DDoS 防护

操作指南

腾讯云

文档目录

操作指南
操作概览

最近更新时间：2025-06-10 15:12:42

您在使用 DDoS 基础防护、DDoS 高防包、DDoS 高防 IP 时，可能碰到例如配置实例、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 防护的常用操作，供您参考。

概览与限制

- 防护概览（总览）
- 使用限制

资产中心

- 云资产列表
- 云上防护实例
  - 查看实例信息
  - 管理防护对象
  - 设置实例别名与标签
  - 升级防护
  - 修改弹性防护宽带
  - 续费实例
  - 删除实例
  - 解封防护 IP

业务接入

- IP 透明接入
- 域名接入
- IP 接入
- 端口接入
- 配置会话保持
- 配置健康检查

调度与解封

智能调度

防护配置

DDoS 防护

- DDoS 防护等级
- IP 黑白名单
- 端口过滤

- 协议封禁
- 水印防护
- 连接类攻击防护
- AI 防护
- 区域封禁
- IP 端口限速
- 特征过滤

CC 防护

- CC 防护开关及清洗阈值
- 智能 CC 防护
- 精准防护
- CC 频率限制
- 区域封禁
- IP 黑白名单

安全运营

- 攻击分析
- 业务分析
- 操作日志
- 日志服务
  - 日志投递

服务管理

解封中心

- 查看封堵时间
- 解除封堵
- 连接已被封堵的服务器

告警中心

- 设置安全事件通知
- 设置通知方式

防护概览（总览）

最近更新时间：2024-04-18 15:48:52

查看攻击态势

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**防护概览** > **防护总览**，进入防护总览页面。
2. 在实时防御态势模块中，展示业务 IP 状态数据，可以快速了解业务 IP 健康状态。

3. 在攻击态势模块中，还可以直观查看各项数据情况。

字段说明：

- 总攻击次数：受到攻击的总数，包括基础防护的业务、接入高防实例。
- 被攻击 IP 数：受到攻击的业务 IP 总数。包括基础防护被攻击 IP 数、接入高防包后被攻击的业务 IP 数、高防 IP 实例被攻击数。
- 被封堵 IP 数：被屏蔽所有外网访问的业务 IP 数。包括基础防护的业务 IP、接入高防包的业务 IP 和高防 IP 实例。
- 攻击峰值：当前攻击事件中的最高攻击带宽。
- 攻击包速率：当前攻击事件中的最高攻击包速率。
- 攻击请求峰值：当前攻击事件中最高攻击请求。

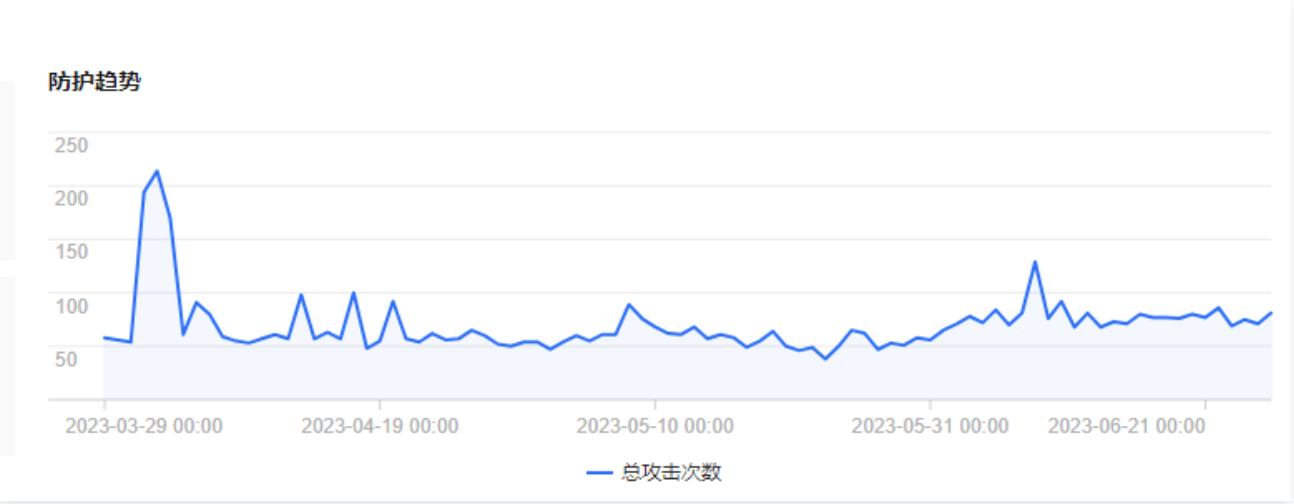
查看防御态势

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**防护概览** > **防护总览**，进入防护总览页面。
2. 在实时防御态势模块中，展示业务 IP 状态数据，可以快速了解业务 IP 健康状态。

字段说明：

- IP 总数：当前全部业务 IP 总数，包括基础防护的业务 IP、接入高防包的业务 IP 和高防 IP 实例。
- 已防护 IP 数：接入高防包的业务 IP 和高防 IP 实例。
- 封堵 IP 数：被屏蔽所有外网访问的业务 IP 数。包括基础防护的业务 IP、接入高防包的业务 IP 和高防 IP 实例。

3. 在防御态势模块的防护趋势中，展示一周内全量业务受攻击总次数的，可以快速了解近期攻击状态分布情况。



4. 在防御态势模块的防护建议中，展示基础防护状态下受到攻击的业务 IP，提示接入高级防护。方便用户快速为被攻击 IP 接入高级防护，保证业务安全。

查看防护实例详情

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**防护概览** > **防护总览**，进入防护总览页面。
2. 在防护实例详情模块中，展示高防资源的安全状态，可以快速全面了解风险业务分布。右侧展示防护配额状态，可以快速了解高防包、高防 IP 已用防护配额。

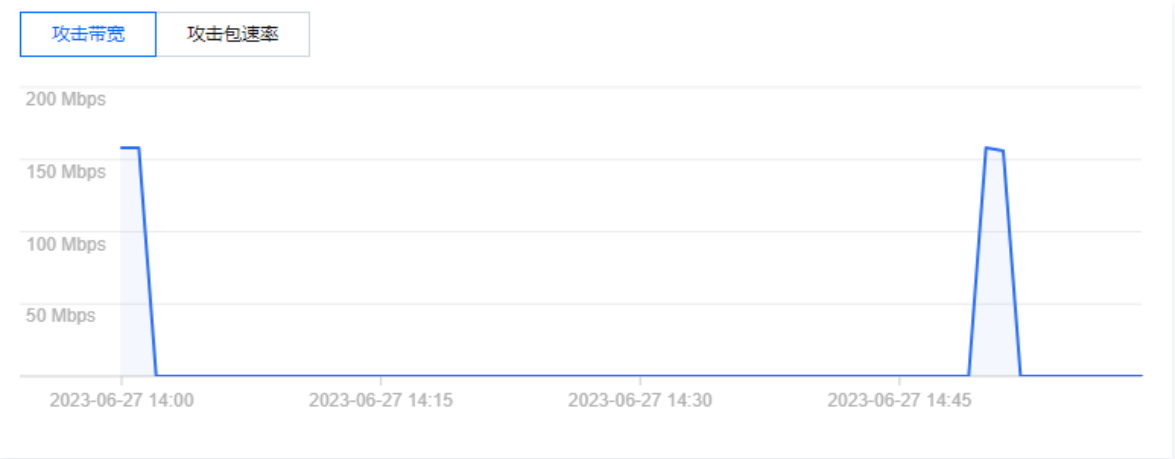
查看近期安全事件

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**防护概览** > **防护总览**，进入防护总览页面。
2. 在近期安全事件模块中，展示最近全量的攻击事件。单击**查看详情**，进入事件详情页面，供用户进行 DDoS 攻击分析及溯源支撑。

3. 在事件详情页面的攻击信息模块，查看该时间范围内的 IP 遭受的攻击情况，包括被攻击 IP、状态、攻击类型（采样数据）、攻击带宽峰值和攻击包速率峰值、开始时间结束时间基础信息。

4. 在事件详情页面的攻击趋势模块，可查看网络攻击流量带宽或攻击包速率趋势。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。

> **说明：**
> 此处数据为该攻击时间段全量实时数据。



5. 在事件详情页面的攻击统计模块，可通过攻击流量协议分布、攻击类型分布，查看这两个数据维度下的攻击分布情况。

> **说明：**
> 此处数据为该攻击时间段内攻击采样数据，非全量数据。

字段说明：

- 攻击流量协议分布：查看该时间范围内，所选择的 DDoS 防护实例遭受攻击事件中各协议总攻击流量的占比情况。
- 攻击类型分布：查看该时间范围内，所选择的 DDoS 防护实例遭受的各攻击类型总次数占比情况。

6. 在事件详情页面 “TOP5 展示”模块，可查看攻击源 IP TOP5 和攻击源地区TOP5，准确把握攻击源的详细情况便于精准防护策略的制定。

> **说明：**
> 此处数据为该攻击时间段内攻击采样数据，非全量数据。

7. 在事件详情页面的攻击源信息模块，可查看该攻击时间段内攻击详情的随机采样数据，尽可能详细的展示出此次攻击的细节，主要包括攻击源 IP、地域、累计攻击流量、累计攻击包量。

> **说明：**
> 此处数据为该攻击时间段内攻击采样数据，非全量数据。

8. 在近期安全事件模块中，可展示所遭受的 DDoS 攻击事件。
   - 选择所需事件，单击**查看详情**，右侧将展示该事件的具体详情。支持查看攻击源信息、攻击源地区、产生的攻击流量及攻击包量大小等。供用户进行 DDoS 攻击分析及溯源支撑。

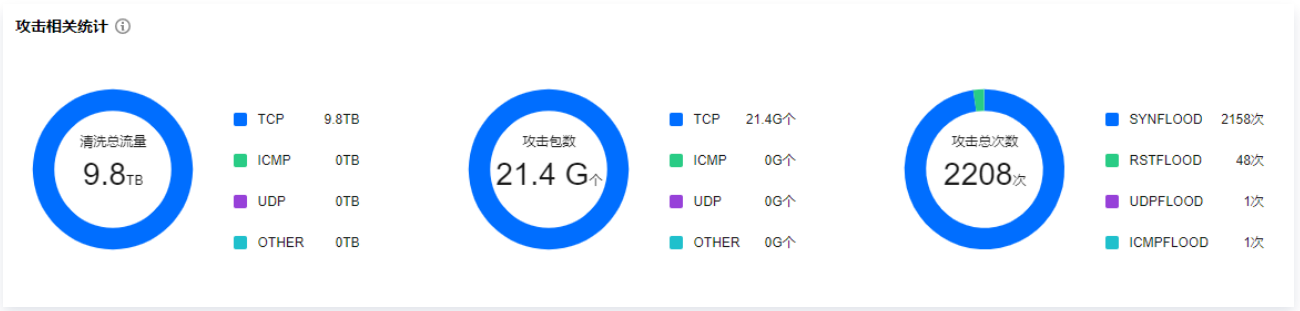
   - 选择所需事件，单击攻击包下载，在攻击包列表中，选择所需 id，可下载本次攻击计时间段的攻击包采样数据，详细了解攻击数据和类型，用户制定针对性的防护方案提供数据支撑。

查看 DDoS 攻击防护情况

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**防护概览** > **攻击态势**。
2. 在 DDoS 攻击页签，设置查询时间范围，选择目的地域、线路和高防包实例，查看是否存在攻击。默认展示全量资产的 DDoS 攻击数据。

3. 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和攻击包速率趋势。

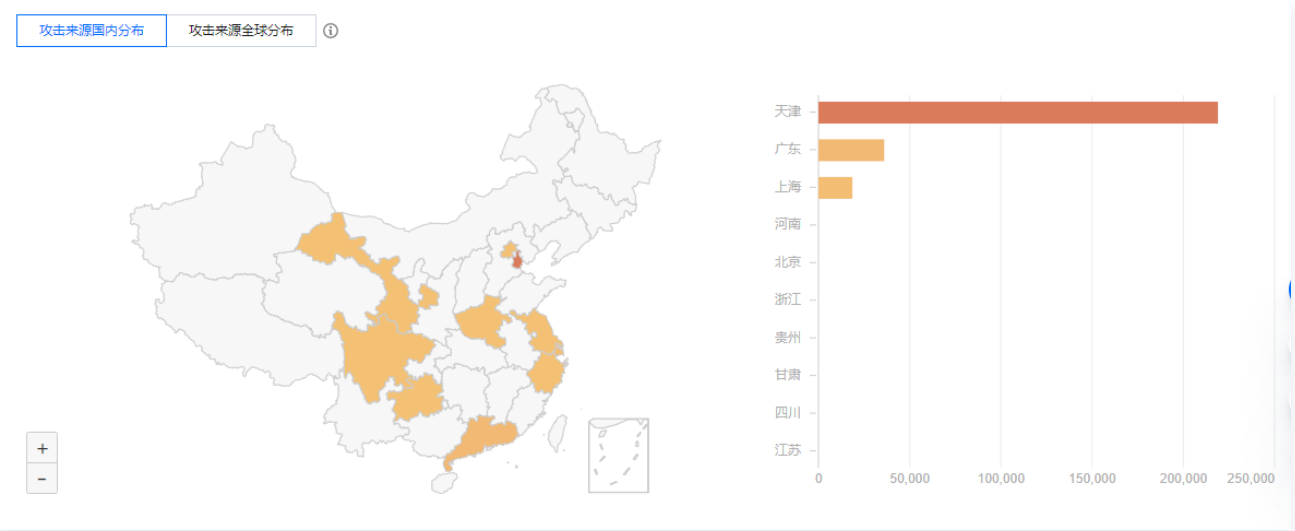
4. 在攻击统计模块中，可通过攻击流量协议分布、攻击包协议分布和攻击类型分布，查看这三个数据维度下的攻击分布情况。



字段说明：

- 攻击流量协议分布：查看该时间范围内，所选择的DDoS 防护 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DDoS 防护 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DDoS 防护 实例遭受的各攻击类型总次数占比情况。

5. 在攻击来源模块中，可查看该时间范围内，所遭受 DDoS 攻击事件的攻击源在国内、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。



查看 CC 攻击防护情况

1. 单击 CC 攻击页签，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。

2. 用户可以选择所需时间，查看所选择的高防实例求数趋势和请求速率的相关数据。通过观察总请求速率、攻击请求速率、总请求数量、攻击请求次数相关数据判定业务受影响程度。

字段说明：

- 总请求速率：统计当前，高防实例接收到的总请求流量的速率（QPS）。
- 攻击请求速率：统计当前，攻击请求流量的速率（QPS）。
- 总请求数量：统计当前，高防实例接收到的总请求数量。
- 攻击请求次数：统计当前，高防实例接收到的攻击请求的次数。

3. 在近期安全事件模块中，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、总请求峰值、攻击请求峰值和攻击源等信息。单击**查看详情**，展示该事件的具体详情。支持查看攻击信息、攻击趋势、CC 详细记录。

使用限制

最近更新时间：2023-09-22 16:05:22

DDoS 基础防护

防护对象限制

为腾讯云内 CVM、CLB 及 NAT 网关等云产品，提供免费的基础 DDoS 防护。

DDoS 高防包

防护对象限制

DDoS 高防包仅适用于腾讯云产品，包含 CVM、CLB、WAF、NAT 网关、VPN 网关、轻量应用服务器等。

接入限制

DDoS 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条记录（IP 地址 + IP 段）。
- CC URL 白名单暂不支持配置。

地域限制

DDoS 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：北京、上海、广州、中国香港、新加坡、首尔、东京、曼谷、法兰克福。

> **说明：**
> 当前 DDoS 高防包境外区域通过开白名单的形式进行售卖，如需购买境外区域的 DDoS 高防包，可以直接 联系我们 开白名单。

DDoS 高防 IP

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。

转发能力限制

1个 DDoS 高防 IP 实例默认支持60个转发规则（四层接入加七层接入共60个），最高支持500个转发规则，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。

> **说明：**
> 转发规则数为 TCP/UDP 协议 + HTTP/HTTPS 协议转发规格条目总数，最高可升级至 500条。对于 TCP、UDP 协议，若使用相同的转发端口值，则需要配置两条。

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。
- URL 不支持白名单配置。

地域限制

目前已开放 DDoS 高防 IP 的地域覆盖中国大陆区域和非中国大陆区域，非中国大陆区域包括中国香港、中国台湾、新加坡、首尔、东京、弗吉尼亚、法兰克福。

资产中心
云资产列表

最近更新时间：2025-01-24 14:25:42

查看资产安全状态

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**云资产列表**页面。
2. 在资产安全状态模块中，展示业务 IP 安全状态数据，可以快速了解业务 IP 安全状态。

3. 在资产防护状态模块中，展示业务 IP 防护状态数据，可以快速了解业务 IP 安全状态，可直接接入防护。

查看资产实例详情

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**云资产列表**页面。
2. 以云主机为例。在详情页面可以查看该资产的详细信息，包括资产实例名称、IP 地址、防护类型、防护实例ID、防护能力、攻击状态等信息。

使用 DDoS 高防可为如下产品提升 DDoS 防护能力：

- 云服务器：是腾讯云提供的可扩展的计算服务。使用云服务器 CVM 避免了使用传统服务器时需要预估资源用量及前期投入的问题，帮助您在短时间内快速启动任意数量的云服务器并即时部署应用程序。
- 负载均衡：提供安全快捷的流量分发服务，访问流量经由 CLB 可以自动分配到云中的多台云服务器上，扩展系统的服务能力并消除单点故障。
- Web 应用防火墙：是一款基于 AI 的一站式 Web 业务运营风险防护方案。

- NAT 网关：是一种支持 IP 地址转换服务，提供 SNAT 和 DNAT 能力，可为私有网络（VPC）内的资源提供安全、高性能的 Internet 访问服务。
- VPN 连接：是一种基于网络隧道技术，实现本地数据中心与腾讯云上资源连通的传输服务，它能帮您在 Internet 上快速构建一条安全、可靠的加密通道。
- 裸金属云服务器：是一种可按需购买、按量付费的物理服务器租赁服务，提供给您云端专用的高性能、安全隔离的物理服务器集群。
- 全球应用加速：全球应用加速（Global Application Acceleration Platform，GAAP）依赖全球节点之间的高速通道、转发集群及智能路由技术，实现各地用户的就近接入，通过高速通道直达源站区域，帮助业务解决全球用户访问卡顿或者延迟过高的问题。
- 弹性网卡：是绑定私有网络（VirtualPrivate Cloud，VPC）内云服务器的一种弹性网络接口，可在多个云服务器间自由迁移。弹性网卡对配置管理网络与搭建高可靠网络方案有较大帮助。
- 轻量应用服务器：是新一代开箱即用、面向轻量应用场景的云服务器产品，助力中小企业和开发者便捷高效的在云端构建网站、Web 应用、小程序/小游戏、App、电商应用、云盘/图床和各类开发测试环境，相比普通云服务器更加简单易用且更贴近应用，以套餐形式整体售卖基础云资源并提供高带宽流量包，将热门开源软件融合打包实现一键构建应用，提供极简上云体验。

管理云资产

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**云资产列表**。
2. 在云资产列表页面，可单击上方的产品，找到该产品的资产。如果实例数量较多可以使用右上角的搜索框过滤。

3. 选中所需资产后，可以对该资产进行如下操作：
   - 单击**设置告警阈值**，可以根据需求自定义告警策略，单击**确定**。

   - 升级防护，当业务增长需要同一个高防包防护多个业务 IP 时，可以升级防护为覆盖所有业务 IP 的防护。详情请参见 升级防护 。

- 单击**攻击分析**，页面跳转至防护概览（总览）页面，查看攻击态势。

- 单击**防护配置**，页面跳转至 DDoS 防护页面，查看 DDoS 防护配置。

云上防护实例
查看实例信息

最近更新时间：2024-04-18 15:48:52

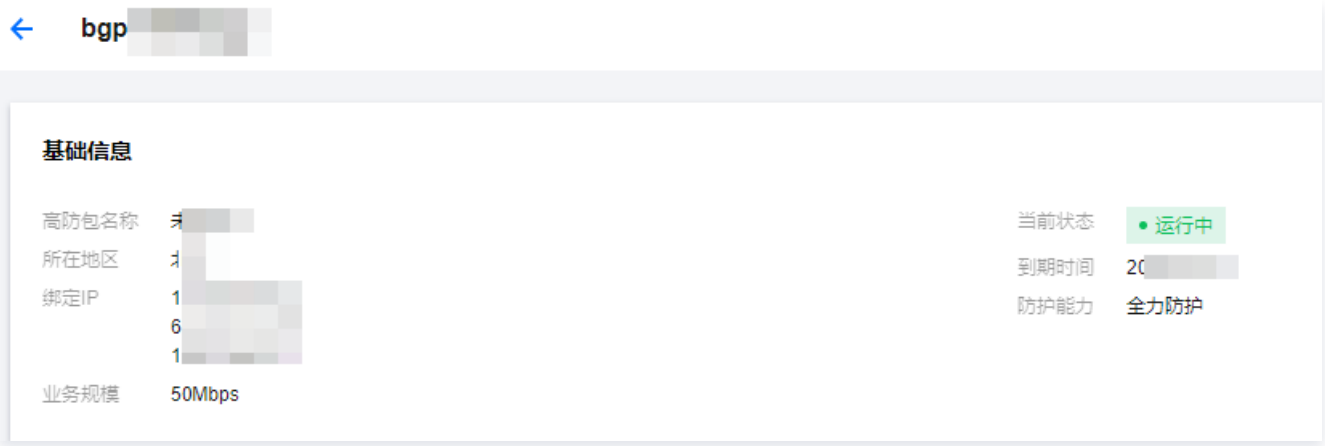
1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**云上防护实例**，进入云上防护实例页面。
2. 在云上防护实例页面，支持查看所购买的 DDoS 高防包的基础信息（如实例保底防护峰值、运行状态）；所购买的 DDoS 高防 IP 的基础信息（如实例保底防护峰值及运行状态）及实例的弹性防护配置。

操作步骤

示例：查看 DDoS 高防包 “bgp-00000jt3”的实例信息

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**云上防护实例**，进入云上防护实例页面。
2. 在云上防护实例页面，可单击上方的**全部地域**选择地域或选择**防护套餐类型**，找到实例 ID 为 “bgp-00000jt3”的高防包，单击 ID “bgp-00000jt3”查看实例详细信息。如果实例数量较多可以使用右上角的**搜索框**过滤。

3. 在弹出的页面中查看如下信息：



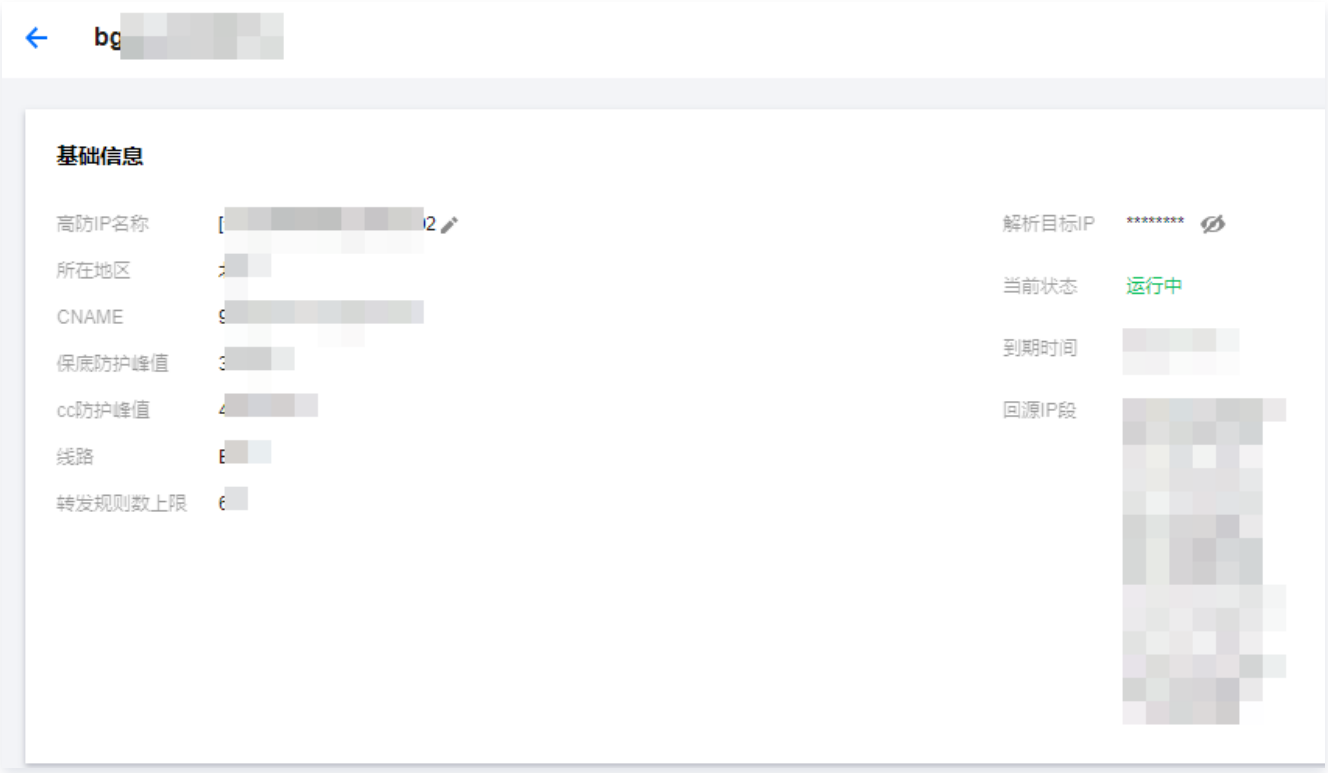
参数名称	说明
高防名称	该 DDoS 高防包实例的名称，用于辨识与管理 DDoS 高防实例。长度为1 - 20个字符，不限制字符类型。资源名称由用户根据实际业务需求自定义设置。
所在地区	为购买 DDoS 高防 时选择的地域。
当前状态	DDoS 高防例当前的使用状态。状态包括运行中，清洗中以及封堵中等。 • 创建中：正在创建高防实例。 • 运行中：实例防护进行中。 • 受攻击：遭受攻击。 • 封堵中：正在对实例进行封堵。

	• 解封中：实例正在解封中。 • 回收中：实例已到期，正在进行回收。
到期时间	根据购买时选择的购买时长以及支付购买订单的具体时间计算所得，精确到秒级。DDoS 高防资源到期前7天内，系统会向您推送资源即将到期提醒，消息通过站内信、短信、邮件、微信等方式（实际接收方式以您在消息中心订阅配置为准）通知到腾讯云账号创建者以及所有协作者。具体详情请参见 欠费说明 。

示例：查看高防 IP 实例“bgpip-0000070j”的实例信息

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**云上防护实例**，进入云上防护实例页面。
2. 在云上防护实例页面，选择所需实例 ，单击 “ID”查看实例详细信息。如果实例数量较多可以使用右上角的搜索框过滤。

3. 在弹出的页面中查看如下信息：



参数名称	说明
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。
解析目标 IP	该 DDoS 高防 IP 实例具有高防属性的 IP。此 IP 地址将不定期更换。 **注意：建议将您的 DNS 解析地址修改至 CNAME，避免 DNS 解析失败。**

所在地区	购买 DDoS 高防 IP 时选择的地域。
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。
CNAME	该 DDoS 高防 IP 实例的 CNAME。由该 CNAME 解析至拥有高防属性的 IP 上，通过清洗中心后并转发回源站，实现防护。 **注意：建议将您的 DNS 解析地址修改至 CNAME，避免 DNS 解析失败。**
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。
到期时间	根据购买时选择的购买时长以及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 IP 实例所属的标签名称，可以编辑、删除。
回源 IP 段	清洗集群转发至源站所用 IP。

管理防护对象

最近更新时间：2025-02-10 10:57:53

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，可以增加或删除 DDoS 高防包实例的防护对象 IP。

前提条件

设置防护对象 IP，您需要成功 购买 DDoS 高防包 。

> **说明：**
> DDoS 高防包（企业版）仅针对腾讯云弹性公网 IP下的高防 EIP 生效，使用企业版高防包需要将云上普通 IP 更换为高防 EIP，购买企业版高防包需与最终绑定云资源的地域相同，并绑定高防 EIP后才实际生效。高防 EIP 操作详情请参见 高防 EIP 创建使用指引 。

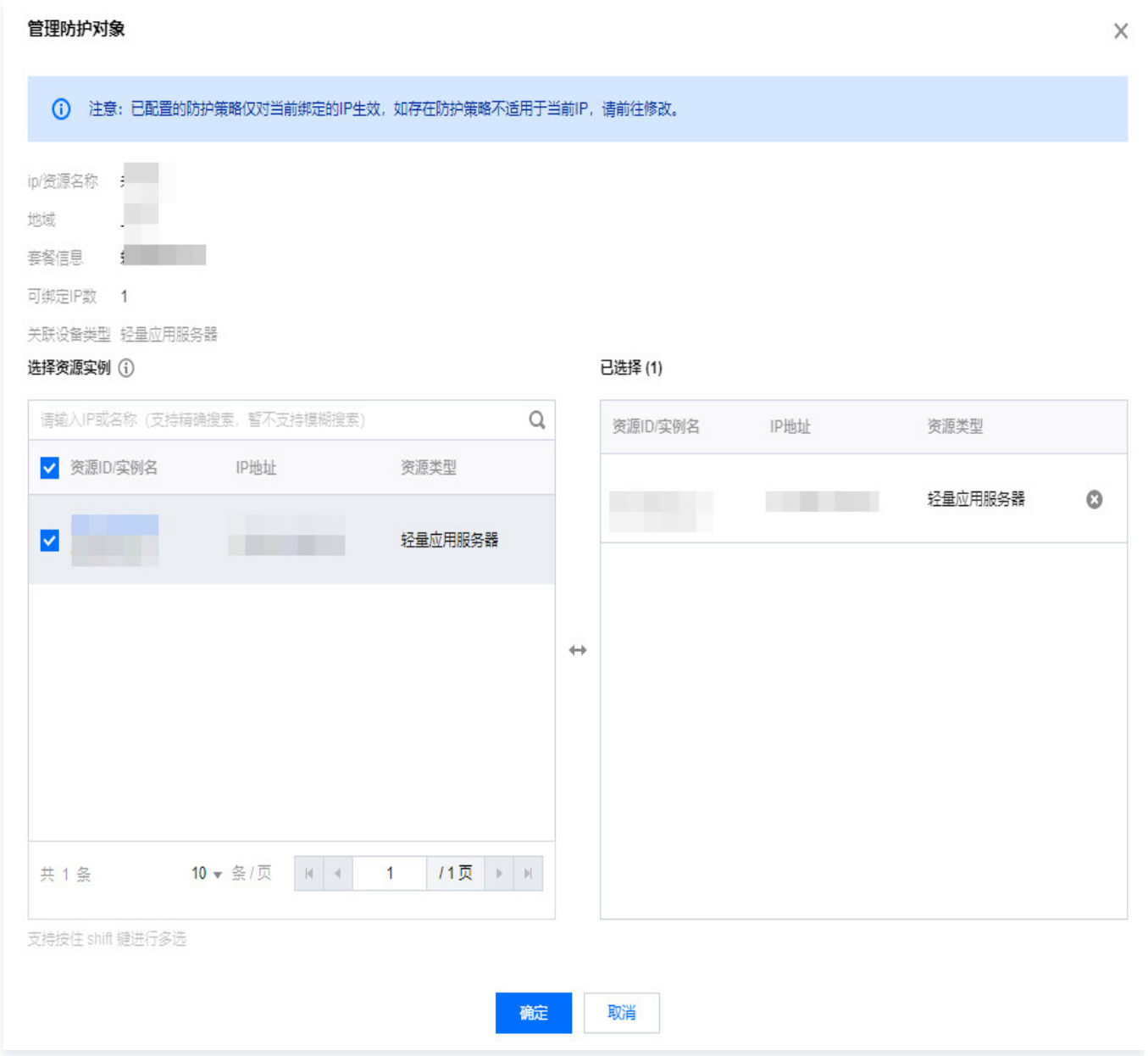
操作步骤

1. 登录 DDoS防护（新版）控制台，在左侧导航中，单击**云上防护实例**。
2. 在云上防护实例页面，单击目标 DDoS 高防包实例所在行的**管理防护对象**。

3. 在**管理防护对象**页面，根据实际防护需求选择关联设备类型与资源实例。
   - 关联设备类型：支持云主机，负载均衡，Web 应用防火墙等公有云具有公网 IP 的资源。

     > **说明：**
     > 高防包企业版仅支持高防 EIP。

   - 选择资源实例：单击资源 ID 前面的选项复选框，将资源添加到高防包的防护对象，允许多选，选择资源实例数量不得超过可绑定 IP 数。
   - 已选择：单击资源后面的**删除**，将资源从高防包的防护对象中删除。



说明：

- DDoS 高防包如果有 IP 处于被攻击中或封堵状态下，则不允许用户解绑该 IP。
- 当关联云资产时，支持批量搜索和选择。
- 当前支持检测 CLB、 CVM 产品的销毁状态，并进行解绑。

4. 单击**确定**即可。

设置实例别名与标签

最近更新时间：2024-04-18 15:48:52

使用多个 DDoS 高防包实例或 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。

前提条件

您需要成功购买 DDoS 高防包 或 DDoS 高防 IP。

操作步骤

方式一

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**云上防护实例**。
2. 在云上防护实例页面，单击目标实例的“ID/名称”列的第二行 ，输入名称即可。

> **说明：**
> 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（新版）控制台，在左侧导航栏中，单击**云上防护实例**。
2. 在云上防护实例页面，单击目标实例的“ID/名称/标签”列的实例 ID，进入实例的基础信息页面。

3. 在实例的基础信息页面中，单击高防包名称或高防 IP 名称右侧的 ，输入名称即可。

> **说明：**
> 名称长度为1 - 20个字符，不限制字符类型。


bgp
基础信息
名称
未命名
所在地区
绑定IP
业务规模

升级防护

最近更新时间：2025-01-24 14:25:42

当业务增长需要同一个高防防护多个业务 IP 时，可以升级防护为覆盖所有业务 IP 的防护。

前提条件

设置防护对象 IP，您需要成功购买 DDoS 高防包 或 DDoS 高防 IP 。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航中，单击**云上防护实例**。
2. 在云上防护实例页面，选择目标实例，单击**升级**。

3. 在升级页面，根据实际防护需求选择 IP 数量、防护次数和业务规模。
   - IP 数量：升级高防支持的 IP 数量。
   - 防护次数：升级高防一个月防护的次数。
   - 业务规模：被防护业务的正常业务规模，可按照预估业务入方向或出方向流量最大峰值选择。

4. 单击**确定接入**完成支付，即可升级。

修改弹性防护带宽

最近更新时间：2024-09-19 15:57:53

弹性防护峰值指 DDoS 高防服务可提供抵御攻击流量的能力范围。若攻击流量超过最高防护峰值，则被攻击 IP 将触发封堵。

前提条件

您需要成功 购买 DDoS 高防 IP 。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**云上防护实例**。
2. 在目标 DDoS 高防 IP 实例所在行的防护规格中，单击弹性峰值后 。

3. 在设置弹性防护弹框中，根据实际防护需求选择弹性防护峰值。

> **说明：**
> 由于弹性防护峰值和费用受到不同地区以及不同版本的影响，实际弹性防护峰值和费用以控制台显示为准。

4. 选择完成后，单击**确定**即可。

续费实例

最近更新时间：2024-04-18 15:48:52

DDoS 高防包 / DDoS 高防 IP 的到期时间即将临近，续费高防包享受连续稳定的 DDoS 防护。

前提条件

设置防护对象 IP，您需要成功 购买 DDoS 高防包 或 DDoS 高防 IP 。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**云上防护实例**。
2. 在目标 DDoS 高防包/高防 IP 实例所在行右侧操作栏，单击**续费**。

3. 在续费页面，根据实际防护需求选择续费时长：
   - DDoS 高防包：续费时长支持3个月、6个月、1年、2年、3年。

   - DDoS 高防 IP：续费时长支持1个月、2个月、3个月、4个月、5个月、6个月、1年、2年、3年。

4. 单击**确定**完成支付流程即可。

删除实例

最近更新时间：2024-09-19 15:57:53

当实例不再使用，可以 联系我们 将实例进行删除。

注意：

- 读写实例删除后，数据将无法找回。
- 实例删除后 IP 资源同时释放，删除前请确认无业务访问该实例。

解封防护 IP

最近更新时间：2024-10-17 21:14:31

DDoS 防护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（新版）控制台 进行自助解封操作。

自助解封次数

使用 DDoS 高防包或 DDoS 高防 IP 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。

> **说明：**
> - 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，建议增加防护 IP 数量和防护次数，以便足够防御大流量攻击，避免被持续封堵。
> - DDoS 高防包（轻量版）解封次数为每月三次。

自助解封操作

1. 登录 DDoS防护（新版）控制台，在左侧导航中，单击**解封中心**。
2. 在解封操作页面，找到状态为“自动解封中”的防护 IP，单击**解封**。

解封操作记录

1. 登录 DDoS防护（新版）控制台，在左侧导航中，选择**解封中心** > **解封记录**。
2. 在解封记录页面，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、自助解封等操作记录。

业务接入
IP 透明接入

最近更新时间：2024-04-18 15:48:52

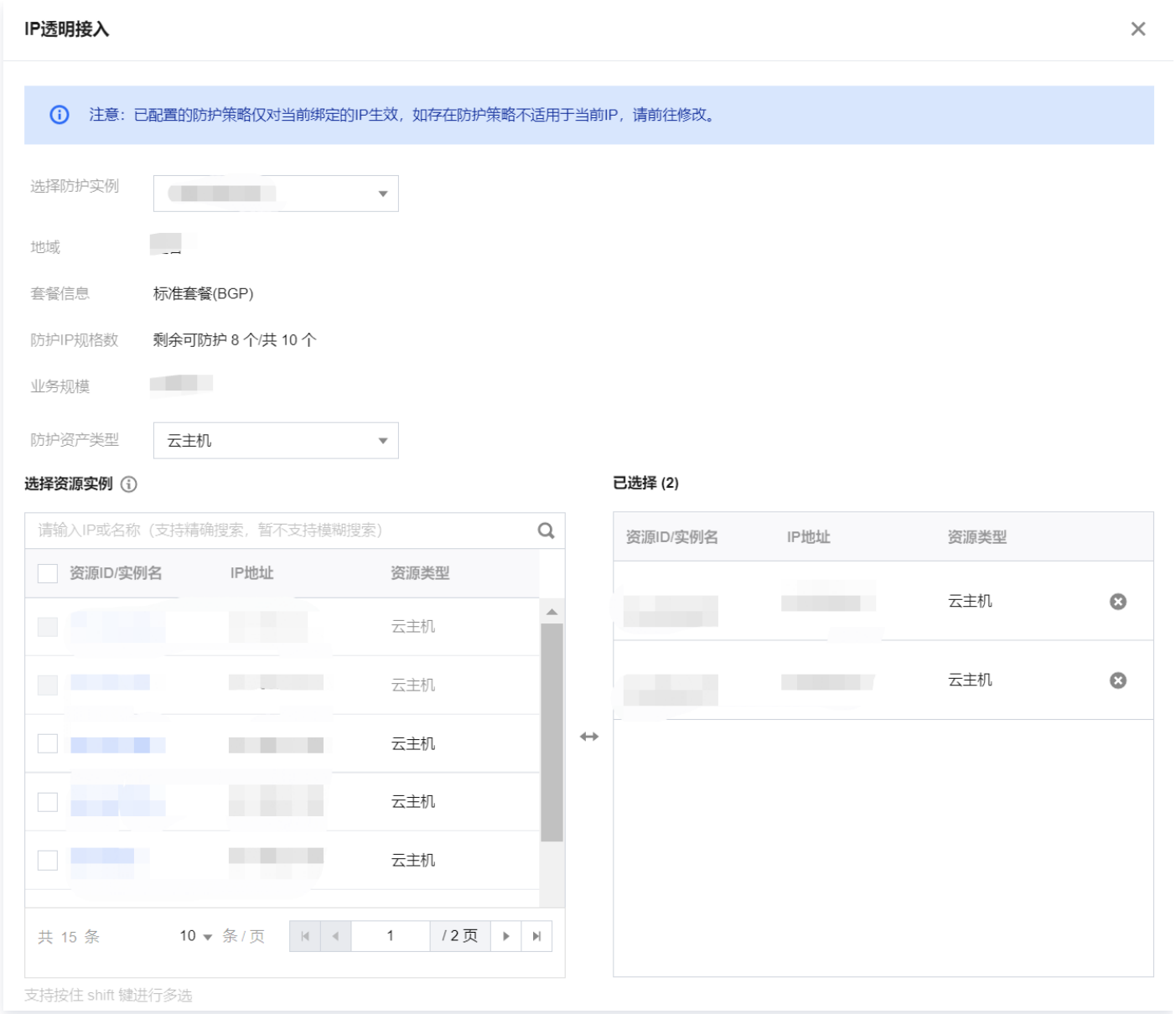
> **注意：**
> IP 透明接入为 DDoS 高防包直接绑定云上资产的接入方式，一键接入，配置便捷；如您购买的实例为 DDoS 高防包（企业版），则需要前往 CVM 控制台解绑原公网 IP 并重新绑定 EIP，如您需要对外隐藏源站 IP，请根据业务需要通过高防 IP 的形式选择端口业务或域名业务接入。

前提条件

设置防护对象 IP，您需要成功 购买 DDoS 高防包 。

操作步骤

1. 登录 DDoS防护（新版）控制台，在左侧导航中，单击**业务接入** > **IP 透明接入**。
2. 在 IP 透明接入页面，单击**开始接入**。
3. 在 IP 透明接入页面，选择防护实例。



说明：

- DDoS 高防包如果有 IP 处于封堵状态下，则不允许用户解绑该 IP。
- 当关联云资产时，支持批量搜索和选择。
- 当前支持检测 CLB、 CVM 产品的销毁状态，并进行解绑。

4. 单击**确定**即可。

域名接入

最近更新时间：2024-04-18 15:48:52

> **注意：**
> 高防资源将提供 CNAME，请将 DNS 解析地址修改为该 CNAME 高防资源。CNAME 解析目的高防 IP 将不定期更换。（不涉及三网资源）

接入规则

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**业务接入** > **域名接入**。
2. 在域名接入页面，单击**开始接入**。

3. 在域名业务接入页面，选择关联实例 ID，单击**下一步：协议端口**。

> **说明：**
> 支持多选，多实例同时接入。

4. 选择转发协议，填写业务域名，单击**下一步：回源方式**。

5. **选择回源方式，填写源站 IP+端口或源站域名。如有备用源站可选中备用源站，添加备用源站及权重，单击下一步：修改 DNS 解析。**

> **说明：**
> **备用源站：当源站转发异常会自动切换转发至备用源站。**

6. 单击**完成**，接入的规则会出现在域名接入列表中，在接入状态查看是否接入成功。

> **说明：**
> - 当因证书问题配置失败时，接入状态右侧会冒泡提醒“因所选证书获取失败，请到 SSL 证书管理 查看详情”。
> - 当已经接入成功的域名更新证书时，会产生秒级闪断，如需更新证书，建议低峰期更新。

配置规则

1. 在 域名接入页面，选择所需规则，单击操作列的**配置**。

2. 在配置七层转发规则页面，可修改相关参数，单击**确定**保存。

删除规则

1. 在 域名接入页面，支持删除单个或批量删除规则。
   - 单个：选择所需规则，单击操作列的**删除**，弹出删除规则弹窗。

   - 批量：选择一个或多个规则，单击**批量删除**，弹出删除规则弹窗。

2. 在删除规则弹窗，单击**删除**，即可删除所选规则。

IP 接入

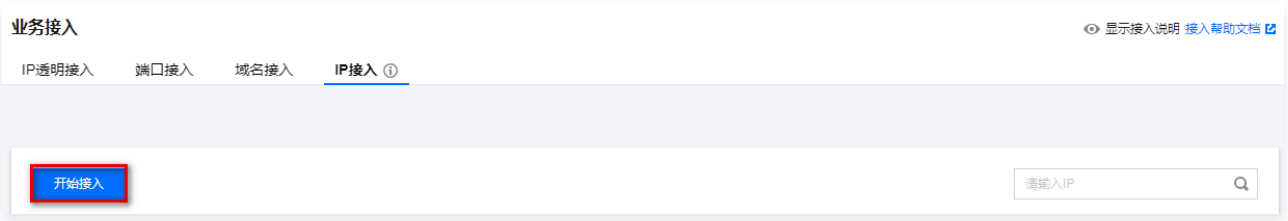
最近更新时间：2024-10-15 11:15:11

前提条件

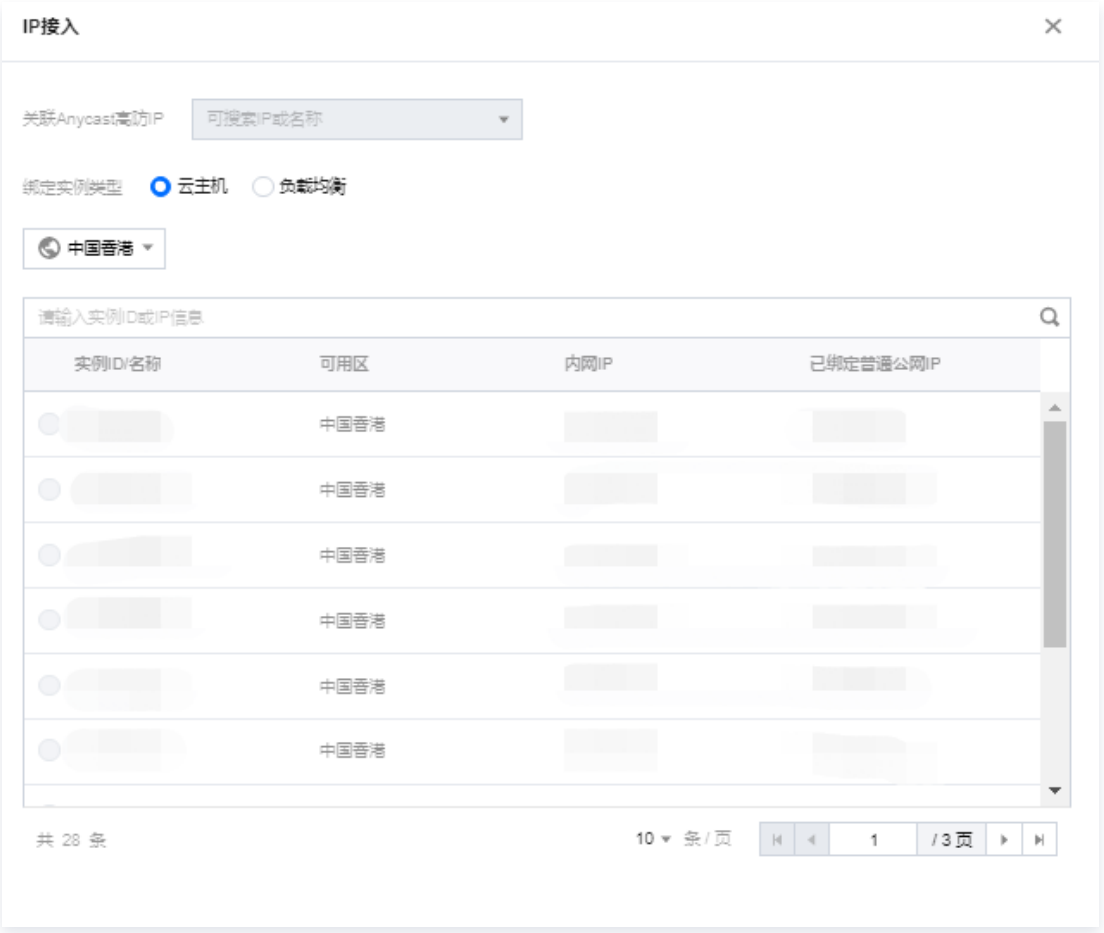
在绑定防护 IP 前，您需要成功购买 DDoS 高防 IP（境外企业版），如需购买请 联系我们。

接入规则

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**业务接入** > **IP 接入**。
2. 在 IP 接入页面，单击**开始接入**。



3. 在 IP 接入页面，选择关联 Anycast 高防 IP。



删除规则

1. 在 IP 接入页面，选择所需规则，单击操作列的**删除**，弹出删除规则弹窗。

2. 在删除规则弹窗，单击**删除**，即可删除所选规则。

端口接入

最近更新时间：2024-04-18 15:48:52

> **注意：**
> 高防资源将提供 CNAME，请将 DNS 解析地址修改为该 CNAME 高防资源。CNAME 解析目的高防 IP 将不定期更换。（不涉及三网资源）

接入规则

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**业务接入** > **端口接入**。
2. 在端口接入页面，单击**开始接入**。

3. 在端口业务接入页，选择关联实例 ID，单击**下一步：协议端口**。

> **说明：**
> 支持多选，多实例同时接入。

4. 选择转发协议，填写转发端口和源站端口，单击**下一步：回源方式**。

5. 选择回源方式，填写源站 IP+端口或源站域名。如有备用源站可选中备用源站，添加备用源站及权重，单击**下一步：修改 DNS 解析**。

说明：

- 备用源站：当源站转发异常会自动切换转发至备用源站。

- 在端口业务接入的**第二步协议端口**。输入转发端口后，会判定此高防 IP 资源下此端口是否已被占用。若是被占用，无法进入下一步。

6. 单击**完成**，即可完成接入规则。

配置规则

1. 在 端口接入页面，选择所需规则，单击操作列的**配置**。

2. 在配置四层转发规则页面，可修改相关参数，单击**确定**保存。

查询规则

在端口接入页面，单击搜索框通过源站 IP/域名、源站端口、关联高防 IP、转发协议、转发端口和关联高防资源（CNAME）关键字对规则进行查询。

删除规则

1. 在端口接入页面，支持删除单个或批量删除规则。
   - 单个：选择所需规则，单击操作列的**删除**，弹出删除规则弹窗。

   - 批量：选择一个或多个规则，单击批量删除，弹出删除规则弹窗。

2. 在删除规则弹窗，单击**删除**，即可删除所选规则。

配置会话保持

最近更新时间：2024-04-18 15:48:52

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进行处理。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秒 - 3600秒中的任意整数值，若超过该时间阈值，且会话中无新的请求，则自动断开连接。

操作步骤

1. 登录 DDoS 防护（新版）控制台 ，在左侧目录中，单击**业务接入** > **端口接入**。
2. 在端口接入页签，选择目的 DDoS 高防 IP 实例和相应规则，单击其会话保持列下的**编辑**。

3. 在会话保持编辑页面，设置保持时间，单击**确定**即可。

> **说明：**
> 默认关闭会话保持，在设置保持时间时，建议使用默认值。

配置健康检查

最近更新时间：2024-04-18 15:48:52

应用场景

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。

四层业务健康检查

DDoS 高防 IP 四层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。

七层业务健康检查

DDoS 高防 IP 七层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。

> **注意：**
> 配置转发规则时，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

四层业务健康检查配置

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**业务接入** > **端口接入**。
2. 在端口接入页签，选择目的 DDoS 高防 IP 实例和相应规则，单击其健康检查列下的**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。

> **说明：**
> - 默认开启健康检查。在配置健康检查时，建议使用默认值。
> - 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。

七层业务健康检查配置

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**业务接入** > **域名接入**。
2. 在域名接入页签，选择目的 DDoS 高防 IP 实例和相应规则，单击其健康检查列下的**配置**。

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。

> **说明：**
> 默认关闭健康检查。

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。
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。

智能调度

最近更新时间：2025-01-24 14:25:42

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。

说明：
- 支持设置解析的高防实例有 DDoS 高防包、DDoS 高防 IP ，其中 DDoS 高防 IP 包括 BGP 高防 IP、电信高防 IP、联通高防 IP 和移动高防 IP。
- 如果只有一条高防线路时不需要智能调度。

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 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。

  注意：
  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。

  说明：
  - 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 端口接入 或 域名接入。

- 在修改 DNS 解析前，您需要成功购买域名解析产品，例如腾讯云的云解析 DNS。

设置路线优先级

请参考以下步骤，按照设想的调度方案为您的高防实例设置优先级：

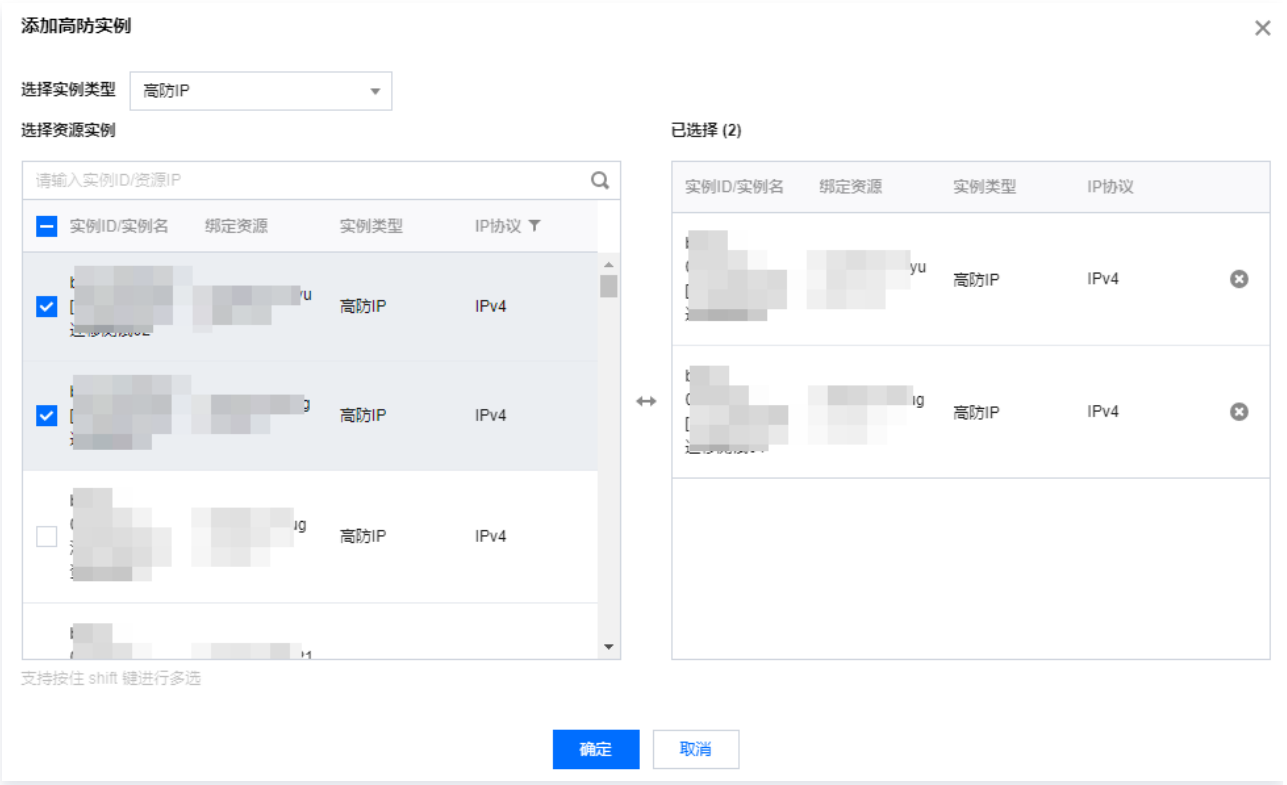
1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**智能调度**。
2. 在智能调度页面，单击**新建调度**，系统自动生成一个 CNAME 记录。

3. 在新建智能调度页面，TTL 值默认60秒，取值范围为1（秒）- 3600（秒），调度模式默认优先级。回切时间，当多个资源发生联动时，触发回切流程的等待时间。考虑封堵解除等待时间以及避免频繁触发联动切换，最短时间为10分钟。默认推荐设置为60分钟。

4. 在新建智能调度页面，分为优先级模式和定向模式，不同模式操作如下所示：

   4.1 优先级模式：以优先级的方式设置（通过数值的方式），提供资源之间的调度。

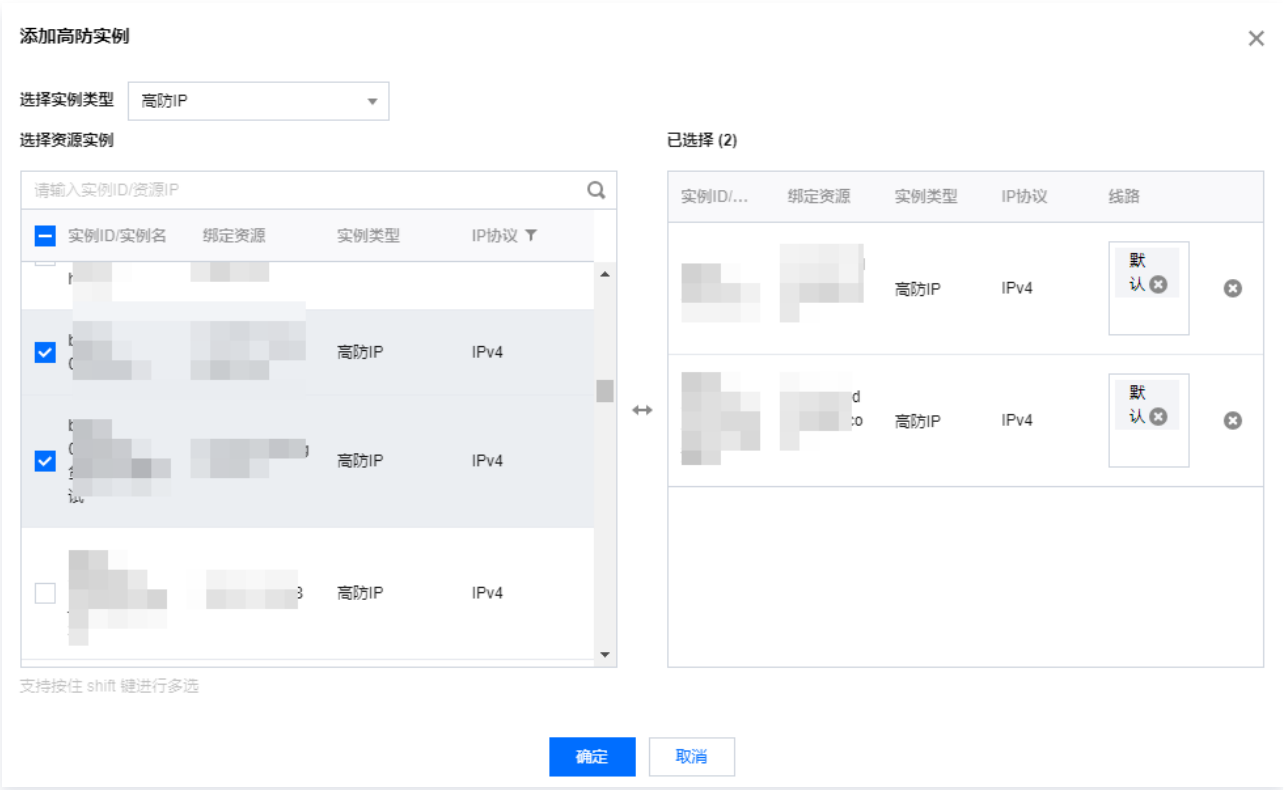
4.1.1 单击**添加高防资源 IP**，勾选需要设置智能调度的高防实例及 IP，单击**确定**。



4.1.2选择高防 IP 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。

4.2 定向模式：通过定向模式，指定资源间的调度关系。

4.2.1单击**添加高防资源 IP**，勾选需要设置智能调度的高防实例及 IP，并选择需要的线路，单击**确定**。



4.2.2在新建智能调度页面，看到选择调度的资源，单击**配置联动资源**。

4.2.3 在联动资源管理页，单击**添加资源**，输入联动 IP，并选择自相应线路，单击**确认**，即可配置指定资源间的调度关系。

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。

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。

1. 登录腾讯云 云解析 DNS 控制台，在左侧导航栏中，单击**我的解析**。
2. 在我的解析页面，找到目标域名所在行，单击**解析**。

3. 单击**添加记录**，输入需要添加记录的域名，记录类型选择 CNAME，记录值内输入智能调度系统自动生成的 CNAME 地址，单击**确认**。

> **说明：**
> 单击**批量操作 > 批量添加记录**，可以进行批量添加解析记录。

防护配置
DDoS 防护
DDoS 防护等级

最近更新时间：2024-06-18 17:14:21

应用场景

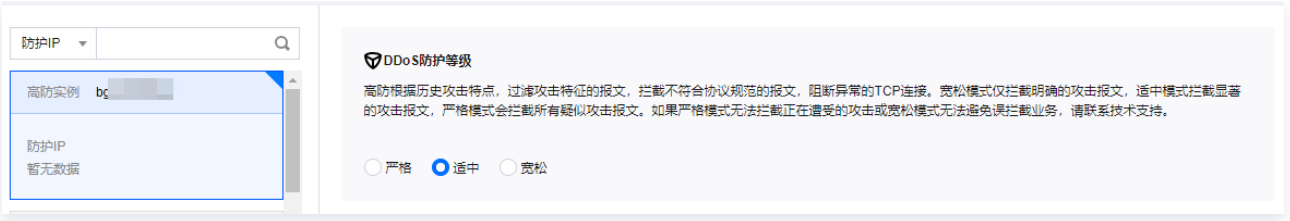
DDoS 防护服务提供防护策略调整功能，针对 DDoS 攻击提供三种防护等级供您选择，各个防护等级的具体防护操作如下：

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。 • 建议在怀疑有误拦截时启用，遇到复杂攻击时可能会有攻击透传。
适中	• 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。 • 默认为适中模式。
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。 • 严格检查过滤具有明确攻击特征的 UDP 数据包和基于 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。	清洗策略相对严格，建议在正常模式出现攻击透传时使用。

说明：
当被防护的 IP 处于被攻击状态时生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **DDoS 防护**。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"。



3. 在 DDoS 防护等级卡片中，设置防护等级即可。

IP 黑白名单

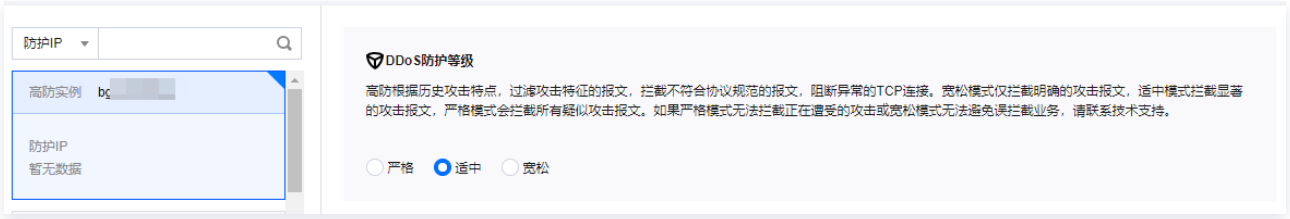
最近更新时间：2024-06-18 17:14:21

DDoS 高防支持通过配置 IP 黑名单和白名单实现对访问 DDoS 高防的源 IP 封禁或者放行，从而限制访问您业务资源的用户。配置 IP 黑白名单后，当白名单中的 IP 访问时，将被直接放行，不经过任何防护策略过滤。当黑名单中的 IP 访问时，将会被直接阻断。

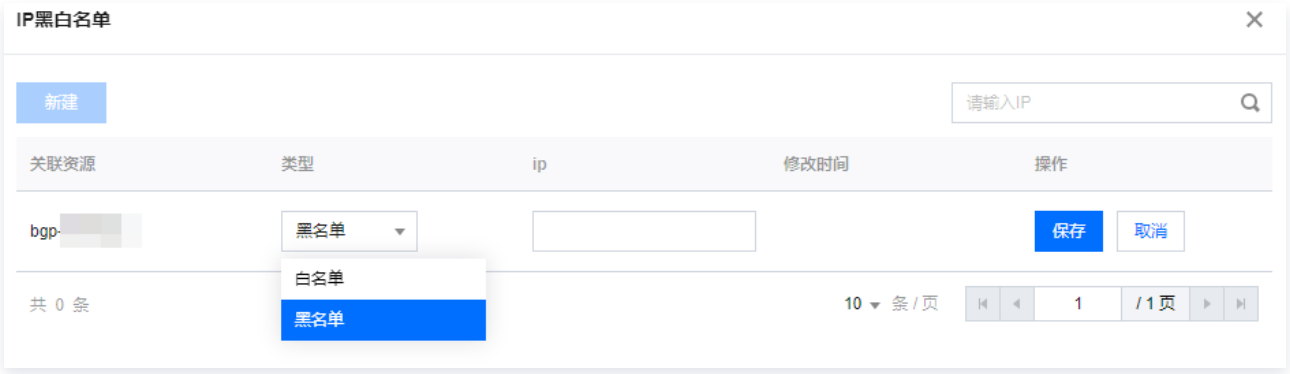
> **说明：**
> 当被防护的 IP 处于被攻击状态时生效。

操作步骤

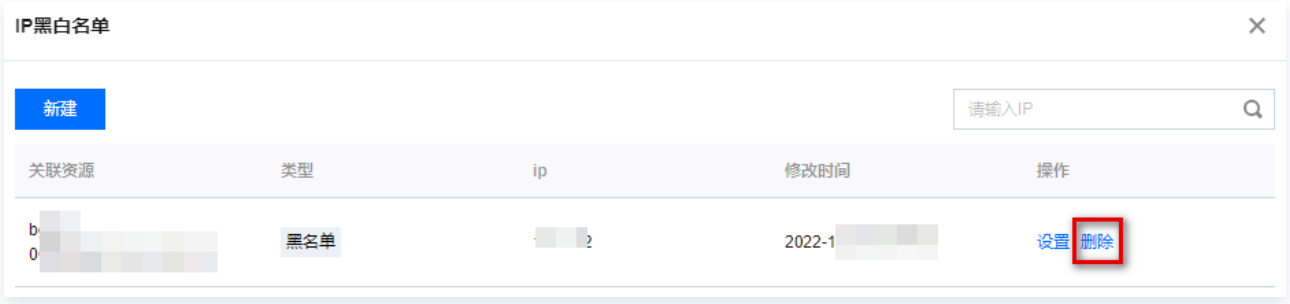
1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **DDoS 防护**。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"。



3. 在 IP 黑白名单卡片中，单击**设置**，进入 IP 黑白名单页面。
4. IP 黑白名单页面，单击**新建**，选择黑白名单类型，填写相关字段，单击**保存**。



5. 新建完成后，IP 黑白名单列表将新增一条IP黑白名单规则，可以在右侧操作栏中，单击**删除**，删除 IP 黑白名单规则。



端口过滤

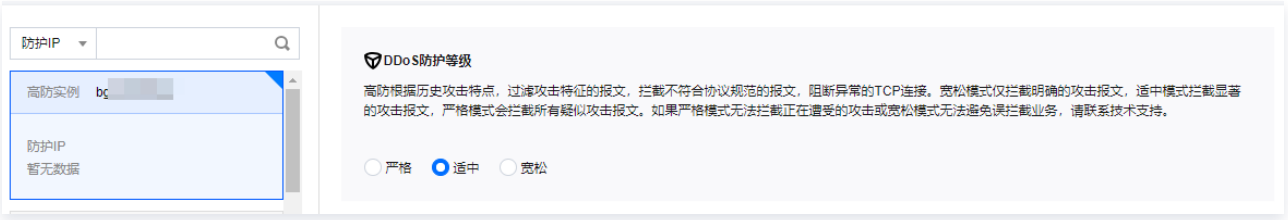
最近更新时间：2024-06-18 17:14:21

DDoS 高防支持针对访问 DDoS 高防的源流量，基于端口进行一键封禁或者放行。开启端口过滤后，可以根据需求自定义协议类型、源端口范围、目的端口范围的组合，并对匹配中的规则进行设置丢弃、放行、继续的防护策略动作。端口过滤可以针对访问的源流量精准制定端口设置的防护策略。

> **说明：**
> 当被防护的 IP 处于被攻击状态时生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **DDoS 防护**。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"。



3. 在端口过滤卡片中，单击**设置**，进入端口过滤页面。
4. 在端口过滤页面，单击**新建**，创建端口过滤规则，根据需求，选择不同防护动作并填写相关字段，单击**保存**。

> **说明：**
> 支持选择多个实例资源批量创建，未绑定防护资源的实例，不允许创建规则。

5. 新建完成后，在端口过滤列表，将新增一条端口过滤规则，可以在右侧操作列，单击**配置**，可以修改端口过滤规则。

协议封禁

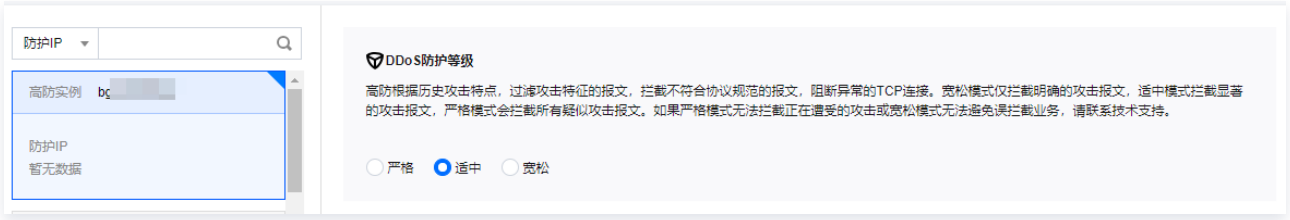
最近更新时间：2024-06-18 17:14:21

DDoS 高防支持对访问 DDoS 高防的源流量按照协议类型一键封禁。您可配置 ICMP 协议封禁、TCP 协议封禁、UDP 协议封禁和其他协议封禁，配置完成后，当检测到攻击流量有相关访问请求会被直接截断。
由于 UDP 协议的无连接性（如 TCP 具有三次握手过程）具有天然的不安全性缺陷，若您没有 UDP 业务，建议封禁 UDP 协议。

> **说明：**
> 当被防护的 IP 处于被攻击状态时生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **DDoS 防护**。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"。



3. 在协议封禁卡片中，单击**设置**，进入协议封禁页面。
4. 在协议封禁页面，单击  ，修改协议封禁规则开关。

水印防护

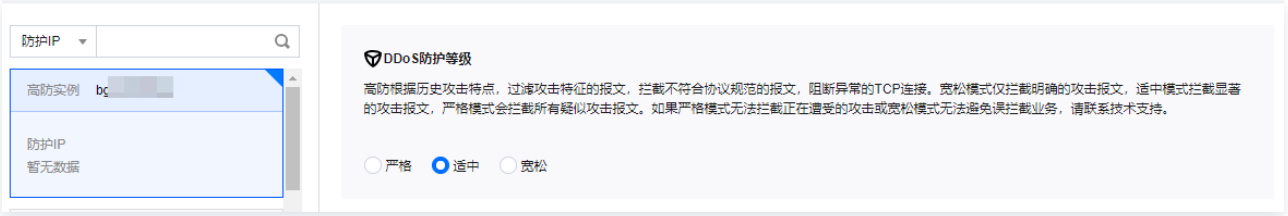
最近更新时间：2024-06-18 17:14:21

DDoS 高防支持对业务端发出的报文增加水印防护，在您配置的 UDP 和 TCP 报文端口范围内，业务端和 DDoS 防护端共享水印算法和密钥，配置完成后，客户端每个发出的报文都嵌入水印特征，而攻击报文无水印特征，借此甄别出攻击报文并将其丢弃。通过接入水印防护能高效全面防护四层 CC 攻击，如模拟业务报文攻击和重放攻击等。

> **说明：**
> 当被防护的 IP 处于被攻击状态时生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **DDoS 防护**。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"。



3. 在水印防护卡片中，单击**设置**，进入水印防护页面。
4. 在水印防护页面，单击**新建**，并填写相关字段，单击**确定**，创建水印防护规则。

5. 新建完成后，水印防护列表将新增了一条水印防护规则，可以在右侧操作列，单击**配置密钥**，可以查看和配置密钥。

6. 在配置密钥的界面，用户可以查看或复制密钥，并支持添加或删除密钥，只有在两个密钥时可以删除一个密钥，最多只能有两个水印密钥。

连接类攻击防护

最近更新时间：2024-06-18 17:14:21

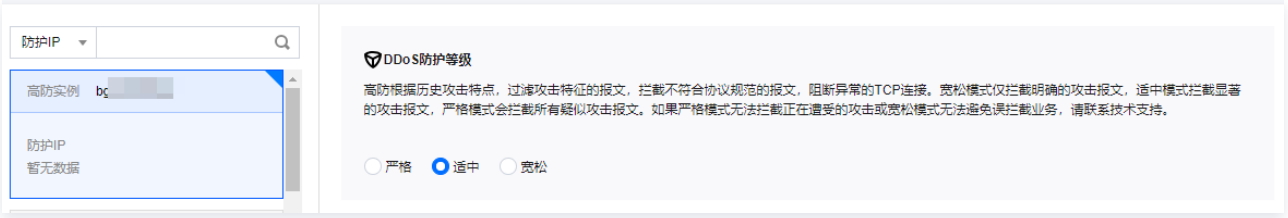
当连接类发起异常， DDoS 高防支持自动发起封禁惩罚策略。在源 IP 最大异常连接数开启防护后，如果 DDoS 高防检测到同一个源 IP，在短时间内频繁发起大量异常连接状态的报文时，会将该源 IP 纳入黑名单中进行封禁惩罚。其中封禁时间为15分钟，等封禁时间过后可恢复访问。

说明：

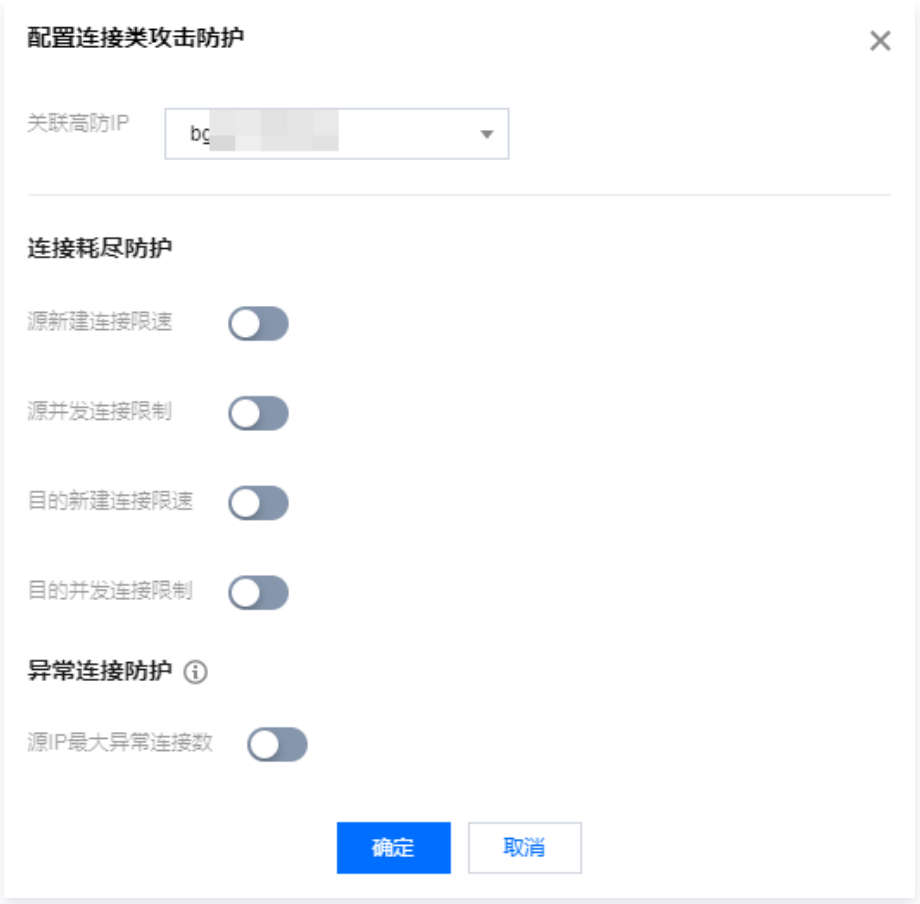
- 轻量应用服务器（Lighthouse）定制版不支持 DDoS 防护的自定义防护配置。
- 链接类攻击防护支持以下字段：
  - 源新建连接限速：基于源地址端口新建连接频率限制。
  - 源并发连接限制：访问源某一刻 TCP 的活跃连接数达到限制。
  - 目的新建连接限速：目的 IP 地址端口新建连接频率限制。
  - 目的并发连接限制：目的 IP 地址某一刻 TCP 的活跃连接数达到限制。
  - 源 IP 最大异常连接数：访问源 IP 支持最大的异常连接数。
- 当被防护的 IP 处于被攻击状态时生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **DDoS 防护**。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"



3. 在连接类攻击防护卡片中，单击**设置**，进入连接类攻击防护页面。
4. 在连接类攻击防护页面，单击**新建**，并开启连接耗尽防护和异常连接防护，单击**确定**。



5. 新建完成后，连接类攻击防护列表将增加一条连接类攻击防护规则，可以在右侧操作列，单击**配置**，修改异常连接规则。

AI 防护

最近更新时间：2024-06-18 17:14:21

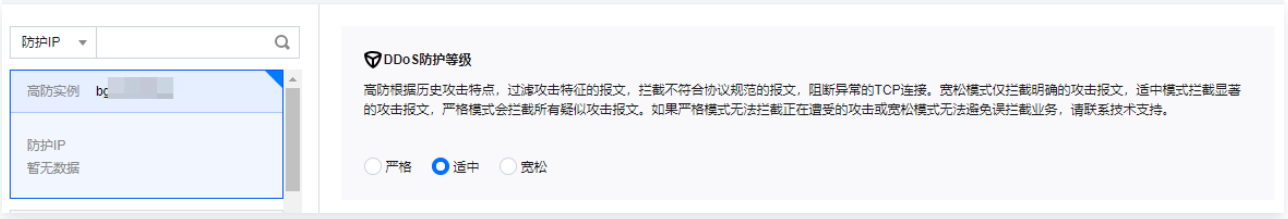
DDoS 高防支持智能 AI 防护功能。开启 AI 防护后，DDoS 高防将通过算法自主学习连接数基线与流量特征，自适应调整清洗策略，发现并阻断四层连接型 CC 攻击，提供最佳防御效果。

说明：

- DDoS 高防包（轻量版）不支持 DDoS 防护、CC 防护的自定义防护配置。
- 当被防护的 IP 处于被攻击状态时生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **DDoS 防护**。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"



3. 在 AI 防护卡片中，单击  ，打开 AI 防护开关。

区域封禁

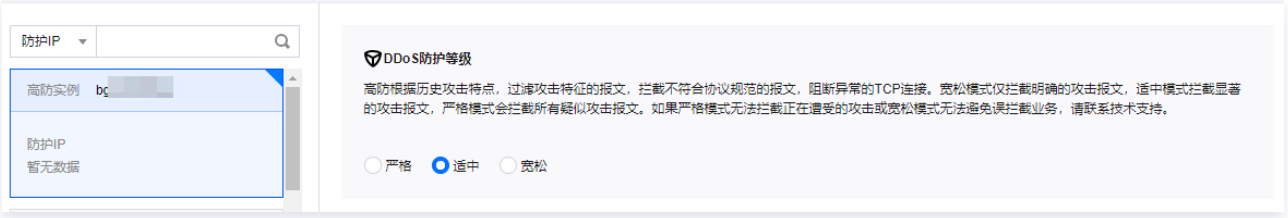
最近更新时间：2024-06-18 17:14:21

DDoS 高防支持对访问 DDoS 高防的源流量，按照源 IP 地理区域在清洗节点进行一键封禁。支持多地区、国家进行流量封禁。

> **说明：**
> 当被防护的 IP 处于被攻击状态时生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **DDoS 防护**。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"



3. 区域封禁卡片中，单击**设置**，进入区域封禁页面。
4. 在区域封禁页面中，单击**新建**，并选择封禁区域，单击**确定**，创建区域封禁规则。

5. 新建完成后区域封禁列表，将新增一条区域封禁规则，可以在右侧操作列，单击**配置**，修改区域封禁规则。

IP 端口限速

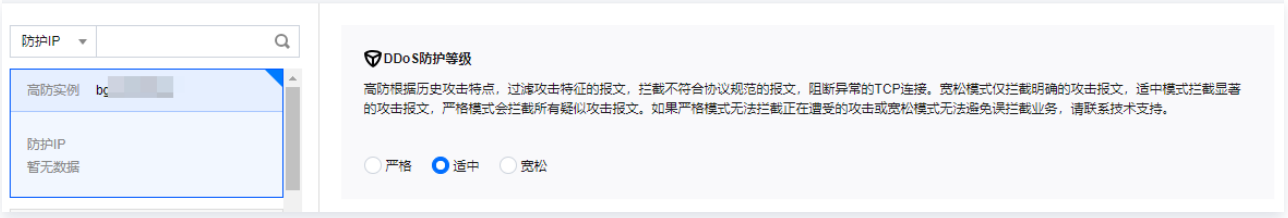
最近更新时间：2024-06-18 17:14:21

DDoS 高防支持对于业务 IP，基于 IP+端口的维度进行流量访问限速。

> **说明：**
> 当被防护的 IP 处于被攻击状态时生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **DDoS 防护**。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"



3. 在 IP 端口限速卡片中，单击**设置**，进入 IP 端口限速页面。
4. 在 IP 端口限速页面中，单击**新建**，弹出新建 IP 端口限速弹窗。

5. 在新建 IP 端口限速弹窗中，选择所需协议、端口和限速模式，并输入限速阈值后，单击**确定**，创建 IP 端口限速规则。

6. 新建完成后，IP 端口限速列表将新增一条 IP 端口限速规则，可以在右侧操作列，单击**配置**，修改 IP 端口限速规则。

特征过滤

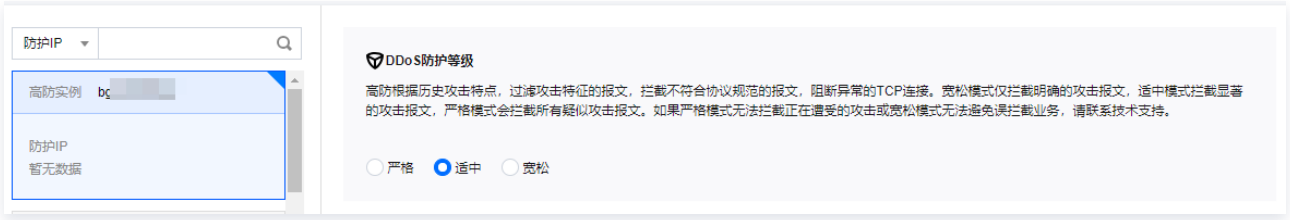
最近更新时间：2025-01-24 14:25:43

DDoS 高防支持针对 IP，TCP，UDP 报文头或载荷中的特征自定义拦截策略。开启特征过滤后，您可以将源端口、目的端口、报文长度、IP 报文头或荷载的匹配条件进行组合，并对命中条件的请求设置放行、丢弃、丢弃并拉黑15分钟、继续防护等策略动作，特征过滤可以精准制定针对业务报文特征或攻击报文特征的防护策略。

> **说明：**
> 当被防护的 IP 处于被攻击状态时生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **DDoS 防护**。
2. 在 DDoS 防护页面的左侧列表中，选中高防包/高防IP的 ID，如"bgp-00xxxxxx"



3. 在特征过滤卡片中，单击**设置**，进入特征过滤页面。
4. 在特征过滤页面，单击**新建**，弹出新建特征过滤弹窗。

5. 在新建特征过滤弹窗中，创建特征过滤规则，根据需求，选择不同防护动作并填写相关字段，单击**确定**。

6. 新建完成后，特征过滤列表将新增一条特征过滤规则，可以在右侧操作列，单击**配置**，可以修改特征过滤规则。

CC 防护
CC 防护开关及清洗阈值

最近更新时间：2024-06-18 17:14:21

防护说明

CC 防护根据访问特征和连接状态判定恶意行为来阻断黑客的攻击。可根据不同的攻击场景配置相应的防护策略，保证业务稳定。清洗阈值是高防产品启动清洗动作的阈值。

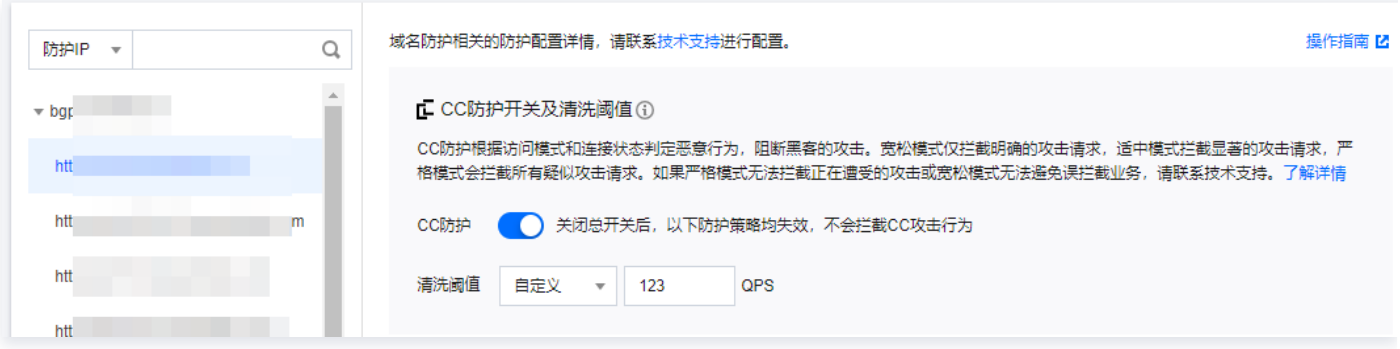
> **说明：**
> 当被防护的 IP 处于被攻击状态时生效。

前提条件

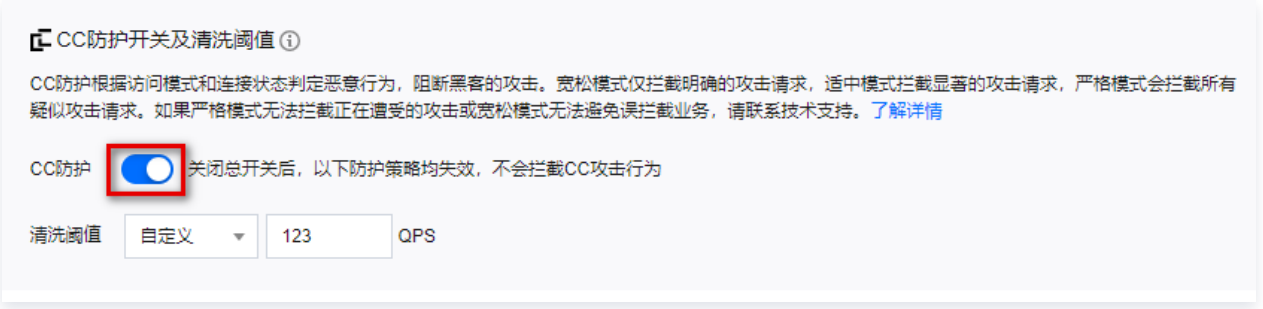
1. 您需要已成功购买 DDoS 高防 IP，并设置防护对象。
2. CC 防护当前仅支持域名接入的规则生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 CC 防护。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。



3. 在右侧 CC 防护开关及清洗阈值卡片中，单击 开启CC 防护，当防护开启后必须进行清洗阈值设置否则无法开 CC 防护。



> **说明：**
> CC 防护开关是控制是否启用 CC 防护的总开关，开启后下方的防护策略才能生效。

4. 清洗阈值是高防产品启动清洗动作的阈值，当接入的域名收到的 HTTP 请求超过清洗阈值时，触发 CC 防护。当 CC 防护开启后，业务实例的清洗阈值采用默认值（推荐），并随着接入业务流量的变化规律，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。同时，您也可以根据实际业务情况自定义清洗阈值。

> **说明：**
> - 自定义具体的阈值可以设置为正常业务峰值的1.5倍。
> - 自定义阈值越小，检测要求越严格。
> - 当清洗阈值低于默认值时，可能存在误杀。当清洗阈值高于默认值时，可能存在透传。推荐开启默认清洗阈值。

智能 CC 防护

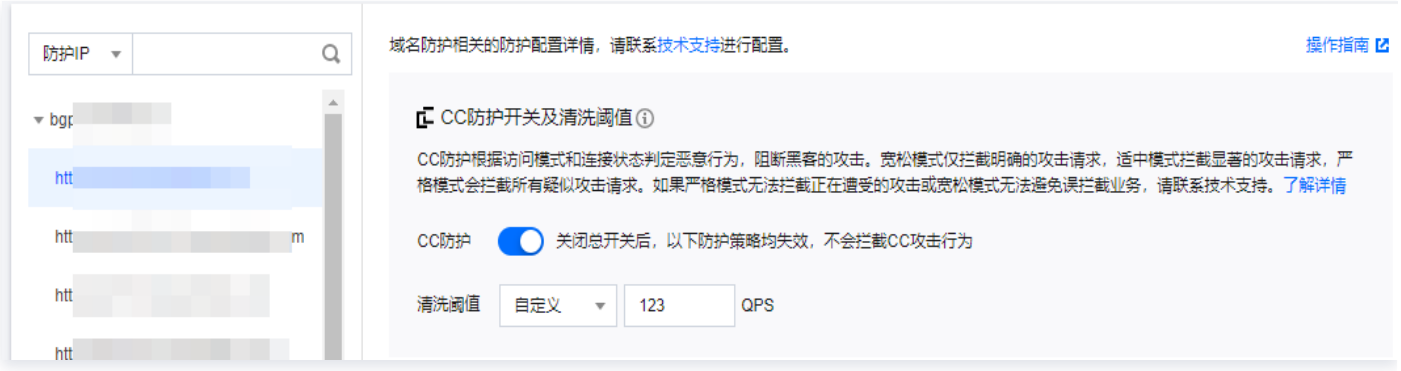
最近更新时间：2024-06-18 17:14:21

开启智能防护后，AI 智能防护基于腾讯云的大数据能力，能够自学习网站业务流量基线，结合算法分析攻击异常，并自动下发精确的防护规则，动态调整业务防护模型，帮助您及时发现并阻断恶意攻击。

> **说明：**
> 当被防护的 IP 处于被攻击状态时生效。

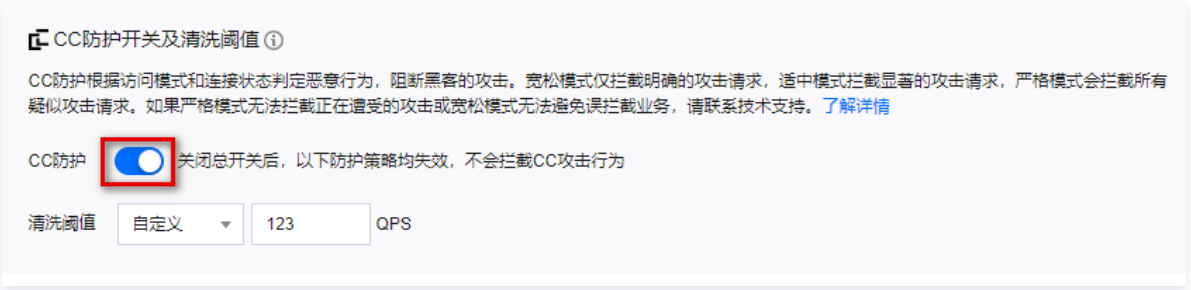
操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 CC 防护。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。

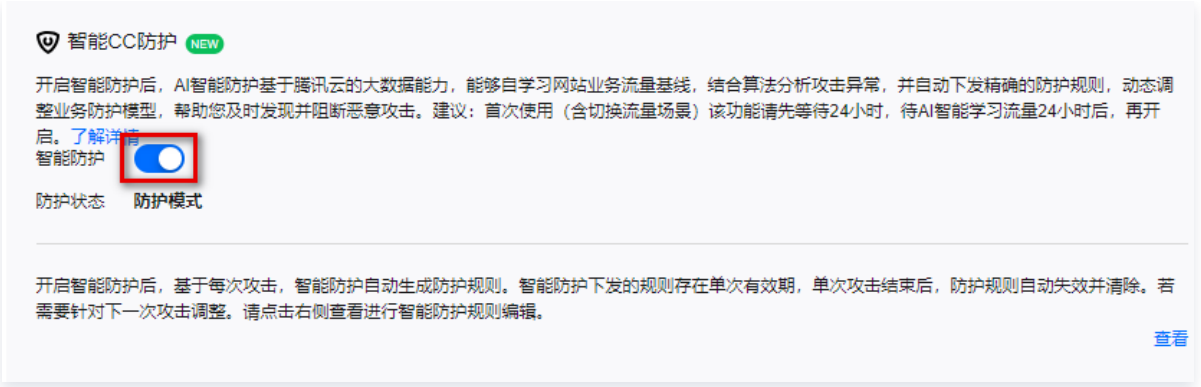


3. 在 CC 防护开关及清洗阈值卡片中，单击 开启 CC 防护开关，当防护开启后必须设置清洗阈值，否则无法使用智能 CC 防护。

> **说明：**
> - 清洗阈值是高防产品启动清洗动作的阈值，当指定域名收到的 HTTP 请求超过阈值时，将触发 CC 防护。
> - 当高防包的 IP 为“Web 应用防火墙” 的 IP 时，需要先到 Web 应用防火墙控制台 为此 IP 开启 CC 防护，详情请参见 CC 防护规则设置 。



4. 在智能 CC 防护卡片中，单击 开启智能防护。



5. 单击**查看**，可查看智能生成的防护规则。若需要调整，请单击右侧**查看**编辑智能防护规则。

> **注意：**
> - 开启智能 CC 防护后，基于每次攻击，智能防护自动生成防护规则。
> - 防护模式：智能防护下发的规则存在单次有效期，单次攻击结束后，防护规则自动失效并清除。
> - 观察模式：仅生成规则展示，不生效。

6. 智能防护规则基于单次攻击自动生成与生效。智能防护下发的规则存在单次有效期，单次攻击结束后，防护规则自动失效并清除。根据防护需求，可单击**删除**，删除对应防护规则。

精准防护

最近更新时间：2024-06-18 17:14:21

应用场景

DDoS 高防 IP 支持对已接入防护的网站业务配置精准防护策略。开启精确访问控制后，您可以对常见的 HTTP 字段（例如 URI、UA、Cookie、Referer、Accept 等）做条件组合防护策略，筛选访问请求，并对命中条件的请求设置人机校验、丢弃或放行策略动作。精准防护支持业务场景定制化的防护策略，可用于精准定制针对性的 CC 防御。

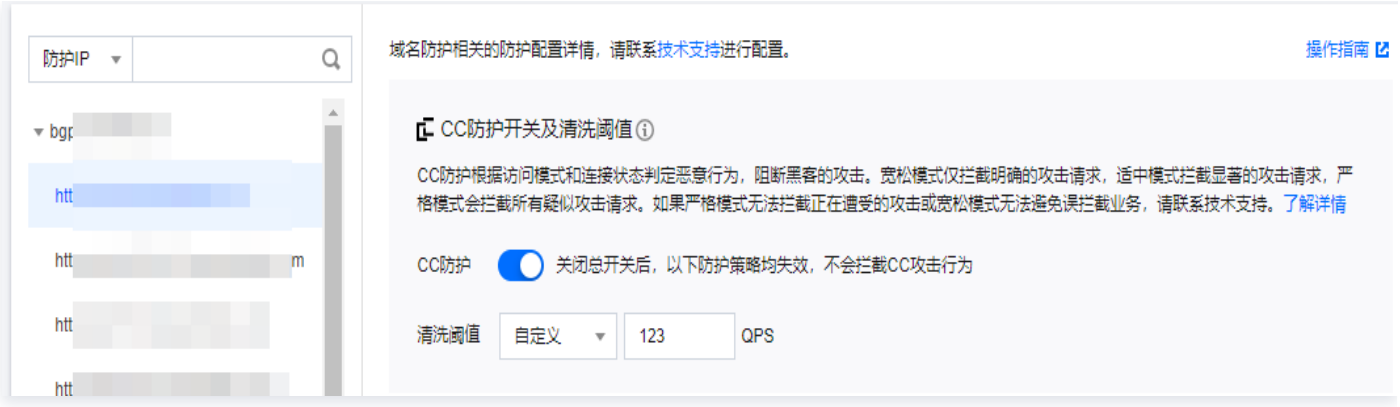
> **说明：**
> 当被防护的 IP 处于被攻击状态时生效。

匹配条件定义了要识别的请求特征，具体指访问请求中 HTTP 字段属性特征。精确防护规则支持匹配的 HTTP 字段如下表所示。

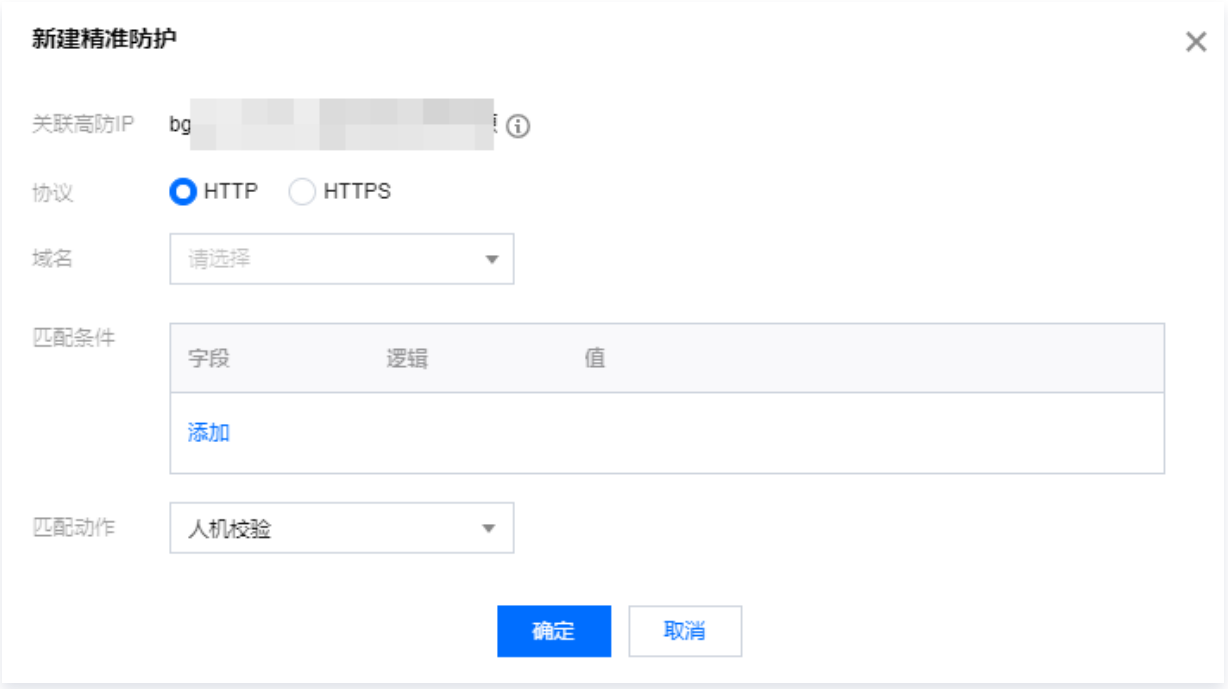
匹配字段	字段描述	适用逻辑
URI	匹配请求的 URI。例如:/example.html • 忽略大小写 • 不包含 Hostname • 不包含查询参数	等于、包含、不包含
URL	匹配请求的 URL。例如:/example.html?region=cn • 忽略大小写 • 不包含 Hostname • 包含 URL 查询参数	等于、包含、不包含
Path	匹配请求 URL的路径部分。例如:/example.html 或者 /api/v2/login • 忽略大小写 • 不包含 Hostname • 不包含查询参数	等于、包含、不包含
UA	发起访问请求的客户端浏览器标识等相关信息	等于、包含、不包含
Cookie	匹配指定请求 Cookie 头部参数值，需指定 Cookie 参数名称。 • 忽略大小写	等于、包含、不包含
Referer	访问请求的来源网址，即该访问请求是从哪个页面跳转产生的	等于、包含、不包含
Accept	发起访问请求的客户端希望接受的数据类型	等于、包含、不包含
Srcip	访问请求的来源网址	等于、不等于

操作步骤

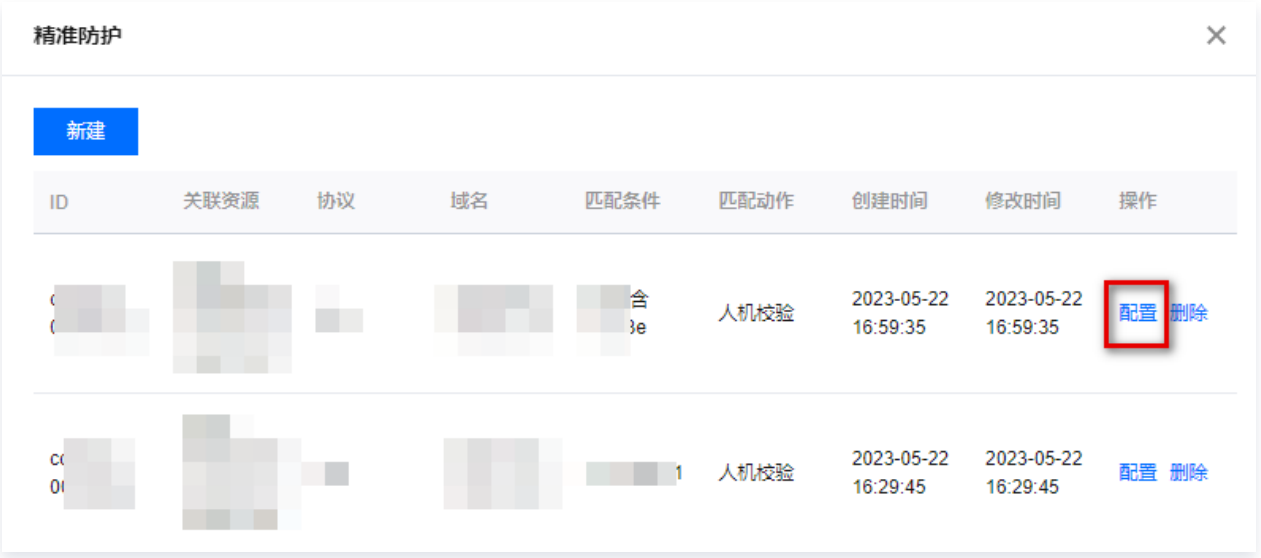
1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 CC 防护。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。



3. **在精准防护卡片中，单击设置，进入精准防护页面。**
4. **在精准防护页面，单击新建，创建精准防护规则，填写相关字段，填写完成后，单击确定。**



5. **新建完成后，在精准防护列表将新增一条精准防护规则，可以在右侧操作列，单击配置，修改精准防护规则。**



CC 频率限制

最近更新时间：2024-06-18 17:14:21

DDoS 高防 IP 为已接入防护的网站业务提供 CC 频率限制防护策略，支持限制源 IP 的访问频率。频率控制防护开启后自动生效，默认使用超级宽松防护模式，频率控制防护提供多种防护模式，供您在不同场景下调整使用。您也可以自定义频率限制规则，检测到单一源 IP 在短期内异常频繁地访问某个页面时，将设置人机校验或丢弃策略。

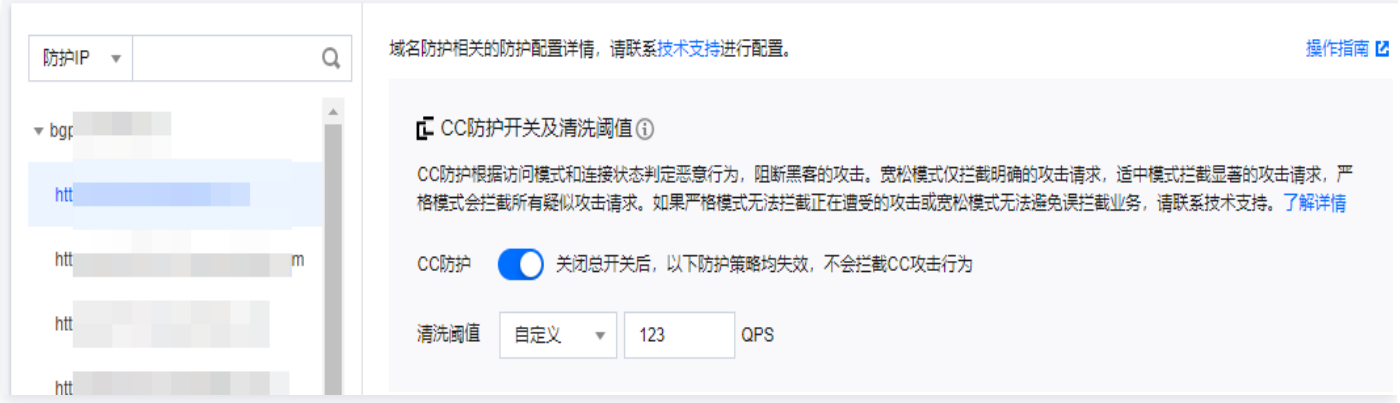
> **说明：**
> 当被防护的 IP 处于被攻击状态时生效。

频率控制防护提供不同的防护模式，允许您根据网站的实时流量异常调整频率控制策略，具体包括以下模式。

等级分类	说明
宽松等级	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。 注意：当发生攻击时，可切换防护等级进行防护。也可以配置自定义 CC 频率限制策略进行防护。
适中等级	将启动人机校验算法，访问者通过算法验证后才允许访问源站。 注意：此防护等级只适用于 Web 网站业务，不适用于 API/APP 类业务。如果为 API/APP 类业务，请配置自定义 CC 频率限制策略进行防护。 攻击紧急：当发现源站访问量突然增加，导致源站服务器负载过高或者响应异常时，可选择此等级进行防护。
严格等级	针对全网每一个访问者都会进行人机识别验证，同时验证算法升级，认证过程更加严格，可能会存在一定误判。 注意：此防护等级只适用于 Web 网站业务，不适用于 API/APP 类业务。如果为 API/APP 类业务，请配置自定义 CC 频率限制策略进行防护。
攻击紧急	当发现源站访问量突然增加，导致源站服务器负载过高或者响应异常时，可选择此等级进行防护。
自定义	基于设置的自定义频控规则进行防护，针对特征符合频控规则设置条件的流量进行访问频率限制。

操作步骤

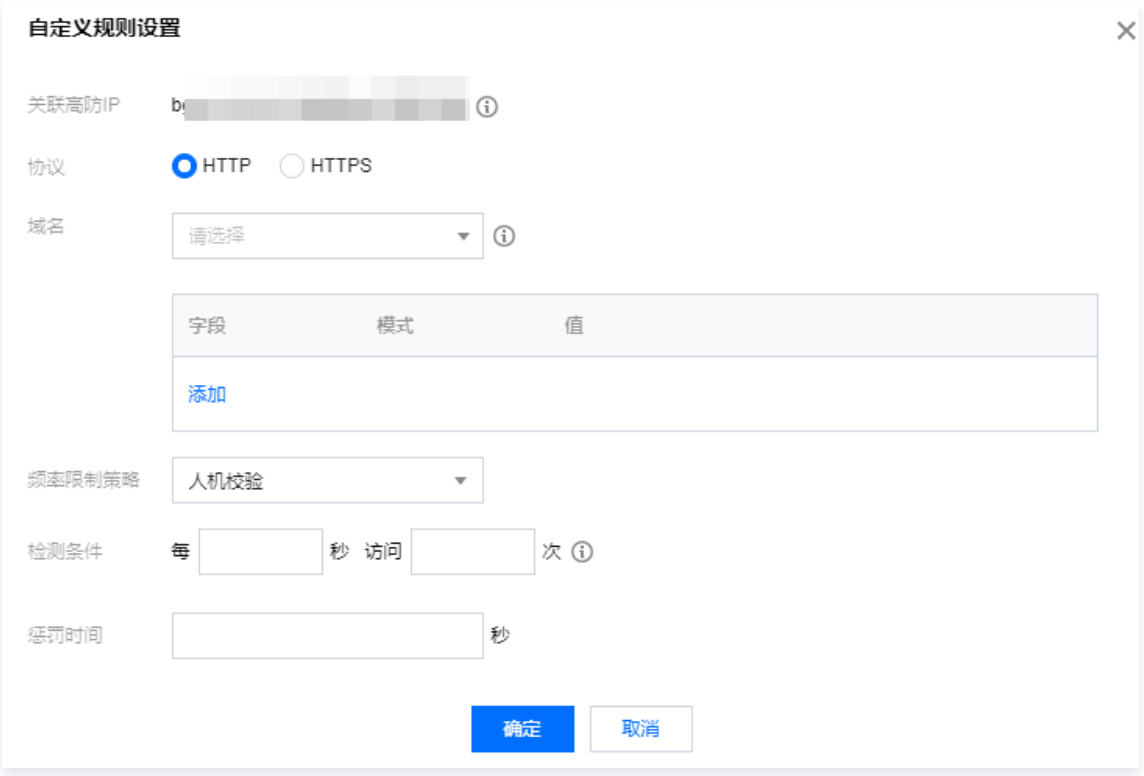
1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **CC 防护**。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。



3. 在 CC 频率限制卡片中，单击 开启 CC 频率限制功能，选择符合业务需求的防护等级，单击**设置**进入 CC 频率限制列表。

4. 在 CC 频率限制规则列表中，默认展示该域名下全部规则。单击**新增规则**，创建频率限制规则，填写相关字段。

> **注意：**
> - 当没有创建规则时，自定义等级不允许开启。
> - 经过优化后，无需添加首条默认规则；并且支持配置子域名频控限速。



5. 新建完成后，在 CC 频率限制列表中，将新增一条 CC 频率限制规则，可以在右侧操作列单击**配置**，修改 CC 频率限制规则。

区域封禁

最近更新时间：2024-06-18 17:14:21

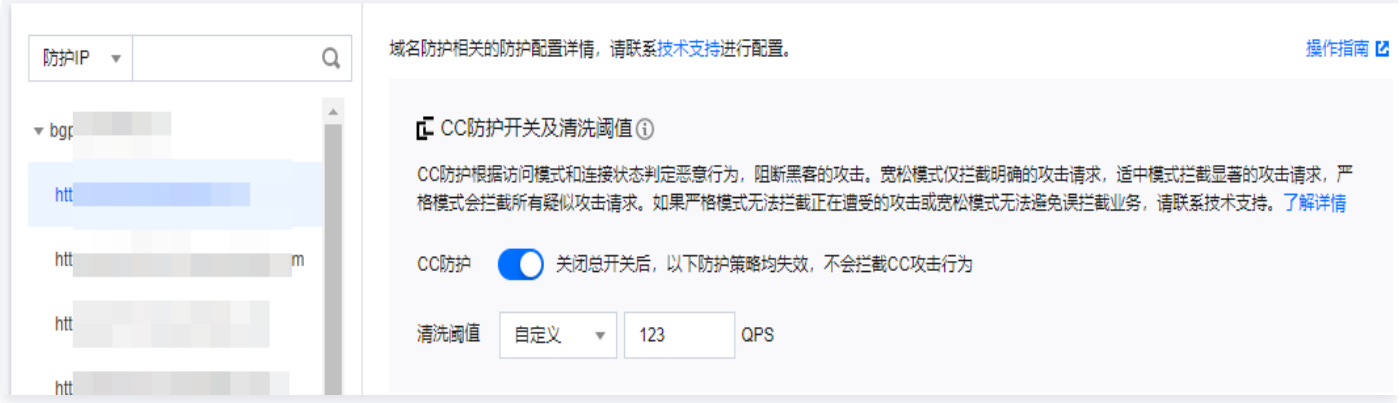
DDoS 高防 IP 支持对已接入防护的网站业务设置基于地理区域的访问请求封禁策略。开启针对域名的区域封禁功能后，您可以一键阻断指定地区来源 IP 对网站业务的所有访问请求。支持多地区、国家进行流量封禁。

说明：

- 在配置了区域封禁后，该区域的攻击流量依然会被平台统计和记录，但不会流入业务源站。
- 当被防护的 IP 处于被攻击状态时生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **CC 防护**。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。



3. 在区域封禁卡片中，单击**设置**，进入区域封禁页面。
4. 在区域封禁页面，单击**新建**，选择 IP、协议、域名和所封禁的区域，单击**确定**，创建区域封禁规则。

5. 新建完成后，在区域封禁列表，将新增一条区域封禁规则，可以在右侧操作列，单击**配置**，修改区域封禁规则。


区域封禁
新建
关联资源
协议
域名
封禁区域
修改时间
操作
http
配置
删除
共 1 条
10 条/页
1
/ 1 页

IP 黑白名单

最近更新时间：2024-06-18 17:14:21

DDoS 高防 IP 支持通过配置 IP 黑名单和白名单，实现对访问 DDoS 高防 IP 已接入防护的网站业务封禁或者放行，从而限制访问您业务资源的用户。配置 IP 黑白名单后，当白名单中的 IP 访问时，将被直接放行，不经过任何防护策略过滤。当黑名单中的 IP 访问时，将会被直接阻断。

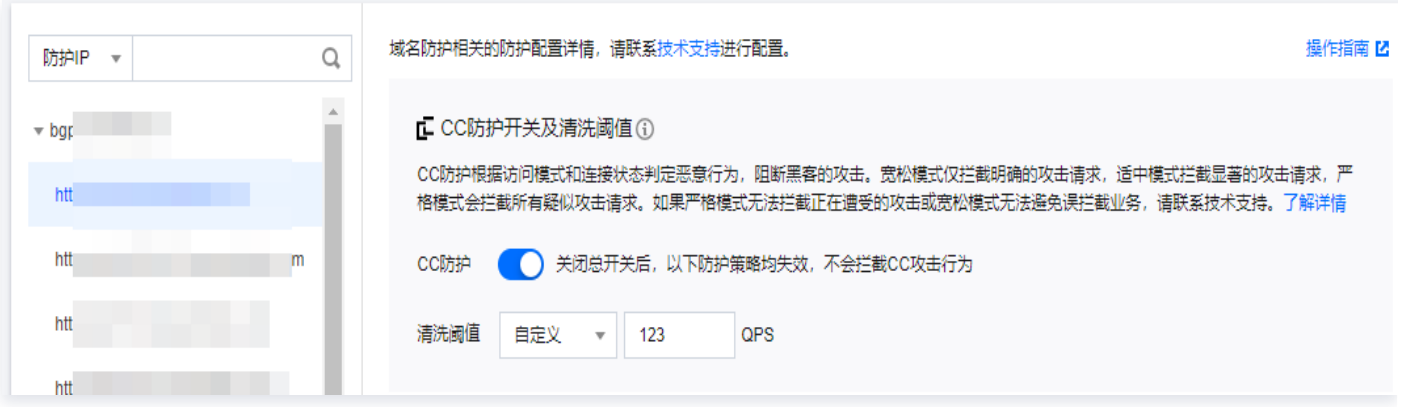
说明：

发生 CC 攻击时，IP 黑白名单的过滤才会生效。

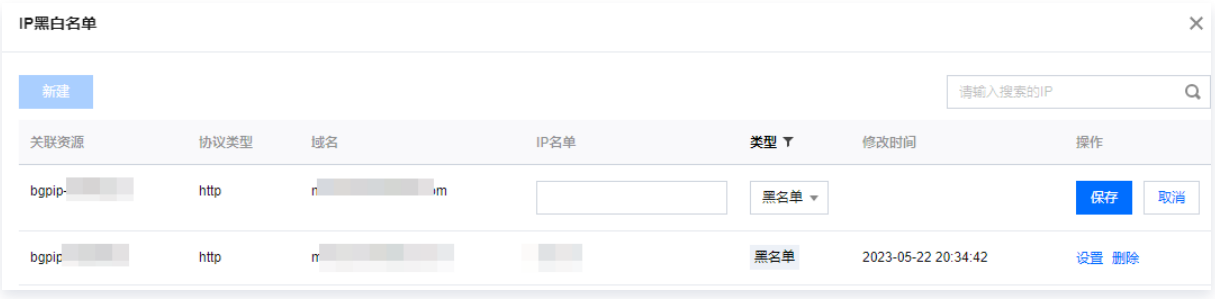
- 白名单中的 IP，访问时将被直接放行，不经过任何防护策略过滤。
- 黑名单中的 IP，访问时将会被直接阻断。
- 当被防护的 IP 处于被攻击状态时生效。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击 **CC 防护**。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。



3. 在 IP 黑白名单卡片中，单击**设置**，进入 IP 黑白名单页面。
4. 在 IP 黑白名单页面，单击**新建**，填写相关字段，填写完成后，单击**保存**。



5. 新建完成后，IP 黑白名单列表将新增一条 IP 黑白名单规则，可以在右侧操作栏中，单击**删除**，删除 IP 黑白名单规则。


IP黑白名单
新建
请输入搜索的IP
关联资源
协议类型
域名
IP名单
类型
修改时间
操作
bgpip-
http
黑名单
2023-05-22 20:34:42
设置
删除
bgpip-
http
白名单
2023-05-22 16:57:48
设置
删除

安全运营
攻击分析

最近更新时间：2024-04-18 15:48:52

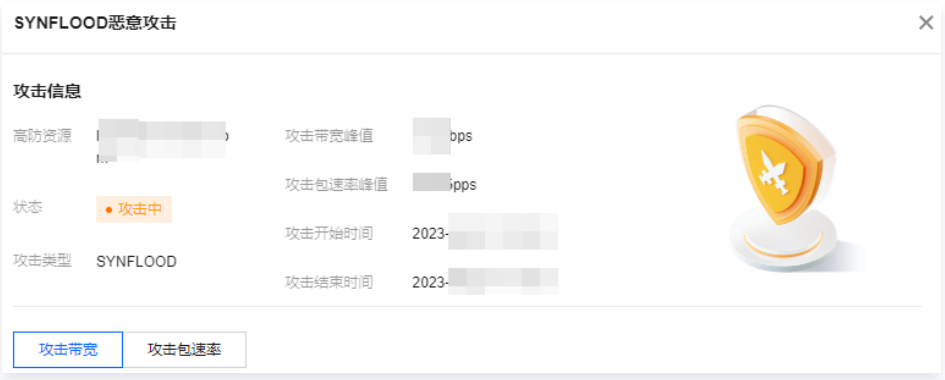
查看攻击概况统计

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**攻击分析**。
2. 在攻击概况统计模块中，可查看当前业务被攻击总次数、总封堵次数、正在攻击中、正在封堵中、攻击带宽峰值、攻击请求峰值。右侧可以查看7天/30天的攻击趋势。

查看近期安全事件

1. 在事件详情页面，可通过资产ID/IP地址，尽可能详细的展示出此次攻击的细节，主要包括攻击源名称、被攻击资产、IP 地址、攻击时间、攻击时长、攻击峰值、防护实例 ID、防护类型、攻击状态。

2. 在事件详情页面的攻击信息模块，查看该时间范围内的 IP 遭受的攻击情况，包括被攻击 IP、状态、攻击类型（采样数据）、攻击带宽峰值和攻击包速率峰值、开始时间结束时间基础信息。



3. 在事件详情页面的攻击趋势模块，可查看网络攻击流量带宽或攻击包速率趋势。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。

> **说明：**
> 此处数据为该攻击时间段全量实时数据。

4. 在事件详情页面的攻击统计模块，可通过攻击流量协议分布、攻击类型分布，查看这两个数据维度下的攻击分布情况。

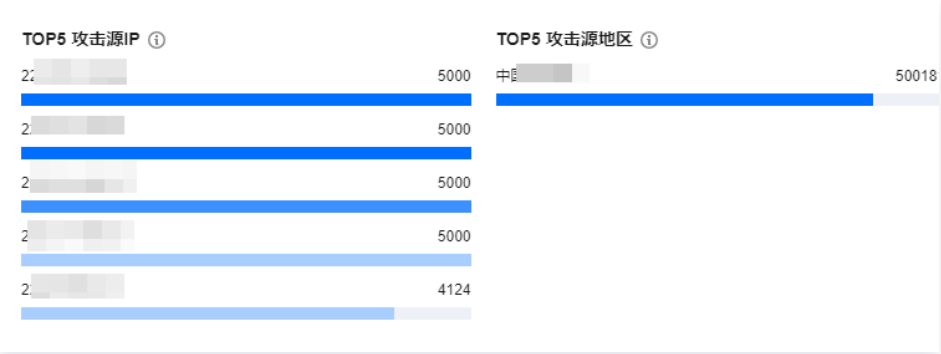
> **说明：**
> 此处数据为该攻击时间段内攻击采样数据，非全量数据。

字段说明：

- 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。

5. 在事件详情页面 “TOP5 展示”模块，可查看攻击源 IP TOP5 和攻击源地区TOP5，准确把握攻击源的详细情况便于精准防护策略的制定。

> **说明：**
> 此处数据为该攻击时间段内攻击采样数据，非全量数据。



6. 在事件详情页面的攻击源信息模块，可查看该攻击时间段内攻击详情的随机采样数据，尽可能详细的展示出此次攻击的细节，主要包括攻击源 IP、地域、累计攻击流量、累计攻击包量。

> **说明：**
> 此处数据为该攻击时间段内攻击采样数据，非全量数据。

攻击源信息

攻击源IP	地区	累计攻击流量	累计攻击包量
[illegible]	[illegible]	638.9 KB	1331
[illegible]	[illegible]	690.7 KB	1439
[illegible]	[illegible]	489.6 KB	1020

业务分析

最近更新时间：2024-04-18 15:48:53

DDoS 防护支持查看近90天内的日志，包括业务保护天数、已接入业务数、受攻击业务数。如有需要，可通过实例 ID 进行搜索。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**业务分析**。
2. 在业务分析页面，单击**立即处理**。

3. 在防护待办页面，支持进行如下操作：
   - 单击**去解封**，跳转至解封中心。

   - 单击**升级防护**，进入升级页面，根据实际防护需求选择“IP 数量”与“防护次数”。

操作日志

最近更新时间：2024-04-18 15:48:53

DDoS 防护（新版）控制台支持查看近90天内重要操作的日志，可查看的日志包含以下类别：

- 防护对象 IP 更换日志。
- DDoS 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。
- 资源名称的修改日志。

操作步骤

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**操作日志**。
2. 在操作日志页面，支持设置时间范围，查询相关操作记录。

日志服务
日志投递

最近更新时间：2025-01-08 15:23:52

DDoS 防护提供日志投递功能，通过日志投递，可采集来源为 DDoS 防护实例的慢日志和错误日志数据，并投递至日志服务（Cloud Log Service，CLS）进行分析，以便快速监控和定位业务问题。本文为您介绍如何通过控制台开启或关闭日志投递功能。

说明：
- 使用该功能前，请确保您已开通 日志服务 CLS 。
- 仅DDoS 高防包实例、DDoS 高防 IP 实例支持使用日志投递功能。

字段说明

DDoS 攻击开始通用字段

字段名称	数据类型	说明
AttackStartTime	Timestamp ISO8601	DDoS 攻击开始的时间。示例值：2024-10-14T05:13:43Z，表示 2024年10月14日 UTC+0 时区时间 05:13:43，等同于 2024年10月14日 UTC+8 时区（北京时间）13:13:43
AttackTraffic	String	攻击流量（单位：Mbps）
AttackPacketRate	String	攻击包速率（单位：pps）
AttackTrafficType	Integer	攻击流量类型

DDoS 攻击结束通用字段

字段名称	数据类型	说明
AttackStartTime	Timestamp ISO8601	DDoS 攻击开始的时间。示例值：2024-10-14T05:13:43Z，表示 2024年10月14日 UTC+0 时区时间 05:13:43，等同于 2024年10月14日 UTC+8 时区（北京时间）13:13:43
AttackEndTime	Timestamp ISO8601	DDoS 攻击结束的时间。示例值：2024-10-14T05:13:43Z，表示 2024年10月14日 UTC+0 时区时间 05:13:43，等同于 2024年10月14日 UTC+8 时区（北京时间）13:13:43
AttackTrafficPeak	String	攻击流量峰值（单位：Mbps）
AttackTrafficType	Integer	攻击流量类型
CumulativeCleanedTraffic	String	累积清洗流量（单位：Mbps）

CC 攻击开始通用字段

字段名称	数据类型	说明
AttackStartTime	Timestamp ISO8601	CC 攻击开始的时间。示例值：2024-10-14T05:13:43Z，表示 2024年10月14日 UTC+0 时区时间 05:13:43，等同于 2024年10月14日 UTC+8 时区（北京时间）13:13:43
CurrentRequestRate	String	当前请求速率（单位：QPS）
CurrentCleaningRate	String	当前清洗速率（单位：QPS）

CC 攻击结束通用字段

字段名称	数据类型	说明
AttackStartTime	Timestamp ISO8601	CC 攻击开始的时间。示例值：2024-10-14T05:13:43Z，表示 2024年10月14日 UTC+0 时区时间 05:13:43，等同于 2024年10月14日 UTC+8 时区（北京时间）13:13:43
AttackEndTime	Timestamp ISO8601	CC 攻击结束的时间。示例值：2024-10-14T05:13:43Z，表示 2024年10月14日 UTC+0 时区时间 05:13:43，等同于 2024年10月14日 UTC+8 时区（北京时间）13:13:43
MaxRequestRate	String	最大请求速率（单位：QPS）
MaxCleaningRate	String	最大清洗速率（单位：QPS）
CumulativeBlockedIllegalRequestCount	String	累积拦截非法请求数（单位：QPS）

封堵事件通用字段

字段名称	数据类型	说明
BlockTime	Timestamp ISO8601	IP 封堵的时间。示例值：2024-10-14T05:13:43Z，表示 2024年10月14日 UTC+0 时区时间 05:13:43，等同于 2024年10月14日 UTC+8 时区（北京时间）13:13:43
ExpectedUnblockTime	Timestamp ISO8601	预计 IP 解封的时间。示例值：2024-10-14T05:13:43Z，表示 2024年10月14日 UTC+0 时区时间 05:13:43，等同于 2024年10月14日 UTC+8 时区（北京时间）13:13:43
AttackTrafficPeak	String	攻击流量峰值（单位：Mbps）
BlockType	Integer	封堵类型

解封事件通用字段

字段名称	数据类型	说明
UnblockTime	Timestamp ISO8601	IP 解封的时间。示例值：2024-10-14T05:13:43Z，表示 2024年10月14日 UTC+0 时区时间 05:13:43，等同于 2024年10月14日 UTC+8 时区（北京时间）13:13:43
UnblockMethod	Integer	接触封堵方式
RemainingSelfUnblockCountToday	String	当前剩余自助解封次数

日志示例

单条 DDoS 攻击开始日志示例

```
{
"AttackTraffic":"309999"
"AttackPacketRate":"988888"
"AttackStartTime":"2024-11-27T17:50:38Z"
"AttackTrafficType":"TCPFLOOD"
}
```

单条 DDoS 攻击结束日志示例

```
{
"AttackTrafficPeak":"309999"
"AttackStartTime":"2024-11-27T17:51:14Z"
"AttackEndTime":"2024-11-27T18:06:14Z"
"AttackTrafficType":"TCPFLOOD"
"CumulativeCleanedTraffic":"80"
}
```

单条 CC 攻击开始日志示例

```
{
"CurrentCleaningQPS":"999999"
"CurrentRequestQPS":"123456"
"AttackStartTime":"2024-11-27T16:25:00Z"
}
```

单条 CC 攻击结束日志示例

```
{
"MaxCleaningQPS":"999999"
"AttackStartTime":"2024-11-27T16:45:00Z"
"AttackEndTime":"2024-11-27T16:55:00Z"
"CumulativeBlockedIllegalRequestCount":"9"
```

```
"MaxRequestQPS":"123456"
}
```

单条封堵事件日志示例

```
{
"ExpectedUnblockTime":"2024-11-28T16:55:00Z"
"AttackTrafficPeak":"20029"
"BlockType":"tix"
"BlockTime":"2024-11-27T17:00:00Z"
}
```

单条解封事件日志示例

```
{
"UnblockMethod":"自动解封"
"RemainingSelfUnblockCountToday":"3"
"UnblockTime":"2024-11-27T17:01:00Z"
}
```

服务管理
解封中心
查看封堵时间

最近更新时间：2024-04-18 15:48:53

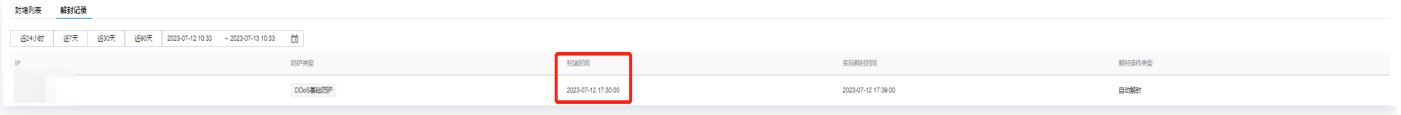
查看未解封 IP 时间

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**解封中心**。
2. 在解封中心页面的解封列表页签，选择所需 IP 的所在行，可在**封堵时间**处，查看该 IP 的封堵时间。

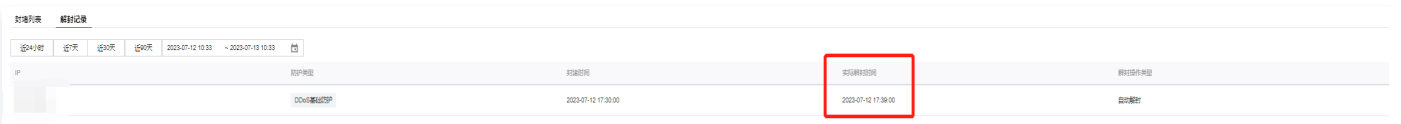
3. 在解封列表页签，选择所需 IP 的所在行，可在**预计解封时间**处，查看该 IP 的预计解封时间。

查看已解封 IP时间

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**解封中心** > **解封记录**。
2. 在解封记录页签，选择所需 IP 的所在行，可在**封堵时间**处，查看该 IP 的封堵时间。



3. 在解封操作记录页面，选择所需 IP 的所在行，可在**预计解封时间**处，查看该 IP 的实际解封时间。



解除封堵

最近更新时间：2025-03-10 10:41:42

自动解封

无需手动操作，等待到达预计解封时间，即可自动解封。可按照以下操作查看预计解封时间：

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**解封中心**。
2. 在解封中心页面的解封列表页签，选择所需 IP 的所在行，可在“封堵时间”处，查看该 IP 的封堵时间。

绑定高防包解封

- 已封堵的 IP 绑定 DDoS 高防包（不包含轻量版、高防保险）时，将会自动启用绑定高防包解封。
- 使用 DDoS 高防包（不包含轻量版、高防保险）的用户，每月将获得与其高防包实例“防护 IP 数”规格相对应的**绑定高防包解封**次数。
- 如果高防包（不包含轻量版、高防保险）在当月使用中降配，降低了“防护 IP 数”规格，系统将同时更新解封次数，并减少未使用的**绑定高防包解封**次数。
- 每月首日，**绑定高防包解封**的次数将根据上月末的‘防护 IP 数’进行重置。

自助解封次数

- 使用 DDoS 高防包（不包含轻量版、普惠版、高防保险）和 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。
- 使用 DDoS 高防包（轻量版）的用户每月提供三次自助解封能力，自助解封能力仅可用于解封轻量服务器资源。
- 使用 DDoS 高防包（普惠版）10Gbps 规格的用户每月提供三次自助解封能力，当月超过三次后将无法进行解封操作。

说明：

- 同一个账号内拥有多个高防产品，该账号每日自助解封的次数上限为三次。
- 由于解封涉及腾讯云 DDoS 防护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。

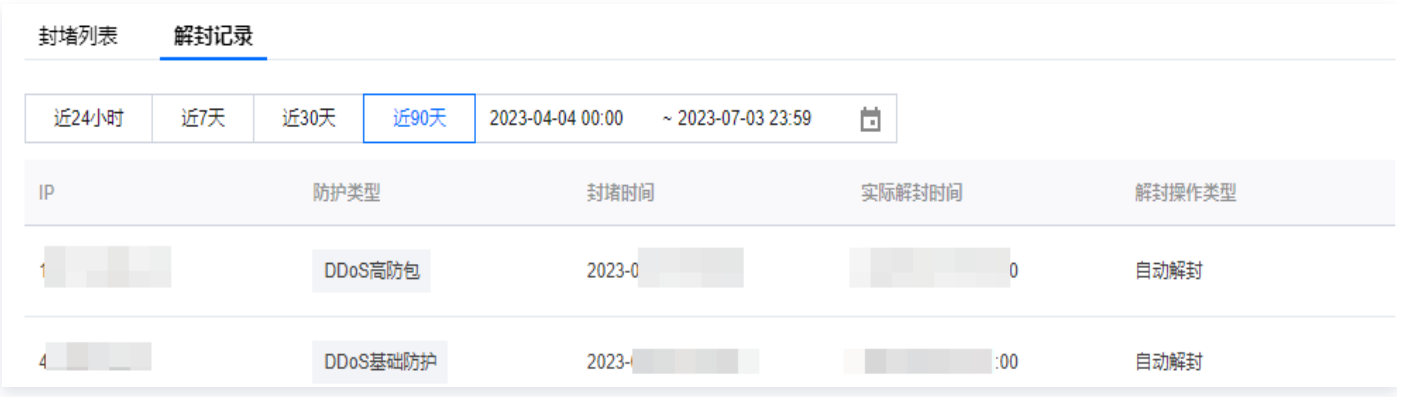
自助解封

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**解封中心**。
2. 在解封中心页面的解封列表页签，找到状态为“自动解封中”的防护 IP，在右侧操作栏中，单击**解封**。

3. 在“解除封堵”对话框中，单击**确定**，您会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

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**解封中心 > 解封记录**。
2. 在解封记录页签，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、自助解封等操作记录。



连接已被封堵的服务器

最近更新时间：2025-01-24 14:25:43

本文档为您介绍如何连接已被封堵的服务器。

操作步骤

1. 登录 云服务器控制台，在左侧导航中，单击**实例**，进入实例页面。
2. 在实例页面，单击左上角的区域下拉框，切换地域。
3. 在实例页面，单击搜索框，通过“实例名、实例 ID、实例状态”等关键字，查找对应的封堵服务器。

4. 在被封堵服务器所在行，单击**登录**，弹出登录 Linux 实例弹窗。

5. 在登录 Linux 实例弹窗，单击 **VNC 登录**，即可通过浏览器 VNC 方式连接。


登录
腾讯云产品
云服务器（CVM）
连接协议
免密连接（TAT）
终端连接（SSH）
连接网络
公网
连接端口
22
验证方式
密码验证
密钥验证
输入密码
使用托管密码
用户名
root
密码
请输入密码
忘记密码?
保存登录信息与登录凭证，下次快速登录
如何快速登录
登录
其他登录方式
VNC登录
自助检测工具
点击检测
参考文档进行问题排查：
无法登录Linux实例

告警中心
设置安全事件通知

最近更新时间：2024-04-18 15:48:53

当您所接入高防包的防护 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、微信等方式实际接收方式以您在 消息中心订阅 配置为准，向您推送告警消息：

- 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 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 DDoS 防护（新版）控制台，在左侧导航栏中，单击**告警通知**。
2. 在右侧的功能卡片中可以分别设置“单 IP 入流量告警阈值”、“DDoS 清洗阈值”和“CC 清洗阈值”。

3. 单击功能卡片的**高级设置**，进入告警配置列表为每个高防包资源设置不同的告警阈值。
   - 单 IP 入流量告警

   - DDoS 清洗阈值

   - CC清洗流量告警

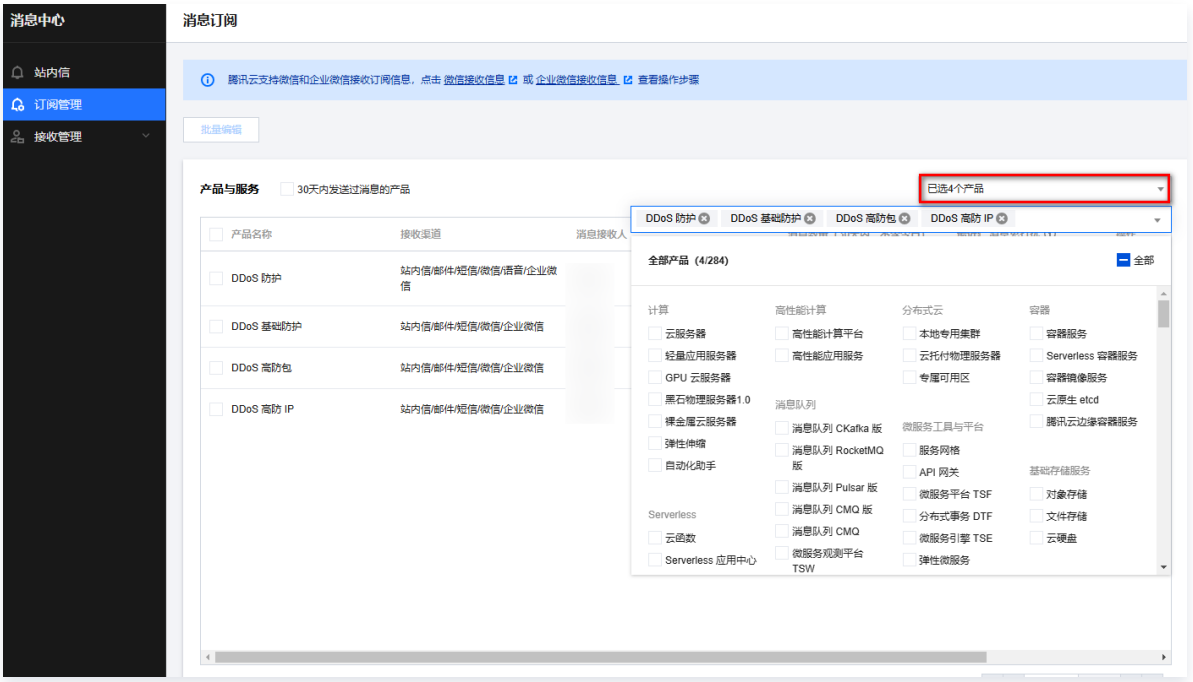
设置通知方式

最近更新时间：2025-02-10 10:56:22

1. 登录您的腾讯云账号，进入 消息中心。

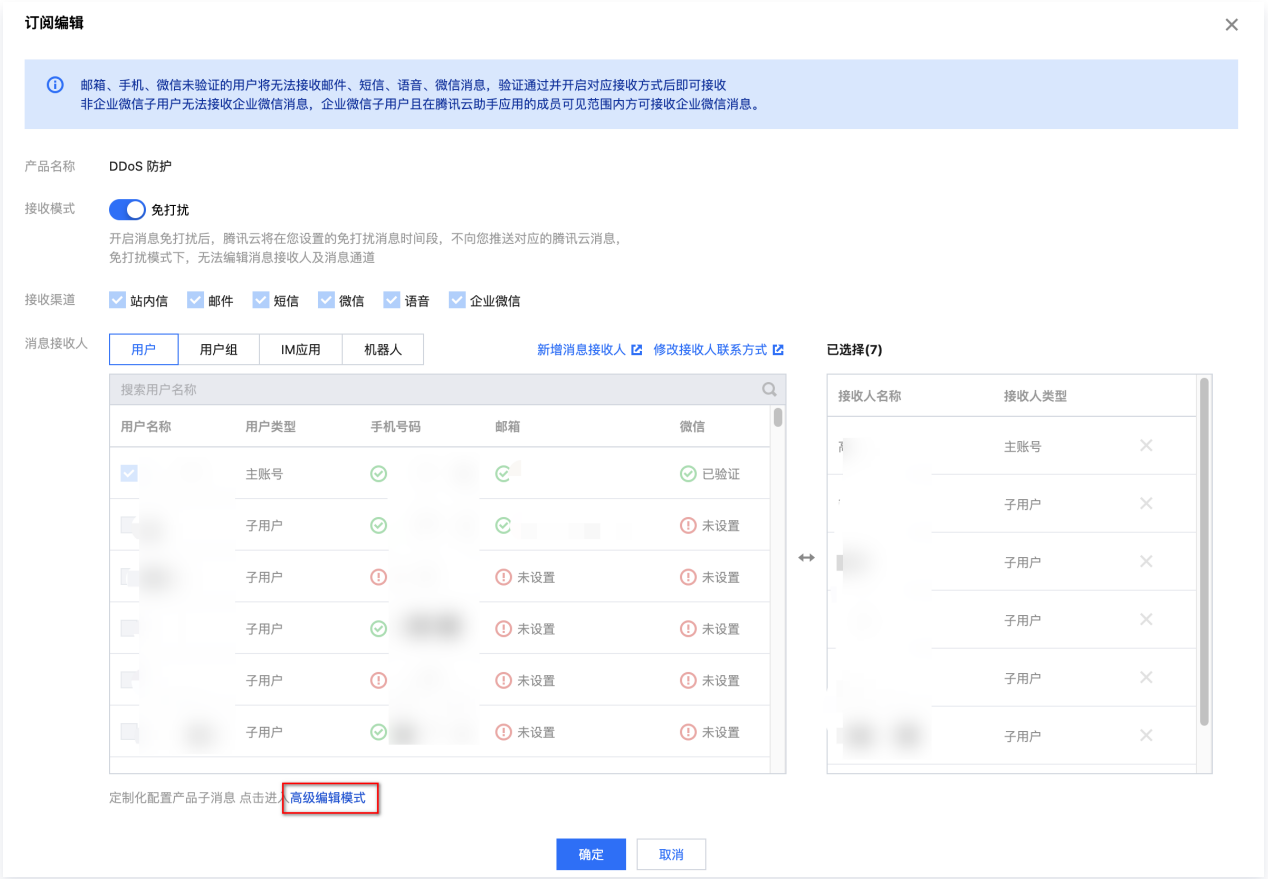
> **说明：**
>
> 您也可以登录 控制台，单击右上角的，在弹出页面单击**查看更多**，进入消息中心。

2. 在左侧目录中单击**订阅管理**，并选择需要接收消息的产品。

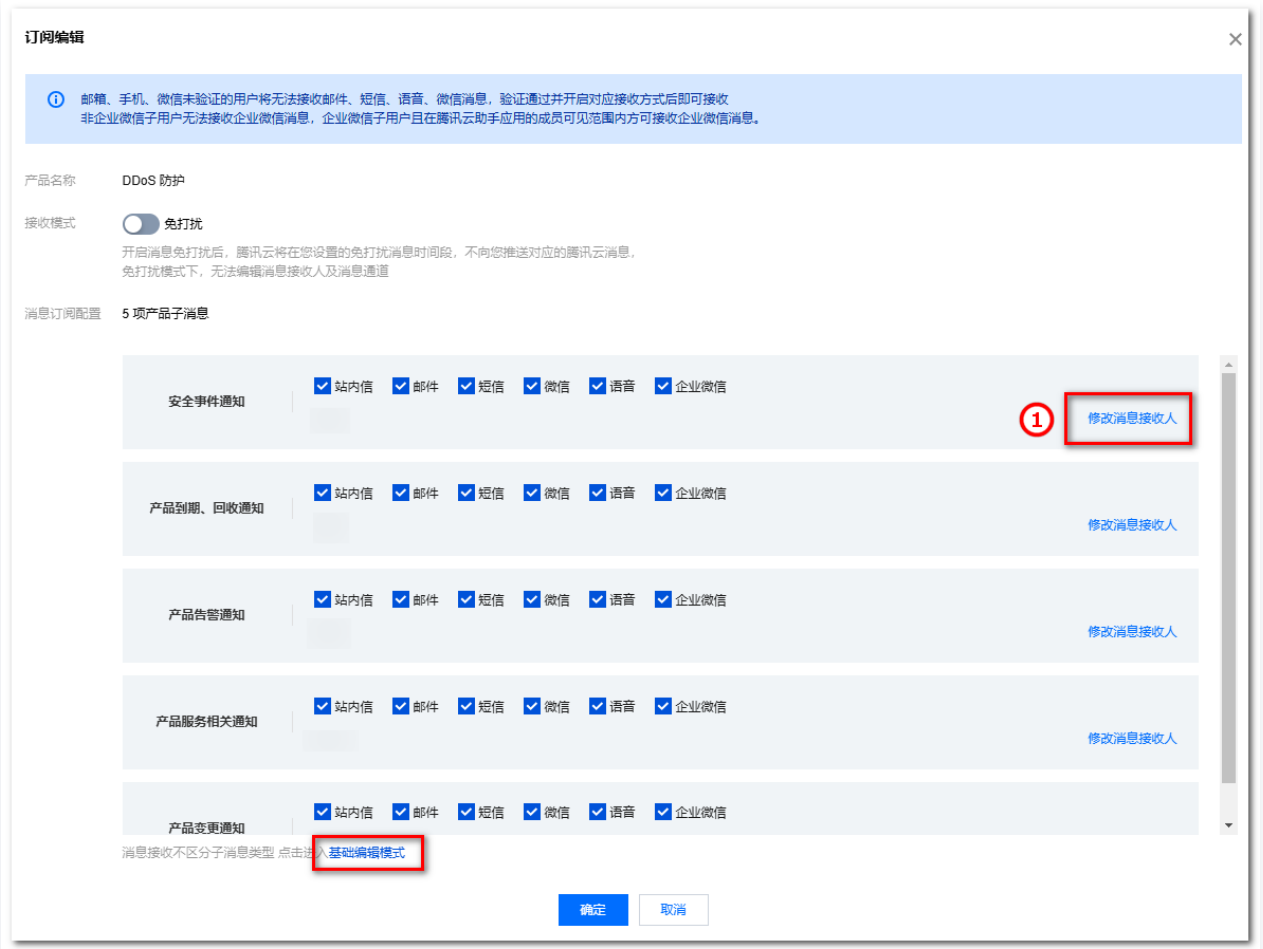


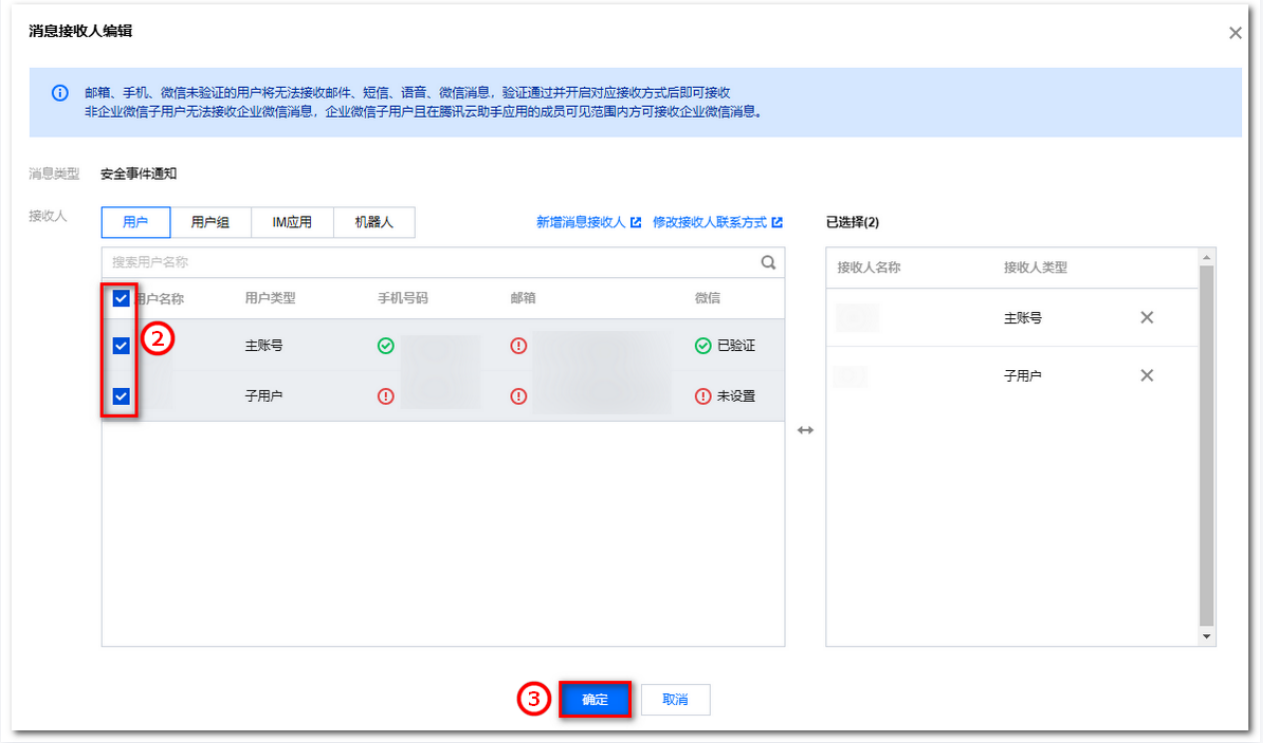
3. 在消息订阅页面，选择接收方式，单击**编辑**。

4. 在订阅编辑弹窗中，分为基础模式和高级模式，支持在左下角处进行模式切换。
   - 基础编辑：进行消息接收人的设置，设置完成后单击**确定**即可。



- **高级编辑：单击产品子消息右侧的修改消息接收人，进行消息接收人的设置，设置完成后单击确定即可。**


订阅编辑
邮箱、手机、微信未验证的用户将无法接收邮件、短信、语音、微信消息，验证通过并开启对应接收方式后即可接收
非企业微信子用户无法接收企业微信消息，企业微信子用户且在腾讯云助手应用的成员可见范围内方可接收企业微信消息。
产品名称
DDoS 防护
接收模式
免打扰
开启消息免打扰后，腾讯云将在您设置的免打扰消息时间段，不向您推送对应的腾讯云消息，
免打扰模式下，无法编辑消息接收人及消息通道
消息订阅配置
5 项产品子消息
安全事件通知
站内信 邮件 短信 微信 语音 企业微信
1
修改消息接收人
产品到期、回收通知
站内信 邮件 短信 微信 语音 企业微信
修改消息接收人
产品告警通知
站内信 邮件 短信 微信 语音 企业微信
修改消息接收人
产品服务相关通知
站内信 邮件 短信 微信 语音 企业微信
修改消息接收人
产品变更通知
站内信 邮件 短信 微信 语音 企业微信
消息接收不区分子消息类型 点击进入 基础编辑模式
确定
取消


消息接收人编辑
邮箱、手机、微信未验证的用户将无法接收邮件、短信、语音、微信消息，验证通过并开启对应接收方式后即可接收
非企业微信子用户无法接收企业微信消息，企业微信子用户且在腾讯云助手应用的成员可见范围内方可接收企业微信消息。
消息类型
安全事件通知
接收人
用户
用户组
IM应用
机器人
新增消息接收人
修改接收人联系方式
已选择(2)
搜索用户名称
用户名称
用户类型
手机号码
邮箱
微信
2
主账号
已验证
子用户
未设置
接收人名称
接收人类型
主账号
子用户
3
确定
取消

访问管理

概述

最近更新时间：2024-05-30 16:36:01

如果您在腾讯云中使用 DDoS 防护服务，需知这些服务虽由不同人员管理，但均共享您的云账号密钥，这将带来以下问题：

- 密钥被多人共享，增加了泄露的风险。
- 无法限制其他人的访问权限，容易因误操作产生安全风险。

针对此问题，您可以使用 访问管理（Cloud Access Management，CAM），通过子账号分配不同的人来管理不同的服务，从而规避上述问题。默认情况下，子账号没有使用 DDoS 防护或其相关资源的权限，需要创建策略以授予子账号使用所需资源的权限。如果您不需要对子账户进行 DDoS 防护相关资源的访问管理，可以跳过此章节。跳过这部分不会影响您对文档中其余内容的理解和使用。

访问管理

访问管理（Cloud Access Management，CAM）可以帮助您安全、便捷地管理对腾讯云服务和资源的访问。您可以使用 CAM 创建子用户、用户组和角色，并通过策略控制其访问范围。CAM 支持用户和角色 SSO 能力，您可以根据具体管理场景针对性设置企业内用户和腾讯云的互通能力。
您最初创建的腾讯云主账号，拥有整个账号全部腾讯云服务和资源的完全访问权限，建议您保护好主账号的凭证信息，日常使用子用户或角色进行访问，并开启多因素校验和定时轮换密钥。
策略能够授权或者拒绝用户使用指定资源完成指定任务，当您在使用 CAM 时，可以将策略与一个用户或一组用户关联起来进行权限控制。DDoS 防护已接入 CAM，您可以使用 CAM 对 DDoS 防护相关资源进行权限控制。

相关概念

CAM 用户

CAM 用户 是您在腾讯云中创建的一个实体，每一个 CAM 用户仅同一个腾讯云账户关联。您注册的腾讯云账号身份为**主账号**，您可以通过 用户管理 来创建拥有不同权限的**子账号**进行协作。子账号的类型分为 子用户 、协作者 以及 消息接收人 。

策略

策略 是用于定义和描述一条或多条权限的语法规范，腾讯云的策略类型分为预设策略和自定义策略。

- 预设策略：由腾讯云创建和管理的策略，是被用户高频使用的一些常见权限集合，如资源全读写权限等。预设策略操作对象范围广，操作粒度粗，且为系统预设，不可被用户编辑。
- 自定义策略：由用户创建的策略，允许进行细粒度的权限划分。例如，为子账号关联一条使用策略，使其有权管理弹性伸缩的伸缩组，而无权管理云数据库实例。

资源

资源（resource） 是策略的元素，描述一个或多个操作对象，例如弹性伸缩的启动配置和伸缩组。

可授权的 API 操作及资源类型

最近更新时间：2024-06-18 17:14:21

简介

本文档将会为您介绍 DDoS 防护（Anti-DDoS）相关可授权的资源类型，API 操作以及预设策略。您可以在访问管理（Cloud Access Management，CAM）控制台，使用可视化的操作授予子账号预设的权限策略，如您需要授予子账号更为细致的权限，请参考本文档下方相关产品接口说明以及 授权策略语法 。

预设策略

Anti-DDoS 预设策略

Anti-DDoS 预设策略如下：

策略	说明
QcloudAntiDDoSFullAccess	DDoS 防护（AntiDDoS）全读写访问权限
QcloudAntiDDoSReadOnlyAccess	DDoS 防护（AntiDDoS）只读访问权限

其他产品预设策略

Anti-DDoS 预设策略中不包含腾讯云其他产品的相关权限，通常情况下，您还需要授予其他产品预设策略，才能正常使用 DDoS 防护控制台的全部功能，您可以授予子账号以下相关的预设策略：

策略	说明
QcloudCVMReadOnlyAccess	云服务器（CVM）相关资源只读访问权限
QcloudAPIGWReadOnlyAccess	API 网关（API Gateway）只读访问权限
QcloudTSEReadOnlyAccess	腾讯云微服务引擎（TSE）只读访问权限
QcloudBMEIPReadOnlyAccess	黑石弹性公网 IP（BM EIP）只读访问权限
QcloudBMInnerReadOnlyAccess	黑石物理服务器（BM）只读访问权限
QcloudBMLBReadOnlyAccess	黑石负载均衡（BM LB）只读访问权限
QcloudLighthouseReadOnlyAccess	轻量应用服务器（Lighthouse）只读访问权限

自定义策略

可授权的资源类型

资源类型描述了资源的层次关系并且用于指定操作的具体资源。例如，若子用户需要查询某个地域的高防包实例列表，则可以通过云访问管理（Cloud Access Management，CAM）将 Anti-DDoS 的资源类型配置到策略中。

资源类型	描述	资源描述方式
antiddos	高防包实例	qcs::antiddos:${Region}:${uin}/${Owneruin}:antiddos/${resourceId}

可授权的操作及产品权限

为了配置更精确的 Anti-DDoS 资源访问控制，您需要为子用户配置产品的 API 操作权限，具体操作权限如下表：

API操作	描述
cvm:DescribeInstances	获取实例列表
lighthouse:DescribeInstances	获取轻量应用服务器实例列表
clb:DescribeLoadBalancers	获取负载均衡实例列表
vpc:DescribeNatGateways	获取 NAT 网关列表
vpc:DescribeVpngateways	获取 VPN 网关列表
vpc:DescribeNetworkInterfaces	获取弹性网卡列表
vpc:DescribeDirectConnectGateways	获取专线网关列表
apigateway:DescribeExclusiveInstancesStatus	获取独享网关实例状态
tke:DescribeClusters	获取集群列表
bmlb:DescribeLoadBalancers	获取黑石负载均衡实例列表
bmvpc:DescribeEips	获取黑石弹性 IP
tag:GetTagKeys	获取标签键列表

授权策略语法

最近更新时间：2024-05-30 16:36:01

简介

本文档将会为您介绍 DDoS 防护（Anti-DDoS）相关的授权策略语法，方便您进行更细致的授权操作。

策略语法

Anti-DDoS 支持的 CAM 策略。

```
{
        "version":"2.0",
        "statement":
        [
           {
              "effect":"effect",
              "action":["action"],
              "resource":["resource"],
           }
       ]
}
```

- **版本 version** 是必填项，目前仅允许值为"2.0"。
- **语句 statement** 是用来描述一条或多条权限的详细信息。该元素包括 effect、action、resource，condition 等多个其他元素的权限或权限集合。一条策略有且仅有一个 statement 元素。
- **影响 effect** 描述声明产生的结果是“允许”还是“显式拒绝”。包括 allow（允许）和 deny（显式拒绝）两种情况。该元素是必填项。
- **操作 action** 用来描述允许或拒绝的操作。操作可以是 API（以 name 前缀描述）或者功能集（一组特定的 API，以 permid 前缀描述）。该元素是必填项。
- **资源 resource** 描述授权的具体数据。资源是用六段式描述。每款产品的资源定义详情会有所区别。该元素是必填项。

Anti-DDoS 的操作

在访问管理（Cloud Access Management，CAM）策略语句中，您可以从支持 CAM 的任何服务中指定任意的 API 操作。对于 Anti-DDoS，请使用以 `antiddos:` 为前缀的 API。例如：`antiddos:DescribeListBGPInstances` 或者 `antiddos:DescribeCloudProtectInstance`。
如果您要在单个语句中指定多个操作的时候，请使用逗号将它们隔开，如下所示：

```
"action":["antiddos:DescribeListBGPInstances","antiddos:DescribeCloudProtectInstance"]
```

您也可以使用通配符指定多项操作。例如，您可以指定名字以单词“Describe”开头的所有操作，如下所示：

```
"action":["antiddos:Describe*"]
```

如果您要指定 Anti-DDoS 中所有操作，请使用 * 通配符，如下所示：

```
"action": ["antiddos:*"]
```

Anti-DDoS 的资源路径

每个 CAM 策略语句都有适用于自己的资源。 资源路径的一般形式如下：

```
qcs:project_id:service_type:region:account:resource
```

- **qcs**：qcloud service 的简称，表示是腾讯云的云资源。
- **project_id**：描述项目信息，仅为了兼容 CAM 早期逻辑，无需填写。
- **service_type**：产品简称，如：antiddos。
- **region**：地域信息，如：ap-guangzhou。
- **account**：资源拥有者的根账号信息，如：`uin/1234567890。
- **resource**：各产品的具体资源详情，如：`antiddos/bgp-00000012` 或者 `antiddos/*` 。例如，您可以指定高防实例 (bgp-00000012)，如下所示：

  ```
  "resource":["qcs::antiddos:ap-guangzhou:uin/1234567890:antiddos/bgp-00000012"]
  ```

您还可以使用 * 通配符指定属于特定账户的所有实例，如下所示：

```
"resource":["qcs::antiddos:ap-guangzhou:uin/1234567890:antiddos/*"]
```

您要指定所有资源，或者如果特定 API 操作不支持资源级权限，请在 Resource 元素中使用 * 通配符，如下所示：

```
"resource": ["*"]
```

如果您想要在一条指令中同时指定多个资源，请使用逗号将它们隔开，如下所示为指定两个资源的例子：

```
"resource":["resource1","resource2"]
```

下表描述了 Anti-DDoS 能够使用的资源和对应的资源描述方法。在下表中，$为前缀的单词均为代称。

- 其中，region 指代的是地域。
- 其中，account 指代的是账户 ID。
- 其中，resourceId 指代的是高防实例 ID。

资源	授权策略中的资源描述方法
高防实例	`qcs::${antiddos}:${Region}:uin/${OwnerUin}:antiddos/${resourceId}`

授权策略示例

最近更新时间：2024-05-30 16:36:01

操作场景

您可以通过使用访问管理（Cloud Access Management，CAM）策略，授予用户在 DDoS 防护（Anti-DDoS）控制台中查看和使用特定资源的权限。本文档提供了查看和使用特定资源的权限示例，指导用户如何使用控制台的特定部分的策略。

操作示例

Anti-DDoS 的全读写策略

如果您希望用户能够管理 Anti-DDoS 实例的权限，您可以将策略 QcloudAntiDDoSFullAccess 应用于该用户。该策略允许用户操作 Anti-DDoS 下的所有资源，但您还需要授予防护资源产品的相关权限，以确保用户能够正常使用 Anti-DDoS。权限详情请参见 可授权的 API 操作及资源类型 。具体操作步骤如下：请按照 授权管理 中的指引，将预设策略 QcloudAntiDDoSFullAccess 授权给用户。

Anti-DDoS 的只读策略

如果您希望用户拥有查询 Anti-DDoS 实例的权限，但不具备操作资源的权限，您可以将策略 QcloudAntiDDoSReadOnlyAccess 应用于该用户。该策略旨在通过授予用户权限来操作 Anti-DDoS 中所有以“Describe”和“List”开头的操作，从而实现其目的。此外，您还需要授予用户防护资源产品的相关权限，以确保他们能够正常使用 Anti-DDoS。具体操作步骤如下：参考 授权管理 ，将预设策略 QcloudAntiDDoSReadOnlyAccess 授权给用户。

授权用户拥有特定 Anti-DDoS 操作权限策略

如果您希望授权用户拥有特定 Anti-DDoS 操作权限，可将以下策略关联到该用户。具体操作步骤如下：

1. 登录 访问管理控制台 ，在左侧导航中，单击**策略**。
2. 在策略页面，单击**新建自定义策略**，选择**策略语法创建**和**空白模板**，单击**下一步**。
3. 在编辑策略页面，创建一个自定义策略。

   该策略允许用户拥有所有对 ID 为 bgp-1，地域为广州的 DDoS 防护实例的操作权限，策略内容可参考以下策略语法进行设置：

```
{
 "version": "2.0",
 "statement": [
  {
      "action": ["antiddos:*"],
      "resource": ["qcs::antiddos:ap-guangzhou::antiddos/bgp-1"],
      "effect": "allow"
  }
 ]
}
```

4. 单击**完成**后，找到创建的策略，在该策略行的 “操作” 列中，单击**关联用户/用户组/角色**。
5. 在弹出的“关联用户/用户组/角色”窗口，勾选要关联的用户，单击**确定**，完成通过策略关联用户操作。

> **说明：**

> 此处账户字段为空，代表创建该策略的 CAM 用户所属主账号下的资源，如您仍有疑问，可参考 资源描述方式 。

授权用户拥有特定地域 Anti-DDoS 的操作权限策略

如果您希望授权用户拥有特定地域 Anti-DDoS 的操作权限，可将以下策略关联到该用户。具体操作步骤如下：

1. 登录 访问管理控制台 ，在左侧导航中，单击**策略**。
2. 在策略页面，单击**新建自定义策略**，选择**策略语法创建**和**空白模板**，单击**下一步**。
3. 在编辑策略页面，创建一个自定义策略。

   该策略允许用户拥有对广州地域的 DDoS防护实例的所有操作权限，策略内容可参考以下策略语法进行设置：

```
{
 "version": "2.0",
 "statement": [
  {
      "action": ["antiddos:*"],
      "resource": ["qcs::antiddos:ap-guangzhou::*"],
      "effect": "allow"
  }
 ]
}
```

4. 单击**完成**后，找到创建的策略，在该策略行的 “操作” 列中，单击**关联用户/组/角色**。
5. 在弹出的“关联用户/用户组/角色”窗口，勾选要关联的用户，单击**确定**，完成通过策略关联用户操作。

自定义策略

如果您觉得预设策略不能满足您的要求，您可以通过创建自定义策略达到目的。具体操作步骤请参考 策略 。更多 Anti-DDoS 相关的策略语法请参考 授权策略语法 。