DDoS 高防 IP

操作指南

产品文档

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

操作指南
操作概览

最近更新时间：2022-04-26 18:57:18

您在使用 DDoS 高防 IP 时，可能碰到如配置 DDoS 高防 IP 实例、查看安全防护概览、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。

概览与限制

- 防护概览
- 使用限制

防护配置

DDoS 防护

- DDoS 防护等级
- 协议封禁
- 水印防护
- 特征过滤
- AI 防护
- 异常连接防护
- IP 黑白名单
- 端口过滤
- 区域封禁
- IP 端口限速
- 连接类攻击防护

CC 防护

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

业务接入

- 端口接入
- 域名接入
- 配置会话保持
- 配置健康检查

实例管理

- 查看实例信息
- 设置实例别名与标签
- 修改弹性防护带宽

调度与解封

配置智能调度

操作日志

查看操作日志

封堵相关操作

- 查看封堵时间
- 设置安全事件通知
- 连接已被封堵的服务器
- 解除封堵

防护概览

最近更新时间：2022-04-26 18:58:25

防护概览（总览）

全部业务安全状态展示，您可以在 DDoS 防护控制台的防护概览页查看全量实时、业务指标和 DDoS 攻击事件的防护情况，包括基础防护业务、DDoS 高防包防护业务、DDoS 高防 IP 防护业务，便于您分析与溯源。

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. 在攻击态势模块中，可查看当前业务是否存在风险，和最近一次攻击的时间的攻击类型。当有攻击存在时，单击**升级防护**可进入购买页。

3. 在攻击态势模块中，还可以直观查看各项数据情况。

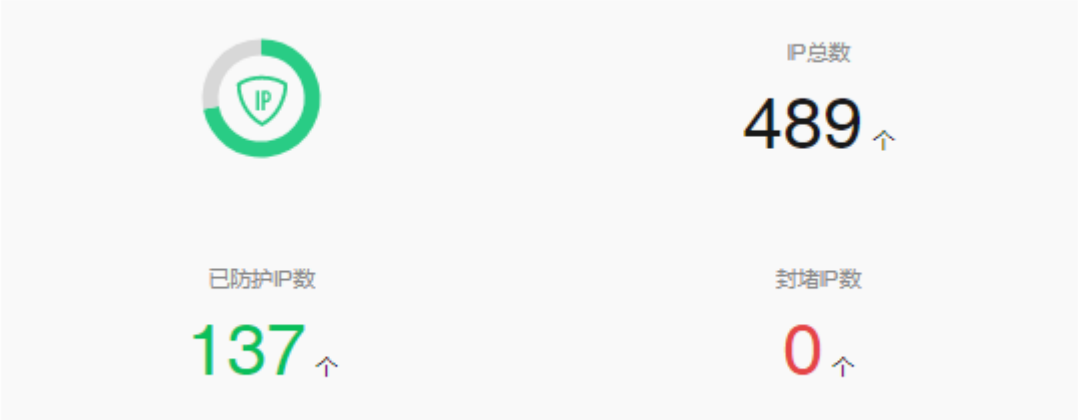
字段说明：

- 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。

- 已防护 IP 数：接入高防包的业务 IP 和高防 IP 实例。
- 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。
- 被攻击域名数：高防 IP 被攻击的域名数、被攻击的端口所影响的域名数。
- 已防护域名数：高防 IP 实例的域名接入数量。
- 攻击峰值：当前攻击事件中的最高攻击带宽。

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. 在防御态势模块的统计图中，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，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。

查看高防 IP 实例统计

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. 在高防实例统计模块中，展示高防 IP 资源的安全状态，可以快速全面了解风险业务分布。

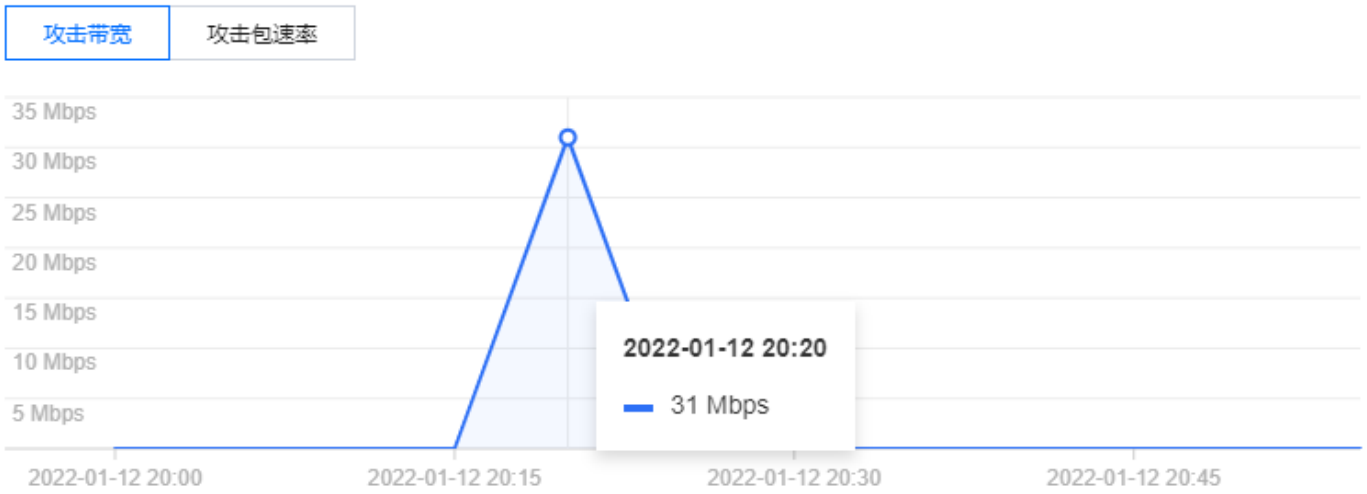
查看近期安全事件

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。

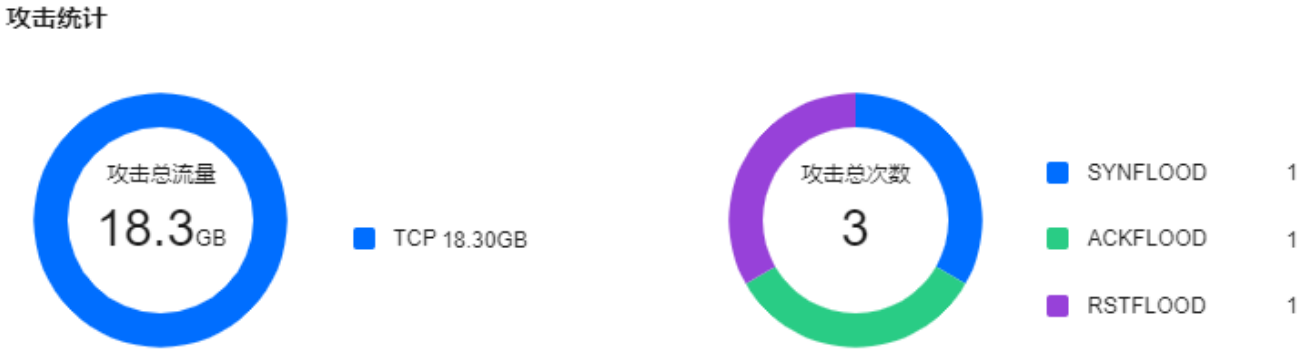
4. 在事件详情页面的攻击趋势模块，可查看网络攻击流量带宽或攻击包速率趋势。当遭受攻击时，在流量趋势图中可以明显看出攻击流量的峰值。

> **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。

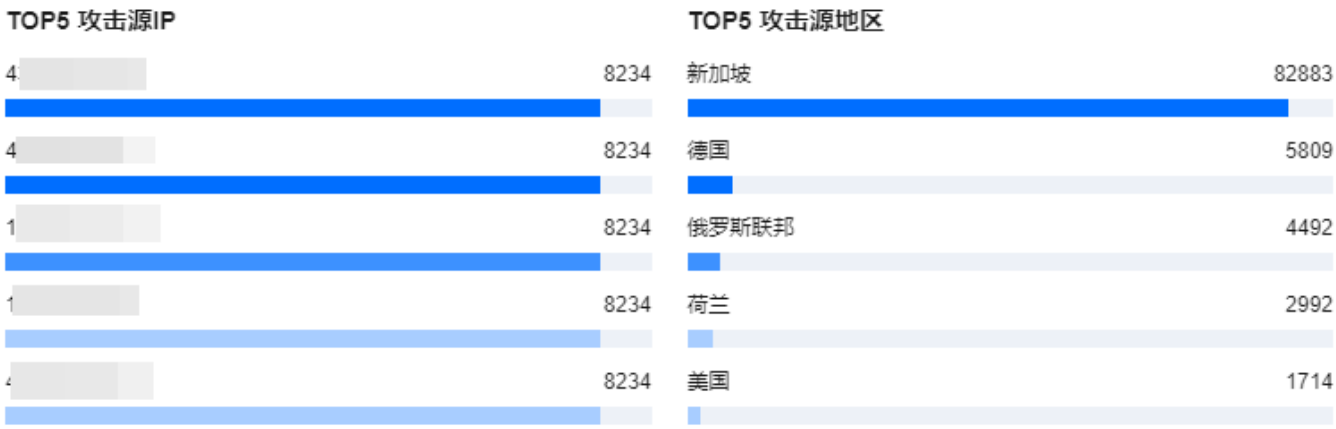


字段说明：

- 攻击流量协议分布：查看该时间范围内，所选择的高防 IP 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 IP 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。

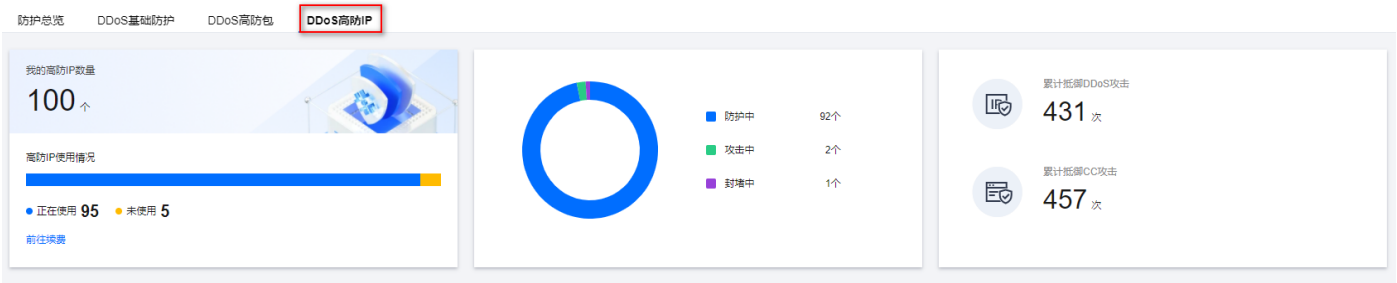
攻击源IP	地区	累计攻击流量	累计攻击包量
[redacted]	未知	10.4 MB	132
[redacted]	[redacted]技	660.3 MB	8234
[redacted]	[redacted]技	660.3 MB	8234

DDoS 高防 IP 概览

将防护 IP 接入到 DDoS 高防 IP 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（新版）控制台，在左侧导航栏中，单击**防护概览** > **DDoS 高防 IP**。

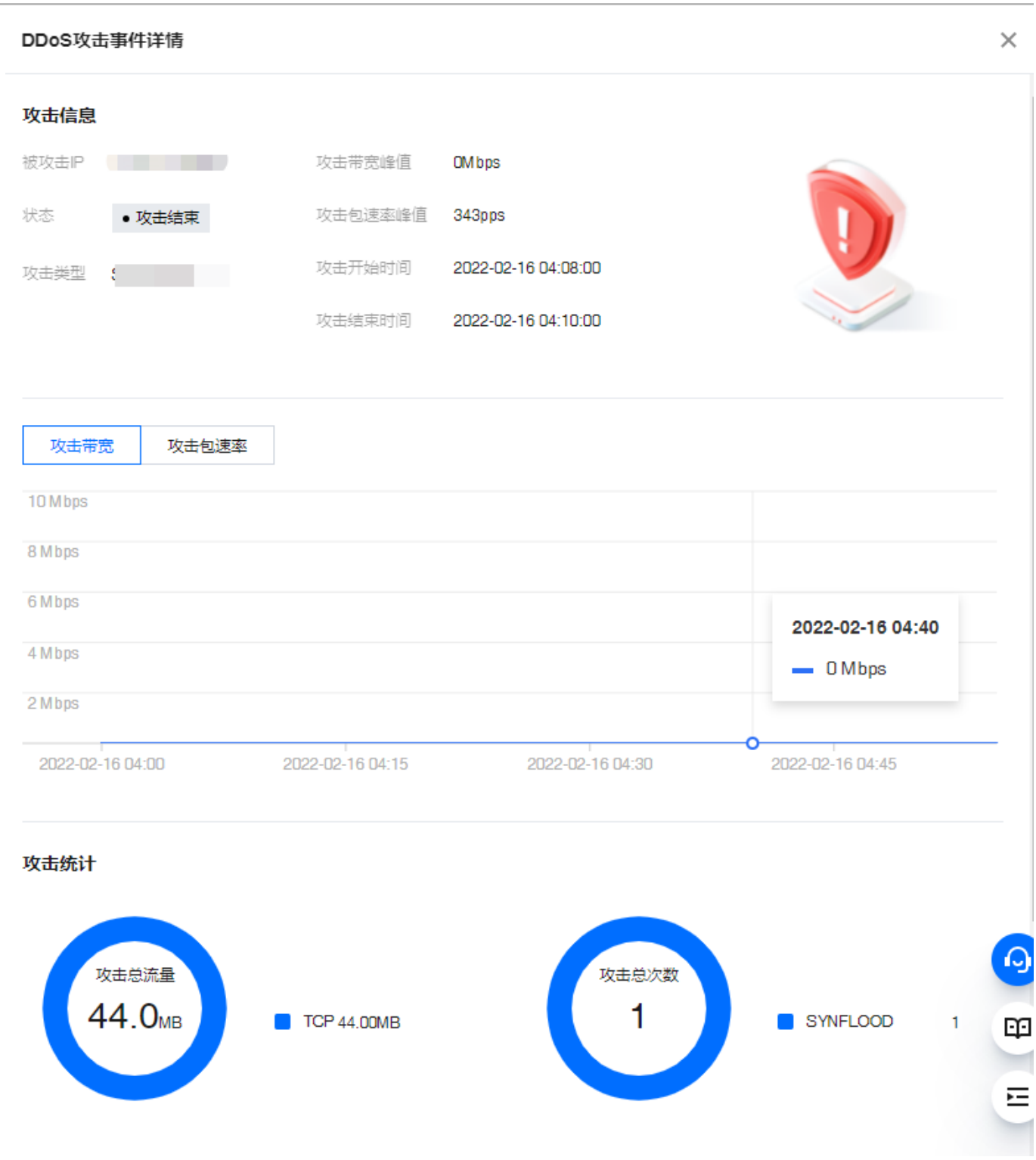


2. 在 DDoS 攻击页签，设置查询时间范围，选择目的地域、线路和高防 IP 实例，查看是否存在攻击。默认展示全量资产的 DDoS 攻击数据。

> **说明：**
> 支持查询最多180天以内的攻击流量信息及 DDoS 攻击事件。

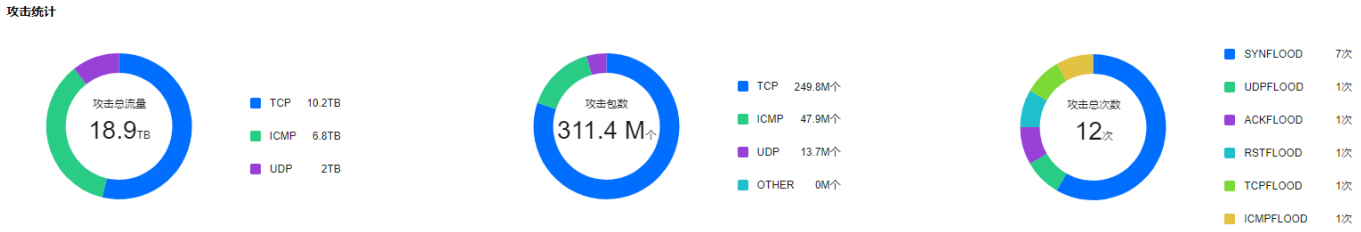
3. 查看该时间范围内所选择的高防 IP 防护遭受的攻击情况，包括网络攻击流量带宽和攻击包速率趋势。

4. 在近期安全事件模块中，可展示所遭受的 DDoS 攻击事件。可单击**查看详情**，可查看该事件的具体详情；可单击**攻击包下载**，可看到该攻击时间段的攻击采样数据列表。
   - 查看详情：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。



- **攻击包下载：下载本次攻击计时间段的攻击包采样数据，了解攻击详情，为制定针对性的防护方案提供数据支撑。**

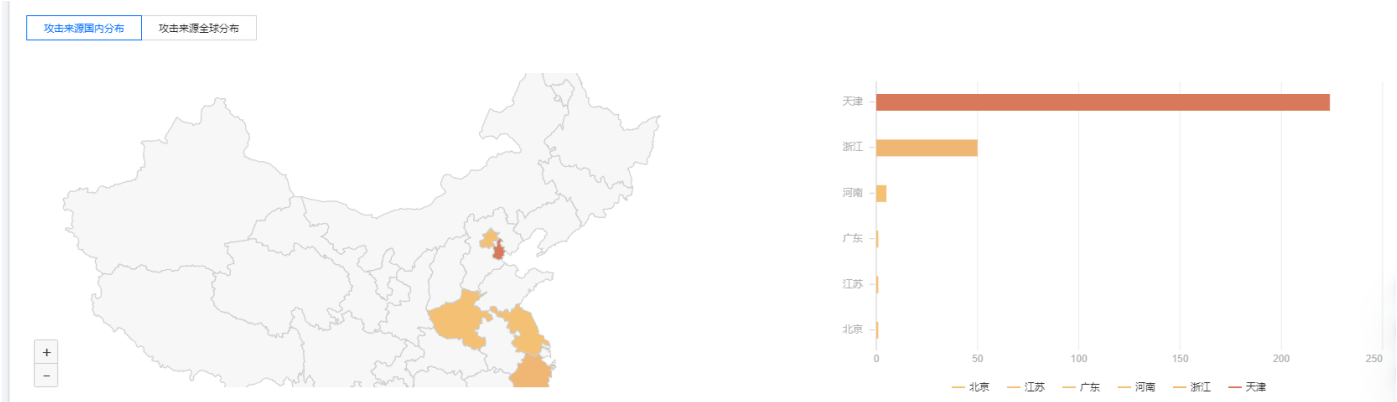
5. 在攻击统计模块中，可通过攻击流量协议分布、攻击包协议分布和攻击类型分布，查看这三个数据维度下的攻击分布情况。



字段说明：

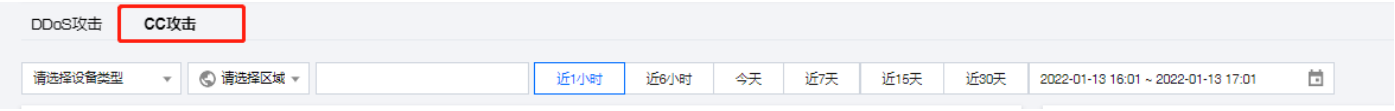
- 攻击流量协议分布：查看该时间范围内，所选择的高防 IP 实例遭受攻击事件中各协议总攻击流量的占比情况。
- 攻击包协议分布：查看该时间范围内，所选择的高防 IP 实例遭受攻击事件中各协议攻击包总数的占比情况。
- 攻击类型分布：查看该时间范围内，所选择的高防 IP 实例遭受的各攻击类型总次数占比情况。

6. 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**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。



2. 用户可以选择**今天**，查看所选择的高防包的请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：

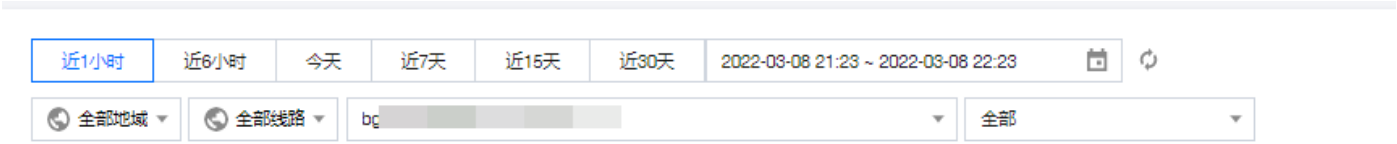
- 总请求速率：统计当前，高防 IP 接收到的总请求流量的速率（QPS）。
- 攻击请求速率：统计当前，攻击请求流量的速率（QPS）。
- 总请求数量：统计当前，高防 IP 接收到的总请求数量。
- 攻击请求次数：统计当前，高防 IP 接收到的攻击请求的次数。

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、被攻击 URI 、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。

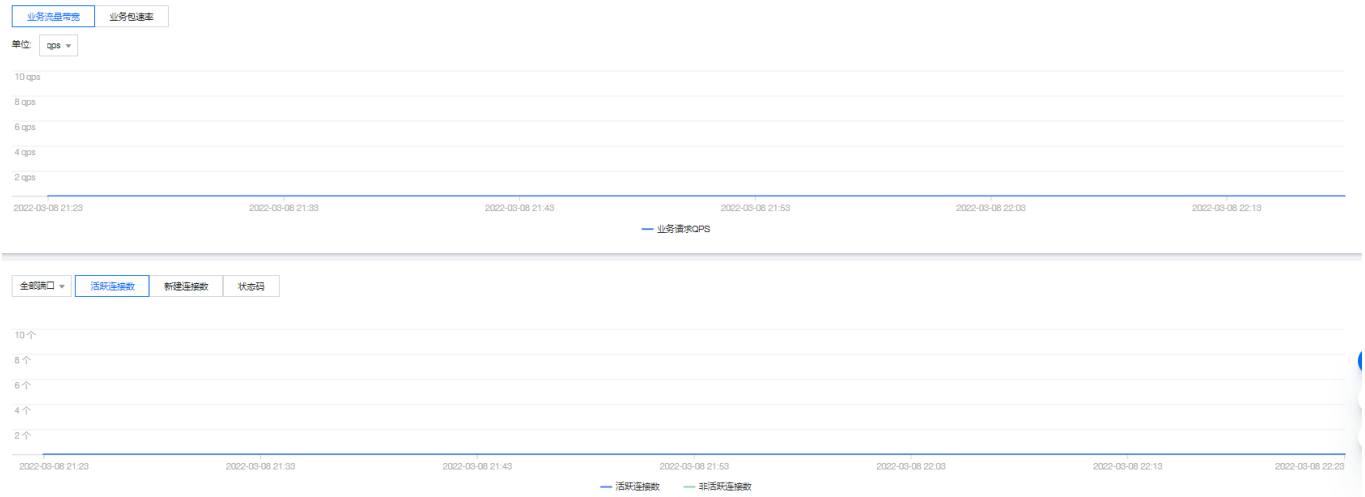
查看业务流量情况

1. 登录 DDoS 防护（新版）控制台，在左侧导航栏中，单击**DDoS 高防 IP > 业务流量**。
2. 在业务流量页面，设置查询时间范围，选择目的地域、线路和高防 IP 实例，查看是否存在攻击。默认展示全量资产的 DDoS 攻击数据。

> **说明：**
> 支持查询最多180天以内的业务流量信息及 DDoS 攻击事件。



3. 在业务流量页面，可查看该时间范围内所选择的高防 IP 下域名业务流量情况，入/出业务流量带宽趋势、入/出业务包速率的趋势及活跃连接数和新建连接数的趋势。同时，还可以查看该时间范围内的业务带宽峰值、业务连接数峰值和业务请求峰值。
   - 活跃连接数：当前时间所有 established 状态的 TCP 连接数。
   - 新建连接数：客户端每秒内新增的与高防 IP 建立通信的 TCP 连接数。



使用限制

最近更新时间：2023-02-20 15:53:14

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、硅谷、法兰克福。

防护配置
DDoS 防护
DDoS 防护等级

最近更新时间：2022-04-12 11:12:13

本文档将为您介绍针对 DDoS 攻击，DDoS 高防 IP 提供的不同防护等级的相关操作及应用场景，并为您介绍如何在控制台中设置 DDoS 防护等级。

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：

宽松防护

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。

适中防护

防护等级	防护操作	描述
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。

严格防护

防护等级	防护操作	描述

防护等级	防护操作	描述
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：

- **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 IP（境外企业版）实例采用适中防护等级,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。**

前提条件

您需要成功 购买 DDoS 高防 IP ，并设置防护对象。

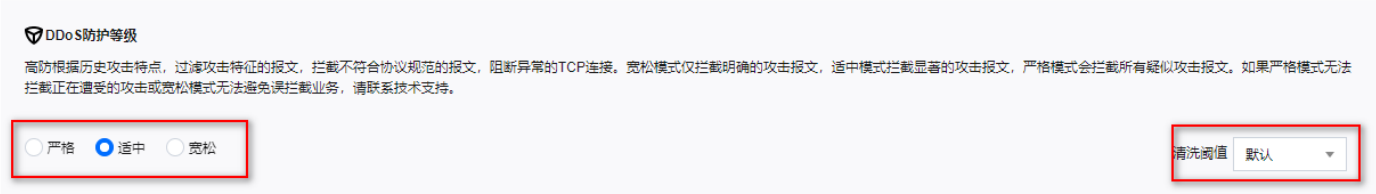
操作步骤

1. 登录 DDoS 高防 IP 控制台，在左侧导航中，单击**防护配置** > **DDoS 防护**。
2. 在 DDoS 防护页面的左侧，选中高防 IP 的 ID，如“bgpip-xxxxxx”。

3. 在 DDoS 防护等级卡片中，设置“防护等级”与“清洗阈值”。

说明：

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。



配置参数说明：

- **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 实例采用适中防护等级，您可以根据实际业务防护需求自由调整 DDoS 防护等级。

- **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。

协议封禁

最近更新时间：2022-12-01 11:14:58

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，配置后相关访问请求会被直接截断。由于 UDP 协议的无连接性（不像 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。

前提条件

您需要已成功 购买 DDoS 高防 IP，并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP 控制台，在左侧导航中，单击**防护配置** > **DDoS 防护**。
2. 在 DDoS 防护页面的左侧，选中高防 IP 的 ID，如“bgpip-xxxxxx”。

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**新建**。

> **说明：**
> 仅首次使用协议封禁时，会出现新建按钮。

5. 在新建协议封禁弹窗中，单击开启所需协议后，单击**确定**，创建协议封禁规则。

6. 新建完成后，协议封禁列表将新增一条协议封禁规则，单击 ，修改协议封禁规则开关。

水印防护

最近更新时间：2022-04-22 10:56:03

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4层 CC 攻击，如模拟业务报文攻击和重放攻击等。

前提条件

您需要已成功 购买 DDoS 高防 IP ，并设置防护对象。

> **说明：**
> 此功能为额外付费功能，请 联系我们 进行开通。

操作步骤

1. 登录 DDoS 高防 IP 控制台，在左侧导航中，单击**防护配置** > **DDoS 防护**。
2. 在 DDoS 防护页面的左侧，选中高防 IP 的 ID，如“bgpip-xxxxxx”。

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**。

5. 在新建水印防护弹窗中，填写相关字段，单击**确定**，创建水印防护规则。

6. 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。

7. 在配置密钥的界面，用户可以查看或复制密钥。

8. 在配置密钥界面，可以添加或删除密钥，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。

特征过滤

最近更新时间：2022-04-12 11:22:04

DDoS 高防支持针对 IP、TCP 及 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、拦截、丢弃、拦截并拉黑15分钟、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。

前提条件

您需要成功 购买 DDoS 高防 IP ，并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP 控制台，在左侧导航中，单击**防护配置** > **DDoS 防护**。
2. 在 DDoS 防护页面的左侧，选中高防 IP 的 ID，如“bgpip-xxxxxx”。

3. 在特征过滤卡片中，单击**设置**，进入特征过滤页面。

4. 在特征过滤页面中，单击**新建**。

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。

AI 防护

最近更新时间：2022-04-12 11:24:16

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。

前提条件

您需要成功 购买 DDoS 高防 IP，并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP 控制台，在左侧导航中，单击**防护配置** > **DDoS 防护**。
2. 在 DDoS 防护页面的左侧，选中高防 IP 的 ID，如“bgpip-xxxxxx”。

3. 在 AI 防护卡片中，单击  ，打开 AI 防护开关。

IP 黑白名单

最近更新时间：2022-12-13 11:00:43

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，当流量超过清洗阈值时，若白名单中的 IP 进行访问，将被直接放行，不经过任何防护策略过滤。若黑名单中的 IP 进行访问，将会被直接阻断。

前提条件

您需要成功 购买 DDoS 高防 IP，并设置防护对象。

> 说明：
> 创建 IP 黑白名单后常态化生效。
>
> - 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。

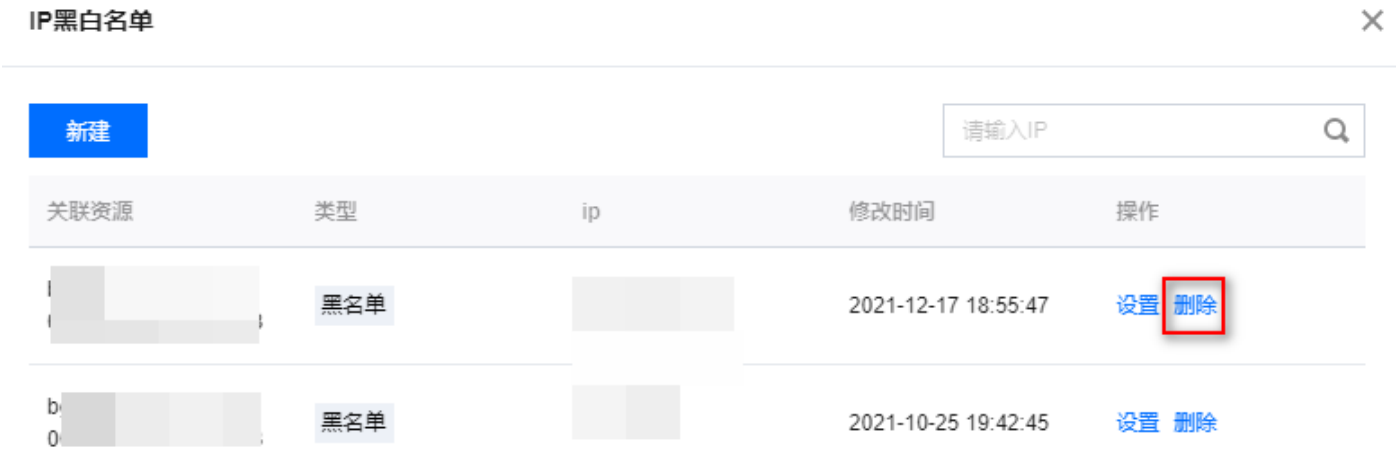
操作步骤

1. 登录 DDoS 高防 IP 控制台，在左侧导航中，单击**防护配置** > **DDoS 防护**。
2. 在 DDoS 防护页面的左侧，选中高防 IP 的 ID，如“bgpip-xxxxxx”。

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 黑白名单页面中，单击**新建**，创建 IP 黑白名单规则，选择黑白名单类型，单击**保存**。

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



端口过滤

最近更新时间：2022-04-12 14:40:54

DDoS 高防 IP 支持针对访问 DDoS 高防 IP 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。端口过滤可以精准制定针对访问的源流量，进行端口设置的防护策略。

前提条件

您需要成功 购买 DDoS 高防 IP，并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP 控制台，在左侧导航中，单击**防护配置** > **DDoS 防护**。
2. 在 DDoS 防护页面的左侧，选中高防 IP 的 ID，如“bgpip-xxxxxx”。
3. 在端口过滤卡片中，单击**设置**，进入端口过滤页面。

4. 在端口过滤页面中，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。
> - 优先级：请填写一个介于1-1000的数字，数字越小优先级越高，该条规则排列位置越靠前，默认优先级为10。

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**，可以修改特征端口规则。

区域封禁

最近更新时间：2022-04-12 11:27:36

区域封禁支持对访问 DDoS 高防 IP 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：**
> 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。

前提条件

您需要成功 购买 DDoS 高防 IP，并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP 控制台，在左侧导航中，单击**防护配置** > **DDoS 防护**。
2. 在 DDoS 防护页面的左侧，选中高防 IP 的 ID，如“bgpip-xxxxxx”。

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**。

5. 在“新建区域封禁”弹窗中，选择封禁区域，单击**确定**，创建区域封禁规则。

6. 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。

IP 端口限速

最近更新时间：2022-04-12 11:31:03

DDoS 高防 IP 支持对于业务 IP，基于 IP+端口的维度进行流量访问限速。

前提条件

您需要成功 购买 DDoS 高防 IP，并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP 控制台，在左侧导航中，单击**防护配置** > **DDoS 防护**。
2. 在 DDoS 防护页面的左侧，选中高防 IP 的 ID，如“bgpip-xxxxxx”。

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**。

5. 在新建 IP 端口限速弹窗中，选择相关协议与具体的端口，并输入限速阈值。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。

连接类攻击防护

最近更新时间：2022-04-12 11:31:32

当连接类发起异常， DDoS 高防 IP 支持自动发起禁封惩罚策略。在源 IP 最大异常连接数开启防护后，当 DDoS 高防 IP 检测到同一个源 IP 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，封禁时间为15分钟，等封禁解除后可恢复访问。支持以下字段：

> 说明：
>
> - 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。

前提条件

您需要成功 购买 DDoS 高防 IP，并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP 控制台，在左侧导航中，单击**防护配置** > **DDoS 防护**。
2. 在 DDoS 防护页面的左侧，选中高防 IP 的 ID，如“bgpip-xxxxxx”。

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中，单击**新建**，配置连接类攻击防护。
5. 在配置连接类攻击防护弹窗中，开启异常连接防护，单击**确定**。

6. 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。


连接类攻击防护
新建
请输入IP
关联资源
源新建连接限速
源并发连接限制
目的新建连接限速
目的并发连接限制
源IP最大异常连接数
操作
配置

CC 防护
CC 防护开关及清洗阈值

最近更新时间：2022-05-25 16:36:12

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：
> CC 防护的防护配置详情引导，请参见 CC 防护策略配置最佳实例。

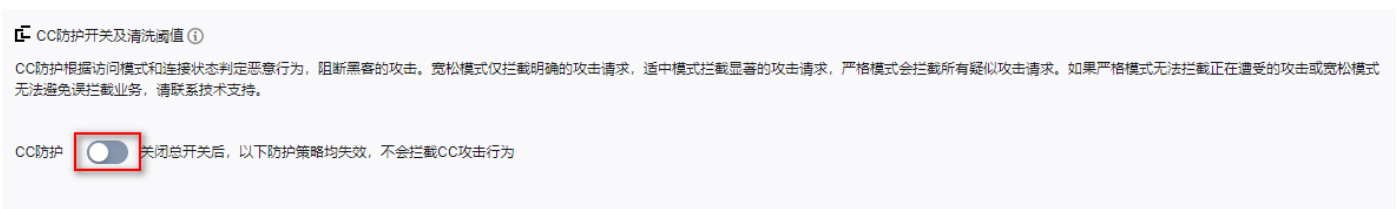
前提条件

- 您需要已成功 购买 DDoS 高防 IP，并设置防护对象。
- 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 高防 IP（新版）管理控制台，在左侧导航中，单击**防护配置** > **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启 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：2023-07-18 09:53:00

开启智能防护后，AI 智能防护基于腾讯云的大数据能力，能够自主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。

前提条件

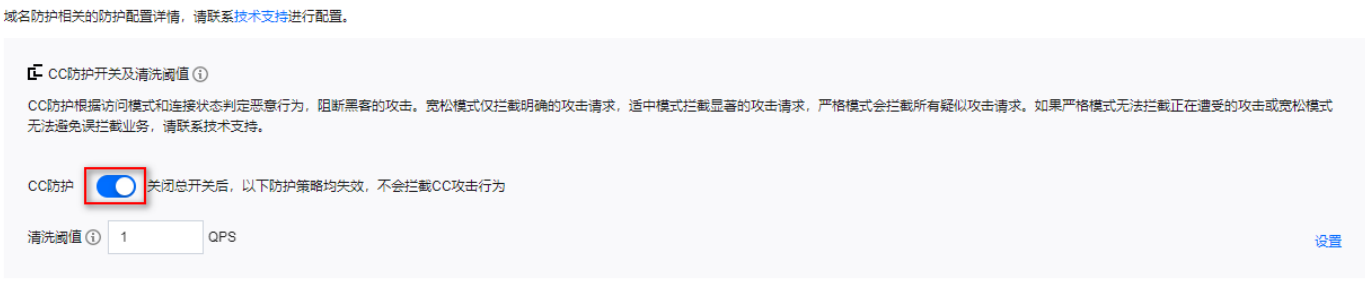
- 您需要已成功 购买 DDoS 高防 IP，并设置防护对象。
- 智能 CC 防护当前仅支持域名接入的规则生效。

操作步骤

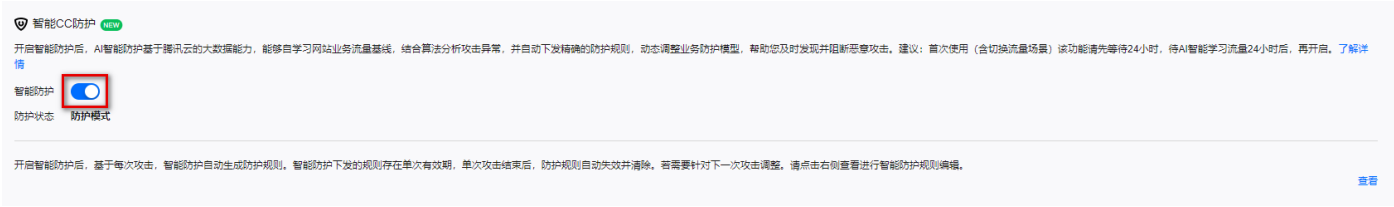
1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航中，单击**防护配置** > **CC 防护**。
2. 在 CC 防护页面的左侧列表中，选中高防 IP 的 ID 下面的域名。

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。

智能防护

以下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，可删除以下防护规则。

IP

匹配条件	策略	生效时间	操作
暂无数据			

共 0 条

10 条 / 页 1 / 1 页

精准防护

最近更新时间：2022-11-30 17:53:42

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。

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	访问请求的 URI 地址	长度小于、长度等于、长度大于、不包含
UA	发起访问请求的客户端浏览器标识等相关信息	长度小于、长度等于、长度大于
Cookie	访问请求中的携带的 Cookie 信息	等于、包含、不包含、内容为空、不存在
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、长度小于、长度等于、长度大于、不存在、内容为空
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
Method	访问请求的方法，具体包括 HEAD、GET、POST、DELTET、PUT	等于、不等于
自定义	自定义设置	等于、不等于、包含、不包含、内容为空、不存在、长度小于、长度等于、长度大于

前提条件

您需要成功 购买 DDoS 高防 IP，并设置防护对象。

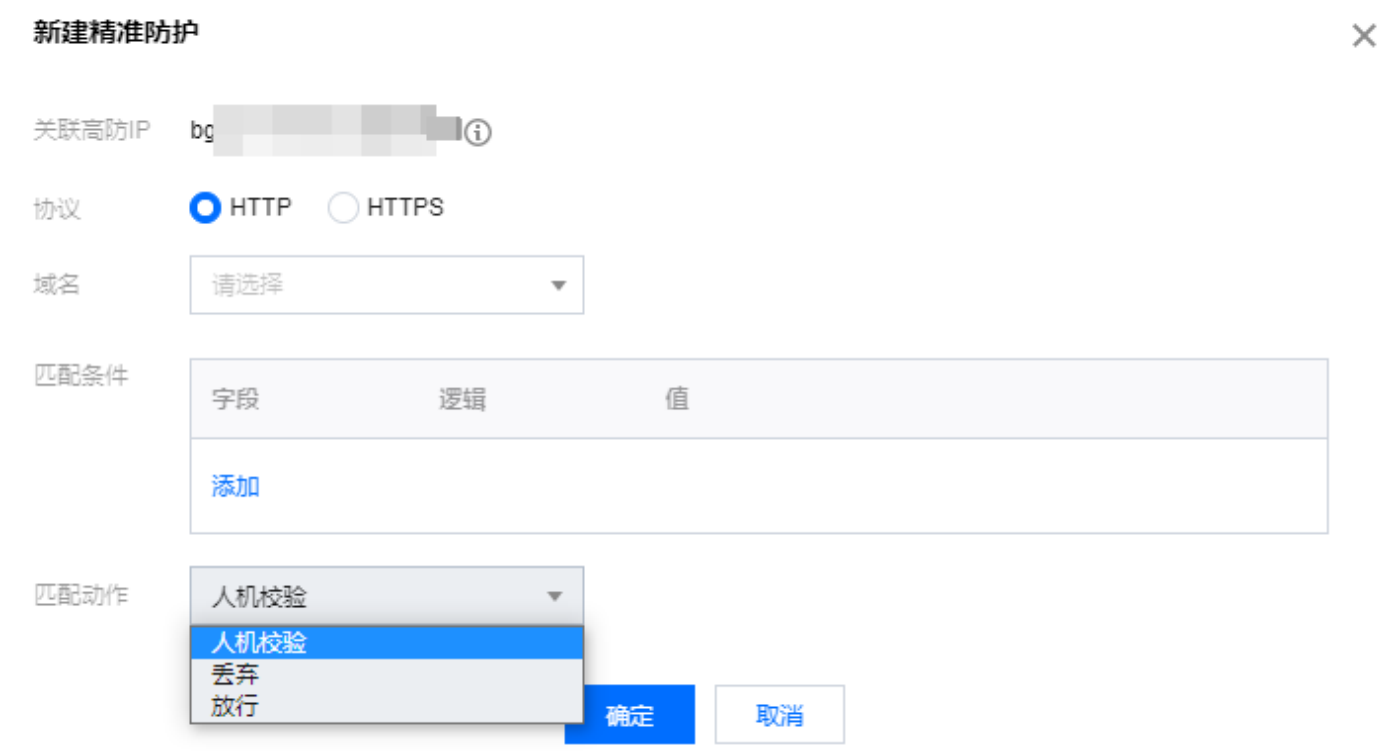
操作步骤

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航中，单击**防护配置** > **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**，进入精准防护规则列表。

4. 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：2022-04-12 11:36:04

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。

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。

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，可能会存在一定误杀。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。

前提条件

您需要成功 购买 DDoS 高防 IP，并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航中，单击**防护配置** > **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：2022-11-30 17:52:06

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。

前提条件

您需要成功 购买 DDoS 高防 IP ，并设置防护对象并接入了域名业务的防护。

操作步骤

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航中，单击**防护配置** > **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**。

5. 在新建区域封禁弹窗中，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。

6. 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。

IP 黑白名单

最近更新时间：2022-11-30 17:51:14

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：
> 当发生 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。

前提条件

您需要成功 购买 DDoS 高防 IP，并设置防护对象。

操作步骤

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航中，单击**防护配置** > **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 IP 黑白名单卡片中，单击**设置**，进入 IP 黑白名单列表。

4. 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。

业务接入
端口接入

最近更新时间：2022-12-15 10:29:14

> **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 高防 IP（新版）管理控制台，在左侧目录中，单击**业务接入** > **端口接入**。
2. 在端口接入页面，单击**开始接入**。

3. 在端口业务接入页面，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。**

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、转发协议和转发端口关键字对规则进行查询。

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。

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。

导入规则

1. 在 端口接入页面，单击**批量导入**。
2. 在批量导入四层转发规则弹窗，填写所需规则，单击**确定**。

导出规则

1. 在 端口接入页面，单击**导出规则**。
2. 在批量导出四层转发规则弹窗，选择所需规则，单击**复制**。

域名接入

最近更新时间：2022-12-16 09:17:42

> **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 高防 IP（新版）管理控制台，在左侧目录中，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。

导入规则

1. 在域名接入页面，单击**批量导入**。
2. 在批量导入七层转发规则弹窗，填写所需规则，单击**确定**。

导出规则

1. 在域名接入页面，单击**导出规则**。

2. 在批量导入七层转发规则弹窗，选择所需规则，单击**复制**。

配置会话保持

最近更新时间：2022-04-12 14:51:07

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 高防 IP（新版）管理控制台，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：2022-11-15 15:20:01

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 高防 IP（新版）管理控制台 ，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，单击其健康检查列下的**编辑**。

转发协议	转发端口	源站端口	源站	关联高防IP	负载均衡方式	健康检查	会话保持	修改时间	操作
TCP	9000	80			加权轮询	关闭 编辑	关闭 编辑	2020-04-27 21:46:24	配置 删除
TCP	8000	8000			加权轮询	关闭 编辑	开启 编辑	2020-04-27 22:07:49	配置 删除

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 高防 IP（新版）管理控制台，在左侧目录中，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。

实例管理
查看实例信息

最近更新时间：2022-05-16 15:36:50

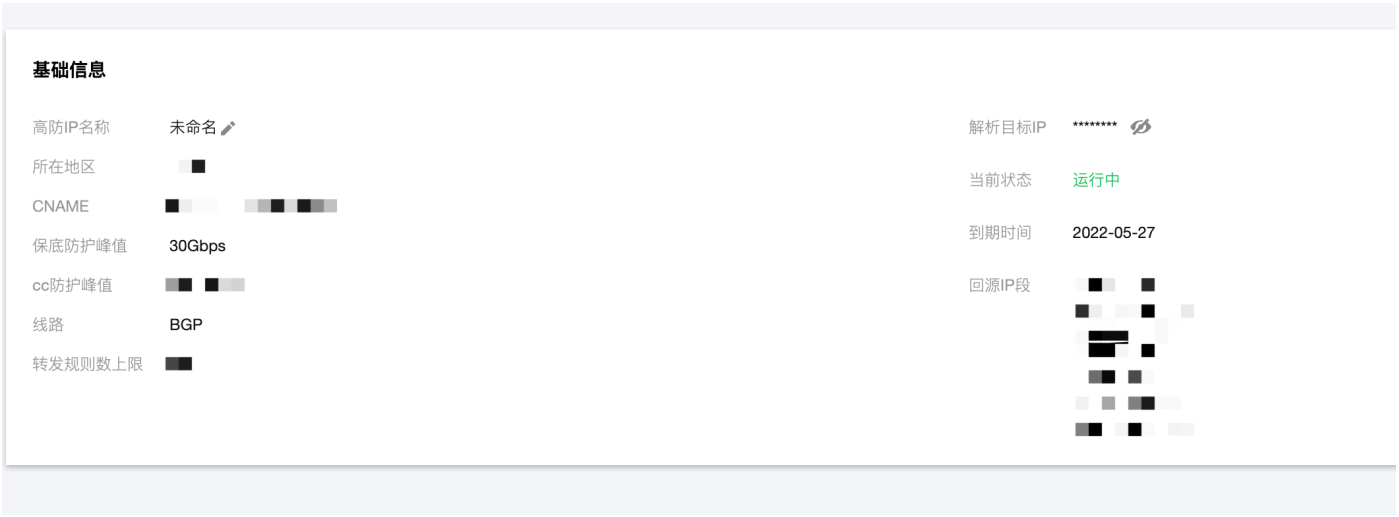
您可以通过 DDoS 防护管理控制台，查看所购买的 DDoS 高防 IP 的基础信息（如实例保底防护峰值及运行状态）及实例的弹性防护配置。

操作步骤

示例：查看高防 IP 实例“bgpip-000002jf”的实例信息。

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航栏中，单击**实例列表**，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。

2. 在弹出的页面中查看如下信息：



- **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。
- **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**。
- **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。
- **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。

设置实例别名与标签

最近更新时间：2021-09-26 17:49:41

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。

前提条件

您需要成功 购买 DDoS 高防 IP 。

操作步骤

方式一

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航栏中，单击**实例列表**。
2. 在实例列表中，找到需要编辑名称的实例，单击目标实例的“ID/名称/标签”列第二行的图标，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 高防 IP（新版）管理控制台，在左侧导航栏中，单击**实例列表**。
2. 在实例列表中，找到需要编辑名称的实例，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 IP 名称右侧的图标，输入名称。

> 说明：
> 名称长度为1 - 20个字符，不限制字符类型。

基础信息

高防IP名称	未命名
所在地区	中国香港
IP	[redacted]
保底防护峰值	50Gbps

修改弹性防护带宽

最近更新时间：2023-07-11 15:22:46

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。

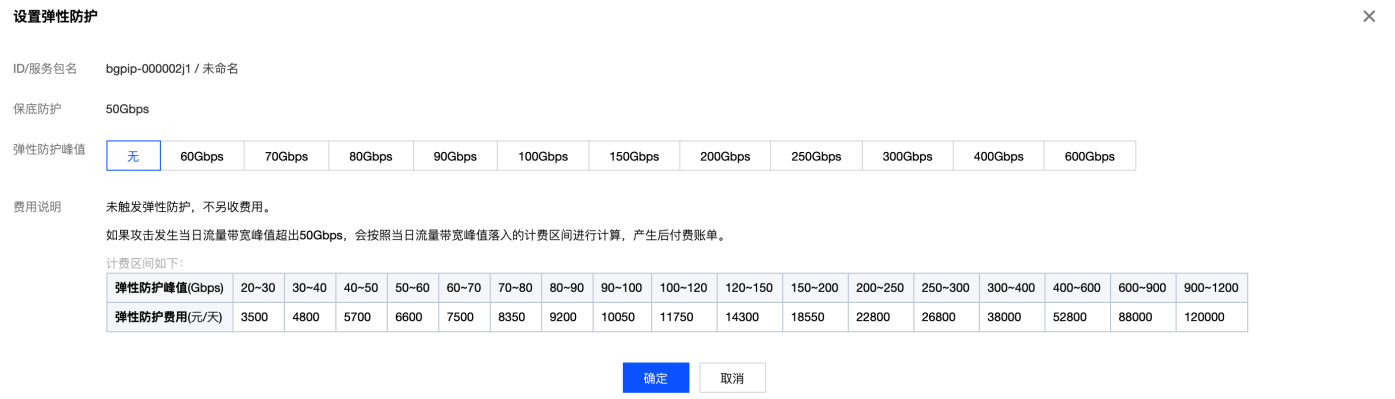
前提条件

您需要成功 购买 DDoS 高防 IP 。

操作步骤

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航栏中，单击**实例列表**。
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 图标。

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。

配置智能调度

最近更新时间：2022-09-01 15:13:51

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。

> 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。

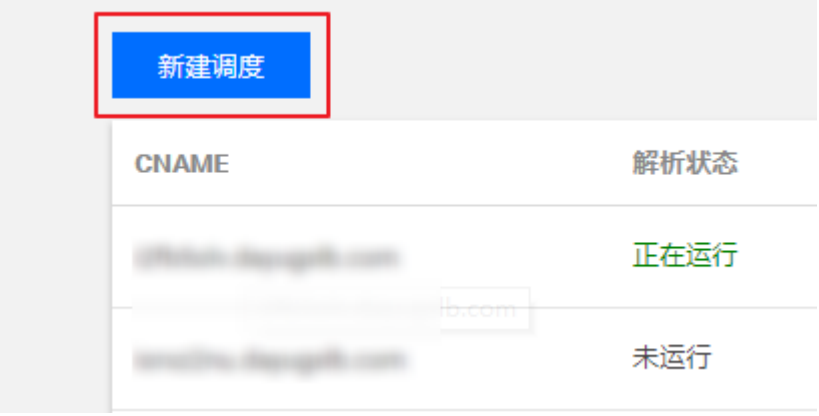
> 说明：
>
> - 若您需要将防护的云上产品 IP 添加至已购买的高防包实例，请参见 DDoS 高防包 快速入门。
> - 若您需要将四层或七层业务添加至已购买的 DDoS 高防 IP 实例，请参见 DDoS 高防 IP 端口接入 或 域名接入 。

- 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 DNS 解析 DNSPod。

设置线路优先级

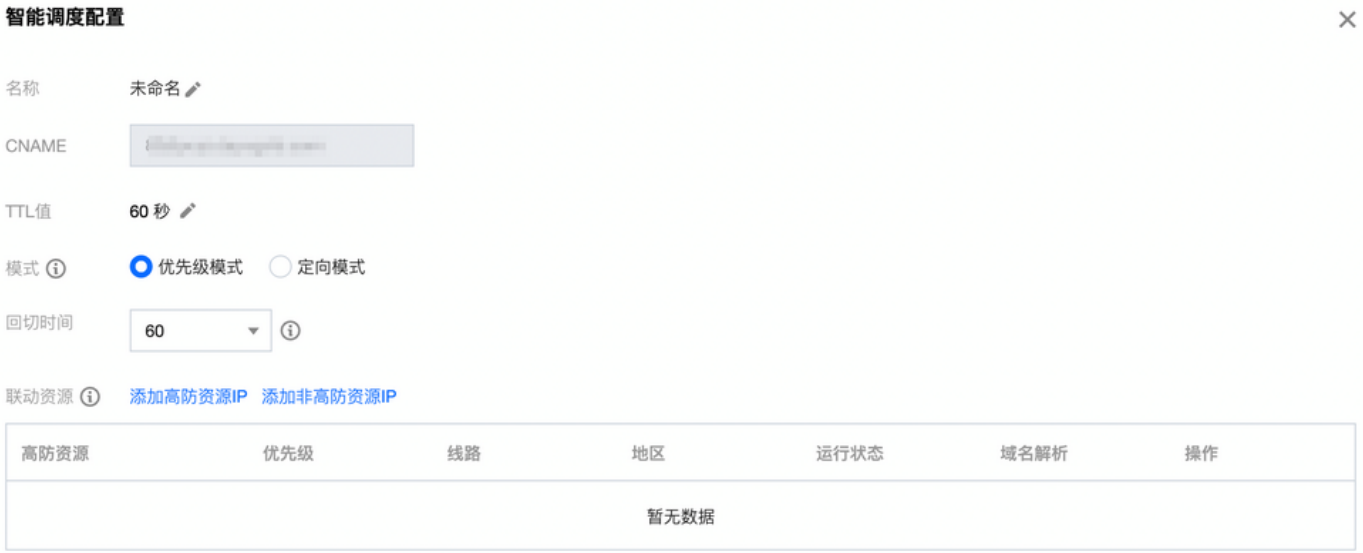
请参考以下步骤，按照设想的调度方案为您的高防实例设置优先级：

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航栏，单击**智能调度**，进入列表页面，单击**新建调度**，系统自动生成一个 CNAME 记录。



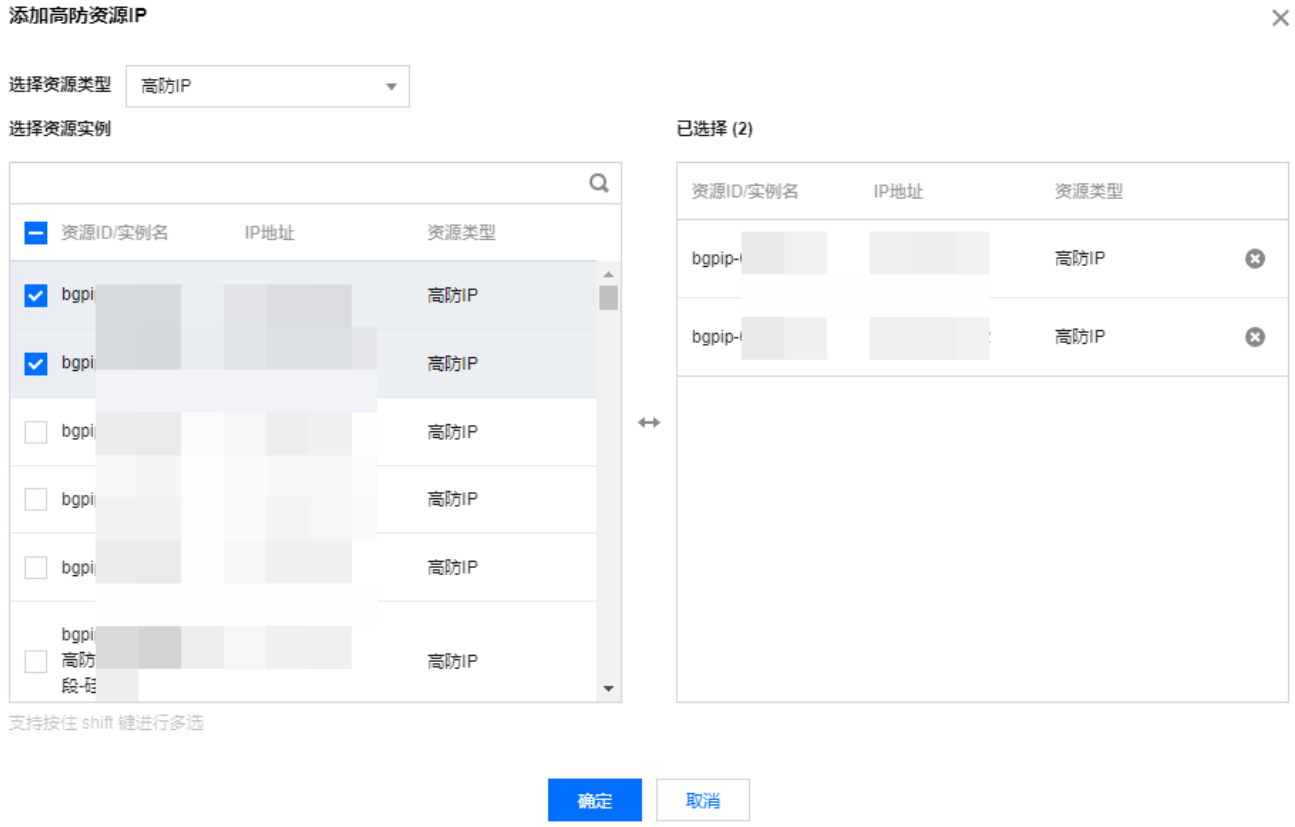
2. 找到该 CNAME 记录所在行，单击**添加高防实例**，进入智能调度编辑页面。

3. 在智能调度编辑页面中，TTL 值默认60秒，取值范围为1（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. 在智能调度编辑页面中，分为优先级模式和定向模式，不同模式操作如下所示：
   - **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。

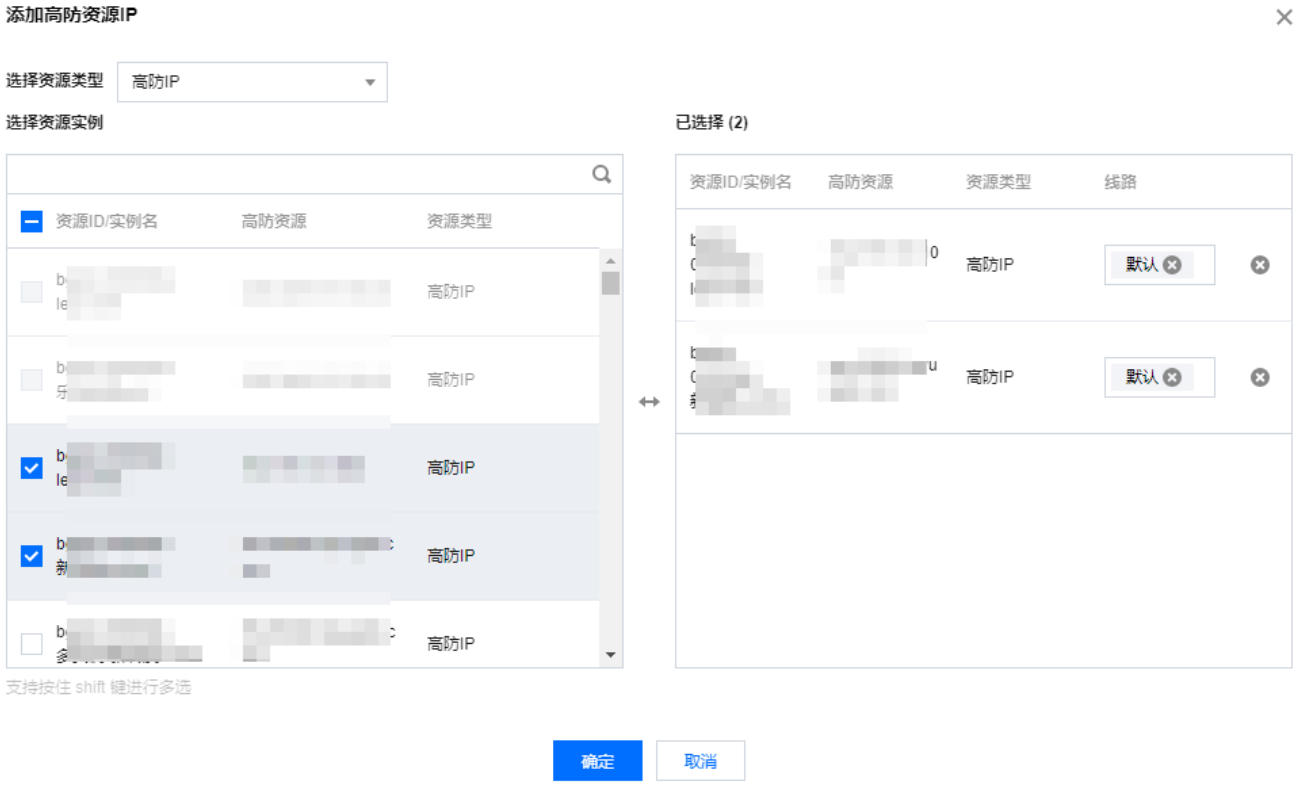
a. 单击**添加高防资源 IP**，勾选需要设置智能调度的高防实例及 IP，单击**确定**。



b. 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。

- **定向模式**：通过定向模式，指定资源间的调度关系。

a. 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**。



b. 在智能调度编辑页面中，看到选择调度的资源，单击**配置联动资源**。

c. 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。

> **说明：**
> 联动资源最多可配置5个。

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。

资源ID	IP地址	线路	优先级	地区	运行状态	域名解析	操作
net-00000		联通	100	华东地区(上海)	运行中		解除绑定
bgpip-00000		电信	2	华东地区(上海)	运行中		解除绑定
bgp-00000		BGP	1	华东地区(上海)	运行中		解除绑定

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 DNS 解析 DNSPod 控制台，在左侧导航栏中，单击**我的域名**。

2. 在域名解析列表页面，找到目标域名所在行，单击**解析**。

3. 单击**记录管理** > **添加记录**，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**保存**。

查看操作日志

最近更新时间：2021-09-26 17:55:12

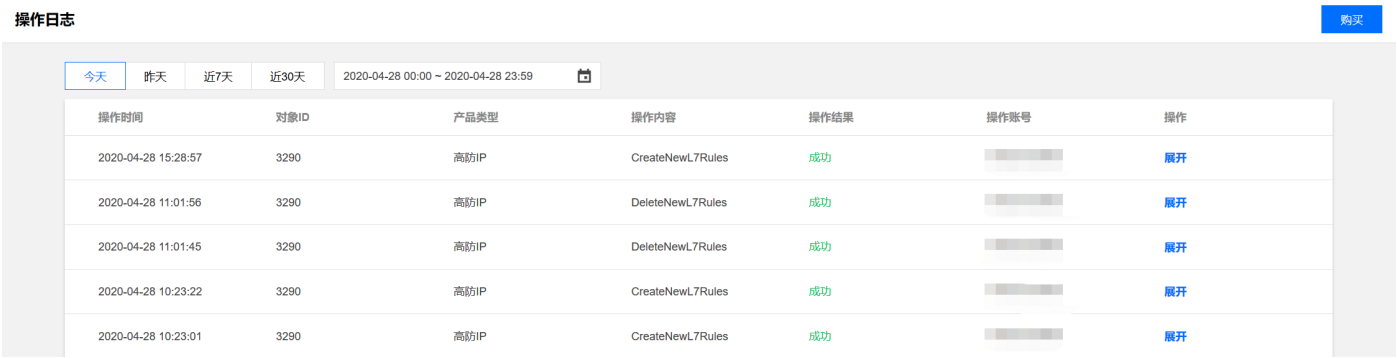
操作场景

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

- 转发规则变更操作日志
- 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
- 实例名称的修改日志

操作步骤

1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航栏中，单击**操作日志**。
2. 在操作日志页面，可根据时间范围查询对应的操作记录，在右侧操作栏，单击**展开**，可查看日志详情。



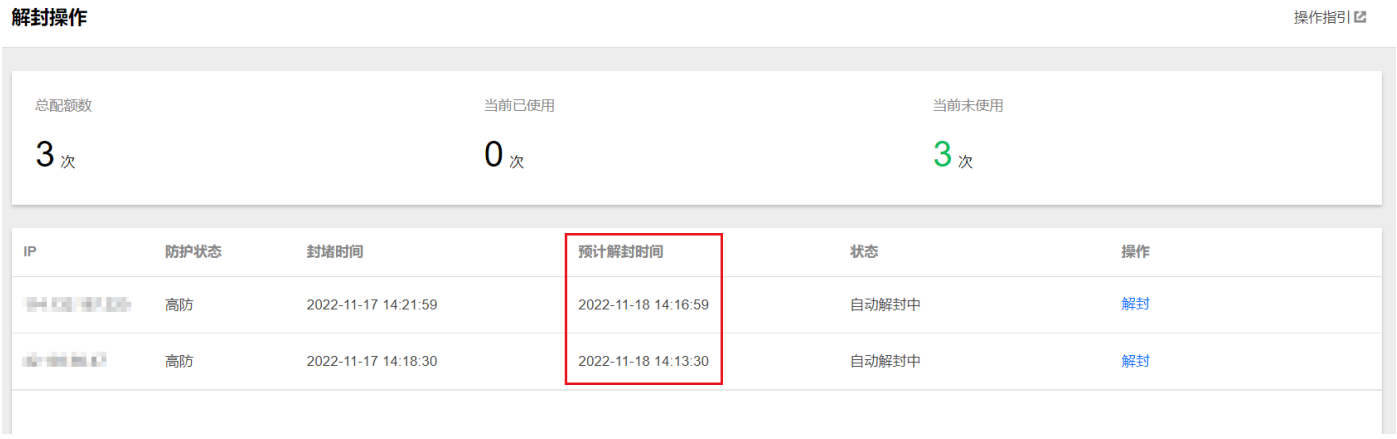
封堵相关操作
查看封堵时间

最近更新时间：2022-11-18 14:54:13

查看未解封 IP 时间

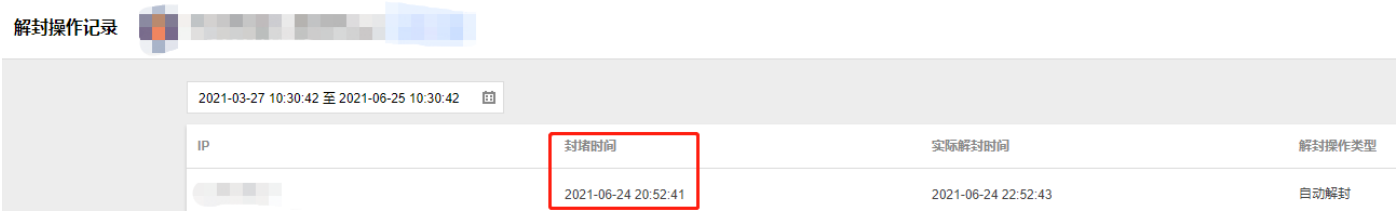
1. 登录 DDoS 防护管理控制台，在左侧导航中，单击**自助解封** > **解封操作**，进入解封操作页面。
2. 在解封操作页面，选择所需 IP 的所在行，可在“封堵时间”处，查看该 IP 的封堵时间。

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 的预计解封时间。



查看已解封 IP 时间

1. 登录 DDoS 防护管理控制台，在左侧导航中，单击**自助解封** > **解封操作记录**，进入解封操作记录页面。
2. 在解封操作记录页面，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“实际解封时间”处，查看该 IP 的实际解封时间。

设置安全事件通知

最近更新时间：2022-08-09 18:04:40

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，系统将以站内信、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：

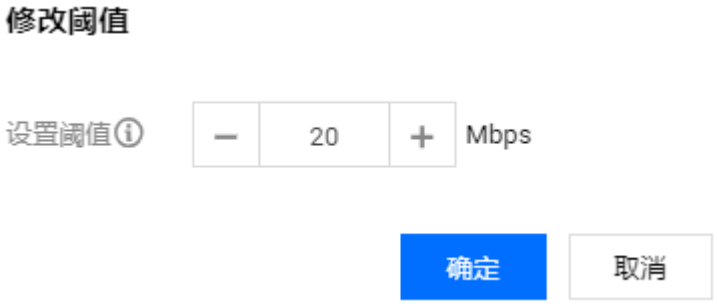
- 攻击开始时，您将会收到攻击开始提示。
- 攻击结束后15分钟，您将收到攻击结束提示。
- IP 被封堵时，您将收到封堵提示。
- IP 解除封堵时，您将收到解除封堵提示。

您可以根据实际情况修改告警信息的接收人和接收方式。

设置告警阈值

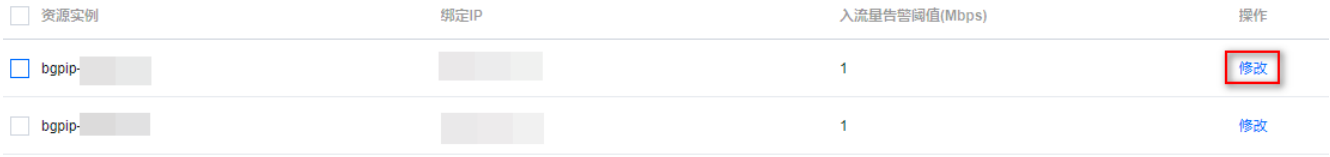
1. 登录 DDoS 高防 IP（新版）管理控制台，在左侧导航中，单击**告警通知**，进入告警通知页面。
2. 在右侧的功能卡片中可以分别设置“单 IP 入流量告警阈值”、“DDoS 清洗阈值”和“CC 清洗阈值”。

3. 单击单 IP 默认阈值右边的 可以修改默认阈值，修改完成后，单击**确定**即可。



4. 在告警通知页面，支持单个或批量为 IP 设置告警阈值，具体操作如下。
   - **单个设置告警阈值**
     a. 单击卡片的**高级设置**，可以进入 IP 告警设置列表。

b. 选择所需实例，单击操作列下的**修改**，输入所需的告警阈值，单击**确定**即可保存。



- **批量设置告警阈值**

a. 单击卡片的**高级设置**，可以进入 IP 告警设置列表。

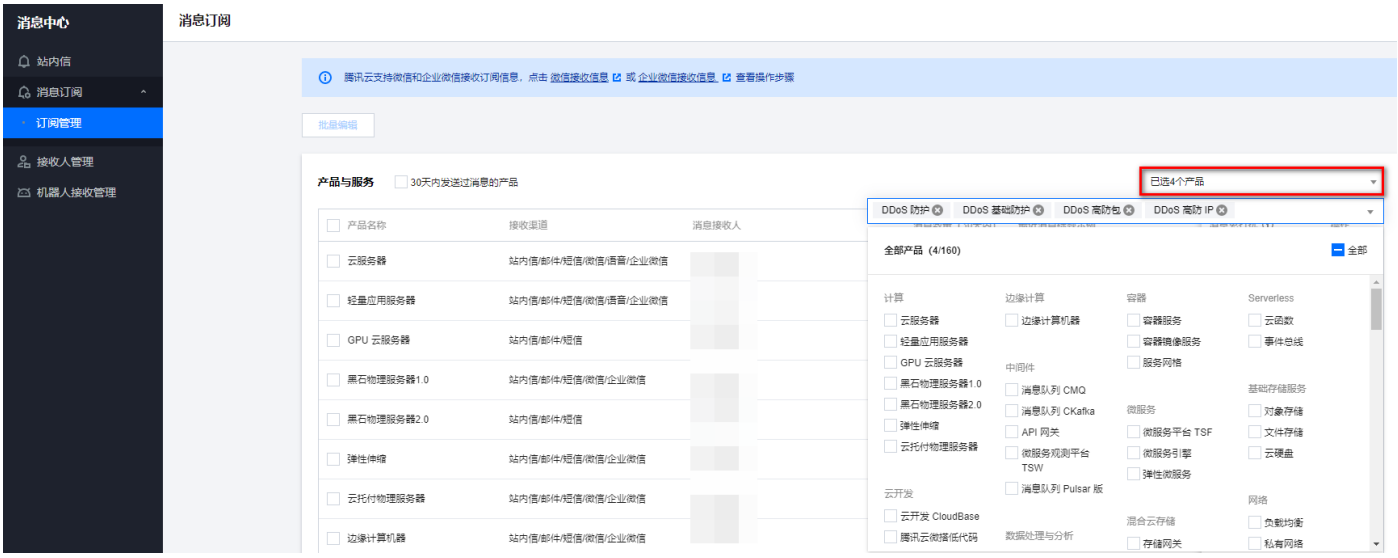
b. 选择多个实例，单击**批量修改**，输入所需的告警阈值，单击**确定**即可保存。

设置通知方式

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**消息订阅 > 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，进行消息接收人的设置，设置完成后单击**确定**即可。

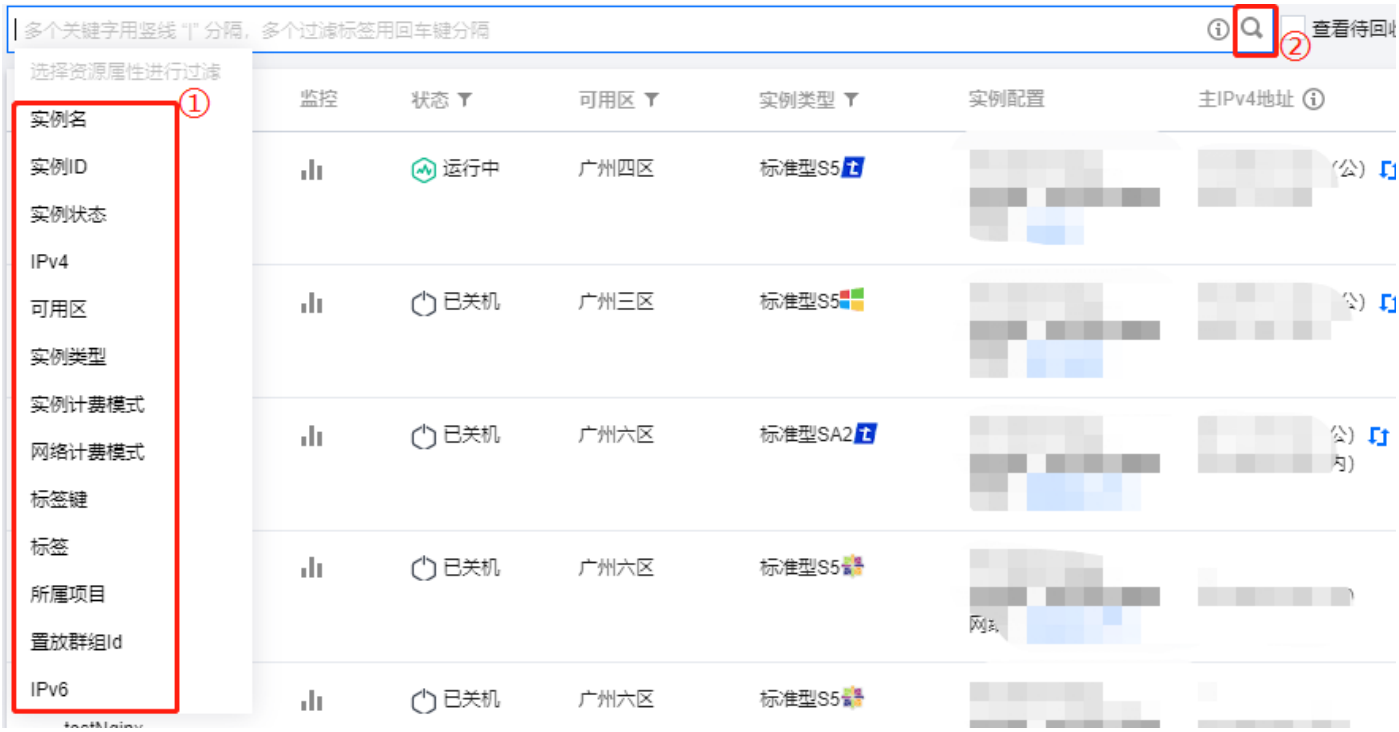
连接已被封堵的服务器

最近更新时间：2022-08-09 18:05:05

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，选择使用 VNC 登录单击**立即登录**，即可通过浏览器 VNC 方式连接。

解除封堵

最近更新时间：2022-11-15 16:45:03

解封操作

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 防护管理控制台，在左侧导航中，单击**自助解封** > **解封操作**，进入解封操作页面。
2. 在解封操作页面，选择所需 IP 的所在行，可在“预计解封时间”处，查看该 IP 的预计解封时间。

自助解封次数

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。

> 说明：
>
> - 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

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择**自助解封** > **解封操作**，进入解封操作页面。
2. 在解封操作页面，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

登录 DDoS 防护管理控制台，在左侧导航中，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、自助解封等操作记录。