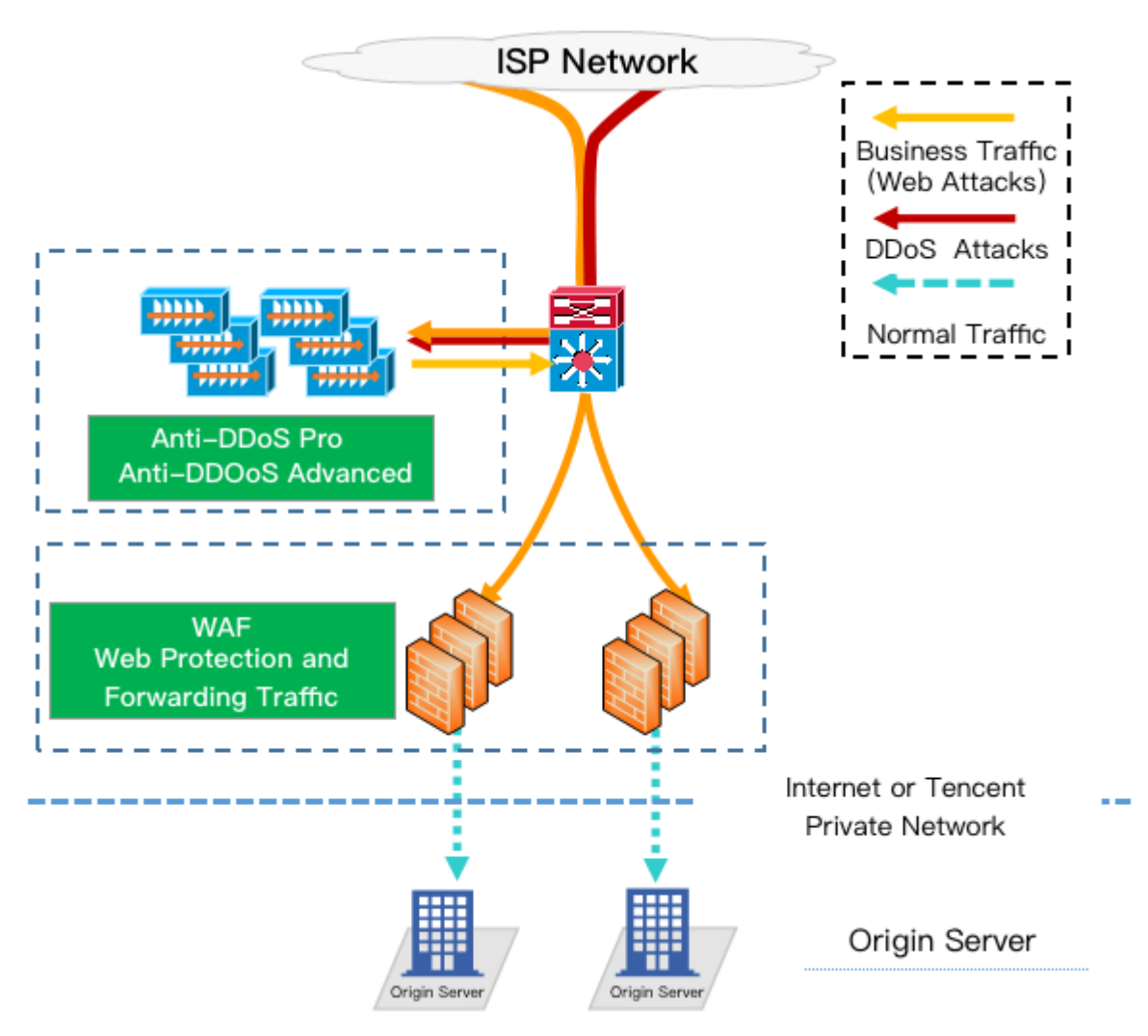
最佳实践
DDoS 高防包与 Web 应用防火墙结合使用

最近更新时间：2020-03-30 11:38:01

DDoS 高防包支持联动 Web 应用防火墙，为用户提供全方位安全防护。

- DDoS 高防包一键提供上百 Gbps DDoS 防护能力，轻松应对 DDoS 攻击，保障业务稳定运行。
- Web 应用防火墙实时防护，有效拦截 Web 攻击行为，保障用户业务的数据和信息安全。

部署方案



配置过程

配置 Web 应用防火墙

如需快速接入 Web 应用防火墙，详情请参见 Web 应用防火墙快速入门。

配置 DDoS 高防包

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择【DDoS 高防包】>【资产列表】。
   - 若您的 DDoS 高防包实例是独享包，则选择【独享包】页签。
   - 若您的 DDoS 高防包实例是共享包，则选择【共享包】页签。
2. 选择目的高防包实例所在地域，并在目的高防包实例所在行的右侧操作栏，单击【绑定设备】。
3. 在【绑定设备】页面，选择【关联设备类型】为【Web 应用防火墙】，设置【选择关联机器】为对应 Web 应用防火墙防护的 IP 地址。

   > 共享包实例可绑定多个 Web 应用防火墙防护的 IP 地址。

4. 设置完成后，单击【确定】即可。

   > 若是负载均衡型 Web 应用防火墙，在绑定界面选择【关联设备类型】为【负载均衡】，设置【选择关联机器】为对应负载均衡的公网 IP 地址。

高防包异地防护方案

最近更新时间：2020-04-02 10:00:59

需求背景

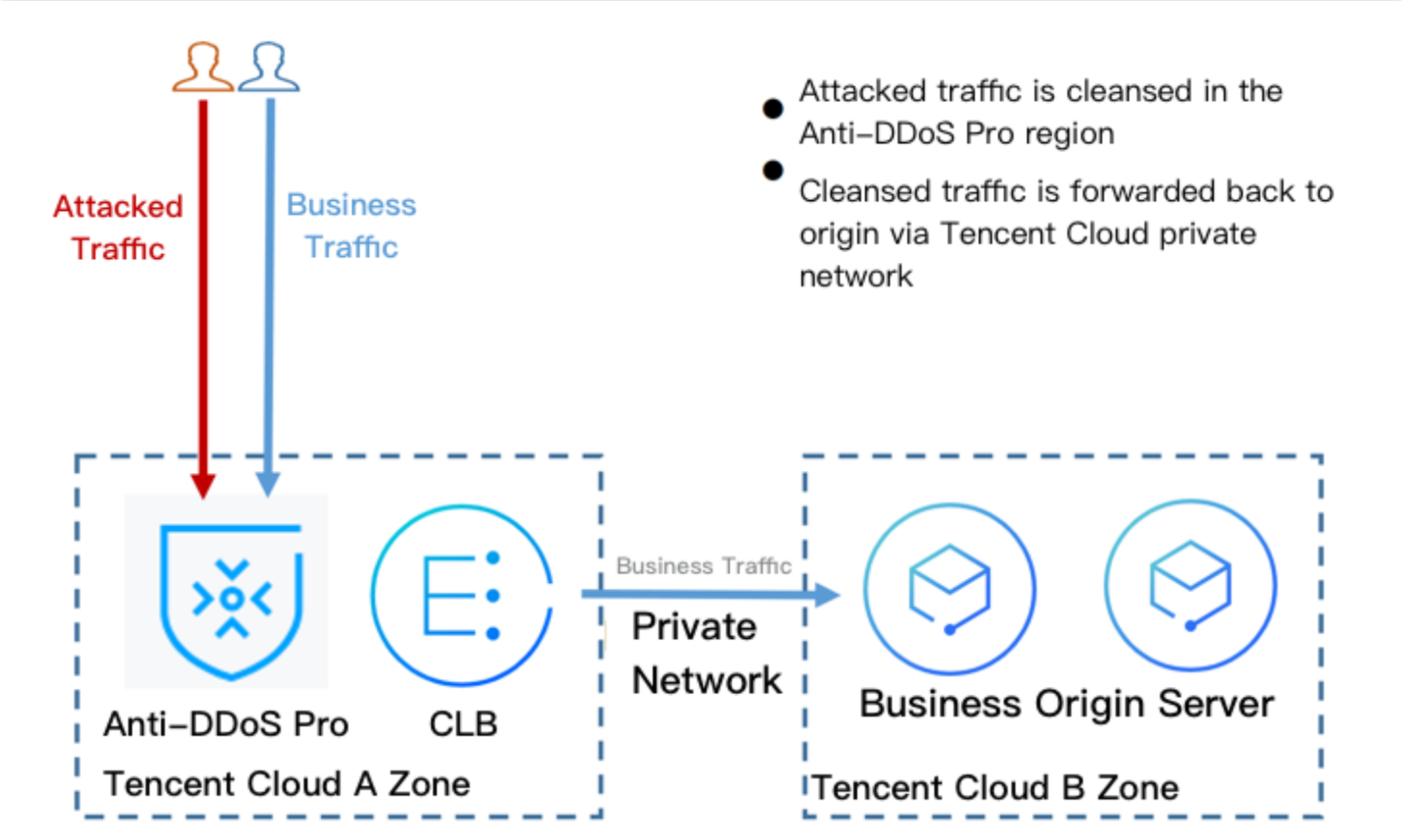
受客观因素影响，DDoS 高防包在北京、上海和广州可售卖的最大防护能力有所差异，上海可售卖的最大防护能力为300Gpbs，广州和北京两地可售卖防护能力均小于上海。除此之外，中国内地（大陆）成都、重庆等区域尚未上线高防包产品。
如果用户业务源站部署在腾讯云，并且需要使用腾讯云非源站所在地区的 DDoS 防护能力时，可参考本方案。

防护方案

本方案主要由 DDoS 高防包、CLB 负载均衡、源站业务 Server 组成。在具有 DDoS 高防包资源的地区部署 CLB 负载均衡，并将其与 DDoS 高防包进行绑定。配置 CLB 的内网回源规则，确保通过 CLB 的公网 IP 可以访问业务。

- 常态化情况下，业务可根据需要解析到源站业务的公网 IP（或直接解析到异地的 CLB 公网 IP），业务流量就近访问源站。
- 在发生攻击后，将业务解析到 CLB 的 IP，对 DDoS 攻击流量进行清洗，完成清洗后，由 CLB 通过内网专线将流量转发回到源站。

具体的防护方案如下图：



方案效果

- 打破地域防护能力的限制，可具有最大300Gpbs的 DDoS 高防包 DDoS 防护能力。
- 业务流量使用腾讯云的内网专线进行转发，可靠性高、延迟小。
- 充分享用腾讯云 DDoS 网络的优势，所有公网 IP 均为 BGP IP，延迟低。

建议与注意事项

- 提前部署 DDoS 高防包和 CLB 负载均衡。
- 建立业务可用性监测机制，在未部署自动切换机制的情况下，发现源站访问异常及时介入处理。
- 定期进行验证和演练，了解和熟悉方案细节，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：2020-04-02 10:00:59

压力测试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的建议，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：2020-04-02 10:01:00

DDoS 高防包所防护的 IP 被封堵了该怎么办？

如果正使用的 DDoS 高防包实例未调整到最高弹性防护峰值，可以在 DDoS 高防包管理控制台中更改 DDoS 高防包实例的弹性防护峰值，提升弹性防护能力，抵御更大的攻击流量。
另外，使用 DDoS 高防包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？

1. 升级保底容量后，可自动提前解封。
2. 使用 DDoS 高防包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 高防包的用户每天将拥有**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。

如何连接已被封堵的服务器？

如需进行数据迁移等操作，可参考以下两种方式连接已被封堵的服务器：

- 通过同地域的其它云服务器通过内网 IP 连接被封堵服务器。
- 通过 云服务器控制台，在被封堵服务器所在行，单击【登录】即可通过浏览器 VNC 方式连接。

怎样预防被封堵？

购买 DDoS 高防包 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。

功能相关问题

最近更新时间：2020-04-02 10:01:00

DDoS 高防包支持云外的 IP 接入防护吗？

不支持。DDoS 高防包仅对腾讯云内的公网 IP 提供 DDoS 防护支持。如需云外的防护，请 购买 DDoS 高防 IP。

如果绑定的资源已过期，DDoS 高防包实例还未过期，会怎么样？

DDoS 高防包实例是按月购买的，且以 IP 为媒介提供防护能力。如果绑定的防护对象资源过期，不及时更换 DDoS 高防包实例所绑定的 IP，那么该 DDoS 高防包实例在有效期内会持续为已绑定的 IP 提供防护，但该 IP 对应的资源不一定是您的。建议您及时为云服务续费，或更换新的防护对象 IP。

DDoS 高防包支持域名的防护吗？

不支持。若有域名防护以及应用层的防护需求，请 购买 DDoS 高防 IP。

DDoS 基础防护的防护带宽是2Gbps，又购买了 DDoS 高防包的套餐，最终的防护峰值是否会叠加？

用户享有的最终防护峰值，以 DDoS 高防包购买套餐里的防护峰值为准，不会叠加 DDoS 基础防护的默认防护带宽。
假设某云服务器的 IP 原本享有2Gbps的免费防护带宽。因经常遭受攻击，用户又为该 IP 购买了20Gbps的 DDoS 高防包套餐，则最大防护能力为20Gbps。

DDoS 高防包和 DDoS 高防 IP 的区别是什么？

- 防护对象：
  - DDoS 高防包只针对腾讯云内的服务提升 DDoS 防护能力。
  - DDoS 高防 IP 面向云外用户，为非腾讯云的业务 IP/域名提供防护。
- 接入：
  - DDoS 高防包的接入配置更加便捷，无需变更公网 IP 地址。
  - DDoS 高防 IP 需修改 DNS 解析或修改业务 IP 后才能接入防护。

DDoS 高防包与三网高防的区别是什么？

差异点	DDoS 高防包	三网高防
接入成本	无需更换服务器 IP，直接为云产品提升防御能力，即时生效，接入成本低	需要将服务器 IP 更换为三网 IP，填写域名与端口信息，配置相当复杂
访问质量	采用 BGP 带宽，减少跨网访问延迟，访问速度提升30%以上	无 BGP 带宽，网络延迟大，质量不佳

差异点	DDoS 高防包	三网高防
定价策略	计费灵活，支持保底+弹性，可共享	计费复杂，需要付流量费

计费相关问题

最近更新时间：2019-09-26 11:10:19

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 高防包实例规格是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 高防包所防护的 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 高防包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。不支持保底防护进行扩展或降配。

业务遭受攻击过程中，是否支持升级弹性防护峰值？

支持。BGP 高防包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 计费概述。

> 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 高防包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的攻击流量峰值都超过保底防护，且都在弹性防护范围内，则需要分别收取两个高防实例的弹性防护费用。